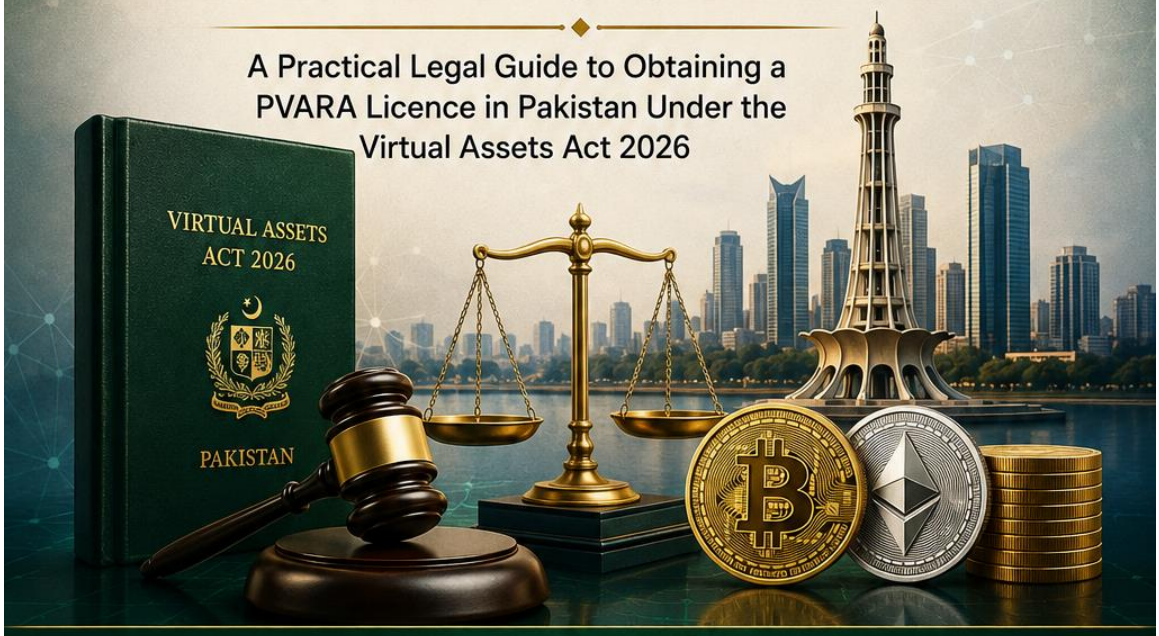
PVARA
PAKISTAN VIRTUAL ASSETS REGULATORY AUTHORITY

PVARA LICENSING HANDBOOK 2026

A Practical Legal Guide to Obtaining a PVARA Licence in Pakistan Under the Virtual Assets Act 2026



LEGAL COMPLIANCE | AML / CFT COMPLIANCE | CYBERSECURITY & RISK MANAGEMENT | REGULATORY SUPERVISION | LICENSING PROCESS

Shahid Jamal Tubrazy

Cryptocurrency & Fintech Lawyer

PVARA Licensing Handbook 2026

Shahid Jamal Tubrazy

Cryptocurrency & Fintech Lawyer

Table of Contents

Appendix C: Key Forms and Application Documents

Virtual Assets Act, 2026

PAKISTAN VIRTUAL ASSET REGULATORY AUTHORITY NOTIFICATION, 2026

GENERAL REGULATIONS, [APPLICABLE ON ALL VIRTUAL ASSET SERVICE PROVIDERS, (VASPs)] 2026

Preface:

The enactment of Pakistan's Virtual Assets Act 2026 and the establishment of the Pakistan Virtual Assets Regulatory Authority (PVARA) represent a historic milestone in the regulation of cryptocurrencies and virtual assets in Pakistan. For the first time, blockchain businesses, cryptocurrency exchanges, token issuers, custodians, and other Virtual Asset Service Providers (VASPs) have a dedicated legal and regulatory framework through which they can establish and operate compliant businesses.

As a cryptocurrency and fintech law practitioner, I have closely followed the evolution of virtual asset regulation both internationally and within Pakistan. During my professional practice, I have advised blockchain startups, cryptocurrency exchanges, Web3 businesses, fintech companies, and digital asset investors on regulatory compliance, licensing, anti-money laundering (AML) obligations, and legal risk management. These experiences highlighted the growing need for a practical guide that explains the PVARA licensing process in a clear, structured, and accessible manner.

This booklet has been prepared to assist entrepreneurs, legal professionals, compliance officers, investors, and blockchain innovators in understanding the legal requirements for obtaining a PVARA licence. Rather than reproducing legislation, it presents a practical overview of the licensing framework, corporate requirements, compliance obligations, regulatory sandbox, and ongoing responsibilities applicable to Virtual Asset Service Providers in Pakistan.

The contents of this booklet are primarily based on the PVARA License Guide 2026 and related publicly available regulatory documents. As Pakistan's virtual asset regulatory framework continues to evolve, readers are encouraged to monitor official announcements and consult qualified legal and regulatory professionals before making business or compliance decisions.

It is my hope that this guide will contribute to a better understanding of Pakistan's emerging virtual asset ecosystem and support the responsible growth of blockchain innovation within a transparent, compliant, and internationally aligned regulatory environment.

Shahid Jamal Tubrazy
Cryptocurrency & FinTech Law Consultant

Disclaimer:

This booklet is intended solely for general informational and educational purposes. It does not constitute legal, financial, tax, investment, accounting, or regulatory advice and should not be relied upon as a substitute for professional advice tailored to specific circumstances.

The information contained in this publication is based primarily on the PVARA License Guide 2026 and other publicly available regulatory materials relating to Pakistan's virtual asset framework. Certain aspects of the regulatory regime—including the Draft Pakistan Virtual Asset Services Regulations 2026, licensing procedures, capital requirements, and regulatory guidance—may be amended, updated, or replaced by the Pakistan Virtual Assets Regulatory Authority (PVARA) or other competent authorities after the publication of this booklet.

Readers should independently verify all current legal and regulatory requirements through official sources, including PVARA, the Securities and Exchange Commission of Pakistan (SECP), the State Bank of Pakistan (SBP), the Financial Monitoring Unit (FMU), and the Federal Board of Revenue (FBR), before submitting any application or making business decisions.

While every effort has been made to ensure the accuracy of the information presented, the author and publisher make no representation or warranty regarding its completeness, accuracy, or continued validity and accept no liability for any loss or damage arising from reliance upon this publication.

Nothing in this booklet should be interpreted as creating a lawyer-client relationship between the author and any reader. Professional legal advice should always be obtained before undertaking any regulatory, licensing, or commercial activity involving virtual assets or Virtual Asset Service Providers in Pakistan.

Chapter 1. Introduction

The rapid growth of blockchain technology, cryptocurrencies, tokenized assets, and decentralized financial services has transformed the global financial landscape. Virtual assets have evolved from a niche technological innovation into a significant component of the digital economy, facilitating cross-border payments, investment opportunities, decentralized applications (DApps), and Web3 business models.

Recognizing both the opportunities and regulatory challenges associated with virtual assets, Pakistan introduced the Virtual Assets Act 2026, establishing a comprehensive legal framework for the regulation, supervision, and licensing of Virtual Asset Service Providers (VASPs). The Act represents Pakistan's first dedicated legislation governing the virtual asset industry and marks an important step toward integrating digital asset businesses into the country's formal financial system.

The Act establishes the Pakistan Virtual Assets Regulatory Authority (PVARA) as the principal regulatory authority responsible for licensing, supervising, and regulating all Virtual Asset Service Providers operating within or from Pakistan. The regulatory framework aims to promote innovation while ensuring investor protection, financial stability, market integrity, and compliance with international Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) standards.

Purpose of the Virtual Assets Act 2026

The Virtual Assets Act 2026 seeks to provide legal certainty for businesses engaged in virtual asset activities while protecting consumers and maintaining confidence in Pakistan's financial system.

The Act establishes a regulatory environment that enables legitimate blockchain and cryptocurrency businesses to operate under government supervision rather than in an unregulated marketplace.

According to the regulatory framework, the principal objectives include:

- Establishing a comprehensive licensing system for Virtual Asset Service Providers.
- Promoting responsible innovation within Pakistan's digital asset ecosystem.
- Protecting consumers and investors.
- Strengthening Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) compliance.
- Preventing financial crimes involving virtual assets.
- Encouraging transparency and accountability within the virtual asset market.

- Aligning Pakistan's regulatory framework with internationally accepted standards.

Establishment of PVARA

One of the most significant developments under the Virtual Assets Act 2026 is the establishment of the Pakistan Virtual Assets Regulatory Authority (PVARA).

The PVARA License Guide explains that the Authority functions as Pakistan's primary regulator for Virtual Asset Service Providers. Its responsibilities include:

- Licensing Virtual Asset Service Providers (VASPs).
- Supervising licensed businesses.
- Monitoring regulatory compliance.
- Administering the Regulatory Sandbox.
- Issuing regulatory guidance and activity-specific handbooks.
- Promoting investor protection and market integrity.

PVARA therefore serves as the central authority responsible for ensuring that virtual asset businesses operate in accordance with the legal and regulatory requirements established under the Virtual Assets Act 2026.

Scope of the Regulatory Framework

The Virtual Assets Act 2026 applies to businesses conducting regulated virtual asset activities in Pakistan.

The accompanying regulatory framework covers a wide range of Virtual Asset Service Providers, including cryptocurrency exchanges, custodians, broker-dealers, lending platforms, token issuers, investment service providers, settlement providers, and advisory businesses operating within the virtual asset ecosystem. The Draft Pakistan Virtual Asset Services Regulations 2026 identify ten licence categories to accommodate these different business models.

The framework is intended to ensure that businesses engaging in virtual asset activities operate under appropriate regulatory oversight while maintaining adequate governance, operational resilience, and compliance systems.

Innovation and Investor Protection

The Virtual Assets Act 2026 seeks to balance technological innovation with effective regulatory oversight.

The PVARA framework recognises that blockchain technology can contribute to financial inclusion, efficiency, and digital innovation. At the same time, it acknowledges the importance of safeguards designed to protect consumers, reduce operational risks, and maintain confidence in the virtual asset market.

To support responsible innovation, the regulatory framework includes a Regulatory Sandbox, allowing eligible businesses to test innovative products and services within a supervised environment before applying for a full licence.

Regulatory Principles

The licensing framework places significant emphasis on compliance and sound corporate governance.

Applicants seeking authorisation are expected to establish effective AML/CFT programmes, implement cybersecurity controls, safeguard customer assets, maintain adequate capital, and satisfy fit-and-proper requirements applicable to directors and senior management.

These principles are intended to promote a secure, transparent, and resilient virtual asset ecosystem capable of supporting long-term industry growth

Why the Act Is Important

The enactment of the Virtual Assets Act 2026 provides businesses with a defined legal pathway for entering Pakistan's virtual asset market.

Instead of operating in an uncertain regulatory environment, blockchain companies and cryptocurrency businesses now have a structured process for obtaining regulatory approval through PVARA, establishing a compliant corporate presence, implementing AML/CFT controls, and progressing toward full commercial operations. The framework also introduces supervisory mechanisms, compliance obligations, and enforcement measures intended to strengthen market confidence and encourage responsible participation in Pakistan's growing digital asset economy.

The Virtual Assets Act 2026 represents a landmark development in Pakistan's financial and technological regulatory landscape. By establishing PVARA and introducing a comprehensive licensing framework for Virtual Asset Service Providers, the Act creates opportunities for innovation while reinforcing the principles of transparency, consumer protection, regulatory compliance, and market integrity.

For entrepreneurs, cryptocurrency exchanges, fintech companies, blockchain developers, and investors, understanding the objectives and structure of the Virtual Assets Act 2026 is the first step toward building compliant and sustainable virtual asset businesses in Pakistan.

The following chapters examine the role of PVARA, the various VASP licence categories, and the practical legal requirements for obtaining and maintaining a licence under Pakistan's evolving virtual asset regulatory framework.

Chapter 2: Pakistan Virtual Assets Regulatory Authority (PVARA)

Introduction

The Pakistan Virtual Assets Regulatory Authority (PVARA) is the principal regulatory authority responsible for licensing, supervising, and regulating Virtual Asset Service Providers (VASPs) in Pakistan. Established under the Virtual Assets Act 2026, PVARA represents Pakistan's commitment to creating a secure, transparent, and internationally aligned regulatory framework for the virtual asset industry. According to the PVARA License Guide 2026, the Authority evolved from the earlier Virtual Assets Ordinance, 2025, and now serves as the country's dedicated regulator for the virtual asset sector.

The establishment of PVARA marks a significant shift from regulatory uncertainty toward a structured legal framework that supports innovation while safeguarding consumers, financial stability, and market integrity.

Objectives of PVARA

PVARA has been established to regulate virtual asset activities through a licensing and supervisory framework that promotes responsible innovation and investor confidence. The Authority's objectives include:

- Licensing Virtual Asset Service Providers (VASPs).
- Supervising regulated virtual asset businesses.
- Promoting investor and consumer protection.
- Maintaining the integrity of Pakistan's virtual asset market.
- Preventing money laundering and terrorist financing.
- Encouraging responsible blockchain innovation.
- Supporting the growth of Pakistan's digital economy.

The Authority seeks to balance innovation with effective regulation by ensuring that virtual asset businesses operate within a transparent legal framework.

Regulatory Powers

The PVARA License Guide explains that PVARA is responsible for issuing licences, supervising regulated entities, administering the Regulatory Sandbox, and enforcing compliance with the applicable laws and regulations governing virtual asset businesses. The Authority also publishes regulations, activity-specific handbooks, licensing requirements, and compliance guidance for Virtual Asset Service Providers.

Its regulatory functions extend throughout the entire lifecycle of a licensed business, from the initial application process to ongoing supervision and enforcement.

Scope of Regulation

PVARA regulates businesses that provide virtual asset services in Pakistan. These businesses are commonly referred to as Virtual Asset Service Providers (VASPs).

The regulatory framework applies to various categories of businesses, including cryptocurrency exchanges, custodial service providers, broker-dealers, virtual asset investment managers, lending and borrowing platforms, transfer and settlement providers, advisory firms, and certain token issuers. The applicable licence category depends on the specific activities undertaken by the business.

Licensing Authority

One of PVARA's most important responsibilities is issuing licences to eligible Virtual Asset Service Providers.

The licensing framework consists of several stages. Most applicants begin by applying for a No Objection Certificate (NOC), followed by company incorporation, establishment of a local presence, registration with the Financial Monitoring Unit (FMU) goAML portal, and ultimately the application for a full VASP licence. Only after completing the required licensing process may a business commence commercial operations in Pakistan.

Regulatory Sandbox

To encourage technological innovation, PVARA has established a Regulatory Sandbox that enables eligible blockchain startups and innovative virtual asset businesses to test new products and services within a controlled regulatory environment.

According to the guide, the Sandbox allows applicants to operate under defined testing parameters with proportionate capital requirements before transitioning to a full licence. Applications are accepted throughout the year and undergo regulatory assessment before approval.

The Sandbox provides an opportunity for businesses to demonstrate innovation while allowing PVARA to monitor risks and consumer protection measures during the testing period.

Compliance Responsibilities

PVARA places significant emphasis on regulatory compliance.

Licensed entities are expected to maintain comprehensive Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) programmes, implement Know Your Customer (KYC)

procedures, conduct transaction monitoring, comply with sanctions screening requirements, register on the FMU goAML platform, and establish appropriate cybersecurity and operational controls.

The Authority also expects businesses to maintain effective governance structures, risk management systems, customer asset protection measures, and ongoing compliance reporting.

Coordination with Other Regulatory Authorities

Although PVARA serves as the primary regulator for virtual asset businesses, the regulatory framework requires coordination with several other Pakistani authorities.

These include:

- Securities and Exchange Commission of Pakistan (SECP) for company incorporation and corporate regulation.
- Financial Monitoring Unit (FMU) for AML/CFT reporting through the goAML platform.
- State Bank of Pakistan (SBP) for banking-related matters.
- Federal Board of Revenue (FBR) for taxation and reporting obligations.

This coordinated approach helps ensure that licensed Virtual Asset Service Providers comply with corporate, financial, tax, and anti-money laundering requirements.

Consumer Protection

Consumer protection is a fundamental component of PVARA's regulatory framework.

The licensing process requires applicants to establish customer asset safeguarding arrangements, cybersecurity controls, dispute resolution mechanisms, risk disclosures, and operational resilience measures designed to protect users of virtual asset services. These requirements aim to promote confidence in Pakistan's regulated virtual asset market.

Importance of PVARA

The establishment of PVARA represents a major step toward integrating Pakistan into the global digital asset economy.

By introducing licensing standards, supervisory oversight, AML/CFT compliance requirements, cybersecurity obligations, and a structured Regulatory Sandbox, PVARA provides businesses with a legal pathway to operate while protecting investors and maintaining financial system integrity.

As Pakistan's virtual asset regulatory framework continues to evolve, PVARA will play a central role in shaping the country's blockchain ecosystem and supporting responsible innovation within a regulated environment.

The Pakistan Virtual Assets Regulatory Authority is the cornerstone of Pakistan's virtual asset regulatory regime. Its licensing, supervisory, compliance, and enforcement functions create a comprehensive framework for Virtual Asset Service Providers seeking to establish compliant operations in Pakistan. Businesses intending to enter Pakistan's digital asset market should become familiar with PVARA's licensing requirements, regulatory expectations, and compliance obligations before commencing any regulated virtual asset activity.

Chapter 3: Virtual Asset Service Providers (VASPs)

Introduction

The Virtual Assets Act 2026 establishes a comprehensive legal framework for regulating businesses that provide services involving virtual assets in Pakistan. These businesses are collectively known as Virtual Asset Service Providers (VASPs). Rather than regulating cryptocurrencies themselves, the regulatory framework focuses on the businesses and individuals that facilitate the issuance, exchange, transfer, custody, management, or other commercial activities relating to virtual assets.

The introduction of the VASP concept aligns Pakistan's regulatory framework with international standards promoted by the Financial Action Task Force (FATF), ensuring that virtual asset businesses operate within a transparent, accountable, and compliant legal environment.

According to the PVARA licensing framework, any person or entity carrying out regulated virtual asset activities in or from Pakistan may be required to obtain the appropriate authorization from the Pakistan Virtual Assets Regulatory Authority (PVARA) before commencing commercial operations.

What is a Virtual Asset Service Provider?

A Virtual Asset Service Provider (VASP) is a business or organization that conducts one or more regulated activities involving virtual assets on behalf of customers or as part of its commercial operations.

Unlike individual cryptocurrency investors who buy or sell digital assets for personal investment purposes, a VASP provides services to third parties as a commercial enterprise.

The objective of regulating VASPs is to protect consumers, maintain market integrity, prevent financial crime, and ensure compliance with anti-money laundering (AML) and counter-terrorist financing (CFT) obligations.

Why Are VASPs Regulated?

The rapid growth of blockchain technology and digital assets has created significant opportunities for innovation and financial inclusion. However, it has also introduced risks relating to money laundering, terrorist financing, fraud, cybercrime, sanctions evasion, and consumer protection.

By licensing and supervising Virtual Asset Service Providers, PVARA seeks to:

- Promote transparency within Pakistan's virtual asset industry.
- Protect investors and consumers.

- Reduce financial crime risks.
- Ensure compliance with AML/CFT requirements.
- Encourage responsible innovation.
- Strengthen confidence in Pakistan's digital asset market.

The regulatory framework aims to strike an appropriate balance between encouraging technological innovation and maintaining effective regulatory oversight.

Categories of Virtual Asset Service Providers

The PVARA licensing framework recognizes several categories of regulated Virtual Asset Service Providers. Depending upon the nature of the proposed business model, an applicant may require authorization for one or more regulated activities.

The principal licence categories include:

- Virtual Asset Exchange
- Custody Services
- Broker-Dealer Services
- Virtual Asset Derivatives
- Lending and Borrowing Services
- Management and Investment Services
- Transfer and Settlement Services
- Advisory Services
- Fiat-Referenced Token Issuance
- Asset-Referenced Token Issuance

Each licence category has its own regulatory requirements, capital obligations, operational standards, and ongoing compliance responsibilities.

Businesses That May Require a PVARA Licence

The requirement to obtain a PVARA licence depends on the nature of the services being provided rather than the technology used.

Examples of businesses that may require authorization include:

- Cryptocurrency exchanges
- Digital asset trading platforms
- Cryptocurrency custodians
- Wallet service providers offering custodial services
- Token issuance platforms
- Stablecoin issuers
- Crypto broker-dealers
- Blockchain investment platforms
- Digital asset portfolio managers
- Virtual asset lending platforms
- Cryptocurrency payment service providers
- Digital asset settlement platforms

Businesses should carefully assess whether their proposed activities fall within one or more regulated categories before commencing operations.

Key Responsibilities of a Licensed VASP

Obtaining a licence is only the beginning of a VASP's regulatory obligations. Licensed entities are expected to maintain effective governance, operational resilience, and ongoing compliance with applicable laws and regulations.

Among the principal responsibilities are:

- Maintaining appropriate corporate governance.
- Conducting customer identification and verification procedures.
- Monitoring customer transactions.
- Reporting suspicious transactions where required.
- Protecting customer assets.
- Implementing cybersecurity controls.
- Maintaining adequate financial resources.
- Keeping accurate business records.

- Cooperating with regulatory authorities.
- Complying with ongoing reporting obligations.

Failure to comply with these responsibilities may expose the VASP to regulatory action, licence suspension, or other enforcement measures under the applicable legal framework.

Benefits of Becoming a Licensed VASP

Operating under a PVARA licence provides several important advantages for businesses seeking to establish a long-term presence in Pakistan's virtual asset market.

These benefits include:

- Legal recognition under Pakistan's regulatory framework.
- Greater confidence among customers and investors.
- Improved access to banking and financial services, subject to applicable regulatory requirements.
- Enhanced credibility with business partners.
- A structured compliance framework.
- Increased opportunities for international cooperation and business expansion.

For foreign companies, licensing also demonstrates a commitment to operating within Pakistan's legal and regulatory environment.

Virtual Asset Service Providers are the foundation of Pakistan's regulated digital asset ecosystem. Through the Virtual Assets Act 2026 and the licensing framework administered by PVARA, Pakistan has established a legal structure designed to promote responsible innovation while protecting consumers and maintaining financial integrity.

Any business intending to provide regulated virtual asset services should first determine whether its activities fall within a regulated VASP category and identify the appropriate licensing pathway. Early legal and regulatory planning can help businesses avoid compliance issues, reduce licensing delays, and establish a strong foundation for long-term operations within Pakistan's evolving virtual asset industry.

Chapter 4: PVARA Licence Categories

The Draft Pakistan Virtual Asset Services Regulations 2026 introduce a structured licensing framework for businesses operating in Pakistan's virtual asset ecosystem. Rather than adopting a single licence for all activities, the regulatory framework establishes separate licence categories based on the nature of the services provided. This approach enables the Pakistan Virtual Assets Regulatory Authority (PVARA) to regulate different business models according to their specific operational, financial, and compliance risks.

According to the PVARA License Guide 2026, there are ten proposed Virtual Asset Service Provider (VASP) licence categories under the Draft Regulations. Each category carries its own regulatory obligations and minimum paid-up capital requirements set out in Schedule I. The guide notes that, depending on the proposed business model, a single licence may authorize more than one regulated activity.

Exchange Licence

An Exchange Licence authorizes a Virtual Asset Service Provider to operate a platform through which users may buy, sell, or exchange virtual assets. This licence category generally applies to centralized cryptocurrency exchanges that facilitate trading between customers.

According to the Draft Regulations, the Exchange Licence has one of the highest minimum paid-up capital requirements due to the scale of customer assets, operational responsibilities, and regulatory oversight associated with exchange operations.

Custody Licence

A Custody Licence applies to businesses that safeguard or control virtual assets on behalf of customers. Custody providers are expected to implement secure storage solutions, cybersecurity controls, private key management, and client asset protection measures.

Because custody providers are entrusted with customer assets, they are subject to enhanced operational and security expectations under the regulatory framework.

Broker-Dealer Licence

The Broker-Dealer Licence applies to businesses that arrange, execute, or facilitate transactions involving virtual assets on behalf of clients. Depending upon the services provided, broker-dealers may act as intermediaries between buyers and sellers while remaining subject to PVARA's conduct and compliance requirements.

Virtual Asset Derivatives Licence

This licence category is intended for businesses offering products linked to virtual asset derivatives. Given the complexity and potential market risks associated with derivative products, applicants are expected to satisfy higher capital and compliance standards as prescribed in the Draft Regulations.

Lending and Borrowing Licence

Businesses facilitating virtual asset lending or borrowing services fall within this licence category. These activities involve additional financial and operational risks and therefore require greater regulatory oversight together with higher minimum paid-up capital requirements.

Management and Investment Services Licence

This licence category applies to businesses providing management or investment-related services involving virtual assets. Depending on the nature of the proposed services, applicants may be required to demonstrate appropriate governance arrangements, internal controls, and compliance procedures before receiving regulatory approval.

Transfer and Settlement Licence

The Transfer and Settlement Licence is designed for businesses facilitating the transfer, settlement, or movement of virtual assets between parties. These service providers play an important role in ensuring secure and efficient transaction processing within the virtual asset ecosystem.

Advisory Services Licence

Businesses providing professional advice relating to virtual assets may fall within the Advisory Services Licence category. According to Schedule I of the Draft Regulations, this licence category has the lowest minimum paid-up capital requirement among the proposed licence types.

Fiat-Referenced Token Issuance Licence

This category applies to businesses issuing fiat-referenced virtual assets or tokens. The guide indicates that token issuers are subject not only to significant minimum paid-up capital requirements but also to reserve obligations intended to support the issued assets.

Asset-Referenced Token Issuance Licence

The Asset-Referenced Token Issuance Licence covers businesses issuing tokens backed or referenced by specified assets. Similar to fiat-referenced token issuers, applicants are expected to satisfy the applicable paid-up capital requirements together with any reserve obligations specified under the Draft Regulations.

Schedule I Minimum Paid-Up Capital

The PVARA License Guide 2026 states that the Draft Regulations prescribe different minimum paid-up capital requirements according to the licence category. The capital ranges from PKR 25 million to PKR 1 billion, depending on the regulated activity. The guide also notes that these figures remain subject to confirmation at the time of filing because the regulations are currently in draft form.

Licence Category	**Minimum Paid-Up Capital***
Advisory Services	PKR 25 Million
Broker-Dealer	PKR 100 Million
Custody	PKR 200 Million
Management & Investment Services	PKR 200 Million
Transfer & Settlement	PKR 200 Million
Virtual Asset Derivatives	PKR 500 Million
Lending & Borrowing	PKR 500 Million
Exchange	PKR 1 Billion
Fiat-Referenced Token Issuance	PKR 1 Billion
Asset-Referenced Token Issuance	PKR 1 Billion

*The above capital figures are derived from the Draft Pakistan Virtual Asset Services Regulations 2026 as referenced in the PVARA License Guide 2026 and should be verified with PVARA before submitting a licence application.

The introduction of multiple licence categories reflects a risk-based regulatory approach under Pakistan's emerging virtual asset framework. By matching regulatory obligations to the specific activities performed by a Virtual Asset Service Provider, PVARA seeks to promote innovation while maintaining market integrity, consumer protection, and compliance with applicable legal and regulatory standards. Businesses intending to enter Pakistan's virtual asset market should carefully determine which licence category or combination of categories best aligns with their proposed operations before commencing the licensing process.

Chapter 5: Eligibility for a PVARA Licence

Obtaining a licence from the Pakistan Virtual Assets Regulatory Authority (PVARA) is the first legal step for any business intending to provide regulated virtual asset services in Pakistan. The licensing framework under the Virtual Assets Act 2026 is designed to ensure that only qualified, financially sound, and compliant businesses are permitted to operate within Pakistan's virtual asset ecosystem. Applicants must satisfy various legal, corporate, financial, technical, and compliance requirements before PVARA will consider granting a licence.

This chapter provides an overview of the principal eligibility requirements based on the PVARA License Guide 2026.

Eligible Applicants

A PVARA licence may be sought by businesses intending to conduct regulated virtual asset activities within Pakistan. Depending on the proposed business model, eligible applicants may include:

- Cryptocurrency exchanges
- Virtual asset custodians
- Broker-dealers
- Token issuers
- Digital asset investment managers
- Virtual asset transfer and settlement providers
- Lending and borrowing platforms
- Blockchain and Web3 companies offering regulated services

Applicants should determine the appropriate licence category before commencing the application process.

Legal Entity Requirement

The licensing framework requires applicants to establish a legal presence in Pakistan before commencing licensed operations.

According to the PVARA License Guide 2026, applicants are expected to:

- Register a company under the Companies Act 2017.

- Incorporate the company through the Securities and Exchange Commission of Pakistan (SECP).
- Establish a principal place of business in Pakistan.
- Maintain a physical office and operational infrastructure within Pakistan.

Foreign companies seeking to enter the Pakistani market are generally expected to establish a locally incorporated entity before obtaining full licensing.

Fit and Proper Criteria

One of the most important licensing requirements is the "Fit and Proper" assessment.

PVARA requires key individuals associated with the applicant to demonstrate integrity, competence, and suitability for operating a regulated financial business.

The assessment generally applies to:

- Directors
- Chief Executive Officer (CEO)
- Compliance Officer
- Ultimate Beneficial Owners (UBOs)

The PVARA License Guide states that applicants should satisfy requirements including:

- Clean criminal record or police clearance certificates.
- No history of significant regulatory sanctions.
- Verification of employment history.
- Verification of educational qualifications.
- Proper authentication of foreign documents through notarisation and apostille where applicable.

Failure to satisfy the fit and proper requirements may affect an applicant's eligibility for licensing.

Financial Capacity

Applicants are expected to demonstrate sufficient financial resources to support their proposed virtual asset business.

The guide provides that minimum paid-up capital requirements vary according to the applicable licence category and are specified in Schedule I of the Draft Pakistan Virtual Asset Services Regulations 2026.

Depending upon the regulated activity, minimum capital requirements range from PKR 25 million to PKR 1 billion. Applicants should verify the applicable capital threshold for their selected licence category before submitting an application.

The guide also notes that PVARA has confirmed there is currently no prescribed application fee, although applicants should verify any future changes before filing.

AML/CFT Readiness

Compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) requirements forms a central component of the licensing process.

Applicants are expected to establish an effective compliance framework incorporating:

- Know Your Customer (KYC)
- Know Your Business (KYB)
- Customer Due Diligence (CDD)
- Transaction monitoring
- Sanctions screening
- Politically Exposed Person (PEP) screening
- Suspicious transaction reporting
- Registration with the FMU goAML portal.

These measures are intended to align Pakistan's virtual asset sector with international AML/CFT standards.

Technical and Cybersecurity Capability

PVARA also evaluates whether applicants possess the technical capacity to operate securely and responsibly.

The guide identifies several technical expectations, including:

- Robust cybersecurity framework.
- Secure private key management.

- Business continuity planning.
- Disaster recovery arrangements.
- Data protection controls.
- Independent third-party security audits.
- Client asset safeguarding measures.

Applicants should ensure that appropriate technical controls are implemented before commencing regulated operations.

Operational Readiness

Beyond corporate registration and financial capacity, applicants should be operationally prepared to deliver the services covered by their proposed licence.

Operational readiness generally includes:

- Qualified management personnel.
- Appropriate compliance functions.
- Internal governance procedures.
- Risk management systems.
- Customer complaint handling mechanisms.
- Record-keeping policies.

Strong governance arrangements assist applicants in demonstrating their ability to comply with ongoing regulatory obligations.

Foreign Applicants

The PVARA framework allows international businesses to participate in Pakistan's regulated virtual asset market.

However, the guide indicates that foreign applicants who are not locally incorporated will generally be required to incorporate a company in Pakistan and register with the relevant local tax authorities as part of the licensing process.

International businesses should therefore plan for local corporate establishment, regulatory compliance, and operational infrastructure before seeking a full licence.

Practical Considerations

Prospective applicants should carefully assess their readiness before beginning the licensing process. Preparing corporate documentation, establishing governance structures, implementing AML/CFT policies, arranging cybersecurity controls, and ensuring adequate financial resources can significantly improve the quality of an application.

Businesses should also monitor regulatory developments, as certain aspects of the Draft Pakistan Virtual Asset Services Regulations 2026 remain subject to finalisation. Current licensing requirements should always be verified directly with PVARA before submitting an application.

Eligibility for a PVARA licence extends beyond simple company registration. Applicants must demonstrate legal incorporation, financial capacity, competent management, robust AML/CFT controls, cybersecurity preparedness, operational capability, and compliance with the fit and proper requirements. Meeting these eligibility standards forms the foundation for obtaining and maintaining authorization to operate as a regulated Virtual Asset Service Provider in Pakistan.

Chapter 6: Regulatory Entry Routes

The Pakistan Virtual Assets Regulatory Authority (PVARA) has introduced a structured framework that allows businesses to enter Pakistan's regulated virtual asset market through different regulatory pathways. Rather than requiring every applicant to immediately obtain a full Virtual Asset Service Provider (VASP) licence, the regulatory framework provides multiple entry routes depending on the nature, maturity, and objectives of the applicant's business.

According to the PVARA License Guide 2026, applicants may enter the regulatory system through one of four primary routes:

- No Objection Certificate (NOC)
- Regulatory Sandbox
- No-Action Relief
- Full VASP Licence

Selecting the appropriate entry route is one of the most important decisions for any cryptocurrency exchange, blockchain startup, fintech company, or digital asset service provider intending to operate in Pakistan. The chosen pathway depends on the applicant's business model, operational readiness, financial capacity, and stage of development.

6.1 No Objection Certificate (NOC)

The No Objection Certificate (NOC) serves as the initial regulatory gateway for many businesses seeking to establish a presence in Pakistan's virtual asset sector. The guide explains that obtaining an NOC does not authorize commercial operations. Instead, it confirms that PVARA has no objection to the applicant proceeding with the next stages of the licensing process.

An NOC enables applicants to:

- Register on the FMU goAML portal.
- Incorporate a local company.
- Establish a physical presence in Pakistan.
- Continue towards a full VASP licence.

The guide specifically notes that an NOC is not a licence and should not be interpreted as permission to provide virtual asset services to customers. Commercial operations may only commence after the applicant has successfully completed the licensing process and obtained the appropriate VASP licence.

6.2 Regulatory Sandbox

The Regulatory Sandbox is designed for innovative blockchain businesses and startups that wish to test new virtual asset products or services within a supervised regulatory environment before obtaining a full licence.

According to the guide, the Sandbox enables applicants to operate under controlled conditions while benefiting from proportionate capital requirements during the testing phase. Applications are accepted throughout the year and are assessed by PVARA based on innovation, governance, consumer protection, cybersecurity, financial readiness, and regulatory compliance.

Applicants are generally expected to submit:

- Form I application.
- Self-assessment checklist.
- Innovation proposal.
- Risk management framework.
- Cybersecurity strategy.
- Consumer protection measures.
- Exit strategy.

Successful applicants receive a Letter of Approval (LoA) that outlines the terms and conditions governing their participation in the Sandbox. In appropriate circumstances, PVARA may also issue a No-Action Letter for specified testing activities during the approved testing period. However, the guide clarifies that a No-Action Letter does not provide legal immunity and may be withdrawn by PVARA if necessary.

6.3 No-Action Relief

The PVARA License Guide 2026 explains that No-Action Relief may be granted to approved Regulatory Sandbox participants during the testing period.

A No-Action Letter indicates that, for the specified activities and duration of the approved testing programme, PVARA does not presently intend to take enforcement action against the participant, provided all applicable terms and conditions are observed.

The guide emphasizes that No-Action Relief:

- Applies only to approved Sandbox participants.
- Is limited to the approved testing activities.

- Does not constitute legal immunity.
- May be withdrawn at any time by PVARA through written notice.

Accordingly, applicants should continue to comply with all applicable obligations relating to consumer protection, AML/CFT requirements, cybersecurity, and reporting throughout the testing period.

6.4 Full VASP Licence

The Full Virtual Asset Service Provider (VASP) Licence represents the final regulatory stage and authorizes eligible businesses to commence commercial operations in Pakistan.

The guide explains that applicants seeking a full licence must satisfy the applicable requirements prescribed under the Draft Pakistan Virtual Asset Services Regulations 2026, including:

- Minimum paid-up capital under Schedule I.
- Corporate governance requirements.
- Fit and Proper criteria.
- AML/CFT compliance.
- Risk management systems.
- Cybersecurity controls.
- Asset segregation.
- Operational audits.
- Activity-Specific Handbook requirements.

Only after meeting these regulatory obligations and receiving approval from PVARA may a Virtual Asset Service Provider legally conduct regulated business activities within Pakistan.

Choosing the Appropriate Entry Route

The PVARA framework recognises that virtual asset businesses differ significantly in size, business model, technological maturity, and regulatory preparedness. Consequently, the availability of multiple entry routes provides flexibility while ensuring that innovation remains subject to appropriate regulatory oversight.

Businesses that are still developing innovative products may find the Regulatory Sandbox suitable for supervised testing. Companies seeking to establish operations may initially pursue an NOC before completing local incorporation and applying for a full licence. Mature businesses with

established governance, financial resources, and compliance frameworks may proceed directly toward obtaining a Full VASP Licence where appropriate.

Regardless of the chosen pathway, applicants should ensure that their business model, governance arrangements, compliance programme, and operational controls are fully aligned with the requirements prescribed by PVARA before submitting an application.

Chapter 7: Phase One – No Objection Certificate (NOC)

Introduction

The first stage in establishing a regulated Virtual Asset Service Provider (VASP) in Pakistan is obtaining a **No Objection Certificate (NOC)** from the Pakistan Virtual Assets Regulatory Authority (PVARA). According to the PVARA License Guide 2026, the NOC serves as the primary entry point into Pakistan's virtual asset licensing framework and is intended for businesses that wish to establish a legal presence before applying for a full VASP licence.

The NOC is an important regulatory milestone because it demonstrates that PVARA has no objection to the applicant proceeding with the next stages of the licensing process. However, it is important to understand that an NOC is not equivalent to a licence and does not authorize a business to commence commercial virtual asset services.

Purpose of the NOC

The NOC provides regulatory approval for an applicant to begin establishing its business structure in Pakistan. It allows the applicant to move forward with incorporation, compliance registration, and other preparatory activities required before applying for a full licence.

According to the guide, once the NOC has been granted, the applicant may:

- Register on the FMU goAML portal.
- Incorporate a local company in Pakistan.
- Proceed to the second phase of the licensing process.

The guide directs applicants to submit NOC applications through the official PVARA website.

The NOC Is Not a Licence

One of the most important legal distinctions emphasized throughout the licensing framework is that an NOC should not be confused with a Virtual Asset Service Provider licence.

An NOC does not authorize an applicant to:

- Operate a cryptocurrency exchange.
- Offer virtual asset services to customers.
- Accept client funds or digital assets.
- Advertise regulated virtual asset services as a licensed business.
- Commence full commercial operations.

The NOC simply permits the applicant to continue progressing through the regulatory process before seeking full authorization.

Businesses should therefore avoid representing themselves as licensed VASPs solely because an NOC has been issued.

Preparing the NOC Application

Although the PVARA License Guide provides only a high-level overview, applicants should prepare comprehensive documentation demonstrating the legitimacy of their proposed business.

The guide indicates that applicants are expected to provide information relating to their ownership structure, business activities, management, compliance arrangements, and financial capability before PVARA considers the application.

Preparing complete and accurate documentation at this stage can assist the regulatory review process and reduce delays caused by incomplete submissions.

Regulatory Review

Following submission, PVARA reviews the application to determine whether the proposed business appears suitable to proceed to the next stage of the licensing framework.

During this review, the Authority may assess matters relating to the applicant's proposed activities, corporate structure, compliance arrangements, and readiness to establish a regulated presence within Pakistan.

The guide does not specify a fixed statutory timeline for the issuance of an NOC.

Transition to Phase Two

Once an NOC has been granted, the applicant proceeds to Phase Two of the licensing framework.

According to the guide, this phase includes:

- Registration with the Securities and Exchange Commission of Pakistan (SECP).
- Incorporation of a company under the Companies Act 2017.
- Establishment of a physical office and operational infrastructure in Pakistan.
- Registration with the Financial Monitoring Unit (FMU) through the mandatory goAML portal.

Completion of these requirements prepares the applicant for the final licensing phase.

Importance of Early Compliance Planning

Obtaining an NOC should not be viewed merely as an administrative requirement. It represents the beginning of the applicant's regulatory relationship with PVARA.

Businesses intending to enter Pakistan's virtual asset market should begin developing their internal compliance framework during this stage. This includes planning for corporate governance, anti-money laundering and counter-terrorist financing (AML/CFT) procedures, cybersecurity controls, operational risk management, and customer protection measures that will later form part of the full licensing assessment.

Early preparation can help applicants satisfy the more comprehensive regulatory requirements applicable during Phase Three.

Practical Considerations

Applicants should carefully evaluate their proposed business model before submitting an NOC application. Determining the appropriate licence category, understanding future capital requirements, and establishing an effective compliance strategy at an early stage may significantly improve the efficiency of the overall licensing process.

As the regulatory framework continues to evolve, businesses should verify all current requirements directly with PVARA before filing any application. The PVARA License Guide also notes that certain aspects of the licensing framework remain subject to draft regulations and should be confirmed at the time of filing.

The No Objection Certificate is the foundation of Pakistan's virtual asset licensing process. While it does not authorize commercial operations, it enables applicants to establish their legal presence, complete essential regulatory registrations, and prepare for a full Virtual Asset Service Provider licence. Businesses that approach this phase with careful planning and comprehensive documentation are better positioned to progress smoothly through the subsequent stages of the PVARA licensing framework.

Chapter 8: Phase Two – Company Incorporation and Local Establishment

After obtaining a No Objection Certificate (NOC) from the Pakistan Virtual Assets Regulatory Authority (PVARA), an applicant must proceed to the second stage of the licensing process by establishing a legal and operational presence in Pakistan. According to the PVARA License Guide 2026, this phase enables applicants to satisfy the corporate, regulatory, and anti-money laundering requirements necessary before applying for a full Virtual Asset Service Provider (VASP) licence.

The successful completion of this phase demonstrates that the applicant has established a genuine business presence within Pakistan and is prepared to comply with the country's legal and regulatory framework.

Purpose of Phase Two

The primary objective of Phase Two is to ensure that every prospective Virtual Asset Service Provider operates through a properly incorporated Pakistani entity with an identifiable business location, appropriate corporate governance, and effective AML/CFT controls.

The PVARA License Guide identifies four key requirements during this phase:

- Registration with the Securities and Exchange Commission of Pakistan (SECP)
- Incorporation of a local company
- Establishment of a physical office in Pakistan
- Registration with the Financial Monitoring Unit (FMU) through the goAML portal

These requirements form the foundation upon which the applicant may later seek a full VASP licence.

Company Registration with SECP

Once the NOC has been issued, the applicant is expected to register a company with the Securities and Exchange Commission of Pakistan (SECP). The company should be incorporated under the Companies Act 2017 and operate as the legal entity responsible for conducting virtual asset activities within Pakistan.

Incorporation establishes the company's legal identity and enables it to enter into contracts, employ staff, maintain corporate records, and fulfil regulatory obligations. It also provides transparency regarding the ownership and management of the business.

Establishing a Local Presence

The licensing framework requires applicants to establish a genuine operational presence within Pakistan. According to the guide, this includes maintaining a physical office and appropriate operational infrastructure.

A local office enables regulatory authorities to supervise licensed entities effectively and provides an official location for regulatory inspections, correspondence, compliance activities, and customer support.

Foreign companies intending to operate in Pakistan are generally expected to establish a locally incorporated entity before progressing to full licensing.

Registration with the FMU goAML Portal

Anti-money laundering compliance forms an essential component of Pakistan's virtual asset regulatory framework.

During Phase Two, applicants must register with the Financial Monitoring Unit (FMU) through the mandatory goAML reporting system. The guide identifies FMU registration as a compulsory requirement for AML/CFT compliance.

Registration on the goAML platform enables Virtual Asset Service Providers to fulfil their reporting obligations and participate in Pakistan's national framework for monitoring suspicious financial activities.

Building the Corporate Compliance Framework

Although the principal objective of Phase Two is company establishment, applicants should also begin implementing the internal governance and compliance systems expected during the licensing process.

The guide later identifies several important corporate requirements, including:

- Appropriate corporate governance
- Resident director requirements where applicable
- Fit and Proper assessments for directors and senior management
- Identification of Ultimate Beneficial Owners (UBOs)
- Maintenance of the prescribed paid-up capital
- Physical operational infrastructure in Pakistan

Preparing these governance arrangements during Phase Two can facilitate a smoother transition to the final licensing stage.

Importance of Local Operations

The requirement to establish a local business presence reflects the regulatory objective of ensuring accountability and effective supervision. A locally incorporated company with identifiable management, operational infrastructure, and compliance systems enables PVARA and other competent authorities to oversee licensed activities more effectively.

Local incorporation also assists businesses in developing relationships with service providers, recruiting qualified personnel, implementing internal controls, and preparing for ongoing regulatory compliance.

Transition to Phase Three

Completion of Phase Two does not authorize the applicant to commence commercial virtual asset services. Instead, it prepares the applicant for the final stage of the licensing process.

After incorporating the company, establishing its operational presence, and completing mandatory FMU registration, the applicant may proceed to apply for a full Virtual Asset Service Provider licence under the Draft Pakistan Virtual Asset Services Regulations 2026, subject to satisfying the applicable capital, compliance, cybersecurity, and operational requirements.

Phase Two represents the bridge between regulatory approval in principle and formal commercial licensing. By incorporating a local company, establishing a physical presence, registering with the FMU goAML system, and preparing the necessary governance and compliance structures, applicants position themselves to meet PVARA's licensing standards and advance toward full authorization to operate within Pakistan's regulated virtual asset ecosystem.

Chapter 9: Phase Three – Full VASP Licence

After successfully completing the preliminary stages of the licensing process, including obtaining a No Objection Certificate (NOC) and establishing a local presence in Pakistan, applicants may proceed to apply for a Full Virtual Asset Service Provider (VASP) Licence. According to the PVARA License Guide 2026, this phase authorizes a business to commence full commercial operations as a regulated Virtual Asset Service Provider in Pakistan.

The Full VASP Licence is granted under the Draft Pakistan Virtual Asset Services Regulations 2026, which establish the licensing categories, minimum paid-up capital requirements under Schedule I, and operational standards set out in the Activity-Specific Handbooks 2026. As noted in the guide, these regulations are currently in draft form, and applicants should confirm the latest requirements with PVARA before submitting a licence application.

Purpose of the Full VASP Licence

The Full VASP Licence provides legal authorization for Virtual Asset Service Providers to offer regulated virtual asset services within Pakistan. Unlike a No Objection Certificate, which merely allows applicants to proceed with company incorporation and regulatory preparations, a Full VASP Licence permits commercial operations after all regulatory requirements have been satisfied.

Before granting a licence, PVARA assesses whether the applicant possesses adequate financial resources, operational capability, governance arrangements, and compliance systems necessary to conduct virtual asset activities in a secure and responsible manner.

Minimum Capital Requirements

Applicants must satisfy the applicable minimum paid-up capital prescribed in Schedule I of the Draft Pakistan Virtual Asset Services Regulations 2026. The amount of paid-up capital depends upon the category of licence being sought and ranges from PKR 25 million to PKR 1 billion.

The guide explains that these capital requirements are recoverable paid-up share capital rather than application fees. PVARA has also confirmed that there is currently no prescribed application fee, although applicants should verify any future fee requirements directly with the Authority.

Operational Readiness

Before issuing a Full VASP Licence, PVARA expects applicants to demonstrate that their operational systems are capable of supporting secure and compliant virtual asset services.

The guide identifies several operational requirements, including:

- Independent cybersecurity and systems reviews.

- Robust risk management systems.
- Segregation of customer assets.
- Proof of reserves where applicable, including reserve requirements for token issuers.
- Compliance with Activity-Specific Handbook standards relevant to the licence category. These measures are intended to promote financial stability, consumer protection, and operational resilience within Pakistan's virtual asset market.

Corporate Governance

Applicants are expected to establish appropriate governance structures before commencing commercial operations.

The guide specifies that a licensed VASP should maintain:

- Registration under the Companies Act 2017.
- A principal place of business in Pakistan.
- A physical office and operational infrastructure.
- Minimum paid-up capital applicable to the licence category.
- A resident director where required under company law.

Strong governance assists regulators in ensuring accountability and effective supervision of licensed businesses.

Fit and Proper Requirements

Directors, chief executive officers, compliance officers, and ultimate beneficial owners must satisfy PVARA's fit-and-proper criteria before a licence may be granted.

According to the guide, these assessments include:

- Clean criminal records or police clearance certificates.
- Verification of qualifications and employment history.
- Foreign documents that are notarised and apostilled where required.
- No significant history of regulatory sanctions.

These requirements help ensure that licensed businesses are managed by competent and trustworthy individuals.

AML/CFT Compliance

Compliance with Anti-Money Laundering and Counter-Terrorist Financing obligations is a fundamental licensing requirement.

The guide requires applicants to establish comprehensive AML/CFT systems that include:

- Customer identification and verification (KYC).
- Business customer due diligence (KYB).
- Customer due diligence procedures.
- Transaction monitoring.
- FATF Travel Rule compliance.
- Sanctions and Politically Exposed Person (PEP) screening.
- Suspicious activity reporting.
- Registration on the FMU goAML portal.

These controls are designed to reduce financial crime risks and support compliance with international AML standards.

Cybersecurity Requirements

The protection of digital assets and customer information is an important element of the licensing framework.

The guide requires applicants to implement:

- Robust cybersecurity controls.
- Secure cryptographic key management.
- Business continuity and disaster recovery plans.
- Data protection measures.
- Independent third-party security audits.
- Custody controls designed to safeguard client assets.

Effective cybersecurity controls assist in maintaining operational integrity and protecting customer assets against cyber threats.

Commencement of Commercial Operations

The guide makes it clear that a Virtual Asset Service Provider may commence full commercial operations only after successfully completing Phase Three and obtaining the Full VASP Licence. Until the licence is granted, an applicant holding only an NOC or participating in the Regulatory Sandbox is not authorized to conduct unrestricted commercial activities.

Practical Considerations

Businesses preparing for Phase Three should ensure that their legal, financial, operational, and compliance documentation is complete before filing a licence application. Corporate governance arrangements, AML/CFT policies, cybersecurity frameworks, internal controls, and capital adequacy should all be reviewed in advance to facilitate the regulatory assessment process.

Since the Draft Pakistan Virtual Asset Services Regulations 2026 remain subject to amendment, applicants should verify all current licensing requirements, capital thresholds, and procedural updates directly with PVARA before submitting their applications.

The Full VASP Licence represents the final stage of Pakistan's licensing framework for Virtual Asset Service Providers. It reflects PVARA's objective of creating a regulated virtual asset ecosystem that promotes innovation while maintaining high standards of transparency, consumer protection, cybersecurity, and regulatory compliance.

Chapter 10: Corporate Governance Requirements

Corporate governance is one of the fundamental pillars of the PVARA licensing framework. Every Virtual Asset Service Provider (VASP) seeking authorization to operate in Pakistan must establish an appropriate corporate structure, implement effective internal controls, and demonstrate that its governance arrangements are capable of supporting safe, transparent, and compliant business operations.

The PVARA License Guide 2026 emphasizes that licensing extends beyond financial capability or technological infrastructure. Applicants are also expected to maintain sound corporate governance practices that promote accountability, operational integrity, consumer protection, and regulatory compliance. These requirements are intended to ensure that licensed VASPs operate responsibly while maintaining confidence in Pakistan's emerging virtual asset ecosystem.

Company Registration

Before a business can obtain a full PVARA licence, it must establish a legal presence in Pakistan. According to the guide, applicants are required to register a company with the Securities and Exchange Commission of Pakistan (SECP) under the Companies Act 2017. The company must also establish its principal place of business and maintain operational infrastructure within Pakistan.

A locally incorporated company enables regulatory oversight, facilitates communication with government authorities, and provides the legal foundation for licensing, taxation, and ongoing compliance.

Local Presence

The guide requires applicants to establish a genuine operational presence rather than merely maintaining a registered office. This includes maintaining a physical office, appropriate business infrastructure, and sufficient operational resources to conduct regulated virtual asset activities within Pakistan.

Maintaining a local presence allows regulators to supervise licensed entities more effectively and supports compliance with applicable legal and regulatory obligations.

Paid-Up Capital

Corporate governance also includes maintaining adequate financial resources. The guide provides minimum paid-up capital requirements for each licence category under Schedule I of the Draft Pakistan Virtual Asset Services Regulations 2026. These capital requirements vary according to the nature of the regulated activity and are intended to ensure that licensed entities possess sufficient financial capacity to conduct their operations responsibly.

Applicants should confirm the applicable capital requirement for their proposed licence category before submitting an application, as the regulations remain in draft form.

Resident Director

The guide specifies that applicants must comply with the corporate governance requirements of the Companies Act 2017, including the appointment of a resident director where required. A resident director assists in maintaining regulatory communication and supports the company's compliance with Pakistani corporate laws.

Fit and Proper Standards

Corporate governance extends beyond the corporate entity itself and includes the suitability of individuals responsible for managing the business.

According to the guide, directors, the Chief Executive Officer, the compliance officer, and Ultimate Beneficial Owners (UBOs) are expected to satisfy fit and proper requirements before licensing is granted. These assessments include reviewing criminal history, regulatory compliance history, qualifications, employment background, and overall integrity. Foreign documents may require notarisation and apostille authentication before submission.

These requirements are intended to ensure that individuals responsible for managing licensed VASPs possess the competence, honesty, and professional reputation necessary to safeguard customers and maintain confidence in the financial system.

Governance Policies and Internal Controls

Although the guide does not prescribe a detailed governance manual, it makes clear that applicants are expected to implement robust governance arrangements capable of supporting regulatory compliance.

Effective governance typically includes clearly defined management responsibilities, documented decision-making processes, internal reporting procedures, risk oversight, compliance monitoring, record retention, and appropriate segregation of duties. These governance measures support transparency and assist organizations in identifying and managing operational, legal, financial, and cybersecurity risks.

Risk Management

The guide identifies robust risk management systems as an important requirement before a full VASP licence is granted. Licensed entities are expected to identify, assess, monitor, and mitigate risks arising from their business activities while maintaining appropriate governance arrangements to ensure ongoing compliance.

Risk management should address operational risks, financial risks, cybersecurity risks, money laundering risks, fraud risks, and risks associated with customer asset protection.

Customer Asset Protection

Corporate governance also encompasses the safeguarding of customer assets. The guide requires applicants to maintain asset segregation arrangements, ensuring that customer assets are properly separated from the company's own assets. This measure strengthens investor protection and reduces the risk of customer losses in the event of financial distress or operational failure.

Compliance Culture

Strong corporate governance requires more than written policies. Senior management should promote a culture of compliance throughout the organization by ensuring that employees understand their legal responsibilities and follow applicable regulatory requirements.

An effective compliance culture supports AML/CFT obligations, cybersecurity controls, consumer protection measures, reporting obligations, and responsible business conduct. It also assists licensed VASPs in maintaining long-term regulatory compliance and operational resilience.

Corporate governance is a central component of the PVARA licensing framework. Establishing a locally incorporated company, maintaining adequate capital, appointing qualified management, implementing effective internal controls, and promoting a culture of compliance all contribute to responsible operation within Pakistan's regulated virtual asset sector.

Applicants that invest in strong governance structures from the outset are better positioned to meet regulatory expectations, manage business risks, protect customers, and support the long-term development of Pakistan's digital asset ecosystem.

Chapter 11: Fit and Proper Criteria

A fundamental requirement of the PVARA licensing framework is that every applicant must demonstrate that the individuals responsible for owning, managing, and controlling the Virtual Asset Service Provider (VASP) are suitable to operate within Pakistan's regulated virtual asset sector. This assessment is commonly referred to as the "Fit and Proper Criteria."

The objective of these requirements is to ensure that licensed VASPs are managed by competent, honest, financially responsible, and reputable individuals who possess the integrity necessary to safeguard customers, maintain market confidence, and comply with applicable laws and regulations.

According to the PVARA License Guide 2026, the Fit and Proper assessment applies to key individuals associated with the applicant, including directors, the Chief Executive Officer (CEO), compliance officers, and Ultimate Beneficial Owners (UBOs). These individuals must successfully satisfy PVARA's suitability assessment before a licence may be granted.

Purpose of the Fit and Proper Assessment

The Fit and Proper assessment enables PVARA to evaluate whether those responsible for managing a VASP possess the competence, integrity, experience, and financial soundness necessary to conduct regulated virtual asset activities responsibly.

The assessment also assists in preventing individuals involved in fraud, financial crime, money laundering, terrorist financing, or other serious misconduct from obtaining control over licensed virtual asset businesses.

Individuals Subject to Assessment

The PVARA License Guide specifies that the Fit and Proper Criteria apply to:

- Directors
- Chief Executive Officer (CEO)
- Compliance Officer
- Ultimate Beneficial Owners (UBOs)

These individuals are expected to demonstrate honesty, competence, professional integrity, and the ability to manage a regulated financial business responsibly.

Criminal Background Verification

One of the principal components of the assessment is verification of the applicant's criminal history.

The guide states that each relevant individual should possess a clean criminal record and provide appropriate police clearance certificates from every country in which they have resided, where applicable. This requirement assists PVARA in determining whether an applicant has previously been involved in criminal conduct that could adversely affect the integrity of the financial system.

Applicants should ensure that all criminal record documentation is accurate, current, and obtained from the appropriate authorities before submitting their licence application.

Verification of Qualifications and Employment History

Professional competence is another important consideration.

The licensing guide provides that employment history and educational qualifications may be verified during the assessment process. Applicants should therefore be prepared to provide documentary evidence supporting their academic credentials, professional certifications, previous employment, and relevant industry experience.

Maintaining complete and verifiable documentation can help facilitate the review process and reduce unnecessary delays.

Foreign Documentation

Where directors, shareholders, or Ultimate Beneficial Owners reside outside Pakistan, supporting documentation originating from foreign jurisdictions may require notarisation and apostille certification before submission.

The guide specifically notes that foreign documents should be notarised and apostilled where required, ensuring their authenticity and acceptance during regulatory review.

Applicants should confirm the documentary requirements applicable to their particular jurisdiction before filing.

Regulatory History

PVARA also considers the regulatory history of key individuals.

The licensing guide states that directors, compliance officers, CEOs, and Ultimate Beneficial Owners should have no prior history of significant regulatory sanctions.

A previous record of regulatory enforcement, licence revocation, financial misconduct, or serious compliance failures may adversely affect the assessment of an applicant's suitability to operate a regulated virtual asset business.

Relationship with Corporate Governance

The Fit and Proper Criteria should not be viewed as a one-time licensing requirement.

Maintaining suitable directors, senior management, and compliance personnel forms an important element of ongoing corporate governance throughout the life of the licence. Changes in ownership or senior management may require notification to PVARA and continued compliance with applicable regulatory requirements.

Applicants should therefore adopt internal governance procedures that ensure only appropriately qualified individuals are appointed to key positions.

Preparing for the Assessment

Before submitting a licence application, applicants should consider preparing the following documentation:

- Valid identification documents
- Police clearance certificates
- Curriculum vitae of key individuals
- Educational qualifications
- Professional certifications
- Employment verification documents
- Corporate ownership information
- Ultimate Beneficial Owner declarations
- Notarised and apostilled foreign documents where applicable

Organising these records in advance may contribute to a more efficient licensing process.

Practical Considerations

The Fit and Proper assessment reflects PVARA's commitment to maintaining confidence in Pakistan's virtual asset market.

Businesses seeking authorisation should carefully evaluate their proposed directors, shareholders, senior executives, and compliance officers before submitting an application. Ensuring that these individuals possess appropriate integrity, competence, and regulatory standing will contribute to a stronger application and demonstrate a commitment to responsible corporate governance.

As the regulatory framework continues to develop, applicants should consult the latest guidance issued by PVARA and ensure that all supporting documentation is complete, accurate, and up to date before filing their licence application.

Chapter 12: AML/CFT Compliance Framework

An effective Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) framework is one of the fundamental requirements for obtaining and maintaining a licence under Pakistan's Virtual Assets Act 2026. As Virtual Asset Service Providers (VASPs) facilitate the transfer, exchange, custody, and management of digital assets, they are expected to implement comprehensive compliance systems that prevent the misuse of their platforms for money laundering, terrorist financing, sanctions evasion, and other financial crimes.

According to the PVARA License Guide 2026, every licensed VASP is required to establish a risk-based AML/CFT programme aligned with applicable legal requirements and international standards. The framework should be proportionate to the size, complexity, and nature of the applicant's business and should be reviewed regularly to ensure its continued effectiveness.

Importance of AML/CFT Compliance

The virtual asset sector presents unique challenges due to the speed of transactions, cross-border transfers, and the use of blockchain technology. A strong AML/CFT framework helps protect the financial system, enhances investor confidence, reduces operational risk, and supports Pakistan's commitment to implementing international standards issued by the Financial Action Task Force (FATF).

Failure to implement appropriate AML/CFT controls may expose a business to regulatory action, financial penalties, licence suspension, or revocation.

Risk-Based Compliance Approach

The Guide requires VASPs to adopt a risk-based approach to compliance. Rather than applying identical controls to every customer or transaction, businesses should identify, assess, and manage risks according to factors such as:

- Nature of products and services
- Customer profile
- Geographic exposure
- Transaction size and frequency
- Delivery channels
- Technology risks
- Emerging financial crime threats

The risk assessment should be documented and updated whenever significant changes occur within the business.

Customer Due Diligence (CDD)

Customer Due Diligence is one of the core elements of the AML framework. Before establishing a business relationship, a VASP should verify the customer's identity using reliable documentation and independent information.

Customer due diligence generally includes:

- Customer identification
- Identity verification
- Collection of residential or business address
- Verification of beneficial ownership
- Assessment of the intended purpose of the business relationship
- Risk classification of the customer

Higher-risk customers may require Enhanced Due Diligence before services are provided.

Know Your Customer (KYC)

The Guide specifically identifies comprehensive Know Your Customer (KYC) procedures as a licensing requirement.

A robust KYC programme should include:

- Government-issued identification
- Address verification
- Biometric verification where appropriate
- Source of funds information
- Source of wealth information for higher-risk customers
- Ongoing customer profile updates

Accurate customer identification reduces the likelihood of anonymous misuse of virtual asset services.

Know Your Business (KYB)

Where customers are legal entities rather than individuals, businesses should implement Know Your Business (KYB) procedures.

KYB typically involves:

- Verification of company registration
- Identification of directors
- Identification of Ultimate Beneficial Owners (UBOs)
- Review of corporate ownership structure
- Verification of business activities
- Assessment of regulatory status

Understanding the ownership and control structure of corporate customers assists in identifying potential financial crime risks.

Enhanced Due Diligence (EDD)

Enhanced Due Diligence should be applied where customers or transactions present elevated risks.

Examples include:

- Politically Exposed Persons (PEPs)
- High-value transactions
- High-risk jurisdictions
- Complex ownership structures
- Unusual transaction patterns
- Cross-border virtual asset transfers

Additional documentation and management approval may be required before establishing or continuing the business relationship.

Transaction Monitoring

The Guide identifies transaction monitoring as a mandatory AML/CFT obligation.

VASPs should implement automated or manual monitoring systems capable of detecting:

- Unusual transaction activity

- Large or complex transfers
- Rapid movement of assets
- Structuring or smurfing activities
- Transactions involving sanctioned wallets
- Behaviour inconsistent with customer profiles

Monitoring should continue throughout the customer relationship rather than only during onboarding.

FATF Travel Rule Compliance

The Guide requires compliance with the FATF Travel Rule for applicable virtual asset transfers.

Where applicable, VASPs should collect, verify, and securely transmit required originator and beneficiary information during qualifying virtual asset transfers while maintaining appropriate privacy and security safeguards.

Sanctions Screening

Every VASP should establish procedures for sanctions screening to prevent transactions involving prohibited persons or entities.

Screening should be conducted:

- During customer onboarding
- Before executing transactions
- On an ongoing basis as sanctions lists are updated

Effective sanctions screening assists businesses in complying with national and international legal obligations.

Politically Exposed Persons (PEP) Screening

The Guide also identifies Politically Exposed Person screening as an important component of AML compliance.

PEPs may present increased corruption or bribery risks. Consequently, businesses should identify such customers, perform enhanced due diligence where appropriate, and maintain ongoing monitoring of the relationship.

Suspicious Transaction Reporting

Where unusual or suspicious activity is identified, VASPs should maintain procedures for documenting, investigating, and reporting such activity in accordance with applicable legal requirements.

Employees should receive appropriate training to recognise indicators of money laundering, terrorist financing, fraud, sanctions evasion, and other financial crimes.

FMU goAML Registration

The Guide states that registration on the Financial Monitoring Unit's goAML portal is mandatory for licensed Virtual Asset Service Providers.

The goAML system facilitates regulatory reporting and supports Pakistan's national AML/CFT framework.

Internal AML Governance

An effective AML programme should be supported by appropriate governance arrangements, including:

- Appointment of a qualified compliance officer
- Written AML/CFT policies and procedures
- Regular staff training
- Independent compliance reviews
- Internal reporting mechanisms
- Record retention procedures
- Periodic risk assessments

Senior management should ensure that adequate resources are allocated to maintain compliance with regulatory obligations.

Record Keeping

VASPs should maintain accurate records relating to:

- Customer identification
- Transaction history
- Risk assessments
- Due diligence documentation

- Internal investigations
- Regulatory reports

Proper record keeping assists regulatory supervision and supports future investigations where necessary.

AML/CFT compliance is not simply a licensing requirement; it is an ongoing regulatory responsibility that underpins the integrity of Pakistan's virtual asset ecosystem. The PVARA License Guide 2026 requires VASPs to implement comprehensive KYC, KYB, customer due diligence, transaction monitoring, FATF Travel Rule compliance, sanctions screening, suspicious transaction reporting, and FMU goAML registration as part of a robust risk-based compliance framework. Businesses that invest in strong governance, effective internal controls, and continuous compliance monitoring will be better positioned to meet regulatory expectations while protecting customers and maintaining confidence in Pakistan's rapidly developing digital asset market.

Chapter 13: Cybersecurity and Technology Requirements

Cybersecurity forms one of the most important pillars of Pakistan's regulatory framework for Virtual Asset Service Providers (VASPs). Under the PVARA licensing framework, applicants are expected to establish secure and resilient technology systems capable of protecting digital assets, customer information, and operational infrastructure from cyber threats. The objective is not only to safeguard virtual assets but also to maintain public confidence, market integrity, and operational resilience within Pakistan's emerging digital asset ecosystem.

Unlike traditional financial institutions, VASPs manage highly sensitive digital assets that can be transferred globally within seconds. This makes cryptocurrency exchanges, custodians, wallet providers, and blockchain businesses attractive targets for cybercriminals. Consequently, cybersecurity is treated as a core licensing requirement rather than merely an operational consideration.

Cybersecurity Framework

The PVARA License Guide requires applicants to implement a robust cybersecurity framework appropriate to the size, complexity, and nature of their business operations. This framework should identify cybersecurity risks, establish preventive controls, detect security incidents, and provide effective response and recovery mechanisms.

A comprehensive cybersecurity programme should cover all critical information systems, blockchain infrastructure, customer-facing platforms, internal networks, cloud services, and third-party service providers involved in delivering virtual asset services.

Key Management

One of the most sensitive aspects of virtual asset operations is the protection of cryptographic private keys. The guide specifically identifies key management as a technical requirement for licensing.

Private keys provide access to digital assets and therefore require strong security controls throughout their lifecycle. Appropriate governance, access controls, secure storage, backup procedures, and recovery mechanisms should be established to reduce operational risks and unauthorized access.

Custody and Client Asset Safeguarding

Businesses providing custody services or holding customer assets must implement appropriate safeguards to protect client assets from loss, theft, misuse, or unauthorized transfer.

The guide requires custody controls and client asset safeguarding mechanisms as part of the technical licensing requirements. These measures support investor protection and help ensure that customer assets remain appropriately protected throughout business operations.

Business Continuity and Disaster Recovery

Operational resilience is another important component of the licensing framework.

Applicants are expected to establish business continuity and disaster recovery plans capable of maintaining critical services during cyber incidents, technical failures, natural disasters, or other operational disruptions.

Business continuity planning should identify critical business functions, define recovery procedures, allocate responsibilities, and establish communication processes that support timely restoration of operations.

Data Protection

Virtual Asset Service Providers process significant amounts of confidential customer information, including identity verification records, financial information, transaction histories, and compliance documentation.

Accordingly, the guide requires appropriate data protection measures to secure sensitive information against unauthorized disclosure, alteration, or destruction.

Effective data governance supports customer privacy while strengthening overall cybersecurity resilience.

Independent Security Audit

The licensing framework also emphasizes independent third-party security audits.

Independent assessments provide assurance that technology systems, cybersecurity controls, and operational safeguards function effectively and remain consistent with regulatory expectations. External audits may identify vulnerabilities that require remediation before licensing or during ongoing operations.

Operational Risk Management

Cybersecurity should be integrated into an organization's broader risk management framework.

The guide identifies robust risk management systems as part of the licensing requirements, recognising that operational, technological, and cybersecurity risks must be identified, monitored, and appropriately managed throughout the life of the business.

An effective risk management framework supports regulatory compliance while reducing operational vulnerabilities.

Cybersecurity in the Regulatory Sandbox

Applicants seeking admission to the PVARA Regulatory Sandbox are also expected to demonstrate appropriate cybersecurity readiness.

The Sandbox application process requires applicants to submit information relating to their cybersecurity strategy, threat model, mitigation measures, technology architecture, operational resilience, and data privacy controls. Applicants must also explain how technology risks will be managed during the testing period.

The guide further identifies cybersecurity, private key protection, operational resilience, and data privacy compliance as important assessment criteria for Sandbox participation.

Consumer Protection Through Technology

Technology controls also contribute directly to consumer protection.

The guide links cybersecurity with fraud prevention, client asset safeguarding, dispute resolution mechanisms, risk disclosure, and investor protection. These measures help maintain trust in virtual asset markets while supporting responsible innovation under the Virtual Assets Act 2026.

Cybersecurity is not simply an IT function under the PVARA licensing framework; it is a fundamental regulatory obligation. Applicants are expected to establish secure technology infrastructure, protect customer assets, implement effective cybersecurity controls, maintain operational resilience, safeguard sensitive information, and continuously manage technology-related risks. Businesses that integrate cybersecurity into their governance and compliance programmes will be better positioned to satisfy licensing requirements and operate responsibly within Pakistan's regulated virtual asset ecosystem.

Chapter 14: Capital Requirements and Financial Obligations

A sound financial foundation is one of the most important requirements for obtaining and maintaining a Virtual Asset Service Provider (VASP) licence in Pakistan. Under the PVARA licensing framework, applicants are expected to demonstrate adequate financial capacity before commencing regulated virtual asset activities. The capital requirements are intended to promote financial stability, protect customers, reduce operational risks, and ensure that licensed entities possess sufficient resources to conduct their business responsibly.

According to the PVARA License Guide 2026, the minimum paid-up capital requirements are set out in Schedule I of the Draft Pakistan Virtual Asset Services Regulations 2026. The amount of paid-up capital varies depending on the nature of the regulated activity and the category of licence being sought. The guide notes that these capital figures remain in draft form and applicants should confirm the applicable amount with PVARA before submitting an application.

The draft capital requirements identified in the guide are as follows:

- Advisory Services – PKR 25 million
- Broker-Dealer – PKR 100 million
- Custody Services – PKR 200 million
- Management and Investment Services – PKR 200 million
- Transfer and Settlement Services – PKR 200 million
- Virtual Asset Derivatives – PKR 500 million
- Lending and Borrowing – PKR 500 million
- Exchange Services – PKR 1 billion
- Fiat-Referenced Token Issuance – PKR 1 billion
- Asset-Referenced Token Issuance – PKR 1 billion, together with applicable reserve requirements.

The guide explains that these amounts represent minimum paid-up share capital rather than licensing fees. It further states that the paid-up capital is recoverable and, where applicable, may be reduced for participants admitted to the Regulatory Sandbox under the relevant provisions of the draft regulations.
Importantly, the guide states that PVARA has confirmed there is currently no prescribed application fee for licensing. Nevertheless, applicants are advised to verify whether any

administrative or processing fees have been introduced before filing their application, as regulatory requirements may change over time.

Financial obligations extend beyond maintaining the required paid-up capital. Applicants are expected to demonstrate that they possess sufficient financial resources to establish and operate their proposed business model. During the Regulatory Sandbox application process, the guide requires applicants to provide evidence of financial readiness, including available funding, operating budgets, and clearly defined Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs).

The guide also highlights the importance of maintaining adequate insurance coverage for client indemnification during Sandbox participation. This requirement forms part of the broader consumer protection framework designed to safeguard users and reduce operational risk. For applicants involved in token issuance, additional financial safeguards may apply. The guide specifies that token issuers may be required to demonstrate proof of reserves and maintain adequate asset backing before commencing commercial operations. These measures are intended to strengthen market confidence and ensure that issued virtual assets are supported in accordance with applicable regulatory requirements.

Businesses seeking a PVARA licence should also establish robust financial governance arrangements. Appropriate accounting records, internal financial controls, budgeting procedures, and capital management policies contribute to regulatory compliance and assist applicants in demonstrating their financial capability during the licensing process.

Foreign applicants intending to establish operations in Pakistan should also consider the financial implications of incorporating a local company, maintaining operational infrastructure, meeting paid-up capital requirements, and complying with Pakistani tax laws. The guide notes that foreign companies participating in the Regulatory Sandbox will be required to incorporate locally and register with the relevant tax authorities as part of the regulatory process.

Capital adequacy should not be viewed merely as a regulatory obligation. Adequate capitalization enables a Virtual Asset Service Provider to invest in compliance systems, cybersecurity, customer protection measures, technology infrastructure, and qualified personnel. A financially resilient business is generally better positioned to manage operational risks, respond to market developments, and maintain long-term regulatory compliance.

As the Draft Pakistan Virtual Asset Services Regulations 2026 continue to evolve, prospective applicants should verify the latest Schedule I capital requirements and all related financial obligations directly with PVARA before making investment decisions or submitting a licence application.

Chapter 15: The PVARA Regulatory Sandbox

Innovation is one of the driving forces behind the blockchain and virtual asset industry. New technologies, decentralized applications, digital payment solutions, tokenized assets, and blockchain-based financial services often require testing before they are introduced into the wider market. Recognizing this need, the Pakistan Virtual Assets Regulatory Authority (PVARA) has introduced the Regulatory Sandbox under the Regulatory Sandbox Guidelines 2026, issued pursuant to the Virtual Assets Act 2026.

The Regulatory Sandbox provides a controlled regulatory environment in which innovative Virtual Asset Service Providers (VASPs), blockchain startups, and fintech companies may test new products, services, or business models under the supervision of PVARA. Rather than requiring a full licence from the outset, eligible participants may conduct limited testing while remaining subject to regulatory oversight.

Purpose of the Regulatory Sandbox

The primary objective of the Regulatory Sandbox is to encourage responsible innovation while maintaining appropriate safeguards for consumers, investors, and the financial system. According to the PVARA License Guide 2026, the Sandbox is designed to:

- Enable supervised testing of innovative virtual asset products and services.
- Promote financial innovation in a controlled regulatory environment.
- Support investor protection and market integrity.
- Allow eligible participants to operate with proportionate capital requirements under Regulation 7(5) before meeting the full Schedule I capital requirements.
- Establish structured procedures for application, assessment, supervision, and exit.
- Facilitate coordination with domestic and international regulatory authorities where appropriate.

The Sandbox therefore serves as an important bridge between innovation and full regulatory compliance.

Who Should Consider the Sandbox?

The Regulatory Sandbox is particularly suitable for businesses developing innovative blockchain or virtual asset solutions that may not yet be ready for full commercial licensing.

Examples may include:

- Blockchain technology startups.

- Cryptocurrency exchanges developing new trading models.
- Digital wallet providers.
- Tokenization platforms.
- Decentralized finance (DeFi) solutions.
- Blockchain payment systems.
- Digital asset custody technologies.
- Financial technology companies introducing innovative virtual asset services.

The Sandbox enables these businesses to validate their products while working closely with the regulator.

Key Features of the Sandbox

The guide highlights several important characteristics of the Regulatory Sandbox.

Applications are accepted throughout the year without fixed application windows, providing flexibility for innovators.

PVARA aims to complete its assessment within approximately sixty working days.

Successful applicants receive a Letter of Approval outlining the testing parameters, regulatory conditions, and operational limitations applicable during the Sandbox period.

Following completion of the testing programme, participants may either progress toward a full VASP licence or exit the Sandbox in an orderly manner if the project is not continued.

No-Action Relief

Where appropriate, PVARA may issue a No-Action Letter to approved Sandbox participants.

According to the guide, this indicates that PVARA does not presently intend to take enforcement action regarding specified activities conducted during the approved testing period.

However, the guide makes it clear that a No-Action Letter does not provide legal immunity. PVARA retains the authority to withdraw such relief by written notice if circumstances require.

Undertaking by Approved Participants

Upon approval, Sandbox participants are required to submit a formal undertaking accepting the terms and conditions of participation.

The undertaking includes commitments relating to:

- Consumer protection.
- AML/CFT compliance.
- Data security.
- Regulatory cooperation.
- Access rights for PVARA.

Participants are also expected to notify PVARA promptly of material incidents, submit incident reports within the prescribed period, retain transaction records for the statutory period, and maintain insurance coverage for client indemnification where required.

Eligibility Requirements

Before accepting an application, PVARA considers whether the applicant satisfies the eligibility criteria described in the Regulatory Sandbox Guidelines.

These include:

Fit and Proper Requirements

Directors and key management should have no history of fraud, financial crime, significant regulatory breaches, bankruptcy, or designation as prohibited persons.

Testing Plan

Applicants should submit clearly defined testing objectives, timelines, key performance indicators (KPIs), target users, and a clear exit strategy.

Risk and Governance

Applicants are expected to demonstrate an appropriate governance structure, identify ultimate beneficial owners, conduct enterprise risk assessments, implement customer screening procedures, establish complaint handling mechanisms, and maintain AML/CFT safeguards.

Consumer Protection

Applicants should explain how customer data, client assets, and consumer interests will be protected throughout the testing period.

Cybersecurity

The application should demonstrate appropriate cybersecurity controls, private key protection, operational resilience, and data privacy measures.

Scalability

Applicants should demonstrate sufficient technical capability, financial resources, and human expertise to expand operations following successful completion of the Sandbox programme.

Foreign Applicants

The guide provides that foreign companies wishing to participate in the Regulatory Sandbox will generally be required to incorporate a company in Pakistan and register with the relevant local tax authorities before Sandbox approval can be granted.

Sandbox Application Process

The Regulatory Sandbox follows a structured application process consisting of six principal stages:

1. Submission of Form I together with the required innovation description, blockchain technology details, cybersecurity strategy, regulatory analysis, and risk management information.
2. Submission of the Annexure-A Self-Assessment Checklist covering innovation, scalability, technology security, consumer benefit, readiness, and money laundering and terrorist financing preparedness.
3. Initial screening by PVARA to determine whether the application is complete.
4. Comprehensive regulatory assessment, during which PVARA may seek additional information or consult other regulators.
5. Issuance of a Letter of Approval where the application satisfies the required standards.
6. Supervised testing followed by submission of a completion report and either transition to full licensing or an orderly wind-down of the project.

Information Required in Form I

According to the guide, Form I should include comprehensive information about the proposed innovation, including:

- Innovation summary.
- Blockchain or distributed ledger technology architecture.
- Cybersecurity framework.
- Legal and regulatory compliance analysis.
- Risk management assessment.
- Financial readiness and budget.

- Consumer protection measures.
- Testing objectives.
- Exit strategy.
- Company background.
- Funding information.
- Contact details.

Practical Benefits

Participation in the Regulatory Sandbox offers several practical advantages.

Businesses are able to engage with regulators at an early stage, identify compliance issues before full commercial launch, refine governance arrangements, improve cybersecurity controls, and demonstrate regulatory commitment to prospective investors and business partners.

The Sandbox also provides regulators with valuable insight into emerging technologies while helping ensure that innovation develops within an appropriate legal framework.

The PVARA Regulatory Sandbox represents an important feature of Pakistan's Virtual Assets Act 2026. It provides an opportunity for innovative blockchain businesses to develop and test new products under regulatory supervision before obtaining a full VASP licence. By combining flexibility with appropriate consumer protection and compliance standards, the Sandbox seeks to encourage responsible innovation while maintaining confidence in Pakistan's evolving virtual asset ecosystem.

Prospective applicants should carefully review the Regulatory Sandbox Guidelines 2026 and ensure that all eligibility criteria, application requirements, governance arrangements, and compliance obligations are fully addressed before submitting an application to PVARA.

Chapter 16: Banking, Taxation, and Regulatory Coordination

A successful Virtual Asset Service Provider (VASP) requires more than obtaining a licence from the Pakistan Virtual Assets Regulatory Authority (PVARA). To operate legally and sustainably, a business must also comply with banking regulations, taxation laws, anti-money laundering (AML) obligations, and other regulatory requirements administered by various government authorities. The PVARA licensing framework is designed to work in coordination with these agencies, ensuring that licensed VASPs operate within Pakistan's broader financial and legal system.

This chapter explains the roles of the principal regulatory authorities and the banking and tax obligations applicable to licensed VASPs.

Regulatory Coordination

The regulation of virtual assets in Pakistan involves cooperation among several government institutions, each exercising jurisdiction over a specific aspect of the regulatory framework. According to the PVARA License Guide 2026, the principal authorities include PVARA, the Securities and Exchange Commission of Pakistan (SECP), the State Bank of Pakistan (SBP), the Financial Monitoring Unit (FMU), and the Federal Board of Revenue (FBR).

PVARA serves as the primary licensing and supervisory authority for Virtual Asset Service Providers. It is responsible for granting licences, supervising compliance, operating the Regulatory Sandbox, issuing guidance, and ensuring that licensed entities comply with the Virtual Assets Act 2026 and related regulations.

The SECP is responsible for company registration and corporate compliance. Every applicant establishing a local business presence in Pakistan must register under the Companies Act 2017 before proceeding with commercial operations.

The FMU oversees AML/CFT reporting through Pakistan's mandatory goAML platform. Licensed VASPs are expected to register with the FMU and submit suspicious transaction reports where required under applicable AML legislation.

The FBR administers taxation and reporting obligations. The guide notes that the FBR is responsible for tax compliance, including virtual asset reporting requirements applicable to licensed VASPs.

The SBP regulates Pakistan's banking system and plays an important role in facilitating access to banking services for licensed virtual asset businesses.

Banking Facilities for Licensed VASPs

Historically, one of the most significant operational challenges facing cryptocurrency businesses in Pakistan was obtaining banking facilities. Without access to corporate bank accounts,

businesses encountered practical difficulties in managing operational expenses, employee salaries, vendor payments, and regulatory reporting.

The PVARA License Guide highlights a significant regulatory development through SBP Circular No. 10 of 2026. According to the guide, the State Bank of Pakistan has authorised commercial banks to open and maintain bank accounts for PVARA-licensed Virtual Asset Service Providers. This represents an important step in supporting the regulated virtual asset sector and reducing barriers to legitimate business operations.

Businesses should note that banking facilities are linked to regulatory compliance. Financial institutions may require applicants to provide evidence of licensing status, corporate registration, ownership information, compliance policies, and customer due diligence procedures before establishing banking relationships.

Tax Compliance

Every licensed VASP is expected to comply with Pakistan's applicable tax laws. Tax compliance generally extends beyond payment of taxes and includes maintaining proper accounting records, preserving financial documentation, and fulfilling statutory reporting obligations.

The guide specifically refers to the FBR's responsibility for tax compliance and virtual asset reporting requirements applicable to licensed VASPs. Businesses should therefore establish appropriate accounting systems capable of recording transactions accurately and maintaining records for regulatory review.

Foreign companies establishing operations in Pakistan should also consider local tax registration requirements as part of their market entry strategy.

AML and Regulatory Reporting

Tax compliance operates alongside anti-money laundering obligations. Licensed VASPs are expected to implement effective customer due diligence procedures, transaction monitoring systems, sanctions screening, and suspicious transaction reporting mechanisms.

Registration with the FMU goAML portal forms an important component of this compliance framework and supports Pakistan's efforts to align its virtual asset sector with international AML/CFT standards.

Maintaining complete transaction records, customer information, and internal compliance documentation assists businesses in responding efficiently to regulatory inquiries and supervisory inspections.

Importance of Inter-Agency Cooperation

The regulation of virtual assets involves continuous coordination between multiple government authorities. Licensing issued by PVARA does not eliminate obligations arising under company law, banking regulations, tax legislation, or anti-money laundering laws.

Accordingly, successful VASPs should adopt an integrated compliance approach that considers the requirements of all relevant regulatory bodies. Corporate governance, financial reporting, AML compliance, cybersecurity, consumer protection, and tax compliance should operate together as components of a comprehensive compliance programme.

Practical Compliance Considerations

Before commencing commercial operations, applicants should ensure that:

- PVARA licensing requirements have been satisfied.
- Company registration with the SECP has been completed.
- FMU goAML registration has been successfully completed.
- Appropriate banking arrangements have been established.
- Internal accounting and taxation systems are operational.
- AML/CFT policies are fully implemented.
- Corporate governance procedures are documented.
- Regulatory reporting responsibilities have been assigned to qualified personnel.

Establishing these compliance measures during the early stages of business development reduces regulatory risk and promotes long-term operational stability.

The PVARA licensing framework reflects a coordinated regulatory approach involving multiple government institutions. While PVARA serves as the principal licensing authority, successful operation of a Virtual Asset Service Provider also requires compliance with corporate, banking, taxation, and AML/CFT obligations administered by the SECP, SBP, FMU, and FBR. Businesses that maintain effective coordination across these regulatory areas are better positioned to operate lawfully, protect customers, and contribute to the development of Pakistan's regulated virtual asset ecosystem.

Chapter 17: Ongoing Compliance and Reporting Obligations

Obtaining a PVARA licence is not the end of a Virtual Asset Service Provider's regulatory responsibilities. Licensing marks the beginning of an ongoing compliance relationship with the Pakistan Virtual Assets Regulatory Authority (PVARA). Licensed VASPs are expected to maintain effective governance, comply with applicable laws and regulations, implement robust internal controls, and continuously monitor their operations to ensure the protection of customers, market integrity, and financial stability.

The PVARA License Guide 2026 emphasizes that licensed entities must maintain comprehensive risk management systems, segregate customer assets, comply with the applicable Activity-Specific Handbooks, and continue to satisfy the regulatory standards applicable to their licence category. These obligations are intended to ensure that VASPs operate in a safe, transparent, and compliant manner throughout the life of their licence.

Regulatory Reporting

Licensed VASPs should establish procedures for timely submission of all regulatory reports required by PVARA and other competent authorities. Reporting obligations may include operational updates, financial information, compliance reports, incident notifications, and any additional information requested by the regulator.

Accurate reporting enables regulators to monitor compliance, identify emerging risks, and maintain confidence in Pakistan's virtual asset market.

AML/CFT Reporting

Ongoing Anti-Money Laundering and Counter-Terrorist Financing compliance remains one of the most significant responsibilities of every licensed VASP.

The guide requires VASPs to maintain comprehensive AML/CFT programmes that include customer due diligence, transaction monitoring, sanctions screening, politically exposed person (PEP) screening, FATF Travel Rule compliance, suspicious activity reporting, and mandatory registration with the FMU goAML portal.

Compliance programmes should be regularly reviewed and updated to reflect changes in business operations, customer risk profiles, and regulatory expectations.

Customer Due Diligence

Customer identification should not be treated as a one-time onboarding exercise.

VASPs should periodically review customer information, verify changes in ownership or control, reassess customer risk ratings, and apply enhanced due diligence where higher-risk relationships are identified.

Effective customer due diligence contributes to the prevention of money laundering, terrorist financing, sanctions evasion, and fraud.

Transaction Monitoring

Continuous monitoring of customer transactions is an essential component of regulatory compliance.

Licensed entities should maintain systems capable of identifying unusual or suspicious transactions, abnormal trading patterns, large transfers, high-risk jurisdictions, sanctioned wallet addresses, and other indicators of financial crime.

Where suspicious activity is identified, appropriate internal escalation procedures and regulatory reporting mechanisms should be followed.

Record Keeping

Proper record management supports both regulatory compliance and business continuity.

The Regulatory Sandbox section of the guide specifically requires participants to retain transaction records for the statutory period. Maintaining complete records also assists during regulatory inspections, audits, investigations, and customer dispute resolution.

Records should be maintained in a secure manner and remain readily accessible when requested by regulatory authorities.

Cybersecurity Monitoring

Cybersecurity obligations continue throughout the operation of a licensed VASP.

The guide requires businesses to maintain robust cybersecurity controls, secure key management, data protection measures, business continuity planning, disaster recovery procedures, and independent security assessments where applicable.

Regular vulnerability assessments, penetration testing, software updates, and access-control reviews can help reduce operational and cybersecurity risks.

Consumer Protection

Consumer protection remains a continuing regulatory responsibility.

Licensed VASPs should ensure that customer assets remain properly safeguarded, risks are clearly disclosed, complaints are handled fairly, and operational practices remain consistent with applicable regulatory requirements.

Maintaining transparent communication with customers contributes to greater confidence in the regulated virtual asset market.

Risk Management

The guide identifies robust risk management systems as an ongoing licensing requirement.

Risk management should cover operational, financial, technological, legal, compliance, cybersecurity, and reputational risks. Senior management should periodically review risk assessments and implement corrective measures where weaknesses are identified.

Governance and Internal Controls

Strong corporate governance supports long-term regulatory compliance.

Directors and senior management should ensure that compliance policies remain effective, responsibilities are clearly assigned, conflicts of interest are appropriately managed, and internal controls are periodically evaluated.

Independent compliance reviews may assist organizations in identifying areas requiring improvement before regulatory inspections occur.

Incident Reporting

Material operational incidents should be promptly reported in accordance with applicable regulatory requirements.

The Regulatory Sandbox Guidelines require approved participants to notify PVARA promptly of any material incident and submit a detailed incident report within the prescribed timeframe.

Although the guide specifically references Sandbox participants, licensed businesses should establish internal procedures for identifying, documenting, investigating, and escalating significant operational or cybersecurity incidents.

Independent Reviews and Audits

Independent assessments contribute to effective regulatory compliance.

The guide refers to operational audits, independent cybersecurity reviews, and third-party security assessments as part of the licensing and compliance framework.

Periodic reviews help management verify that internal controls remain effective and continue to meet regulatory expectations.

Continuous Regulatory Compliance

Compliance should be viewed as an ongoing process rather than a single regulatory event.

VASPs should continuously monitor changes to legislation, PVARA regulations, Activity-Specific Handbooks, AML/CFT requirements, and other regulatory guidance. Policies, procedures, employee training programmes, and internal controls should be updated whenever regulatory changes occur.

Organizations that maintain a proactive compliance culture are generally better positioned to manage regulatory risks, protect customer interests, and support the long-term development of Pakistan's regulated virtual asset ecosystem.

Chapter 18: Enforcement, Penalties, and Licence Revocation

An effective regulatory framework depends not only on licensing requirements but also on a robust enforcement mechanism. The Virtual Assets Act 2026 and the regulatory framework administered by the Pakistan Virtual Assets Regulatory Authority (PVARA) are designed to promote market integrity, protect investors, and ensure that Virtual Asset Service Providers (VASPs) operate in a safe, transparent, and compliant manner.

According to the PVARA License Guide 2026, licensed entities are expected to maintain continuous compliance with applicable laws, regulations, licence conditions, and regulatory guidance throughout their operations. Failure to comply with these obligations may result in regulatory enforcement actions ranging from corrective measures to licence suspension or revocation.

Regulatory Enforcement

PVARA has the authority to supervise licensed Virtual Asset Service Providers and monitor compliance with the Virtual Assets Act 2026, applicable regulations, Activity-Specific Handbooks, and licence conditions. Regulatory supervision is intended to ensure that licensed businesses continue to meet operational, financial, governance, cybersecurity, and AML/CFT requirements after receiving their licence.

Enforcement action may become necessary where a regulated entity fails to comply with statutory obligations or engages in activities that threaten consumers, market integrity, or the financial system.

Operating Without a Licence

The guide identifies operating a virtual asset business without obtaining the required PVARA licence as one of the most serious regulatory violations.

Businesses that provide regulated virtual asset services without proper authorisation may be subject to significant financial penalties and, where applicable, criminal consequences under the Virtual Assets Act 2026. The guide indicates that penalties for unlicensed operations may include fines of up to PKR 50 million and/or imprisonment, subject to the provisions of the Act. Readers are advised to verify the exact offences and applicable penalties in the legislation before relying upon them.

Unauthorized Virtual Asset Offerings

Businesses must ensure that any token issuance or virtual asset offering complies with the applicable regulatory framework.

The guide states that conducting unauthorized virtual asset offerings may result in regulatory enforcement, including fines that may reach PKR 25 million and/or imprisonment under the Virtual Assets Act 2026. As these figures are derived from the guide, applicants should confirm the final statutory provisions directly from the Act.

Prohibited Activities

The regulatory framework identifies several activities that are prohibited or subject to enforcement action if undertaken in violation of applicable laws or licence conditions.

Examples listed in the guide include:

- Operating without a PVARA licence.
- Market manipulation.
- Insider trading.
- Algorithmic stablecoins without appropriate safeguards.
- Unauthorized virtual asset offerings.
- False or misleading advertising.

Licensed entities should establish internal compliance systems to prevent these activities and ensure adherence to regulatory expectations.

Ongoing Non-Compliance

Regulatory compliance is not limited to the licensing stage. Licensed businesses are expected to maintain continuous compliance throughout their operations.

According to the guide, ongoing non-compliance may result in regulatory action, including suspension or permanent revocation of a licence where warranted by the circumstances.

Examples of ongoing non-compliance may include failure to maintain required compliance programmes, repeated breaches of licence conditions, or failure to satisfy regulatory obligations.

Licence Suspension

Licence suspension is generally intended as a temporary regulatory measure where deficiencies can be corrected.

During a suspension period, a Virtual Asset Service Provider may be required to address regulatory concerns, implement corrective actions, or satisfy additional supervisory requirements before normal operations may continue.

The guide indicates that licence suspension is one of the available enforcement measures for continuing regulatory breaches.

Licence Revocation

Where serious or repeated violations occur, PVARA may permanently revoke a licence.

Licence revocation effectively removes the legal authority of a Virtual Asset Service Provider to conduct regulated activities within Pakistan. Revocation may occur where a business persistently fails to comply with applicable legislation, licence conditions, or regulatory requirements, or where significant risks to consumers or market integrity arise.

The guide identifies permanent revocation as one of the available enforcement outcomes for ongoing non-compliance.

Regulatory Sandbox Enforcement

Participants admitted to the PVARA Regulatory Sandbox remain subject to regulatory oversight throughout the testing period.

The guide explains that PVARA may temporarily suspend or permanently revoke Sandbox approval if a participant fails to comply with agreed testing parameters, causes consumer detriment, or commits a serious compliance breach. In cases of permanent revocation, public notice is required.

The guide also notes that any No-Action Letter issued during Sandbox participation does not provide legal immunity and may be withdrawn by PVARA with written notice.

Importance of Internal Compliance

The enforcement framework highlights the importance of maintaining effective governance and compliance systems.

Licensed Virtual Asset Service Providers should continuously review their internal policies relating to:

- Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT).
- Customer Due Diligence (CDD).
- Know Your Customer (KYC) procedures.
- Risk management.
- Cybersecurity.
- Consumer protection.

- Record keeping.
- Regulatory reporting.
- Internal audits.

A proactive compliance culture helps reduce regulatory risk and supports long-term business sustainability.

Practical Observations

From a legal and compliance perspective, enforcement should not be viewed solely as a punitive mechanism. Effective supervision promotes investor confidence, encourages responsible innovation, and strengthens the credibility of Pakistan's virtual asset market.

Businesses intending to obtain a PVARA licence should regard compliance as an ongoing obligation rather than a one-time licensing requirement. Regular internal reviews, timely regulatory reporting, and prompt correction of identified deficiencies can significantly reduce the likelihood of enforcement action.

As noted throughout the PVARA License Guide 2026, applicants and licensed entities should verify the latest legal requirements directly with PVARA because regulatory procedures, penalty provisions, and licensing conditions may evolve as the framework continues to develop.

Chapter 19: Practical Licensing Tips for Applicants

Obtaining a licence from the Pakistan Virtual Assets Regulatory Authority (PVARA) involves more than submitting an application form. The licensing process requires applicants to demonstrate that they possess the financial capacity, governance structure, compliance framework, technical capability, and operational readiness necessary to conduct virtual asset activities in a safe and compliant manner. Careful planning before filing an application can significantly improve the likelihood of a successful outcome.

Understand Your Business Model

Before beginning the licensing process, applicants should clearly identify the nature of their proposed virtual asset activities. Different business models may fall within different Virtual Asset Service Provider (VASP) licence categories, each carrying distinct regulatory obligations and minimum capital requirements. A well-defined business model also assists in determining whether an applicant should first seek a No Objection Certificate (NOC), participate in the Regulatory Sandbox, or apply for a full VASP licence.

Select the Appropriate Licensing Route

PVARA provides multiple regulatory pathways, including the NOC process, the Regulatory Sandbox, No-Action Relief in appropriate cases, and the full VASP licensing regime. Applicants should carefully evaluate which route best suits their proposed activities, business maturity, and operational readiness. Businesses introducing innovative blockchain products may benefit from testing their services within the Regulatory Sandbox before seeking full commercial authorization.

Prepare a Comprehensive Business Plan

A detailed business plan is one of the most important documents supporting a licence application. The plan should clearly explain the proposed services, target market, revenue model, governance arrangements, operational structure, risk management framework, cybersecurity measures, and long-term business strategy. The information provided should be consistent with all other application documents.

Establish a Strong Corporate Structure

Applicants should ensure that the proposed company structure complies with applicable corporate laws and regulatory expectations. Shareholding arrangements, ownership structures, ultimate beneficial ownership information, and management responsibilities should be clearly documented. Transparent corporate governance promotes regulatory confidence and facilitates the licensing review process.

Appoint Qualified Management

The experience and integrity of directors, senior management, compliance officers, and key personnel play an important role during regulatory assessment. Individuals responsible for managing regulated activities should possess relevant professional qualifications, industry knowledge, and an understanding of virtual asset operations, financial regulation, and compliance obligations.

Develop an Effective AML/CFT Framework

A comprehensive Anti-Money Laundering and Counter-Terrorist Financing programme should be prepared before submitting a licence application. This framework should include customer due diligence procedures, Know Your Customer (KYC) policies, Know Your Business (KYB) procedures, transaction monitoring, sanctions screening, politically exposed person (PEP) screening, suspicious transaction reporting, record retention, employee training, and internal compliance controls.

Invest in Cybersecurity

Virtual asset businesses manage sensitive financial information and digital assets, making cybersecurity a critical licensing consideration. Applicants should establish secure wallet management procedures, private key protection mechanisms, access controls, data encryption, business continuity plans, disaster recovery procedures, and independent security testing wherever appropriate.

Prepare Financial Resources

Applicants should carefully assess the minimum paid-up capital applicable to their chosen licence category and ensure that sufficient financial resources are available before filing the application. Financial projections, funding arrangements, and supporting documentation should demonstrate the applicant's ability to operate sustainably while meeting regulatory obligations.

Establish Internal Policies

Well-documented internal policies demonstrate operational maturity and regulatory preparedness. Depending on the proposed activities, applicants should prepare policies covering governance, compliance, cybersecurity, client asset protection, complaints handling, conflict of interest management, operational risk, business continuity, data protection, outsourcing, and employee conduct.

Maintain Accurate Documentation

Incomplete or inconsistent documentation frequently causes unnecessary delays during regulatory review. Applicants should ensure that all supporting documents are current, accurate, properly certified where required, and internally consistent. Corporate records, financial

statements, identification documents, compliance manuals, and technical documentation should be organized before submission.

Demonstrate Consumer Protection

Protecting customer interests is a central objective of financial regulation. Applicants should establish transparent customer onboarding procedures, clear disclosures regarding risks, effective complaint resolution mechanisms, appropriate safeguarding of client assets, and policies addressing fraud prevention and operational resilience.

Build a Risk Management Framework

Every virtual asset business faces financial, operational, technological, cybersecurity, legal, and reputational risks. Applicants should identify these risks, assess their potential impact, and implement appropriate mitigation measures. A documented enterprise risk management framework demonstrates that management understands the risks associated with the proposed business activities.

Engage Professional Advisors

Although businesses may prepare applications independently, obtaining advice from experienced legal, corporate, tax, compliance, cybersecurity, and accounting professionals may improve the quality of the application and reduce regulatory deficiencies. Professional guidance is particularly valuable for complex business structures, foreign applicants, token issuers, and multi-jurisdictional operations.

Monitor Regulatory Developments

Virtual asset regulation continues to evolve rapidly. Applicants should regularly review official announcements, updated regulations, guidance notes, consultation papers, and licensing requirements issued by PVARA and other relevant regulatory authorities. Remaining informed enables businesses to adapt promptly to regulatory changes.

Respond Promptly to Regulatory Queries

During the assessment process, regulators may request additional information, clarification, or supporting documentation. Applicants should respond promptly, accurately, and comprehensively to all regulatory communications. Timely cooperation demonstrates professionalism and facilitates efficient processing of the application.

Adopt a Long-Term Compliance Culture

Obtaining a licence should not be viewed as the final objective. Regulatory compliance is an ongoing responsibility that extends throughout the life of the business. Licensed Virtual Asset

Service Providers should continuously review internal controls, monitor regulatory developments, update compliance programmes, conduct employee training, maintain accurate records, and strengthen governance practices to support sustainable operations within Pakistan's evolving virtual asset ecosystem.

The introduction of the Virtual Assets Act 2026 and the establishment of PVARA provide businesses with an opportunity to operate within a transparent and regulated digital asset market. Successful applicants are those that approach licensing as a comprehensive compliance exercise rather than a procedural formality. Careful preparation, sound governance, effective risk management, and a commitment to ongoing regulatory compliance are likely to place applicants in a stronger position throughout the licensing process and beyond.

Chapter 20: Frequently Asked Questions (FAQs)

This chapter answers some of the most common questions raised by entrepreneurs, cryptocurrency exchanges, blockchain startups, fintech companies, investors, and legal professionals regarding the PVARA licensing framework. The answers are based on the PVARA License Guide 2026 and should be read together with the applicable legislation, regulations, and official guidance issued by the Pakistan Virtual Assets Regulatory Authority (PVARA).

1. What is PVARA?

The Pakistan Virtual Assets Regulatory Authority (PVARA) is the federal regulatory authority established under the Virtual Assets Act 2026 to regulate, supervise, and license Virtual Asset Service Providers (VASPs) operating in Pakistan. PVARA is responsible for implementing licensing requirements, ensuring compliance, promoting innovation through its Regulatory Sandbox, and protecting consumers and market integrity.

2. What is a Virtual Asset Service Provider (VASP)?

A Virtual Asset Service Provider (VASP) is a business that conducts regulated virtual asset activities, such as operating cryptocurrency exchanges, providing custody services, facilitating transfers, issuing certain virtual assets, offering brokerage services, or managing virtual asset investments. Businesses performing regulated activities generally require authorization from PVARA before commencing operations.

3. Is a PVARA licence mandatory?

Yes. Businesses carrying out regulated virtual asset activities in Pakistan are expected to obtain the appropriate authorization from PVARA before commencing commercial operations. Operating without the required authorization may expose a business to regulatory enforcement and penalties.

4. Can a foreign company apply for a PVARA licence?

Yes. Foreign companies may enter the Pakistani market, but they are generally expected to establish a local presence, comply with Pakistani corporate and regulatory requirements, and satisfy PVARA's licensing conditions before commencing business operations.

5. What is the purpose of the No Objection Certificate (NOC)?

The No Objection Certificate (NOC) serves as the initial regulatory approval for many applicants. It enables the applicant to proceed with company incorporation, FMU goAML registration, and preparation for the next stage of licensing. An NOC does not itself authorize commercial operations.

6. Does an NOC allow a company to start operating?

No. According to the licensing guide, an NOC is not a licence. Commercial operations may only commence after the applicant has successfully completed the required licensing process and received the appropriate authorization from PVARA.

7. What is the Regulatory Sandbox?

The Regulatory Sandbox is a controlled environment established by PVARA to allow eligible businesses to test innovative virtual asset products and services under regulatory supervision before applying for a full licence. The Sandbox supports innovation while maintaining consumer protection and regulatory oversight.

8. Is participation in the Sandbox mandatory?

No. The guide identifies several entry routes, including the NOC process, Regulatory Sandbox, No-Action Relief, and direct licensing, depending on the applicant's business model and regulatory circumstances.

9. How many licence categories are available?

The Draft Pakistan Virtual Asset Services Regulations 2026 identify ten VASP licence categories covering various virtual asset activities, including exchanges, custody, brokerage, lending, derivatives, advisory services, transfers, investment management, and token issuance.

10. How much paid-up capital is required?

Minimum paid-up capital depends upon the licence category and, according to the draft regulations, ranges from PKR 25 million to PKR 1 billion. Because these figures remain subject to final regulatory confirmation, applicants should verify current requirements before submitting an application.

11. Is there an official application fee?

The PVARA License Guide states that there is currently no prescribed application fee. However, applicants should confirm any changes with PVARA before filing their applications.

12. What corporate requirements must applicants satisfy?

Applicants are generally expected to establish a locally incorporated company, maintain a principal place of business in Pakistan, establish operational infrastructure, appoint appropriate management, and comply with the Companies Act 2017 and applicable regulatory requirements.

13. What is the Fit and Proper Test?

The Fit and Proper assessment evaluates directors, senior management, compliance officers, and ultimate beneficial owners. It typically considers integrity, professional competence, criminal history, regulatory record, and overall suitability to manage a regulated virtual asset business.

14. What AML/CFT measures are required?

Applicants are expected to implement comprehensive Anti-Money Laundering and Counter-Terrorist Financing programmes, including customer due diligence, Know Your Customer (KYC), Know Your Business (KYB), transaction monitoring, sanctions screening, suspicious transaction reporting, and compliance with applicable regulatory requirements.

15. Is FMU goAML registration mandatory?

Yes. The licensing guide identifies registration on the FMU goAML portal as a mandatory compliance requirement for Virtual Asset Service Providers operating within the regulatory framework.

16. Are cybersecurity controls required?

Yes. Applicants are expected to establish appropriate cybersecurity measures, private key management procedures, disaster recovery planning, business continuity arrangements, independent security assessments, and customer asset protection controls.

17. Can multiple regulated activities be conducted under one licence?

The licensing guide indicates that certain licences may authorize more than one regulated activity depending on the approved business model and regulatory approval granted by PVARA.

18. What happens if a company operates without a licence?

The Virtual Assets Act 2026 provides enforcement mechanisms for unauthorized operations. Businesses operating without the required authorization may face regulatory action, financial penalties, licence restrictions, or other legal consequences as provided under the applicable legislation.

19. Can PVARA suspend or revoke a licence?

Yes. PVARA has regulatory authority to suspend or revoke approvals where a licensee fails to comply with regulatory obligations or commits serious compliance breaches, subject to the applicable legal framework.

20. What is customer asset segregation?

Customer asset segregation requires regulated businesses to maintain appropriate separation between customer assets and company assets, helping protect client funds and improve operational transparency.

21. Will licensed VASPs have access to banking services?

The guide notes that SBP Circular No. 10 of 2026 authorizes commercial banks to open and maintain accounts for PVARA-licensed Virtual Asset Service Providers, subject to applicable banking requirements.

22. Are tax obligations applicable to licensed VASPs?

Yes. Licensed businesses are expected to comply with applicable Pakistani tax laws and regulatory reporting obligations administered by the Federal Board of Revenue (FBR).

23. How long does the licensing process take?

The guide specifies a 60-working-day assessment period for Regulatory Sandbox applications. It does not prescribe a universal processing period for all licence applications, and actual timelines may vary depending on the completeness of the application and regulatory review.

24. What documents are generally required during the licensing process?

Applicants should expect to provide corporate documents, business plans, ownership information, governance documentation, AML/CFT policies, cybersecurity documentation, financial information, compliance manuals, and other supporting information requested by PVARA.

25. Where should applicants obtain the latest regulatory information?

Applicants should always consult official publications issued by the Pakistan Virtual Assets Regulatory Authority (PVARA) and other competent authorities, including the Securities and Exchange Commission of Pakistan (SECP), State Bank of Pakistan (SBP), Financial Monitoring Unit (FMU), and the Federal Board of Revenue (FBR). As aspects of the regulatory framework remain subject to change, official sources should always take precedence over secondary guidance.

Chapter 21: Important Government Authorities and Resources

The regulatory framework established under the Virtual Assets Act 2026 involves several government authorities, each performing a distinct role in the licensing, supervision, taxation, financial regulation, and anti-money laundering oversight of Virtual Asset Service Providers (VASPs). Understanding the responsibilities of these institutions is essential for businesses seeking to establish and operate legally within Pakistan's virtual asset ecosystem.

This chapter provides an overview of the principal government authorities and official resources that every applicant should become familiar with before commencing the licensing process.

Pakistan Virtual Assets Regulatory Authority (PVARA)

The Pakistan Virtual Assets Regulatory Authority (PVARA) is the primary regulator responsible for licensing, supervising, and regulating Virtual Asset Service Providers in Pakistan.

PVARA administers the licensing framework established under the Virtual Assets Act 2026 and oversees applications for No Objection Certificates (NOCs), Regulatory Sandbox participation, and full VASP licences. It also issues regulations, regulatory guidance, activity-specific handbooks, and compliance standards applicable to licensed entities.

Businesses intending to operate cryptocurrency exchanges, custody services, broker-dealer platforms, token issuance platforms, or other regulated virtual asset activities should consider PVARA their principal point of contact throughout the licensing process.

Official Website: https://pvara.gov.pk

Securities and Exchange Commission of Pakistan (SECP)

The Securities and Exchange Commission of Pakistan (SECP) regulates company incorporation and corporate governance in Pakistan.

Following approval of a PVARA No Objection Certificate, applicants are generally required to incorporate a local company under the Companies Act 2017 and establish a legal corporate presence in Pakistan.

The SECP also administers company registration, statutory filings, corporate record maintenance, and governance requirements applicable to locally incorporated entities.

Official Website: https://www.secp.gov.pk

State Bank of Pakistan (SBP)

The State Bank of Pakistan (SBP) serves as Pakistan's central bank and regulates the country's banking sector.

According to the licensing guide, SBP Circular No. 10 of 2026 authorizes commercial banks to open and maintain accounts for PVARA-licensed Virtual Asset Service Providers. This development significantly improves banking accessibility for licensed crypto businesses operating within the regulatory framework.

Businesses should consult both SBP regulations and their banking institutions regarding operational banking requirements.

Official Website: https://www.sbp.org.pk

Financial Monitoring Unit (FMU)

The Financial Monitoring Unit (FMU) functions as Pakistan's Financial Intelligence Unit responsible for monitoring Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) compliance.

All licensed Virtual Asset Service Providers are expected to register on the FMU goAML platform and comply with applicable reporting obligations relating to suspicious transactions and financial crime prevention.

Compliance with FMU requirements forms an important component of the overall AML/CFT framework applicable to regulated crypto businesses.

Official Website: https://goaml.fmu.gov.pk

Federal Board of Revenue (FBR)

The Federal Board of Revenue (FBR) administers Pakistan's taxation system.

Virtual Asset Service Providers must comply with applicable tax laws, maintain proper financial records, satisfy tax registration obligations, and submit statutory reports as required by Pakistani tax legislation.

Applicants should also remain informed regarding any future taxation rules specifically applicable to virtual assets and digital asset transactions.

Official Website: https://www.fbr.gov.pk

Pakistan Crypto Council (PCC)

The Pakistan Crypto Council plays an important role in supporting Pakistan's digital asset policy initiatives and promoting the responsible development of the blockchain ecosystem.

Although the Council is not the licensing authority, it contributes to national policy discussions concerning blockchain innovation, digital assets, investment, and international cooperation.

The licensing guide identifies the Pakistan Crypto Council as an important stakeholder in Pakistan's evolving crypto ecosystem.

Official Regulatory Publications

Applicants should regularly review official publications issued by PVARA, including:

- Virtual Assets Act 2026
- NOC Regulations
- Regulatory Sandbox Guidelines 2026
- Draft Pakistan Virtual Asset Services Regulations 2026
- Activity-Specific Handbooks
- Official Circulars and Regulatory Notices

Since the regulatory framework continues to evolve, businesses should ensure they are relying upon the most recent versions of these publications.

International Resources

Although PVARA regulates Virtual Asset Service Providers within Pakistan, international standards continue to influence domestic regulatory expectations. Businesses should also familiarize themselves with internationally recognized guidance relating to virtual asset regulation, AML/CFT compliance, cybersecurity, and blockchain investigations.

Useful international resources include:

Financial Action Task Force (FATF)
https://www.fatf-gafi.org

International Organization of Securities Commissions (IOSCO)
https://www.iosco.org

Bank for International Settlements (BIS)
https://www.bis.org

Chainalysis
https://www.chainalysis.com

TRM Labs
https://www.trmlabs.com

National Institute of Standards and Technology (NIST)
https://www.nist.gov

These organizations publish guidance and technical resources that can assist Virtual Asset Service Providers in developing effective compliance programmes, cybersecurity controls, risk management frameworks, and governance policies.

Conclusion

Successful licensing under the Virtual Assets Act 2026 requires engagement with multiple regulatory institutions rather than a single authority. While PVARA serves as the primary licensing regulator, applicants must also comply with corporate registration requirements administered by the SECP, banking requirements involving the SBP, AML/CFT obligations overseen by the FMU, and tax obligations administered by the FBR.

By understanding the responsibilities of each authority and regularly consulting official regulatory resources, businesses can improve their preparedness, maintain ongoing compliance, and operate with greater confidence within Pakistan's emerging virtual asset regulatory framework.

Appendix A: Glossary of Virtual Asset Terms

This glossary provides a practical explanation of commonly used legal, regulatory, and technical terms relating to virtual assets, blockchain technology, and the Pakistan Virtual Assets Regulatory Authority (PVARA) licensing framework. The definitions are intended to help readers understand the terminology frequently encountered in the Virtual Assets Act 2026, PVARA regulations, and related compliance documents.

Address

A blockchain address is a unique alphanumeric identifier used to send, receive, or hold virtual assets on a blockchain network. Each address is associated with a public key and may represent an individual user, business, exchange, or smart contract.

AML (Anti-Money Laundering)

AML refers to laws, regulations, policies, and internal controls designed to prevent criminals from disguising illegally obtained funds as legitimate assets. Virtual Asset Service Providers are expected to implement effective AML programmes to identify and report suspicious financial activities.

Asset-Referenced Token

A digital token whose value is linked to one or more underlying assets, such as commodities, currencies, securities, or other financial instruments. Such tokens may be subject to specific licensing and reserve requirements under applicable regulations.

Blockchain

A blockchain is a decentralized digital ledger that records transactions in chronological blocks secured through cryptographic techniques. Once validated, transactions become extremely difficult to alter, providing transparency and data integrity.

Blockchain Explorer

A blockchain explorer is an online tool that allows users to view blockchain transactions, wallet addresses, block confirmations, transaction history, and other publicly available blockchain information.

Broker-Dealer

A Virtual Asset Service Provider authorized to facilitate the purchase, sale, or trading of virtual assets on behalf of clients or for its own account, subject to regulatory approval.

Cold Wallet

A cryptocurrency wallet that stores private keys offline, significantly reducing exposure to cyberattacks and unauthorized access.

Compliance Officer

An individual responsible for ensuring that a Virtual Asset Service Provider complies with applicable laws, regulations, internal policies, and regulatory obligations, including AML/CFT requirements.

Custody Services

Services involving the safekeeping, storage, administration, or control of virtual assets or private cryptographic keys on behalf of clients.

Customer Due Diligence (CDD)

The process of verifying the identity of customers, understanding the nature of their business relationships, assessing risk, and conducting ongoing monitoring to detect suspicious activities.

DAO (Decentralized Autonomous Organization)

A blockchain-based organization governed by smart contracts and community voting rather than traditional corporate management structures.

DeFi (Decentralized Finance)

Financial services operating on blockchain networks through smart contracts without relying on traditional financial intermediaries such as banks or brokerage firms.

Digital Asset

A digitally represented asset that can be stored, transferred, or traded electronically. Digital assets may include cryptocurrencies, tokenized assets, utility tokens, stablecoins, and non-fungible tokens.

Distributed Ledger Technology (DLT)

A technology that enables identical copies of transaction records to be maintained across multiple computers or nodes, reducing reliance on a centralized database.

Exchange

A regulated platform facilitating the buying, selling, conversion, or trading of virtual assets between customers or between virtual assets and fiat currencies.

FATF

The Financial Action Task Force is the international standard-setting body responsible for developing global recommendations relating to Anti-Money Laundering, Counter-Terrorist Financing, and the prevention of proliferation financing.

FATF Travel Rule

An international compliance requirement requiring Virtual Asset Service Providers to collect and transmit specified originator and beneficiary information during qualifying virtual asset transfers.

Fiat Currency

Government-issued legal tender such as the Pakistani Rupee (PKR), US Dollar (USD), Euro (EUR), or British Pound (GBP), which derives its value from government authority rather than physical commodities.

Fiat-Referenced Token

A digital token designed to maintain a stable value by referencing a fiat currency or a basket of fiat currencies.

Financial Monitoring Unit (FMU)

Pakistan's financial intelligence unit responsible for receiving, analyzing, and disseminating suspicious transaction reports and administering the goAML reporting platform.

goAML

A secure reporting system developed by the United Nations Office on Drugs and Crime (UNODC) that enables reporting entities to submit suspicious transaction reports electronically to financial intelligence units.

Hot Wallet

A cryptocurrency wallet connected to the internet, enabling convenient transactions but generally presenting higher cybersecurity risks than offline storage solutions.

KYC (Know Your Customer)

The process of identifying and verifying the identity of customers before establishing or maintaining a business relationship.

KYB (Know Your Business)

A compliance procedure used to verify the legal existence, ownership structure, beneficial ownership, and business activities of corporate customers.

Market Manipulation

Any intentional conduct designed to create false or misleading market activity or artificially influence the price or trading volume of virtual assets.

Mining

The process through which blockchain transactions are validated and added to certain blockchain networks while new cryptocurrency units may be created as protocol rewards.

Multi-Signature Wallet

A cryptocurrency wallet requiring approval from multiple private keys before a transaction can be executed, enhancing security for institutional asset management.

No Objection Certificate (NOC)

An initial regulatory approval issued by PVARA permitting eligible applicants to proceed with company incorporation, FMU registration, and subsequent licensing steps. An NOC does not authorize commercial operations.

Non-Fungible Token (NFT)

A unique blockchain-based digital token representing ownership of a specific digital or physical asset that cannot be exchanged on a one-to-one basis with another identical token.

PEP (Politically Exposed Person)

An individual entrusted with a prominent public function whose position may present an increased risk of corruption or money laundering, requiring enhanced due diligence.

Private Key

A confidential cryptographic key used to access and authorize transactions involving virtual assets. Loss or compromise of a private key may result in permanent loss of digital assets.

Proof of Reserves

A verification process demonstrating that a Virtual Asset Service Provider holds sufficient assets to meet customer obligations and maintain financial integrity.

Public Key

A cryptographic identifier that allows others to send virtual assets to a wallet address without revealing the associated private key.

Regulatory Sandbox

A supervised testing environment established by PVARA that allows eligible businesses to test innovative virtual asset products or services under defined regulatory conditions before obtaining a full licence.

Risk-Based Approach

A regulatory methodology that allocates compliance resources according to the level of money laundering, terrorist financing, fraud, or operational risk presented by customers, products, or transactions.

Sanctions Screening

The process of comparing customers and transactions against domestic and international sanctions lists to prevent prohibited financial dealings.

SECP

The Securities and Exchange Commission of Pakistan is responsible for company incorporation, corporate regulation, and securities oversight relevant to businesses operating in Pakistan.

Smart Contract

A self-executing computer program deployed on a blockchain that automatically performs predefined contractual obligations when specified conditions are satisfied.

Stablecoin

A virtual asset designed to maintain a relatively stable value by referencing fiat currencies, commodities, or other reserve assets.

Token

A digital representation of value or rights recorded on a blockchain network. Tokens may serve utility, payment, governance, investment, or asset-backed functions depending on their characteristics.

Ultimate Beneficial Owner (UBO)

The natural person who ultimately owns or exercises effective control over a legal entity, whether directly or indirectly.

Virtual Asset

A digital representation of value that can be digitally traded, transferred, or used for payment or investment purposes but does not include government-issued legal tender unless specifically recognized by law.

Virtual Asset Service Provider (VASP)

A natural or legal person that conducts one or more regulated virtual asset activities on behalf of another person or as otherwise defined under applicable virtual asset legislation and regulations.

Wallet

Software, hardware, or another technological solution used to store, manage, receive, and transfer virtual assets by securely controlling the associated cryptographic keys.

Web3

A decentralized internet ecosystem built upon blockchain technology that enables users to interact directly through decentralized applications, digital identities, tokenized assets, and smart contracts without relying exclusively on centralized service providers.

Appendix B: Useful References

This appendix provides a collection of official regulatory authorities, legislation, standards, and industry resources that may assist businesses, legal professionals, compliance officers, and Virtual Asset Service Providers (VASPs) in understanding and complying with Pakistan's virtual asset regulatory framework. Readers should always consult the latest versions of official documents, as laws, regulations, and guidance may change over time.

Official Regulatory Authorities

Pakistan Virtual Assets Regulatory Authority (PVARA)

PVARA is the primary regulatory authority responsible for licensing, supervising, and regulating Virtual Asset Service Providers (VASPs) in Pakistan. It administers the licensing framework, No Objection Certificate (NOC) process, Regulatory Sandbox, Activity-Specific Handbooks, and regulatory guidance for the virtual asset sector.

Website:
https://pvara.gov.pk

Securities and Exchange Commission of Pakistan (SECP)

The SECP is responsible for company incorporation, corporate governance, securities regulation, and the administration of the Companies Act 2017. Every applicant establishing a local entity in Pakistan must comply with applicable SECP requirements.

Website:
https://www.secp.gov.pk

State Bank of Pakistan (SBP)

The State Bank of Pakistan regulates the country's banking system and financial institutions. Licensed VASPs should remain informed of applicable banking policies, circulars, and financial sector guidance affecting digital asset businesses.

Website:
https://www.sbp.org.pk

Financial Monitoring Unit (FMU)

The FMU serves as Pakistan's Financial Intelligence Unit and administers the mandatory goAML reporting platform used for suspicious transaction reporting and AML/CFT compliance.

Website:
https://goaml.fmu.gov.pk

Federal Board of Revenue (FBR)

The FBR administers Pakistan's tax laws and is responsible for taxation, reporting obligations, and tax compliance applicable to businesses operating within Pakistan.

Website:
https://www.fbr.gov.pk

Principal Legislation

Virtual Assets Act 2026

The principal legislation establishing the legal framework for regulating virtual assets and Virtual Asset Service Providers in Pakistan.

Available through:
https://pvara.gov.pk

Companies Act 2017

The Companies Act governs the incorporation, management, governance, and regulation of companies registered in Pakistan.

Available through:
https://www.secp.gov.pk

Draft Pakistan Virtual Asset Services Regulations 2026

These draft regulations prescribe licence categories, capital requirements, licensing procedures, conduct obligations, and supervisory requirements applicable to Virtual Asset Service Providers.

Available through:
https://pvara.gov.pk

PVARA NOC Regulations

These regulations establish the procedures and requirements for obtaining a No Objection Certificate before proceeding to full licensing.

Available through:
https://pvara.gov.pk

PVARA Regulatory Sandbox Guidelines 2026

These guidelines establish the framework for testing innovative blockchain and virtual asset products within a supervised regulatory environment before obtaining a full licence.

Available through:
https://pvara.gov.pk

Activity-Specific Handbooks 2026

These handbooks prescribe operational, governance, conduct, consumer protection, and compliance standards applicable to different licence categories.

Available through:
https://pvara.gov.pk

International Standards

Financial Action Task Force (FATF)

FATF develops international standards for combating money laundering, terrorist financing, and proliferation financing. Virtual Asset Service Providers should remain familiar with FATF Recommendations and guidance relating to virtual assets.

Website:
https://www.fatf-gafi.org

Basel Committee on Banking Supervision

The Basel Committee develops international standards for banking supervision and financial risk management.

Website:
https://www.bis.org

International Organization of Securities Commissions (IOSCO)

IOSCO publishes principles and policy recommendations concerning securities regulation, digital assets, investor protection, and market integrity.

Website:
https://www.iosco.org

AML and Financial Crime Resources

Egmont Group of Financial Intelligence Units

The Egmont Group promotes international cooperation among Financial Intelligence Units and supports the exchange of financial intelligence relating to money laundering and terrorist financing.

Website:
https://egmontgroup.org

United Nations Office on Drugs and Crime (UNODC)

UNODC publishes resources relating to financial crime, cybercrime, anti-corruption, and international criminal justice.

Website:
https://www.unodc.org

Blockchain Compliance Resources

Chainalysis

Chainalysis provides blockchain intelligence, transaction monitoring, blockchain investigations, sanctions screening, and compliance solutions used by governments, regulators, and cryptocurrency businesses worldwide.

Website:
https://www.chainalysis.com

TRM Labs

TRM Labs develops blockchain intelligence and compliance solutions supporting AML investigations, sanctions compliance, fraud investigations, and virtual asset monitoring.

Website:
https://www.trmlabs.com

Elliptic

Elliptic provides blockchain analytics, wallet screening, transaction monitoring, sanctions screening, and financial crime compliance solutions.

Website:
https://www.elliptic.co

Cybersecurity Standards

National Institute of Standards and Technology (NIST)

NIST publishes internationally recognized cybersecurity frameworks, information security standards, digital risk management guidance, and best practices applicable to financial institutions and technology companies.

Website:
https://www.nist.gov

Cybersecurity and Infrastructure Security Agency (CISA)

CISA provides cybersecurity advisories, operational security guidance, ransomware prevention resources, and cyber resilience recommendations.

Website:
https://www.cisa.gov

Industry Organizations

Global Digital Finance (GDF)

Global Digital Finance develops industry codes of conduct and best practices for digital asset markets, market integrity, and responsible innovation.

Website:
https://www.gdf.io

Blockchain Association

The Blockchain Association promotes responsible blockchain innovation and develops educational resources concerning cryptocurrency regulation and public policy.

Website:
https://theblockchainassociation.org

Research and Educational Resources

Cambridge Centre for Alternative Finance

The Centre publishes research concerning digital assets, blockchain technology, financial innovation, and global crypto adoption.

Website:
https://www.jbs.cam.ac.uk/ccaf

MIT Digital Currency Initiative

The Digital Currency Initiative conducts research relating to blockchain technology, Bitcoin, digital payments, and financial innovation.

Website:
https://dci.mit.edu

Recommended Reading

Readers seeking a deeper understanding of virtual asset regulation should regularly review official publications issued by PVARA together with guidance published by FATF, IOSCO, SECP, SBP, FMU, and internationally recognized blockchain compliance organizations. Because the regulatory environment continues to evolve rapidly, consulting the latest official publications before making licensing, compliance, or commercial decisions is strongly recommended.

Appendix C: Key Forms and Application Documents

A successful PVARA licence application depends not only on meeting the legal and regulatory requirements but also on submitting complete, accurate, and well-organized documentation. Incomplete applications or insufficient supporting evidence may delay the review process or result in requests for additional information. Applicants should therefore prepare all required forms and supporting documents before submitting an application to the Pakistan Virtual Assets Regulatory Authority (PVARA).

The following documents are commonly referenced in the PVARA licensing framework and should be reviewed carefully before filing an application.

1. PVARA No Objection Certificate (NOC) Application

For many Virtual Asset Service Providers (VASPs), the licensing journey begins with an application for a No Objection Certificate (NOC). The NOC is the initial regulatory approval that allows an applicant to proceed with company incorporation, FMU goAML registration, and other preparatory steps. It does not authorize commercial operations or the provision of virtual asset services to the public.

The application generally requires:

- Applicant details
- Business model description
- Proposed virtual asset activities
- Corporate ownership structure
- Shareholder information
- Director information
- Ultimate Beneficial Owner (UBO) details
- AML/CFT policies
- Technology overview
- Financial capability information

Applicants should ensure that all information is consistent across supporting documents.

2. Company Incorporation Documents

After receiving the NOC, applicants are expected to establish a legal presence in Pakistan by incorporating a company through the Securities and Exchange Commission of Pakistan (SECP). The guide identifies company registration and local establishment as part of the second licensing phase.

Typical corporate documents include:

- Certificate of Incorporation
- Memorandum of Association
- Articles of Association
- Company registration certificates
- Share register
- Registered office details
- Board resolutions
- Tax registration documents

Foreign companies establishing local subsidiaries should prepare equivalent incorporation documents from their home jurisdiction together with local registration records where applicable.

3. Identification Documents

PVARA requires identification of key persons associated with the applicant company.

Applicants should prepare:

- Passport copies
- National identity documents
- Proof of residential address
- Passport-size photographs
- Contact information

These documents may be required for directors, shareholders, senior management, compliance officers, and Ultimate Beneficial Owners.

4. Fit and Proper Documentation

The licensing framework requires directors, CEOs, compliance officers, and Ultimate Beneficial Owners to satisfy fit and proper requirements. Supporting documentation may include:

- Police clearance certificates
- Criminal record declarations
- Employment history
- Professional qualifications
- Curriculum vitae
- Regulatory declarations
- References where required

Foreign documents may need notarisation and apostille certification before submission.

5. Business Plan

A detailed business plan is one of the most important documents submitted during the licensing process.

A comprehensive business plan should explain:

- Business objectives
- Services offered
- Target customers
- Revenue model
- Operational structure
- Technology infrastructure
- Risk management strategy
- Financial projections
- Compliance framework
- Growth strategy

The business plan should clearly identify which regulated virtual asset activities will be conducted.

6. AML/CFT Compliance Manual

Every applicant should prepare a comprehensive Anti-Money Laundering and Counter-Terrorist Financing manual.

The manual should address:

- Customer Due Diligence (CDD)
- Know Your Customer (KYC)
- Know Your Business (KYB)
- Risk assessment
- Customer onboarding
- Enhanced Due Diligence
- Transaction monitoring
- Suspicious transaction reporting
- Sanctions screening
- Politically Exposed Person (PEP) screening
- FATF Travel Rule compliance
- Record retention

The guide also confirms that registration on the FMU goAML portal is mandatory for AML compliance.

7. Cybersecurity Documentation

Technology governance is an essential component of the licensing framework.

Applicants should prepare documentation covering:

- Information security policies
- Cybersecurity framework
- Wallet security
- Private key management
- Multi-signature controls
- Incident response procedures
- Business continuity plans

- Disaster recovery plans
- Penetration testing
- Independent security audit reports

These documents demonstrate operational resilience and customer asset protection.

8. Financial Documentation

Applicants should provide evidence of financial capability and compliance with the applicable capital requirements.

Typical financial documents include:

- Audited financial statements
- Bank reference letters
- Capital confirmation
- Funding sources
- Share capital documentation
- Financial projections
- Proof of reserves where applicable

The applicable minimum paid-up capital depends on the licence category under Schedule I of the Draft Pakistan Virtual Asset Services Regulations 2026.

9. FMU goAML Registration

Registration with Pakistan's Financial Monitoring Unit (FMU) through the goAML system is identified in the guide as a mandatory compliance requirement before commencing regulated activities. Applicants should retain evidence of registration together with internal AML procedures.

10. Regulatory Sandbox Documents

Applicants seeking entry into the Regulatory Sandbox must submit additional documentation as specified in the guide.

The application package includes:

- Form I
- Annexure-A Self-Assessment Checklist

- Innovation summary
- Blockchain architecture description
- Cybersecurity strategy
- Legal and regulatory analysis
- Risk management framework
- Financial readiness information
- Consumer protection measures
- Exit strategy
- Team background
- Funding information

Following approval, successful applicants are required to submit the prescribed Undertaking and comply with the terms of the Letter of Approval before entering the testing phase.

11. Supporting Policies and Procedures

Applicants should maintain internal governance documents that demonstrate their readiness to operate within a regulated environment.

These may include:

- Corporate governance policy
- Risk management policy
- Compliance policy
- Conflict of interest policy
- Client asset protection policy
- Data protection policy
- Complaints handling procedure
- Internal audit procedure
- Outsourcing policy
- Business continuity policy

Maintaining well-documented internal policies demonstrates a commitment to regulatory compliance and sound corporate governance.

Document Preparation Checklist

Before submitting any application to PVARA, applicants should verify that all documents are complete, current, signed where required, and consistent with the proposed business model. Documents issued outside Pakistan should be translated where necessary and authenticated in accordance with applicable legal requirements.

As regulatory requirements may evolve, applicants should always confirm the latest prescribed forms, document checklists, and filing procedures directly with PVARA before making a submission.

[AS PASSED BY THE NATIONAL ASSEMBLY]

A

Bill

to establish a regulatory Authority for the licensing, regulation and supervision of Virtual Assets and Virtual Asset Service Providers

WHEREAS, it is expedient to establish a dedicated Virtual Assets Regulatory Authority to license, regulate and supervise Virtual Assets and Virtual Asset Service Providers, in order to ensure investor protection, transparency and market integrity in Pakistan;

AND WHEREAS, it is necessary to provide a comprehensive legal framework to empower the Authority to combat money laundering, terrorist financing, proliferation financing and other illicit activities involving Virtual Assets, in accordance with international standards, and to provide for matters connected therewith or ancillary thereto;

It is hereby enacted as follows: -

Chapter I

PRELIMINARY

1. **Short title, extent, commencement.** — (1) This Act Shall be called the Virtual Assets Act, 2026.

(2) It extends to the whole of Pakistan.

(3) It shall come into force at once.

2. **Scope of application.**— (1) This Act shall apply to—

(a) any Virtual Asset Service Provider that carries on, or holds itself out as carrying on, a Virtual Asset Service in or from Pakistan; and

(b) any Issuer that offers, originates or distributes, on its own behalf, a Virtual Asset in or from Pakistan.

(2) For the avoidance of doubt, this Act shall not apply to the following digital representations of value or rights, insofar as they meet the conditions stated below—

(a) closed-ecosystem or closed-loop digital tokens, including any digital representation of value or rights that, by design, technical architecture,

or enforceable system controls, satisfies all of the following conditions—

(i) is usable or redeemable solely within a restricted digital platform, ecosystem, application, or network administered by the issuer or operator;

(ii) is not transferable outside such platform, ecosystem, application, or network, whether directly or indirectly;

(iii) is not exchangeable for fiat currency or legal tender outside such ecosystem;

(iv) is not redeemable for real-world goods or services outside such ecosystem;

(v) is not convertible into, exchangeable for, or interoperable with any other Virtual Asset;

(vi) is not saleable, tradable, or transferable on any external market, exchange, or secondary trading venue; or

(vii) is not designed, marketed, or used for payment, investment, or value-transfer purposes beyond such ecosystem.

(b) securities, derivatives, collective investment schemes, depositary receipts, or other traditional financial instruments that fall within the regulatory jurisdiction of the State Bank of Pakistan or the Securities and Exchange Commission of Pakistan;

(c) digital representations of fiat currency issued by the State Bank of Pakistan or any central bank or monetary authority of another sovereign jurisdiction;

(d) a non-fungible token that is not used for payment or investment and does not represent, reference, or derive value from any security, commodity, financial asset, or other regulated instrument;

(e) any non-fungible token or digital collectible that does not constitute a Virtual Asset, having regard to its substance, function, or economic effect; or

(f) any other digital representation of value or rights expressly excluded by the Authority.

3. **Definitions.**— (1) In this Act, unless there is anything repugnant in the subject or context:

(i) "Asset-Referenced Token" means a Virtual Asset that represents, directly or indirectly, ownership rights, claims, or economic interests, including entitlements to receive or share income, returns, or other economic benefits, in respect of one or more underlying assets, or is designed to maintain a stable value by reference to such underlying assets.

(ii) "Authority" or "PVARA" means the Pakistan Virtual Asset Regulatory Authority established under this Act;

(iii) "Blockchain" or "Distributed Ledger Technology" or "DLT" means a technology that enables a distributed ledger, an information repository that records transactions or data across multiple nodes in a synchronized manner using cryptography to ensure integrity, tamper-resistance, immutability, and consensus among participants, as may be further defined by Regulations;

(iv) "Chairperson" means the Chairperson of the Authority appointed under this Act;

(v) "Controller" means a Person who, alone or together with associates, holds or is entitled to exercise twenty percent (20 %) or more of the voting power, ownership interest, or share capital of a Licensee, or otherwise exercises significant influence or control over its management or policies, whether directly or indirectly;

(vi) "Customer" means any natural or legal person who obtains or uses a Virtual Asset Service from a Licensee, or who enters into a business or contractual relationship with a Licensee for the provision of such service, whether on a one-off or ongoing basis;

(vii) "Customer Assets" means Virtual Assets and fiat currency belonging to a customer that a Virtual Asset Service Provider holds, safeguards, or otherwise has custody or control over on that customer's behalf, and excludes assets owned by the Virtual Asset Service Provider;

(viii) "Division concerned" means the Cabinet Division as defined in the Rules of Business, 1973;

(ix) "Fiat-Referenced Token" means a Virtual Asset that purports to maintain a stable value relative to a single Official Currency of any country and is redeemable at par value by its Issuer;

(x) "High-Quality Liquid Assets" or "HQLA" means such high-quality liquid assets as may be prescribed by Regulations;

(xi) "Inside information" means non-public information likely to affect virtual asset prices if disclosed, including client orders, trading intentions, or decisions related to issuance or facilitation, as may be further defined by regulations;

(xii) "Insiders" include Controller, officers, directors, employees, or affiliates of issuers or Virtual Asset Service Providers with access to inside information; family members; or other persons obtaining such information unlawfully or through employment, and as may be further prescribed by Regulations.

(xiii) "Issuer" means the legal Person that originates or creates a Virtual Asset and retains primary control over its initial supply, reserve assets (if any) or on-chain governance, and may distribute such Virtual Asset as part of its initial offering, and that bears the ongoing obligations as prescribed by the Authority.

Explanation: A Person is not an Issuer solely because it markets, advertises, promotes, facilitates secondary-Market trading (including third-party brokerage, distribution or exchange), or provides technical development or maintenance services without control over issuance, supply or reserve assets.

(xiv) "Initial Virtual Asset Offering" means a method of raising funds by an Issuer through the public offering of Virtual Assets in exchange for funds or other Virtual Assets or anything of commercial value, subject to the limitations and disclosure requirements Prescribed under this Act;

(xv) "Key Individual" means any natural Person who occupies or performs - whether on a full-time, part-time, acting or outsourced basis - one or more of the positions listed below in relation to a Licensee:

(a) director (executive or non-executive) registered under the Companies Act, 2017 (XIX of 2017)

(b) Managing Director;

(c) chief financial officer;

(d) chief operating officer;

(e) head of internal audit;

(f) head of compliance;

(g) money-laundering reporting officer (MLRO) or equivalent AML, CFT or CPF compliance officer designed under the AML, CFT and CPF Regulations issued pursuant to the Anti-Money Laundering Act 2010 (VII of 2010);

(h) head of risk management;

(i) head of information-security and cyber-security; or

(j) any other position that the Authority, by written notice to the Licensee, declares to be a Key Individual.

(xvi) "Licensee" means a person who holds a license under this Act;

(xvii) Market Manipulation or Market Abuse means any act, practice or course of conduct that:

(a) gives false or misleading signals as to the supply, demand or price of one or more Virtual Assets;

(b) secures the price of Virtual Assets at an abnormal or artificial level; or

(c) employs any device, deception or artificial means to interfere with the normal operation of supply and demand in Virtual Asset markets, as may be further defined by Regulations.

(xviii) "Managing Director" means the Managing Director of the Authority, appointed under this Act;

(xix) "Virtual Asset Mining" means the process of validating or verifying transactions and recording them on a distributed ledger or blockchain network, using computational or other consensus mechanisms, and, in return, earning virtual assets, transaction fees, or other rewards.

(xx) "Non-Fungible Token" or "NFT" means a unique, non-interchangeable digital representation of value or rights recorded on a distributed ledger or similar technology, where each token is distinguishable from every other token;

(xxi) "Official or Fiat Currency" means a currency issued by the central bank or monetary authority of a country that is recognized as legal tender under the laws of that country;

(xxii) "Person" means a natural or legal Person;

(xxiii) "Prescribed" means prescribed by Rules or Regulations made under this Act;

(xxiv) "Regulations" means Regulations made under this Act;

(xxv) "Rules" means Rules made under this Act;

(xxvi) "Segregated Reserve" means a pool of reserve assets that is kept separate from the Issuer's own assets, held in the name of the Issuer, or in a trust or special vehicle for the benefit of token holders, and under custody, with independent custodian or regulated financial institution, approved by the authority, so that the Issuer or its creditors cannot claim the assets. The Authority may, by Regulations, prescribe additional requirements regarding the types of assets, custody arrangements, audits, attestations, disclosures, and other safeguards;

(xxvii) "Shariah Advisory Committee" means the committee constituted by the Authority for advice on Shariah matters;

(xxviii) "Special Court" means a court notified by the Federal Government to take cognizance of offence as mentioned under this Act;

(xxix) "Sponsor" means a person or group of persons who has contributed initial capital to establish the company or hold a controlling shareholding therein, whether directly or indirectly;

(xxx) "Tribunal" means a Tribunal constituted under this Act;

(xxxi) "Virtual Asset" means a digital representation of value that can be digitally traded or transferred and used for payment or investment purposes, but does not include digital representations of fiat currency, securities or other financial assets regulated under any other law except where represented, issued, or transferred using distributed ledger technology. For the avoidance of doubt, Virtual Assets are not legal tender;

(xxxii) "Virtual Asset Services" means the categories of services set out in section 18 of this Act; and

(xxxiii) "Virtual Asset Service Provider" means any Person who, as a business, provides one or more Virtual Asset Services to third parties on a professional basis.

(2) All other words and expressions not defined in this Act but defined in the State Bank of Pakistan Act, 1956 (XXXIII of 1956), the Securities Act, 2015, (III of 2015) the Anti-Money Laundering Act, 2010 (VII of 2010), or the Companies Act, 2017 (XIX of 2017)

shall, unless the context otherwise requires, have the meanings assigned to them in those Acts.

4. **Extraterritorial application.**— (1) For the purposes of investigation and enforcement under this Act, the Authority may exercise its powers extraterritorially to the fullest extent permitted by law.

(2) In order to facilitate enforcement under this section and the effective regulation of Virtual Asset Services with cross-border implications, the Authority may enter into agreements or arrangements with regulatory authorities and law enforcement agencies in other jurisdictions for mutual assistance, information sharing, and the recognition and enforcement of regulatory decisions, and shall, by Regulations, prescribe the conditions under which a Virtual Asset Service conducted outside Pakistan shall or shall not be deemed to be offered or marketed to Persons in Pakistan.

(3) The Authority shall, where applicable, align its extraterritorial enforcement practices with mutual legal assistance treaties and international cooperation frameworks, including those of the Financial Action Task Force and International Organization of Securities Commissions (IOSCO).

5. **Relationship with other laws.**— (1) The provisions of this Act are in addition to, and not in derogation of, any other law for the time being enforce. In the event of any inconsistency with any other law, other than the Foreign Exchange Regulation Act, 1947 (VII of 1947), this Act shall prevail except as provided ~~in sub-section (2)~~ **below**.

(2) Where any law prescribes measures relating to data protection, data governance, or cybersecurity, financial secrecy or cross-border transfer of personal data, such provisions shall prevail and be complied with by the Authority and Licensees.

(3) The regulation and supervision of Virtual Assets, Virtual Asset Service Providers, tokenization of real-world assets, and blockchain technology shall vest primarily in the Authority under this Act, in coordination with other relevant regulators where applicable.

Chapter 2

PAKISTAN VIRTUAL ASSETS REGULATORY AUTHORITY

6. **Establishment of the Authority**. — (1) After the commencement of this Act, an authority shall be established to be known as the Pakistan Virtual Assets Regulatory Authority, which shall carry out the purposes of this Act.

(2) The Authority shall be a body corporate with perpetual succession and a common seal and may sue and be sued in its name.

(3) The Authority shall be autonomous in the performance of its functions and exercise of its powers, subject to this Act.

(4) The headquarters of the Authority shall be at Islamabad, and it may set up as many offices across Pakistan as required.

7. Composition of Authority. — (1) The Authority shall consist of the following, namely:—

(a) Chairperson – to be appointed by the Federal Government

(b) the Secretary, Ministry of Finance;

(c) the Secretary, Ministry of Law and Justice;

(d) the Governor, State Bank of Pakistan;

(e) the Chairperson, Securities and Exchange Commission of Pakistan;

(f) the Chairman, National AML-CFT Authority;

(g) the Chairperson, Pakistan Digital Authority; and

(h) two independent directors with proven expertise and a strong track record possessing expertise relevant to Virtual Asset markets, digital technology, digital finance, appointed by the Federal Government in the manner Prescribed.

(2) The members of the Authority, other than ex-officio members, shall hold office for a term of three years and shall be eligible for one further term of three years.

(3) The Authority shall determine its own policy and strategic direction and approve its budget and Regulations.

8. Procedures of the Authority. — (1) The Authority may meet any time on requisition of the Chairperson or at requisition of at least fifty percent of the members. Provided however, the Authority shall meet at least twice a year.

(2) The quorum of the Authority's meeting shall be at fifty percent of the total membership with the mandatory presence of the (a) (b) and (d) as mentioned in section 7.

(3) A meeting of the Authority shall be presided over by the Chairperson. In the absence of the Chairperson, a member nominated by the Chairperson shall preside over the meeting.

(4) All decisions in the meeting shall be made with majority of the present members.

9. Objectives, functions and powers of the Authority. — (1) The Authority shall: -

(a) license, regulate and supervise Virtual Asset Service Providers and issuers in accordance with the provisions of this Act and any Rules or Regulations made thereunder;

(b) protect customers and investors and the integrity of Pakistan's Virtual Asset markets by establishing and enforcing appropriate safeguards and conduct of business requirements, prudential, operational-resilience, risk-management standards, and measures to prevent money laundering, terrorist financing and other illicit use of Virtual Assets;

(c) attract investment and encourage companies operating in the fields of Virtual Assets to base their business in Pakistan;

(d) promote responsible innovation, digital financial inclusion and the development of compliant Virtual Asset markets within a framework that manages risks and supports financial stability and market integrity;

(e) promote, develop, govern, and regulate the adoption, deployment, and scalable use of blockchain technology and distributed ledger technology across Pakistan;

(f) assess, determine, and classify any Virtual Asset, service, activity, offering, Issuer, or service provider based on its substantive features, underlying function, method of use, or economic effect, irrespective of the nomenclature, structure, or designation assigned to it. Such classification may include, but is not limited to the determination of whether an asset is a Virtual Asset, whether a Person qualifies as a Virtual Asset Service Provider, or whether an offering constitutes a financial activity within the scope of this Act subject to consultation with the State Bank of Pakistan or the Securities and Exchange Commission of Pakistan where the asset exhibits characteristics falling within their respective mandates;

(g) coordinate with the Financial Monitoring Unit, National AML and CFT Authority, other relevant authorities and law enforcement agencies to combat money laundering, terrorist financing, and other illicit activities associated with Virtual Assets, in accordance with the Anti-Money Laundering Act, 2010 (VII of 2010), other applicable laws, and international standards;

(h) advise the Federal Government, on its own motion or upon request, on regulatory, supervisory, technical or emerging-risk matters relating to Virtual Assets, digital-asset markets, tokenisation, stablecoin structures, blockchain, DLT, cyber-risks or any matter connected with its mandate under this Act; and

(i) do all such acts as may be necessary or incidental to the discharge of its functions and to achieve its objectives under this Act and other applicable laws.

(2) For the purposes of sub-section (1), and without prejudice to the generality of the foregoing, the Authority may—

(a) make Regulations, standards, directives, guidelines, handbooks and circulars, or any other instrument, consistent with the objectives of this Act and other applicable laws;

(b) set prudential, conduct operational resilience, risk-management, cybersecurity, data protection & technical standards;

(c) issue, vary, suspend or revoke licenses, approvals or directives under this Act and prescribe conditions for such actions;

(d) prescribe licensing conditions, eligibility criteria, renewal requirements and any additional obligations for Licensees;

(e) conduct on-site inspections and off-site monitoring of Licensees and other entities to ensure compliance with this Act and relevant Rules and Regulations;

(f) require Licensees to furnish information, documents and data in the manner and timeframe reasonably Prescribed by Regulations;

(g) ensure compliance of data-protection, data-governance and cyber security obligations by Virtual Asset Service Providers subject to supervisory follow-up;

(h) impose administrative sanctions in accordance with the provisions of this Act and any Rules or Regulations made thereunder;

(i) apply to court for civil or criminal remedies as provided under any applicable law;

(j) levy such fees, charges and penalties as may be Prescribed by Rules;

(k) operate regulatory sandboxes in a transparent and accountable manner;

(l) enter into cooperation or mutual assistance arrangements with domestic and foreign regulators and law enforcement agencies to facilitate information sharing and coordinated action, including mutual recognition of Regulations and licenses;

(m) conduct public education and awareness initiatives to promote informed participation in the Virtual Asset ecosystem; and

(n) constitute as many committees as deemed necessary to conduct its functions under this Act.

10. Delegation of powers. — The Authority may delegate any of its powers and functions to the Managing Director, subject to such terms, conditions, and limitations as it may deem appropriate.

11. Appointment and Functions of Chairperson. - (1) The Chairperson of the Authority shall be appointed by the Federal Government on such terms and conditions as it may deem fit. The Chairperson shall have demonstrable expertise in digital finance or technology and a minimum of three years' relevant professional experience, and shall be eligible for re-appointment for maximum two terms on such term or terms as the Federal Government may determine.

(2) The Chairperson shall provide overall guidance, direction, and oversight of the Authority.

(3) The Chairperson shall only be removed prior to the expiry of the term for gross misconduct or incapacity following a show cause notice and opportunity to be heard.

(4) The Chairperson may resign by writing to the Prime Minister.

12. Appointment and Functions of Managing Director.- (1) The Authority shall appoint a Managing Director for a term of three years, extendable for a further maximum of two term of three years only.

(2) The Managing Director shall be a person of proven integrity and competence, and shall meet such qualifications, criteria, and requirements as may be prescribed by Regulations.

(3) The Managing Director shall act as Secretary of the Authority for its proceedings but shall not have voting rights unless specifically authorized.

13. Appointment of Officers, Staff, Consultants, Advisors and other personnel. - (1) The Authority may, from time to time, create and sanction such posts, prescribe required qualifications and experience, and determine terms of service through Regulations as required.

(2) The Authority may, through a transparent and competitive process prescribed by Regulations, appoint such employees, officers, consultants, and technical or professional advisers as are necessary for the performance of its functions and the exercise of its powers under this Act.

(3) The Authority may, as prescribed by Regulations, request any Ministry, Division, public authority, public entity or autonomous or regulatory body to assign an official with requisite expertise to the Authority for such period as may be mutually agreed.

14. Pakistan Virtual Asset Regulatory Authority Fund. —(1) There shall be established a lapsable fund, vested in and administered and controlled by the Authority, to be known as the Pakistan Virtual Asset Regulatory Authority Fund, for meeting expenditures in connection with the performance of the functions and operations of the Authority under this Act.

(2) Subject to the provisions of the Public Finance Management Act, 2019 (V of 2019), the Fund shall consist of—

(a) funds provided by the Federal Government for salaries, infrastructure, administrative, operational, and other expenses, including the day-to-day functioning of the Authority;

(b) loans or funds obtained from the Federal Government, any Provincial Government, a local authority or any other entity with the approval of the Authority;

(c) grants made by the Federal Government;

(d) aids, grants, donations, or loans raised or obtained by the Authority from domestic and international agencies, in consultation with the Division to which the business of finance stands allocated and other relevant Divisions;

(e) contributions from multilateral organisations, international agencies, and philanthropic organisations for purposes consistent with the objectives of the Authority, to be managed in accordance with regulations ensuring transparency and good governance;

(f) all sums or property which may in any manner become payable to or vested in the Authority in connection with the exercise of its powers or performance of its functions;

(g) income from investments and assets of the Authority;

(h) NOC, licensing, supervision, renewal or other fees received by the Authority;

(i) penalties, fines, settlements, and other recoveries imposed or realized under this Act or any Rules or Regulations made thereunder;

(j) charges for services rendered by the Authority, including sandbox participation and other prescribed services; and

(k) any other source as may be prescribed.

(3) The Fund shall be managed and operated in such manner as may be prescribed by Regulations.

(4) The Fund shall be maintained in such manner and with such institutions as the Authority may determine, subject to any requirements prescribed by Regulations.

(5) The Pakistan Virtual Asset Regulatory Authority Fund may be expended for—

(a) paying any expenditure lawfully incurred by the Authority;

(b) payment of salaries and other remunerations payable to the chairperson, Managing Director, Officers, employees, consultants, and advisers of the Authority;

(c) paying any other expenses, costs or expenditures properly incurred or approved by the Authority in the performance of its functions or the exercise of its powers under this Act;

(d) purchasing or hiring equipment, machinery and other materials, acquiring land and constructing buildings, and carrying out any other work or undertakings in connection with the performance of its functions or the exercise of its powers under this Act;

(e) repayment of any loans or advances obtained under this Act, together with any associated interest, charges or fees;

(f) meeting any financial obligations or liabilities that arising out of the performance of the functions of the Authority under this Act;

(g) funding strategic and enabling projects or initiatives necessary to support the objective of this Act or to enhance the operational capabilities of the Authority and its stakeholders;

(h) meeting expenses relating to investigations, inspections, enforcement actions, legal proceedings, arbitration, mediation, and dispute resolution, including court fees, expert fees, and legal costs; and

(i) capacity-building, research, training, certification, and international cooperation activities, including participation in regional or international regulatory forums.

15. Budget, Finance and Audit. — (1) The Authority shall, in respect of each financial year, prepare and approve its budget in accordance with the procedure prescribed through Rules.

(2) The budget statement shall specifically state the estimated receipts and expenditure and the sums which are to be required from the Federal Government during the next financial year.

(3) The Authority shall maintain complete and accurate books of accounts of its receipts of funds and expenditure.

(4) At the end of each financial year, the accounts of the Authority shall be audited by the Auditor General of Pakistan and by a firm of Chartered Accountants nominated by the Auditor General of Pakistan.

(5) The Authority shall produce such accounts, books and documents and furnish such explanations and information as the auditors may require for the purpose of audit.

(6) Copies of the auditor's report on the accounts shall be provided to the Authority.

(7) The Authority shall submit an annual report of the fund under this section to the Prime Minister through the concerned Division within ninety days of the close of each financial year, including audited financial statements and performance against approved objectives, and such other matters as the Authority may consider necessary for transparency and accountability.

16. Code of conduct.— (1) The Chairperson, Members of the Authority including ex-officio Members, Managing Director, officers and employees of the Authority, shall, in the performance of their functions, act with integrity, impartiality, confidentiality and in good faith, and shall avoid any conflict of interest, whether direct or indirect.

(2) The Authority shall prescribe, by Regulations, a Code of Conduct applicable to the Chairperson, Members of the Authority, Managing Director, officers and employees of the Authority, including provisions relating to disclosure of interests, conflict management, restrictions on personal trading in Virtual Assets, confidentiality, and post-tenure obligations.

(3) Any violation of the provisions of this section or the Code of Conduct prescribed thereunder shall constitute misconduct and shall result in removal from office or service, as the case may be, and the initiation of disciplinary proceedings.

17. Inter-agency cooperation and information-sharing.— (1) For the effective regulation and supervision of Virtual Assets and Virtual Asset Service Providers, and to prevent their misuse, the Authority shall cooperate and share supervisory and enforcement information, in a timely and secure manner, with the State Bank of Pakistan, the Securities and Exchange Commission of Pakistan, the Financial Monitoring Unit, the Federal Investigation Agency, the Federal Board of Revenue, and any other competent regulatory or law-enforcement agencies or bodies.

(2) The Authority may, with the prior approval of the Federal Government, enter into cooperation arrangements or information-sharing arrangements with foreign regulatory or supervisory authorities for cross-border supervision, enforcement and mutual assistance relating to Virtual Assets and Virtual Assets Service Providers.

(3) The Authority may establish one or more inter-agency coordination mechanisms, including a regulatory coordination committee, comprising representatives of relevant

public authorities, to facilitate policy coordination, information-sharing, supervision, enforcement, and risk mitigation in relation to Virtual Assets and Virtual Asset Service Providers.

Chapter 3

LICENSING OF VIRTUAL ASSET SERVICE PROVIDERS AND ISSUANCE OF VIRTUAL ASSETS

18. Categories of virtual asset services.— The following constitute Virtual Asset Services and shall be subject to licensing and regulation under this Act:

(a) all services as specified in Schedule I; and

(b) any other service as may be notified by the Federal Government and subsequently included in Schedule I of this Act.

19. Application for License. — (1) Any Person intending to incorporate a company, under the Companies Act, 2017 (XIX of 2017) or any other law for the time being in force, with the primary objective of engaging in Virtual Asset Services shall first apply to the Authority for a No-Objection Certificate before commencing the process of such incorporation.

(2) An application for a No-Objection Certificate under sub-section (1) shall be made in such form and manner, accompanied by such information and fee as may be prescribed by the Authority.

(3) Upon review of an application for No-Objection Certificate, the Authority may, having regard to the objects of this Act and the need to ensure the integrity of the Virtual Asset market, grant the approval or certificate, subject to any conditions, or refuse the application, providing written reasons for refusal.

(4) An application for a license, following incorporation of the company, shall be made to the Authority in such form and manner as may be prescribed. It shall be accompanied by—

(a) the prescribed fee, which shall be non-refundable unless otherwise determined by the Authority; and

(b) such information and documents as may be prescribed or required by the Authority.

20. Fit-and-proper criteria.— (1) The Authority shall determine whether a Controller, Sponsor, Chief Executive Officer and Director is fit and proper in accordance with criteria prescribed by Regulations.

(2) The fit-and-proper criteria shall apply to all Key Individuals. It shall be the responsibility of the applicant for a license or the licensee to assess and maintain the fitness

and propriety of other key individuals not mentioned in sub-section (1), and to submit a written undertaking to the Authority confirming compliance and ongoing maintenance thereof.

(3) The Authority may refuse, suspend or revoke a license where any Controller, Sponsor or Key Individual fails to meet the prescribed fit-and-proper criteria.

(4) Fit-and-proper criteria shall be continuing in nature, and any person subject to such criteria shall notify the Authority of any matter that may affect their fitness and propriety.

(5) The Authority shall prescribe additional requirements for corporate Controllers, including assessment of the corporate behaviour, integrity and track record of Controller and ultimate beneficial owners.

(6) Every Licensee shall maintain a registered office in Pakistan and ensure that at least one Key Individual ordinarily resident in Pakistan is vested with operational and decision-making authority subject to conditions prescribed.

21. Grant, refusal and terms of license. — (1) Subject to this Act and any Rules or Regulations made thereunder, the Authority may —

(a) grant a license, subject to such terms and conditions as it may deem appropriate; or

(b) refuse the application, providing the applicant with written reasons for such refusal.

(2) The Authority may, on a case-by-case basis, grant a provisional or a limited-scope licence to an applicant, subject to such terms and conditions as may be prescribed.

(3) A license granted to a Virtual Asset Service Providers shall specify the Virtual Asset Services that is permitted to undertake and shall remain in force unless suspended or revoked.

(4) The Authority shall maintain and publish an up-to-date register of Licensees on its official website. The register shall include, at a minimum, the name, license number, permitted services and current regulatory status of each Licensee.

22. Ongoing obligations of licensees. — A Licensee shall, at all times—

(a) maintain the prescribed minimum paid-up capital and financial resources;

(b) comply with this Act and all Rules, Regulations, directives and guidelines issued by the Authority;

(c) submit such periodic returns, reports and audited financial statements as may be prescribed;

(d) obtain the prior approval of the Authority for any material change in control or business, in the manner prescribed;

(e) maintain risk-management, compliance and cybersecurity systems in accordance with applicable legal and regulatory requirements including adherence to data privacy standards; and

(f) pay such supervision, renewal or other fees as may be prescribed.

23. Variation, suspension and revocation of license. — (1) The Authority may, by way of written notice and after providing an opportunity of being heard, vary, suspend or revoke a license if it is found that—

(a) the Licensee has contravened any provisions of this Act or any other applicable laws, or any terms or condition of its license;

(b) the Licensee is insolvent or no longer satisfies the fit-and-proper criteria;

(c) the Licensee has ceased to carry on the Virtual Asset Service for which it is licensed; or

(d) such action is necessary or expedient in the public interest, including for the protection of consumers, the integrity of the market, or financial stability; or

(e) the license was obtained by fraud, misrepresentation, or concealment of material facts.

(2) Where a license is revoked, the Licensee shall immediately cease the provision of Virtual Asset Services, and the Authority may notify the Securities and Exchange Commission of Pakistan to initiate winding-up or dissolution proceedings in accordance with the Companies Act, 2017 (XIX of 2017) and any Regulations that may be prescribed under this Act.

(3) The Authority may, by Regulations prescribe further procedures, timelines, and safeguards for variation, suspension, or revocation under this section.

Chapter 4

PRUDENTIAL REQUIREMENTS, SAFEGUARDING AND CUSTODY

24. Segregation of customer assets. — (1) A Licensee shall, at all times, hold Customer Assets in segregated accounts separate from its own assets, in the manner prescribed by Regulations.

(2) Notwithstanding anything to the contrary contained in any other law for the time being in force, Customer Assets held by a Licensee shall not form part of the Licensee's estate in the event of its insolvency or liquidation.

(3) Licensee owes a fiduciary duty to its customers and shall at all times act honestly, fairly, and in the best interests of its customers when dealing with Customer Assets.

(4) A Licensee shall not rehypothecate, lend, pledge, or otherwise encumber Customer Assets, whether Virtual Assets or fiat balances, without the customer's explicit, informed, and revocable written consent.

25. **Minimum financial resource requirements.** — (1) A Licensee shall, at all times, maintain such minimum paid-up capital, liquid assets and financial resources not less than such amounts as may be prescribed.

(2) The Authority may, having regard to the category, size, complexity, or risk profile of a Licensee, prescribe higher financial-resource requirements.

(3) The Authority may, by Regulations, prescribe additional liquidity, margin, risk-based capital or reserve requirements having regard to the risks posed by the Licensee's activities.

(4) The Authority may, in the manner prescribed by Regulations, grant conditional or risk-based exemptions from requirements under this section for limited-scope or low-risk Licensees.

26. **Custody standards and key-management controls.** — (1) A Licensee providing custody services for Virtual Assets shall:

(a) ensure the secure custody and protection of Virtual Assets against unauthorized access, loss, or misuse; and

(b) maintain operational resilience, including robust disaster-recovery and business-continuity arrangements.

(2) The Authority shall prescribe detailed technical standards, operational requirements, and audit procedures to ensure that Licensees meet the obligations under this clause, including but not limited to, standards for key management, custody mechanisms, and verification or assurance processes.

27. **Proof-of-reserves and audit obligations.** — (1) A Licensee shall furnish to the Authority, at such intervals as may be Prescribed by Regulations, cryptographic proof-of-reserves reconciled against its liabilities to customers.

(2) A Licensee shall cause its operations to be audited annually by a firm of Chartered Accountants approved by the Division concerned. Such audit shall include a verification of the segregation of Customer Assets as required under section 24.

28. **Reserve custodians.** — A custodian of reserve assets shall comply with such requirements, oversight and inspection standards as may be prescribed by Regulations.

29. **Customer safeguard or compensation mechanism.** — The Authority may, establish a customer-compensation or safeguard mechanism for losses arising from custodial failure, in such manner as may be prescribed by Regulations.

Chapter 5

FIAT-REFERENCED AND ASSET-REFERENCED TOKENS

30. **Initial Virtual Asset Offerings.**— (1) Only legal entities, as registered in Pakistan and meeting the eligibility criteria prescribed by Regulations shall be permitted to conduct an Initial Virtual Asset Offering.

(2) The Authority may prescribe, by Regulations, the conditions, disclosure requirements, approval processes and ongoing obligations applicable to Initial Virtual Asset Offerings.

31. **Issuance Requirements for Fiat-Referenced Tokens.** — (1) Any Issuer intending to issue a Fiat-Referenced Token in Pakistan shall comply with following requirements:

(a) Hundred percent reserve backing, with High-Quality Liquid Assets (HQLA) or other assets as prescribed for fiat referenced token, held as a segregated reserve;

(b) mechanisms for redemption at par value without undue delay;

(c) audited reserve disclosures as prescribed by the Authority;

(d) robust AML, CFT, CPF and sanctions compliance programs;

(e) prioritized holder protections in insolvency; and

(f) any other requirement prescribed by the Authority.

(2) The Authority may prescribe differentiated requirements based on the size, scope, complexity, or risk profile of the Issuer, including but not limited to, expedited approval, stress testing, ongoing supervision, and consultation with the State Bank of Pakistan on reserve arrangements.

32. **Issuance Requirements for Asset-Referenced Tokens.** — (1) Any Issuer intending to issue Asset-Referenced Token in Pakistan shall comply with following requirements:

(a) a reserve of the underlying assets, as prescribed, for Assets-referenced token held in custody in accordance with Regulations;

(b) audited reserve disclosures as prescribed by the Authority;

(c) robust AML, CFT, CPF and sanctions compliance programs;

(d) prioritized holder protections in insolvency; and

(e) any other requirement prescribed by the Authority.

(2) An Asset-Referenced Token shall at all times be fully backed by the underlying assets and may reference tangible or intangible assets, including but not limited to commodities, real estate, real-world assets, securities, financial assets, or a combination of official currencies, but shall not be backed or derive its value from other Virtual Assets.

(3) The Authority may prescribe differentiated requirements based on the size, scope, complexity, or risk profile of the Issuer, including, but not limited to, expedited approval, stress testing, ongoing supervision, and consultation with the State Bank of Pakistan on reserve arrangements. The Authority may prescribe eligible categories of underlying assets and may restrict or prohibit types of assets for the issuance of Asset-Referenced Token.

33. **Significant issuers.** — (1) An Issuer shall be deemed a Significant Issuer if it meets the thresholds and criteria prescribed by Regulations, having regard to size, scale, systemic importance, market impact, number of holders, and cross-border activity.

(2) Significant Issuers shall be registered with the Authority and shall comply with enhanced requirements, including reporting, disclosure, governance, and risk management, as prescribed in Regulations.

Chapter 6

CYBERSECURITY, SANDBOX AND INNOVATION

34. **Cybersecurity and operational resilience.**— Licensees shall comply with cybersecurity and operational-resilience requirements prescribed by the Authority or under any other applicable laws, including, but not limited to, technical standards, security controls, and reporting mechanisms.

35. **Regulatory sandbox.**— (1) The Authority may establish a regulatory sandbox to facilitate controlled testing of innovative Virtual Asset products or services, in the manner prescribed by Regulations.

(2) Eligibility, application procedures, supervisory arrangements, risk limits, duration and exit requirements shall be prescribed by Regulations.

(3) The Authority may issue guidance, no-objection statements or no-action communications in accordance with Regulations.

36. **Oversight of blockchain technology adoption.** — (1) The Authority shall issue Regulations, standards, directives, and guidelines on the adoption, deployment, and use of blockchain or distributed-ledger technology.

(2) The Authority shall consult with relevant regulators and ministries to ensure harmonization of blockchain adoption across Pakistan.

37. **Regulation of Virtual Asset Mining Activities.** — (1) The Authority may, in consultation with relevant government entities, issue Regulations, standards, and guidelines for mining activities.

(2) Pure mining, by itself, does not constitute a Virtual Asset Service requiring license under section 18 and Schedule I. Mining operations involving customer assets or funds, however, shall be treated as Virtual Asset Services and require licensing.

(3) The Authority may establish a registration or declaration framework for mining operators exceeding thresholds of scale, energy use, or hash rate, as set by Regulations.

38. **Establishment of Strategic Digital Wallet Company.**— (1) The Federal Government may establish or designate, under the Companies Act, 2017 (XIX of 2017), a wholly owned company to be known as the Strategic Digital Wallet Company (SDWC) to perform custody and administration services, and to design, develop, operate and secure wallet infrastructure that enables the Government of Pakistan or other designated public bodies or institutions to manage, transfer and record Virtual Assets in furtherance of the Company's strategic reserve objectives.

(2) The Company shall operate exclusively on behalf of the Government of Pakistan and designated public bodies and shall not provide services to the private persons.

39. **Data localization framework.**— (1) A Licensee may store or process data outside Pakistan, subject to compliance with applicable laws relating to data protection, cybersecurity, and cross-border data transfers, and subject to such safeguards as shall be prescribed by Regulations.

(2) Nothing in this section shall prevent the Authority from requiring immediate localization or restricted cross-border transfer of specific datasets where necessary in the interest of national security, financial stability, consumer protection, or enforcement effectiveness.

40. **Data segregation and protection of sensitive information.**— (1) Every Licensee shall implement appropriate technical, organisational, and governance measures to ensure the segregation of sensitive information from other operational data, in such manner as may be prescribed by Regulations.

(2) For the purposes of this section, "sensitive information" shall include, but not be limited to—

(a) customer identification and due-diligence records;
(b) transaction-level data capable of identifying a customer;
(c) private keys, cryptographic credentials, or wallet authentication data;
(d) proprietary trading data and risk-management systems; and
(e) any other category of information designated as sensitive by the Authority.

(3) A Licensee shall ensure that—

(a) sensitive information is logically and technically segregated from non-sensitive data;

(b) access to sensitive information is strictly controlled on a need-to-know basis;

(c) encryption, tokenization, and secure key-management protocols are implemented in accordance with internationally recognised standards; and

(d) appropriate audit trails and monitoring mechanisms are maintained.

(4) The Authority may prescribe, by Regulations, minimum technical standards, cybersecurity controls, storage architectures, encryption requirements, and data-governance frameworks to give effect to this section.

Chapter 7

MARKET CONDUCT, CONSUMER PROTECTION

41. Duty of integrity and fair dealing. — (1) A Licensee shall conduct its business honestly, fairly and professionally and in accordance with the best interests of its customers and in a manner that upholds the integrity of the market.

(2) The Authority may prescribe, by Regulations, detailed requirements relating to market conduct, including standards of fair dealing, professional behaviour, and customer treatment.

42. Obligations of issuers of Virtual Assets. — (1) An Issuer offering a Virtual Asset to the public shall publish a whitepaper in such form and manner as may be prescribed by Regulations.

(2) Issuers shall make ongoing disclosures of material information including reserve attestations in the manner and frequency prescribed by Regulations.

(3) The Authority may exempt categories of Issuers or offerings from requirements under this section, subject to appropriate safeguards.

(4) The Authority shall prescribe, by Regulations, mandatory risk disclosures, periodic reporting requirements and disclosure templates applicable to Issuers and Licensees.

43. Marketing and conduct restrictions. — (1) No person shall advertise or market a Virtual Asset unless the Issuer holds a valid license or registration under this Act.

(2) All marketing materials shall contain risk disclosures and shall comply with such conditions, standards and limitations, in such form and manner, as may be prescribed by the Authority.

44. Conflict-of-interest management. — A Licensee shall identify, manage, and disclose conflicts of interest and shall not place its own interests above those of its customers, in accordance with detailed requirements on policies, disclosure, and management as may be prescribed by the Authority by Regulations.

45. Complaint-handling and dispute resolution. — (1) Licensees shall establish and maintain internal complaint-handling procedures in accordance with the requirements prescribed by Regulations.

(2) Notwithstanding anything contained in any other law for the time being in force, the Authority may establish or recognize an independent dispute-resolution scheme for claims below a prescribed monetary threshold.

Chapter 8

ANTI-MONEY LAUNDERING, COUNTERING OF TERRORISM FINANCING AND COUNTERING OF PROLIFERATION FINANCING

46. Application of Anti-Money Laundering Act, 2010. — (1) For the purposes of the Anti-Money Laundering Act, 2010 (VII of 2010), Virtual Asset Service Providers licensed under this Act shall be deemed to be financial institutions, and shall comply with all obligations thereunder.

(2) Without prejudice to sub-section (1), every Virtual Asset Service Provider and Issuer shall—

(a) report suspicious transactions to the Financial Monitoring Unit (FMU) in accordance with Anti-Money Laundering Act, 2010 (VII of 2010) and any rules, regulations or guidelines issued thereunder;

(b) maintain records of customer due diligence, transactions and other relevant information for the period prescribed under Anti-Money Laundering Act, 2010 (VII of 2010); and

(c) establish and maintain internal controls and compliance programmes to prevent money laundering and terrorist financing, including the appointment of an AML, CFT or CPF compliance officer.

(3) The Authority shall, through AML, CFT or CPF Regulations, align its supervisory framework with the standards of the Financial Action Task Force (FATF) and may issue additional guidance, consistent with FMU's mandate, to address risks specific to Virtual Assets.

47. **Travel rule and record-keeping obligations.** — (1) A Licensee shall obtain, hold and transmit originator and beneficiary information in any transfer of Virtual Assets meeting or exceeding the threshold prescribed by the Authority, in a manner consistent with Recommendations of Financial Action Task Force, as updated from time to time.

(2) Such obligations shall be implemented in compliance with applicable data protection, data governance, and cybersecurity laws, ensuring the confidentiality, integrity, and security of the information.

(3) The Authority may prescribe detailed procedures, standards, and formats for record-keeping, reporting, and transmission of information through Regulations.

(4) A Licensee shall maintain records of transactions, customer due-diligence data and risk assessments for a period prescribed by Regulations, which shall not be less than the period required under the Anti-Money Laundering Act, 2010 (VII of 2010).

48. **Real-time data access and reporting.** — (1) Licensees shall establish secure reporting channels, and where required secure automated interfaces, enabling the Authority and such other agencies as notified to access prescribed data for supervisory and enforcement purposes.

(2) The Authority shall prescribe, by Regulations, the technical standards, security requirements and data specifications for the reporting and interfaces referred to in sub-section (1).

49. **Data Privacy Obligations for Licensed entities.**- Each licensee shall implement strict limits on the collection, use, and sharing of customer data, requiring explicit, informed, and revocable consent for any non-essential data processing.

Chapter-9

Prohibitions

50. **Prohibition of unlicensed Virtual Asset services.** — (1) No Person shall, by way of business, engage in, or represent themselves as engaging in, any Virtual Asset Services in or from Pakistan, unless that Person:-

(a) is a company incorporated under the Companies Act, 2017 or any other law for the time being in force in Pakistan governing the incorporation of companies; and

(b) holds a valid license granted by the Authority under this Act.

51. Prohibition on Initial Virtual Asset Offerings. — No Person shall conduct or purport to conduct an Initial Virtual Asset Offering, in or from Pakistan, except in accordance with this Act and the Rules or Regulations made thereunder.

52. Prohibition of market manipulation and insider trading. – (1) No person shall engage in market manipulation or Market abuse in relation to virtual assets.

(2) No person shall:

(a) use inside information to trade virtual assets for themselves or others;

(b) recommend or induce trading based on inside information; or

(c) unlawfully disclose inside information.

(3) The Authority shall issue guidelines and regulations specifying the type of manipulative behaviour.

53. Prohibition on Algorithmic tokens. — No Person shall issue, offer, or market a Virtual Asset whose primary mechanism for maintaining value is algorithmic and not fully or adequately collateralized, unless specifically permitted by Regulations and subject to the safeguards prescribed therein.

Chapter-10

ENFORCEMENT, OFFENCES AND PENALTIES

54. Criminal offences.— (1) Whoever, willfully, provides an unlicensed Virtual Asset Service shall be punishable with imprisonment for a term up to five years, or with fine up to fifty million Rupees, or with both.

(2) Whoever conducts an Initial Virtual Asset Offering in contravention of this Act, Rules and Regulations shall be punishable with imprisonment for a term up to three years, or with fine up to twenty-five million Rupees or with both.

(3) Whoever, wilfully, contravenes section 52 shall be punishable:

(a) in the case of natural person, with imprisonment for a term up to three years or with fine up to twenty-five million Rupees or with both.

(b) in the case of a legal person, with fine or three times the amount of any profit gained or loss avoided as a result of the contravention. If the amount of profit gained or loss avoided cannot be determined, a fine not exceeding 15% of the total annual turnover of the body corporate in the preceding financial year.

(4) Whoever, knowingly, makes any false or misleading statement in any application, return or document submitted to the Authority shall be punishable with imprisonment for a term up to three years, or with fine up to twenty million Pakistani Rupees, or with both.

(5) Whoever, obstructs an officer of the Authority in the exercise of powers under this Act shall be punishable with imprisonment for a term up to two years, or with fine up to ten million Pakistani Rupees, or with both.

(6) Whoever, willfully, fails to comply with any order or decision of the Authority shall be punishable with imprisonment up to one year, or with fine up to twenty-five million Pakistani Rupees and the Authority may also impose administrative penalties prescribed in this Act.

(7) All offences punishable under this Act shall be investigated, tried, and punished in accordance with the provisions of the Code of Criminal Procedure, 1898 (Act V of 1898) and the Qanun-e-Shahadat Order, 1984 (Order X of 1984), unless otherwise provided in this Act.

(8) The Federal Government may, by notification in the Official Gazette, designate one or more Special Courts to exercise jurisdiction over offences committed under this Act.

55. **Liability of officers of bodies corporate.**— Where an offence under this Act is committed by a body corporate with the consent, connivance or neglect of any director, manager, secretary or similar officer, such Person shall be deemed to have committed the offence.

56. **Power to Investigate.** — Only an authorized officer of the Authority shall have the power to investigate offences under this Act.

57. **Powers of Authorized Officer.**— (1) For the purpose of investigation of offences under this Act, an authorised officer shall obtain a warrant for search and seizure of evidence of an offence from a court of competent jurisdiction.

(2) The powers specified in sub-section (1), the authorized officer shall, for the purposes of investigation, inquiry, search, seizure, arrest, attachment, confiscation, and other criminal proceedings under this Act, exercise all powers conferred upon an officer incharge of a police station or an investigating officer under the Code of Criminal Procedure, 1898 (Act V of 1898), subject to the provisions of this Act.

(3) Any person who, wilfully, refuses to provide information required by the Authorized Officer under sub-section (1) shall be punishable with imprisonment for a term up to one year or with fine up to one million rupees or with both.

(4) No Court shall take cognizance of any offence under this Act except on a report in writing submitted by an authorized officer of the Authority.

58. **Prosecution of offences.** — (1) All prosecutions under this Act shall be conducted by a special public prosecutor appointed by the Federal Government. The special

public prosecutor, or advocates appointed by the Division concerned, may institute or defend cases, appeals, petitions, applications, and all other matters before any court, including the High Court and Supreme Court, arising from proceedings under this Act.

(2) The personal attendance of any officer authorized by the Authority to file a complaint shall not be required during trial in the presence of the special public prosecutor referred to in sub-section (1).

(3) The court shall, in a manner not inconsistent with this Act, follow the procedure provided under Chapter XXII-A of the Code of Criminal Procedure, 1898 (Act V of 1898), and all prosecutions shall be disposed of and judgments pronounced as expeditiously as possible.

(4) Hearings shall not be adjourned except for sufficient cause to be recorded, and for no more than fourteen days at a time. The court may impose such costs as it deems fit.

59. Administrative sanctions.— (1) Where the Authority is satisfied that a Person has contravened any provision of this Act, or any Rules, Regulations, directions, circulars, or other regulatory requirements made thereunder, it may, impose one or more of the following sanctions—

(a) issue a written reprimand or public censure;

(b) issue a directive requiring the Person to cease or remedy the contravention;

(c) impose a financial penalty up to the maximum amount prescribed by the Rules;

(d) suspend or revoke any license issued under this Act; or

(e) disqualify any Person from holding any office or position of responsibility in a Licensee.

(2) Where the Authority is satisfied that an Issuer has contravened this Act or any Regulations made thereunder, it may impose sanctions under sub-section (1), with such modifications as are appropriate, upon Issuers.

(3) Without prejudice to sub-sections (1) and (2), where a Virtual Asset Service Provider or Issuer contravenes any other law applicable in Pakistan, the Authority may, in accordance with Regulations, impose administrative sanctions as it deems appropriate.

(4) The Authority may impose a fine up to twenty-five million rupees for any contravention of the provisions of this Act.

(5) The court may order restitution, disgorgement of profits or such other relief as it deems appropriate.

60. **Emergency intervention powers.** — In the event of a systemic threat, market manipulation, fraud, or cybersecurity breach, or other serious risk to customers or market integrity, the Authority may issue an order temporarily suspending specified Virtual Asset Services or freezing related assets for a period not exceeding thirty days.

61. **Power to prevent access to unlicensed virtual asset services.** — (1) The Authority may remove, block, or direct the removal or blocking of any online material (e.g., websites, apps, ads, payment links) if, on reasonable grounds, it promotes, operates, or relates to an unlicensed Virtual Asset Service or contravenes this Act, its Rules, or Regulations.

(2) Such directions may be issued to telecommunication authorities, Virtual Asset Service Providers, intermediaries, hosting providers, app stores, search engines, advertising networks, registrars, payment providers, or any person facilitating such material.

(3) All orders or directions shall be in writing, stating reasons and statutory basis, and communicated to the affected person.

(4) The Authority may require preservation of copies, logs, or transactional data for evidentiary purposes.

(5) A person aggrieved by an order may submit a representation within ten days; the Authority shall respond in writing within fifteen days.

Chapter- 11

APPEALS

62. **Establishment of the virtual assets appellate tribunal.** - (1) A Virtual Assets Appellate Tribunal shall be established and no court shall take cognizance of a legal dispute under this Act or the Rules or Regulations made thereunder to which the jurisdiction of the Virtual Assets Appellate Tribunal extends.

(2) The Virtual Assets Appellate Tribunal shall consist of a presiding officer, who shall be a person who is a retired Judge of a High Court, or an advocate having not less than ten years' practice and experience in the relevant field, and two members, one being a technical expert and the other being a financial expert, who shall be Persons of ability, integrity, and have special knowledge and professional experience of not less than ten years in the fields of law, technology, finance, or economics.

(3) The presiding officer and members of the Virtual Assets Appellate Tribunal shall be appointed by the Federal Government, in the manner Prescribed, and hold office for a period of three years and shall be eligible for re-appointment for a similar term or terms and shall cease to hold office on attaining the age of sixty years or the expiry of the term, whichever is earlier.

(4) The terms, conditions, and appointment of the Virtual Assets Appellate Tribunal presiding officer and other members shall be in the manner Prescribed by the Federal Government.

63. **Jurisdiction.-** Any Virtual Asset Service Provider, Licensee, or any other Person aggrieved by an order of the Authority may prefer an appeal before the Virtual Assets Appellate Tribunal within thirty days of the date on which the order was communicated, in accordance with the Prescribed Rules.

64. **Appeal.-** (1) An appeal to the Virtual Assets Appellate Tribunal shall be filed within thirty days from the date of such order in such form, contain such particulars, and be accompanied by such documents and fees as may be prescribed under this Act.

(2) The Virtual Assets Appellate Tribunal shall decide an appeal expeditiously but not later than three months of its presentation to the Tribunal.

(3) The Virtual Assets Appellate Tribunal shall, for the purpose of deciding an appeal, be deemed to be a civil court and shall have the same powers as are vested in such court under the Code of Civil Procedure, 1908 (Act V of 1908), including the powers of —

(a) enforcing the attendance of any Person and examining him on oath;

(b) compelling the production of documents; and

(c) issuing commissions for the examination of witnesses and documents.

(4) It shall be sufficient for the Virtual Assets Appellate Tribunal to establish, or to be satisfied as to any matter on the standard of proof applicable to civil proceedings in a summary manner in a court of law.

(5) The Virtual Assets Appellate Tribunal's determinations or decisions under this Act shall be deemed to be the decrees of a civil court under the Code of Civil Procedure, 1908 (Act V of 1908).

65. **Appeal to Supreme Court.** — Any Person aggrieved by an order of the Virtual Assets Appellate Tribunal may file an appeal to the Supreme Court of Pakistan within thirty days from the date of such order and in such manner as may be prescribed.

Chapter-12

MISCELLANEOUS

66. **Tax Compliance.** — Every Virtual Asset Service Provider licensed under this Act shall comply with the obligations imposed under the Income Tax Act, 2001 and any Rules or Regulations issued by the Federal Board of Revenue.

67. **Power to make Rules.** — The Federal Government may by notification in the official Gazette, make Rules, as deemed necessary for the implementation of and to carry out the purposes of this Act.

68. **Powers to make regulations.** — The Authority may make Regulations in the consultation with Division concerned as deemed necessary for the implementation of and for carrying out the purposes of this Act.

69. **Officers to be Public Servants.** — The Chairperson, Managing Director, members, staff, experts; consultants, advisers, other officers and employees of the Authority shall be deemed to be public servants within the meaning of section 21 of the Pakistan Penal Code; 1860 (XLV of 1860).

70. **Transitional provisions.**— (1) Any Person providing Virtual Asset Services immediately before the commencement of this Act shall, within six months of such commencement, apply to the Authority for a license under this Act or shall cease to provide such services.

(2) After the commencement of this Act, within six months, a Person who has submitted a complete application as per sub-section (1) may continue to provide existing Virtual Asset Services:

Provided that such Person fully complies with any interim directives issued by the Authority and continues to adhere to the core obligations of this Act, particularly regarding customer asset protection under AML, CFT and CPF.

71. **Power of the Federal Government to issue policy directives.**— The Federal Government may, by notification in the official Gazette, give policy directives to the Authority to align its actions with national policies, priorities and interests consistent with the objectives and framework established under this Act. Such policy directives shall not impede the Authority's operational autonomy.

72. **Annual and special reports of the Authority.**— (1) The Authority shall prepare an annual report at the end of the financial year and may at any time prepare special reports on any matter which in its opinion is of particular urgency or importance.

(2) The Division concerned shall cause the annual report and the special reports to be laid before the Majlis-e-Shoora (Parliament) within ninety days.

(3) The report shall be placed on the website of the Authority immediately after its lying before the Majlis-e-Shoora (Parliament) for information of general public.

73. **Removal of difficulties.**— If a procedural or operational difficulty arises in giving effect to any of the provisions of this Act, the Federal Government may, within six months of the commencement of this Act, make such order not inconsistent with the

provisions of this Act, as may appear to it to be necessary or expedient for removing such difficulty.

74. **Savings.**— Notwithstanding the lapse of the Virtual Assets Ordinance, 2025 (VII of 2025), anything done, action taken, appointment made, notification or order issued, or right, privilege, obligation or liability accrued under the said Ordinance shall be deemed to have been validly done, taken, made, issued or accrued under the corresponding provisions of this Act.

SCHEDULE I

(See section 18)

CATEGORIES OF VIRTUAL ASSET SERVICES

The list below shall constitute the types of Virtual Asset Services and their description.

Sr. No	Service Category	Description
(1)	(2)	(3)
1.	**Advisory Services**	means the provision of personalised recommendations, on professional basis, to a customer, either upon request or at the initiative of Virtual Asset Service Providers, relating to one or more actions or transactions involving Virtual Assets. The term "personalised" refers to recommendations that are addressed to a specific customer and take into account (or are presented as taking into account) that customer's individual circumstances, objectives, risk profile or financial situation. General market information, research reports or non-individualised suggestions do not constitute personalised recommendations.

2.	**Broker-Dealer Services**	means any of the following: (a) arranging or facilitating orders for the purchase and sale of Virtual Assets between two parties; (b) soliciting or accepting orders and receiving consideration in fiat currency or Virtual Assets; (c) trading Virtual Assets on the Virtual Asset Service Provider's own account; *Exemption: A Person that deals solely on its own account, does not execute orders on behalf of customers, and does not hold or control Customer Assets is not regarded as carrying on 'broker-dealer services' for the purposes of this Act* (d) market-making using Customer Assets; or (e) providing placement or distribution services for Issuers acting as intermediaries.
3.	**Custody and Administration Services**	means the safekeeping or administration, on behalf of customers and pursuant to their instructions, of: (a) Virtual Assets; or (b) private cryptographic keys or other means of access that allow the customer to transfer or dispose of Virtual Assets independently,

		but excludes the mere provision of software, hardware or infrastructure that enables a customer to retain exclusive control over their own private keys.
4.	**Exchange Services**	means any of the following: (a) exchanging Virtual Assets for fiat currency; (b) exchanging one or more types of Virtual Assets; (c) matching orders between buyers and sellers and executing conversions as described in (a) and (b); or (d) maintaining an order book for the above purposes.
5.	**Lending and Borrowing Services**	means the facilitation, arrangement, intermediation or direct provision (as principal) of lending or borrowing arrangements involving Virtual Assets, where one or more lenders transfer, lend or make available Virtual Assets (or rights thereto) to one or more borrowers, subject to a contractual obligation for the borrower to return equivalent Virtual Assets (together with any agreed interest, fees or rewards) at a specified time or upon demand.
6.	**Virtual Asset Derivatives Services**	means the offering, facilitation, execution, clearing, trading or arranging of transactions in derivatives (including futures, options, swaps, contracts for difference or other similar

		instruments) that have a Virtual Asset (or a basket or index of Virtual Assets) as their underlying reference asset.
7.	**Virtual Asset Management and Investment Services**	means acting in a fiduciary or agency capacity for the purpose of managing or administering another Person's Virtual Assets, including: (a) portfolio or discretionary investment management involving Virtual Assets; and (b) responsibility for staking on behalf of customers to earn validator or network rewards, provided that such staking is performed on a discretionary basis or forms part of a broader investment management mandate.
8.	**Virtual Asset Transfer and Settlement Services**	includes transfer, transmission, or settlement of Virtual Assets between parties, or from one wallet, address, or location to another, on behalf of customers excluding exchange execution.
9.	**Virtual Assets Issuance Services**	Creation, issuance, initial offering, administration, and ongoing management of Virtual Assets, including supply control, reserve management (if any), redemption, governance, and required disclosures.
10.	**Mining-related Virtual Asset Services**	Includes activities where mining operations provide services to third parties involving customer virtual assets or funds. Pure mining for own account is excluded. Licensing and regulatory obligations apply only

STATEMENT OF OBJECTS AND REASONS

Virtual Assets being an evolving component of the modern financial ecosystem, necessitate a dedicated regulatory authority for licensing and supervision of virtual asset service providers, with the aim to ensure investor protection, transparency and market integrity. The Authority will ensure investor protection, foster innovation, and promote transparency in the Virtual Asset Market. This authority will create an enabling environment for safe trading, prevent illegal activities like money laundering and fraud, and enhance global competitiveness.

2. Therefore, a corresponding legal framework, empowering the Authority, is also required to combat money laundering, terrorist financing, and other illicit activities while promoting innovation, financial inclusion, economic growth and development of Shariah complaint virtual asset services aligned with international standards.

3. The Virtual Assets Ordinance, 2025 is designed to achieve the aforementioned purposes.

Senator Muhammad Aurangzeb
Minister for Finance and Revenue

The Gazette of Pakistan Extraordinary

PART II

Notification

PAKISTAN VIRTUAL ASSET REGULATORY AUTHORITY

NOTIFICATION

Islamabad,

August 21, 2026

S.R.O. 1419(I)/2026. In exercise of the powers conferred by section 68 of the Virtual Assets Act, 2026, the Pakistan Virtual Asset Regulatory Authority is pleased to make public the following Pakistan Virtual Asset Services Regulations, 2026 for licensing and regulation of VASPs carrying out one or more Virtual Asset Services as stated by Schedule 1 of the Virtual Assets Act, 2026 and any other service as may be notified by the Federal Government and subsequently included in Schedule I in accordance with section 18 of the Act:

PAKISTAN VIRTUAL ASSET SERVICES REGULATIONS, 2026

CHAPTER – I
General

1. Short Title and Commencement. These Regulations may be cited as the Pakistan Virtual Asset Services Regulations, 2026 (these "Regulations") and shall come into force on the date of their notification in the Official Gazette, or on such later date as may be specified in that notification.

2. Interpretation, application and regulatory architecture. (1) These Regulations are made pursuant to, and shall be read subject to, the Virtual Assets Act 2026 (the "**Act**"), including its provisions on territorial scope and application to activities carried on in or from Pakistan.

(2) In the event of any inconsistency between these Regulations and the Act, the Act shall prevail. These Regulations are in addition to, and do not derogate from, any obligations imposed under other applicable laws and regulations, including the Anti-Money Laundering Act, 2010 (as amended), Foreign Exchange Regulations Act, 1947 (as amended) and rules made thereunder.

(3) A cross-reference to an instrument does not imply that any other applicable instrument is inapplicable. Instruments apply in accordance with the Act and the Rules and Regulations made thereunder.

(4) Use of instruments and legal effect. - Where an obligation is intended to be mandatory and generally applicable to Licensees or a class of Licensees, it shall be imposed in these Regulations or in Rules or Regulations made under the Act in accordance with sections 67 and 68 of the Act. Any written direction to an individual Licensee shall be specific to that Licensee, reasoned, proportionate, risk-based, and time-bound where appropriate, and shall not be used

to establish or impose a requirement of general application on Licensees or a class of Licensees, unless expressly authorized by the Act or by Rules or Regulations made thereunder.

2A. Definitions. (1) In these Regulations, unless there is anything repugnant in the subject or context:

(a) **"Affiliate"** means, in relation to a Person, any other Person that Controls, is Controlled by, or is under common Control with, that Person.
(b) "**Board**" means the governing body of a VASP.
(c) **"Business Day"** means a day on which banks are open for general business in Pakistan or such other place as specified by the Authority; and "Working Day" shall be read as "Business Day".
(d) **"Change of Control"** means any event, transaction, arrangement or series of transactions or arrangements (whether direct or indirect) that results in a Person acquiring, increasing, decreasing or ceasing to have Control of a Licensee, including where:
    (i). a Person becomes a Controller of the Licensee;
    (ii). a Controller ceases to be a Controller;
    (iii). there is any change in the identity of a Controller;
    (iv). a Person's level of Control results in that Person becoming or ceasing to be a Controller within the meaning of the Act (including by reference to voting rights, share capital, decision-making rights or other means of Control); or
    (v). Control is acquired or altered through any means other than share ownership, including arrangements conferring the ability to appoint or remove a majority of directors, to exercise dominant influence, or to direct or materially influence management or policies (including through shareholder agreements, voting arrangements, veto rights, or acting jointly or in concert).
(e) **"Client" and "Customer"** mean the same concept, and unless the context otherwise requires, any reference in these Regulations to a 'Client' shall be read as a reference to a 'Customer' as defined in the Act.
(f) "**Client Agreement**" means the written agreement required under regulation 52.
(g) "**Control**" means the ability to exercise, directly or indirectly, decisive influence over the management or policies of a Person, whether through ownership of voting rights, share capital, contractual arrangements, or otherwise, and includes acting jointly or in concert with others.
(h) **"Counter Proliferation Financing - CPF"** means countering of Proliferation Financing as defined in the AML Act, 2010.
(i) **"Critical Function"** means a Function the disruption, failure, or compromise of which would be likely to:

    (i). materially impair the Licensee's ability to meet its obligations regarding safeguarding of Customer Assets;
    (ii). materially impair market integrity or the orderly operation or wind down of trading;
    (iii). materially impair AML/CFT/CPF compliance (including screening, transaction monitoring, or Travel Rule controls);
    (iv). prevent the Authority from exercising effective supervision, inspection, or access to records; or
    (v). materially impair financial stability.

The Authority may specify additional Critical Functions by Regulations made under the Act or by written instrument issued under the Act.

(j) **"Dormant or In-Operative wallet"** means the wallet in which no customer initiated transaction (debit or credit) or activity (e.g. login) has taken place during the preceding one year.

(k) "**Employee**" means an individual employed by a Licensee on a full-time, part-time, temporary or seconded basis, and includes contractors and secondees where they perform Functions on behalf of the Licensee.

(l) **"ESG"** means environmental, social and governance.

(m) "**Fit and Proper Person**" means a person who meets the Fit and Proper Criteria set out in Schedule-II.

(n) "**Function**" includes any operational, technological, governance, compliance, risk, custody, settlement, customer support, onboarding, screening, monitoring, recordkeeping, or other activity relevant to providing a Virtual Asset Service.

(o) **"Group"** means a group of Persons consisting of a Person and its Affiliates.

(p) **"Independent Director"** means a director who is free of any relationship, interest, or arrangement that could materially interfere with the exercise of independent judgment, including any material business, employment, remuneration (other than director fees), familial, or controlling-shareholder relationship with the Licensee, its Controllers, or its Affiliates in the opinion of the Board and documented in Board minutes.

(q) **"Insolvency Appointee"** means a liquidator, receiver, administrator, compulsory manager, trustee or similar officer appointed in respect of a Person or its assets.

(r) **"Instrument"** means:

  (i). any Rules or Regulations made under the Act; and

  (ii). any direction, circular, standard, directive, guideline or other written instrument issued by the Authority under the Act,

in each case only to the extent, and with the legal effect (if any), expressly provided under the Act or under Rules or Regulations made thereunder, and for the avoidance of doubt, no Instrument may create a generally applicable obligation of a kind that, under the Act, is required to be prescribed by Rules or Regulations.

(s) **"Key Individual"** means any natural Person who occupies or performs whether on a full-time, part-time, acting or outsourced basis, one or more of the following positions in relation to a Licensee:

  (i). director (executive or non-executive) registered under the Companies Act, 2017;

  (ii). Managing Director;

  (iii). chief financial officer;

  (iv). chief operating officer;

  (v). head of internal audit;

  (vi). head of compliance;

  (vii). money-laundering reporting officer (MLRO) or equivalent AML, CFT or CPF compliance officer designated under the AML, CFT and CPF Regulations issued pursuant to the Anti-Money Laundering Act, 2010;

  (viii). head of risk management;

  (ix). head of information-security and cyber-security; or

  (x). any other position that the Authority, by written notice to the Licensee, declares to be a Key Individual.

(t) **"Material"** means any change, event or circumstance relating to a Licensee (or, where relevant, its Controllers, Group, or key arrangements) that may reasonably be expected to have, or give rise to a material risk of, or a material effect on:

(i). the Licensee's continued satisfaction of licensing conditions, including fit and proper status, financial resources, governance, or systems and controls;
(ii). the nature, scope, scale, or risk profile of any Virtual Asset Service for which the Licensee is licensed;
(iii). the safety, segregation, availability, or safeguarding of Customer Assets;
(iv). the Licensee's ability to comply with the Act, these Regulations, or any instruments made thereunder; or
(v). customer protection, market integrity, financial stability, or AML/CFT/CPF outcomes.

Unless otherwise expressly stated, references in these Regulations or any Rulebook to 'material', 'significant', 'harm', 'loss', 'disadvantage', 'change' or similar expressions shall be interpreted by reference to the definition of 'Material' set out in these Regulations, taking into account the nature, scale, complexity and risk profile of the Licensee and the relevant activity.

A matter may be considered material where it gives rise to a material risk to the outcomes specified in the definition of 'Material', whether or not actual harm or loss has occurred.

(u) "**Material Outsourcing**" means Outsourcing of a function which, if disrupted, degraded, or compromised, could materially impair:
(i). the Licensee's ability to comply with the Act, these Regulations, or any instruments made thereunder;
(ii). the Licensee's financial soundness or operational resilience;
(iii). the integrity, availability, confidentiality, or security of Customer Assets or customer data; or
(iv). the Authority's ability to supervise the Licensee effectively.

(v) **"Outsourcing"** means an arrangement (whether contractual or otherwise) under which a Service Provider performs, provides, supports, or makes available to a Licensee a Function, process, service, activity, system, infrastructure, resource, or role that the Licensee would otherwise perform, provide, or manage itself, on a recurrent, ongoing, or material basis. Outsourcing includes:
(i). intra-group arrangements (including where the Service Provider is an Affiliate, related entity, or Group entity);
(ii). arrangements involving sub-outsourcing or chain outsourcing;
(iii). arrangements performed within or outside Pakistan, including cross-border outsourcing; and
(iv). cloud computing.

Outsourcing does not include the mere procurement of standardized, off-the-shelf goods or utilities that do not involve the performance of a function relevant to a Virtual Asset Service.

(w) **"Personal Data"** means any information that relates to an identified or identifiable natural person, and includes any information defined as "personal data" or equivalent under any applicable personal data protection law in force in Pakistan from time to time.

(x) "**Prescribed**" means prescribed by Rules or Regulations made under the Act.

(y) **"Professional Client"** means a Client that meets following criteria:
(i). a regulated financial institution in Pakistan;
(ii). a public company listed on a recognized exchange; and
(iii). a body corporate meeting at least two of the following, as evidenced by its most recent audited financial statements (or such other reliable evidence as may be specified by the Authority):

a. net assets equal or greater than PKR 100,000,000;
b. annual turnover equal or greater than PKR 250,000,000;
c. treasury/investment function with a designated qualified officer;

and includes any other Person meeting experience and knowledge tests as may be prescribed by the Authority.

Without prejudice to the foregoing, a Retail Client may be treated as a Professional Client ("opt-up") where the Licensee has assessed that such Client possesses sufficient knowledge and experience to understand the risks of the relevant Virtual Asset Services, and the Client has provided a written request and written acknowledgement of the loss of protections applicable to retail Clients.

(z) "**Retail Client**" means a Client that is not a Professional Client.

(aa) **"Service Provider"** means any Person (including an Affiliate, related entity, or Group entity) that provides, performs, supports, or makes available any Function, service, process, activity, system, infrastructure, personnel, or resource to or for a Licensee, whether under an Outsourcing arrangement or otherwise.

(bb) **"Related Party"** means, in relation to a Licensee, any of the following Persons, whether acting directly or indirectly and whether within or outside Pakistan:

(i). any Controller of the Licensee;
(ii). any director of the Licensee;
(iii). any Key Individual of the Licensee;
(iv). any Ultimate Beneficial Owner of the Licensee or its Controller (to the extent the Licensee is required to identify such Person under applicable AML/CFT/CPF requirements);
(v). any Subsidiary of the Licensee, any Holding Company of the Licensee, or any other entity within the same Group as the Licensee;
(vi). any entity in which any Person referred to in paragraphs (a) to (d) directly or indirectly:
  a. holds ten percent (10%) or more of the voting rights or share capital; or
  b. has the ability to exercise significant influence over management or policies;
(vii). any close relative of a Person referred to in paragraphs (b) to (d), meaning a spouse, parent, child, sibling, or any other person who is financially dependent on, or whose financial affairs are interdependent with, that Person; and
(viii). any Person or arrangement (including a partnership, trust, or similar structure) where the Authority has reasonable grounds to believe that the relationship creates a material conflict of interest or risk of preferential treatment in relation to the Licensee.

For the avoidance of doubt, a Service Provider is not a Related Party solely because it provides services to the Licensee on arm's length terms.

For the avoidance of doubt, this definition applies for the purposes of the Act and these Regulations and does not limit, replace or modify any obligation relating to Related Parties or related-party transactions arising under the Companies Act, 2017, applicable related-party transaction rules or applicable financial-reporting standards.

(cc) **"Subsidiary"** means, in relation to a Person, any legal person that is controlled by that Person, whether directly or indirectly, including through one or more other Subsidiaries, and "control" means:

(i). the power to exercise more than 50% of the voting rights in that legal person; or

(ii). the power to appoint or remove a majority of the members of the governing body; or

(iii). the power to exercise a dominant influence over that legal person by virtue of a contract, constitutional document, or other arrangement

(dd) **"Ultimate Beneficial Owner" or "UBO"** shall have the meaning assigned to it under the Anti-Money Laundering Act, 2010 and any rules, regulations, or binding directions/guidelines issued under the AML Act, 2010 by the competent authority thereunder, as applicable.

(2) Words and expressions used but not defined in these Regulations shall have the same meanings as assigned to them in the Act, the State Bank of Pakistan Act, 1956, the Securities Act, 2015, the Anti-Money Laundering Act, 2010, or the Companies Act, 2017.

(3) The additional definitions in this Regulation apply for the purposes of these Regulations only.

CHAPTER – II
Scope and Categories of Virtual Asset Service Providers

3. Scope of Regulation. (1) These Regulations apply to any Person who carries on, or holds itself out as carrying on, a Virtual Asset Service:

(a) in Pakistan; or

(b) from Pakistan;

to the extent such activity falls within the scope of the Act and any determination made under the Act

(2) These Regulations apply in addition to the Act and any Rules or Regulations made thereunder, and any standards, directives, guidelines, or other instruments issued by the Authority under the Act, as applicable.

(3) In the event of any inconsistency, the Act shall prevail. These Regulations shall prevail over any standards, directives, guidelines, or other instruments issued by the Authority under the Act, to the extent of such inconsistency.

(4) For the purposes of sub-regulation (1)(a), an activity may be regarded as carried on "in Pakistan" where it targets, solicits, promotes to, or onboard persons in Pakistan, including through marketing (where through website, mobile app or any other medium), payment rails, or provision of services in PKR or through channels accessible to Persons in Pakistan.

(5) Safe harbours. -For the purposes of sub-regulation (1)(a), an activity shall not, of itself, be regarded as carried on "in Pakistan" solely because a website, application or other digital interface is accessible in Pakistan, where the Person: (a) does not market or solicit in Pakistan; (b) does not onboard Persons in Pakistan; (c) does not support PKR payment rails or Pakistan-targeted channels; and (d) takes reasonable steps to prevent onboarding where it does not intend to serve Persons in Pakistan. The Authority may nevertheless determine otherwise only where it has reasonable grounds, recorded in writing, that the Person has in substance targeted Persons in Pakistan or has a real and substantial connection with Pakistan. Any such determination shall be reasoned and communicated in writing.

(6) Virtual assets shall not facilitate, or be used or recognized as, a means of payment for domestic commercial transactions, except where specifically approved by the State Bank of Pakistan pursuant to Section 9(1)(f) of the Act.

4. Categories of License. (1) For operational and licensing purposes, the Authority shall issue Licenses in one or more of the Categories as defined in Schedule I to the Act.

(2) A Person may apply for one or more Licence Categories. A Licence shall specify the Licence Categories authorised and any limitations, conditions, or permissions applicable thereto.

(3) Where an activity could fall within more than one Licence Category, the applicant or Licensee shall seek license for respective category.

(4) Unless expressly stated otherwise, requirements in these Regulations shall be applied in a manner proportionate to the nature, scale, complexity and risk-profile of the Licensee's business and the Virtual Asset Services it provides. Proportionality permits a Licensee to comply with a requirement through systems, controls, governance arrangements, reporting mechanisms, or other measures that are appropriate to its business model, provided that the underlying regulatory objective is achieved. The Authority shall take proportionality explicitly into account in rulemaking, licensing, supervision and enforcement decisions, and shall not impose requirements that are disproportionate to the risks identified that are over and above the ones expressly stated in the Act, the Rules or Regulations. Where a Licensee considers that a requirement has been applied in a manner that is disproportionate to its risk profile, it may make written representations to the Authority and the Authority shall provide a reasoned response. For the avoidance of doubt, nothing in this regulation limits or modifies the application of any offence, penalty, administrative sanction, or enforcement power under the Act, and any contravention of these Regulations shall be enforceable in accordance with the Act, including through administrative sanctions under section 59 of the Act and any criminal sanctions or offences to the extent specified in the Act or in Rules made under section 67 of the Act.

(5) Sub-regulation (4) constitutes the core proportionality obligation for the purposes of these Regulations and shall apply to the interpretation, application and exercise of discretion under these Regulations unless a provision expressly states otherwise. For the avoidance of doubt:

(a) proportionality does not permit a Licensee to disapply or reduce compliance with an express, fixed or unconditional requirement of the Act or the Regulations; and

(b) where these Regulations confer a discretion on the Authority (including in relation to licensing conditions, supervisory requirements, reporting, audits, capital add-ons, or enforcement measures), the Authority shall exercise that discretion consistently with sub-regulation (4), having regard to the risks identified and the regulatory objectives.

(6) With respect to the Mining-related virtual asset activities License, pure Virtual Asset mining, by itself, shall not constitute a Virtual Asset Service requiring a Licence under the Act, in accordance with section 37(2) of the Act. Mining operations involving Customer Assets or Customer funds, or otherwise involving the provision of services to third parties on a professional basis in a manner that falls within the categories of Virtual Asset Services in the Act, shall be treated as Virtual Asset Services and shall require licensing in accordance with the Act. Where the Authority establishes a registration or declaration framework for mining operators exceeding thresholds of scale, energy use, or hash rate, as set by Regulations, a Licensee that engages in mining activities within the scope of such framework shall comply

with the prescribed registration or declaration requirements, in accordance with section 37(3) of the Act.

CHAPTER – III
Licensing of Virtual Asset Service Providers

5. Eligibility criteria. (1) No Person shall, by way of business, engage in, or hold themselves out as engaging in, any Virtual Asset Service in or from Pakistan unless that Person:

(a) is a company incorporated under the Companies Act, 2017 or any other law for the time being in force in Pakistan governing the incorporation of companies, as required under the Act, for the purpose of providing Virtual Asset Services; and

(b) holds a valid Licence granted by the Authority under the Act for the relevant Category or Categories of Virtual Asset Services.

(2) The Authority may, by Regulations, prescribe additional eligibility requirements for specified Licence Categories, including governance arrangements, and prudential requirements, where proportionate to the primary objectives of the Act.

(3) A licence granted by the Authority authorizes the VASP to provide only those categories of Virtual Asset Services which are expressly specified in the Licence and any schedule or annex to it and is subject to such conditions as the Authority may impose.

(4) A Licensed VASP shall not carry on any activity which falls within another category of Virtual Asset Services unless it is also licensed for that category or is otherwise authorised by the Authority in writing.

5A. Transitional arrangements for existing service providers. — (1) Any Person providing Virtual Asset Services immediately before the commencement of the Act shall, within six (6) months of such commencement, apply to the Authority for a Licence under the Act or shall cease to provide such services, in accordance with section 70(1) of the Act and Regulation 6 of these regulations.

(2) Where, within six (6) months of commencement of the Act, such Person has submitted a complete application that satisfies the requirements of the No Objection Certificate application referred herein, it may continue to provide its existing Virtual Asset Services pending the determination of the application, provided that it fully complies with any interim directives issued by the Authority and continues to adhere to the core obligations of the Act, particularly regarding customer asset protection and AML, CFT and CPF, in accordance with section 70(2) of the Act.

Provided further that till the determination of the application, if the applicant intends to conduct any marketing activity, it shall seek prior approval of the Authority.

(3) The Authority may, by written direction, impose proportionate interim limitations or conditions on such Person during the pendency of its application, including limitations on onboarding, products, transaction volumes, or custody arrangements, where necessary to protect customers or market integrity.

(4) Any guideline, direction, circular, approval, exemption, permission, sandbox arrangement, or other instrument issued or granted by the Authority under the Virtual Assets Ordinance (including any regulatory sandbox guideline or permission) and in force immediately before

the commencement of the Act shall, to the extent not inconsistent with the Act or these Regulations, continue in full force and effect as if issued under the corresponding powers of the Act, until amended, replaced, or revoked by the Authority under the Act.

(5) Where the Authority considers that any such instrument requires modification to ensure consistency with the Act, the Authority may, by written notice, amend or impose conditions on the continued application of such instrument, provided that any material modification of general application shall be effected by Rules or Regulations made under the Act.

6. Preliminary Approval / No-Objection Certificate (NOC) for incorporation. — (1) A Person intending to establish a company in Pakistan for the purpose of applying for a Licence to carry on one or more Virtual Asset Services may apply to the Authority for a Preliminary Approval / No-Objection Certificate (NOC).

(2) An application (Form I) under this regulation shall include such minimum information and documents as specified in Annexure to Form 1. The Authority may while reviewing the application seek any additional information as may be required

(3) The Authority shall, within sixty (60) days of receiving a complete application:
(a) grant a NOC, subject to the conditions specified therein; or
(b) refuse the application, providing written reasons.

(4) A NOC granted under this regulation:
(a) does not constitute a Licence or authorization to carry on any Virtual Asset Service;
(b) is without prejudice to the Authority's full assessment of any subsequent Licence application;
(c) may be withdrawn where it was obtained on the basis of materially false, misleading or incomplete information.

(5) A NOC shall be valid for three (3) months from the date of issuance and may, on application made before expiry and for reasons recorded, be extended for a further period not exceeding three (3) months.

(6) Where an application for a NOC is refused, the applicant may submit a fresh application once the grounds for refusal have been addressed, or may request reconsideration in the manner Prescribed.

(7) Where a Person incorporated pursuant to a NOC does not submit a Licence application within the applicable period, the Authority shall give the Person written notice and not less than thirty Business Days to:
(a) submit the Licence application
(b) request an extension for reasonable cause; or
(c) confirm that it will not conduct or hold itself out as conducting a Virtual Asset Service and take any necessary steps under the Companies Act, 2017.

(8) The Authority may refer the matter to SECP where the Person fails to respond within the applicable period or continues to represent that it will conduct a Virtual Asset Service without a Licence.

(9) The Authority may issue guidance. guidelines or other non-binding instruments describing the process and typical documentation for NOC applications, including examples of activities likely to fall within or outside the regulatory perimeter.

7. Application for License. - (1) Following incorporation in Pakistan and within the validity period of an NOC, an applicant shall apply to the Authority for the grant of one or more Licence Categories to carry on Virtual Asset Services, including submission of the documents and information specified in the Annexure to Form I (as updated/amended, where required, from earlier submission at the time of NOC application) and payment of the applicable non-refundable processing fee as prescribed.

(2) An application shall be treated as complete only when the Authority has confirmed, in writing, that all required information and documents have been received in a satisfactory form. Where the Authority requests further information, the time for deciding the application shall be suspended until the requested information is provided.

(3) The Authority shall decide a complete application within ninety (90) days, unless extended in accordance with sub-regulation (4).

(4) The Authority may extend the period in sub-regulation (3) by up to sixty (60) days, for reasons recorded in writing, where the application is complex, involves novel risks, or requires consultation with other competent authorities.

(5) Limited-scope Licence. The Authority may grant a limited scope Licence where necessary to advance the primary objectives of the Act. The Authority shall specify the scope, duration, conditions, and exit criteria in such limited Licence.

(6) Sandbox transition. Participation in a regulatory sandbox does not create an entitlement to a Licence. Where a sandbox participant successfully completes its testing to the satisfaction of the Authority, it may apply directly for a Licence under regulation 7, and shall not be required to apply for or obtain a separate Preliminary Approval / No-Objection Certificate under regulation 6. The Authority may, however, take into account testing outcomes and compliance history in assessing a subsequent Licence application, subject to the applicant meeting all applicable requirements.

(7) NOC Regulation 2025 transition: Where an No-Objection Certificate under NOC Regulation 2025 has been granted, the applicant may directly apply for a License under regulation 7. Further applicants who have submitted NOC application under NOC Regulations 2025 and are in correspondence with the Authority shall not be required to submit fresh NOC application under Regulation 5A and Regulation 6 of these Regulations. The Authority may require any additional information at any point in time.

8. Fit-and-Proper Assessment. - (1) The Authority shall assess the fitness and propriety of Controllers, Directors, sponsors, managing director of an applicant or Licensee in accordance with the Act and these Regulations, and any fit-and-proper requirements prescribed by Regulations made under the Act.

(2) In conducting a fit-and-proper assessment, the Authority shall have regard to:

(a) integrity, honesty and reputation;

(b) competence, capability and relevant experience;

(c) financial soundness; and

(d) conflicts of interest and independence, where relevant to the role.

(3) For the purposes of sub-regulation (1), the Authority may require any information reasonably necessary, which may include criminal record checks, regulatory references, financial/credit information, professional qualifications, and declarations of investigations or enforcement action in Pakistan or any other jurisdiction.

(4) The Authority may conduct interviews, request additional information, and conduct independent verification through third parties or competent authorities, subject to applicable law.

(5) Controllers, Directors, and Key Individuals shall remain fit and proper on an ongoing basis, and the Licensee shall notify the Authority of any matter that may reasonably affect such assessment, including any Material change, in the manner and timeframe prescribed.

9. Grant or refusal of Licence and conditions. — (1) The Authority shall, within the timeframe specified in regulation 7, and after making such inquiries as it considers appropriate, either:

(a) grant a Licence for one or more Licence Categories, subject to such conditions, limitations, and requirements as the Authority considers necessary and proportionate to advance the objectives of the Act; or
(b) refuse the application, providing written reasons.

(2) Before refusing an application or imposing any materially adverse condition or limitation, the Authority shall afford the applicant an opportunity to make representations, except in urgent cases, provided that the applicant shall be given an opportunity to be heard as soon as reasonably practicable thereafter.

(3) A Licence remains in force subject to compliance with the Act, these Regulations, any Rules or Regulations made under the Act, any applicable standards, directives, guidelines or other instruments issued by the Authority under the Act, and the Licence conditions, unless suspended, varied, or revoked by the Authority in accordance with the Act.

(4) The Authority may require a Licensee to commence business within a specified period stated in the Licence. Where the Licensee does not commence within that period, it shall promptly notify the Authority and the Authority may vary, suspend, or revoke the Licence, unless an extension is granted for reasons recorded in writing.

(5) The Licensee shall pay applicable annual supervisory, renewal, and other fees as prescribed by the Authority.

(6) The Authority shall maintain and publish an up-to-date public register of Licensees in accordance with the Act.

10. Ongoing Obligations of Licensee. - (1) A Licensee shall at all times:

(a) conduct its business with due skill, care and diligence and maintain systems and controls appropriate to its nature, scale and complexity;
(b) maintain adequate governance, risk management, compliance, and internal control arrangements, including an effective compliance function and internal audit arrangements commensurate with its business;

(c) maintain books and records sufficient to enable the Authority to assess compliance and the Licensee's financial position, and retain such records for not less than seven (7) years or such longer period as may be required under the applicable law;
(d) prepare financial statements in accordance with the applicable law and international standards as adopted in Pakistan, and submit periodic returns in the manner and frequency specified;
(e) comply with AML/CFT/CPF obligations under AML Act, 2010 and applicable law, including reporting obligations to relevant competent authorities; and
(f) maintain operational resilience, cybersecurity, business continuity, and incident management arrangements in accordance with the Act, these Regulations, any Rules or Regulations made under the Act, and any applicable direction, circular, standard, directive, guideline or other written instrument issued by the Authority under the Act.

(2) Notification duties. - A Licensee shall comply with the notification and reporting requirements set out in these Regulations, and any requirements specified in its Licence conditions, and any Rules or Regulations made under the Act, and any applicable direction, circular, standard, directive, guideline or other written instrument issued by the Authority under the Act.

(3) Capital and prudential requirements. A Licensee shall maintain at all times the minimum paid-up capital and any other prudential requirements applicable to its Licence Category or Categories as set out in Schedule I.

(4) Local presence. - A Licensee shall maintain a registered office in Pakistan and shall ensure that it has one key individual, to be resident in Pakistan and is vested with operational and decision-making authority and accountable to the Authority for regulatory compliance. The Authority may, having regard to the Licensee's nature, scale, complexity and risk profile, require that number of such officers be increased.

(5) Regulatory approvals. A Licensee shall not, without the prior written approval of the Authority:
(a) effect a change in Control or a Material change in ownership;
(b) merge with, acquire, or dispose of a material part of its business or assets; or
(c) outsource a material or critical function in a manner that materially affects its ability to comply with the Act or these Regulations, except as otherwise Prescribed.

(6) For the purposes of regulation 10 (5)(c) above, a Licensee shall obtain the Authority's prior written approval only for the outsourcing of a Critical Function. The licensee shall update its outsourcing register in accordance with Chapter V.

(7) The Authority may provide detailed procedures for matters under these Regulations (including operational resilience, cybersecurity, proof-of-reserves, segregation of customer assets, disclosures, audits and reporting) by issuing standards, directives, guidelines or other instruments under the Act to support implementation..

(8) A Licensee shall be able to demonstrate, its compliance with the Act and these Regulations, including the adequacy and effectiveness of its systems and controls, through such documentation, records, reports, and independent assurance as the Authority may require under the Act and these Regulations.

(9) A Licensee shall disclose the sources of liquidity and funding used in their operations, to support oversight of financial soundness, with the Authority on monthly basis.

11. Payment of fee. - (1) An applicant or Licensee shall pay the processing fees, licensing fees, annual supervisory fees, renewal fees, and any other charges as published in the Rules.

(2) Processing fees are non-refundable. Annual fees are payable in advance in the manner and time specified by the Authority.

CHAPTER – IV
Variation, Suspension, Revocation and Surrender of License

12. Variation of License. – (1) A Licensee may apply to the Authority to vary its Licence to:

(a) add one or more Licence Categories;
(b) remove a Licence Category; or
(c) vary, substitute, or amend any limitation or condition of its Licence,
in the form and manner specified by the Authority.

(2) An application under sub-regulation (1) shall be accompanied by such information and documents as the Authority may reasonably require to assess the proposed variation, which may include an updated business plan, risk assessment, governance arrangements, operational readiness, and AML/CFT/CPF controls, and payment of the applicable non-refundable fee as prescribed.

(3) The Authority may grant the variation subject to such conditions, limitations, or transitional arrangements as it considers necessary and proportionate to advance the objectives of the Act.

(4) The Authority may refuse an application for variation, giving written reasons and affording the applicant an opportunity to make representations, except in urgent cases, provided that an opportunity to be heard shall be given as soon as reasonably practicable thereafter.

(5) The Authority may on its own initiative vary a Licence (including by varying the authorised scope of activities within an existing Licence Category, or varying limitations) where necessary to address material risk, non-compliance, or to protect customers or market integrity, provided that the Authority shall give prior written notice stating reasons and an opportunity to make representations, except in urgent cases to be dealt in accordance with Section 60 of the Act, provided that the applicant shall be given an opportunity to be heard as soon as reasonably practicable thereafter.

13. Suspension of License. – (1) The Authority may suspend a Licence in whole or in part, for a specified period or until specified conditions are met, where the Authority is reasonably satisfied that the Licensee:

(a) is in material breach of the Act, these Regulations, any Rules or Regulations made under the Act, any applicable direction, circular or other regulatory requirement made or issued thereunder, or the Licence conditions;
(b) no longer meets applicable prudential, governance, fit-and-proper, or operational resilience requirements;
(c) has failed to provide required returns or information, or has provided materially false, misleading, or incomplete information;

(d) has suffered a material cybersecurity, operational, or safeguarding incident;
(e) has failed to pay fees due;
(f) is insolvent;
(g) has ceased to carryon Virtual Asset Service for a continuous period of one year, or any other period as specified by the Authority, for which it is licensed;
(h) the license was obtained by fraud, misrepresentation, or concealment of material facts; or
(i) otherwise presents a material risk to customers, market integrity, financial stability, or AML/CFT/CPF objectives.

Or such action is necessary or expedient in the public interest including for the protection of consumers, the integrity of the market or financial stability.

(2) Before suspending a Licence, the Authority shall give written notice stating reasons and the proposed effective date, and afford the Licensee an opportunity to make representations, except in urgent cases where immediate action is necessary, to be dealt in accordance with section 60 of the Act; provided that the Licensee shall be afforded an opportunity to be heard as soon as reasonably practicable thereafter.

(3) A Licensee whose Licence is suspended shall comply with any Direction issued by the Authority, which may include requirements for orderly wind-down, safeguarding and return of Customer Assets, maintenance of records, continued reporting, and restrictions on onboarding or trading.

(4) A Licensee may apply for removal of suspension by demonstrating remediation of the grounds for suspension, supported by evidence. The Authority shall decide such application within a reasonable time and may impose conditions on resumption.

14. Revocation of License. – (1) The Authority may revoke a Licence (in whole or in part) where, after inquiry and consideration of representations, it is satisfied that the Licensee:

(a) has committed:
(i) a serious or repeated contravention of the Act, these Regulations, any Rules or Regulations made under the Act, any applicable direction, circular or other regulatory requirement made or issued thereunder, or the Licence conditions, having regard to the nature, impact, and materiality of the contravention; or
(ii)repeated contraventions of the Act, these Regulations, any Rules or Regulations made under the Act, any applicable direction, circular or other regulatory requirement made or issued thereunder, or the Licence conditions, whether of the same or similar nature, that demonstrate persistent non-compliance or a failure to remediate within a reasonable period;
(b) no longer meets fit-and-proper, governance, prudential, or operational requirements and cannot remediate within a reasonable period;
(c) obtained the Licence through fraud, material misrepresentation, or concealment; or
(d) presents a continuing material risk to customers, market integrity, financial stability, or AML/CFT/CPF objectives such that revocation is necessary and proportionate.
(e) has failed to obtain required approvals for Material changes in control, ownership, or business, or has carried on activities outside the scope of its Licence, where such conduct is material or persistent; or
(f) is in non-compliance with any of the conditions listed in Section 23(1) of the Virtual Assets Act, 2026

Or such action is necessary or expedient in the public interest including for the protection of consumers, the integrity of the market or financial stability.

(2) Prior to revocation, the Authority shall provide written notice stating reasons and the proposed effective date, and afford an opportunity of being heard, except in urgent cases to be dealt in accordance with section 60 of the Act, provided that an opportunity to be heard shall be given as soon as reasonably practicable thereafter.

(3) The Authority may impose conditions or issue Directions to ensure an orderly cessation of operations, including measures relating to Customer Assets, withdrawals, record retention, communications to customers, and continued reporting.

(4) The Authority may publish notice of revocation on its website and through other appropriate means, subject to confidentiality and legal constraints, including, where appropriate, a summary of the reasons for revocation.

(5) Where appropriate, the Authority may notify the Securities and Exchange Commission of Pakistan or other competent authorities and may take steps consistent with applicable law relating to winding-up, administration, or other insolvency processes.

(6) Revocation shall not affect any accrued rights, obligations, or liabilities arising before the effective date of revocation.

15. **Cybersecurity and data protection during variation, suspension, revocation, or surrender. —** (1) Where a Licence is varied, suspended, revoked, or surrendered, the Licensee shall ensure secure preservation, integrity, and (where applicable) orderly transfer or disposal of Customer data, Customer Assets, private keys and credentials, and relevant system logs, in accordance with the Act, these Regulations, any Rules or Regulations made under the Act, and any applicable direction, circular or other regulatory requirement made or issued thereunder.

(2) The Authority may require the Licensee to obtain an independent cybersecurity, systems, or controls assurance report, or may conduct or commission a targeted review, where necessary to manage risks of unauthorized access, tampering, loss, or leakage.

16. Voluntary Surrender of VASP License. – (1) A Licensee may apply in writing to surrender its Licence (in whole or in part), stating reasons and providing such information as the Authority may reasonably require.

(2) Surrender shall not take effect until the Authority confirms in writing that adequate arrangements have been made for an orderly wind-down, including safeguarding and return of Customer Assets, settlement of liabilities, record retention, and customer communications, and any other matters necessary to ensure that the Licensee has met its outstanding obligations.

(3) The Authority may impose conditions or issue Directions in connection with surrender to protect customers and market integrity, including requiring the appointment of an independent person to oversee wind-down where proportionate, and may take such measures as it considers appropriate to ensure an orderly wind-down.

(4) Any Person aggrieved by an order or decision of the Authority under these Regulations may prefer an appeal in accordance with Chapter 11 of the Act and the Prescribed Rules.

17. Administrative sanctions. – (1) Without prejudice to any other power under the Act or these Regulations, where the Authority is reasonably satisfied that any Person has contravened

any provision of the Act, or any Rules, Regulations, directions, circulars, or other regulatory requirements made thereunder, the Authority may impose one or more administrative sanctions in accordance with section 59 of the Act.

(2) Administrative sanctions may include, as applicable:

(a) a written reprimand or public censure;

(b) a directive requiring the Person to cease or remedy the contravention;

(c) a financial penalty up to the maximum amount permitted under the Act and any Rules;

(d) suspension or revocation of a Licence; and

(e) disqualification of any Person from holding any office or position of responsibility in a Licensee, as provided in section 59(1) of the Act.

(3) Before imposing a sanction under these Regulations, the Authority shall provide written notice stating the proposed sanction, reasons, and statutory basis, and shall afford the Person an opportunity to make representations, except where urgency justifies immediate action, provided that an opportunity to be heard shall be given as soon as reasonably practicable thereafter.

(4) The Authority shall communicate its decision in writing stating reasons and statutory basis and may publish such decision where appropriate, subject to confidentiality and legal constraints.

(5) Nothing in these Regulations shall be construed as expanding or modifying the emergency intervention powers set out in section 60 of the Act.

CHAPTER – V
Governance and Operations of Virtual Asset Service Providers

18. Ownership and control structure. - (1) A Licensee shall maintain a transparent ownership and control structure, including a clear chain of ownership and voting rights, such that the Authority can identify each Controller and the basis on which Control is exercised, including, where applicable, ultimate beneficial owners and persons exercising control through other arrangements.

(2) A Licensee shall maintain and keep updated a group structure chart and such supporting information as the Authority may reasonably require, including information on direct and indirect ownership interests, voting arrangements and persons acting in concert, and any delegated authority relevant to the exercise of Control.

(3) For the avoidance of doubt, any requirements relating to identification of beneficial owners for AML/CFT/CPF purposes shall be complied with in accordance with applicable AML/CFT/CPF laws and requirements.

19. Change of Control. - A Licensee shall not affect any Change of Control except with the Authority's prior approval, in accordance with the Act and regulation 48 and 49.

20. Board composition and fitness and propriety. - (1) A Licensee shall appoint at least 3 directors in accordance with the Companies Act, 2017 and the Act.

(2) A Licensee shall ensure that its Board includes Independent Directors to support effective oversight, risk management and customer protection.

(3) Unless the Authority specifies otherwise based on the Licensee's nature, scale, complexity and risk profile, Independent Directors shall comprise at least one third (1/3) of the Board.

(4) The Authority may permit a lower proportion for limited scope licenses under regulation 7(5), or where the Board is small, provided equivalent independent challenge and oversight is achieved through governance arrangements acceptable to the Authority, including through board committees, external advisors, or other mechanisms as may be appropriate.

(5) A Licensee shall ensure that its Board collectively has skills, knowledge and experience proportionate to the nature, scale and complexity of the Licensee and the Virtual Asset Services it provides, including competence in risk management, technology and cybersecurity, and financial crime compliance.

(6) A Person shall not act as a Controller, Sponsor, Managing Director or Director(s) unless that Person meets the fit and proper requirements under the Act and these Regulations, and has been approved by the Authority.

(7) The Authority shall, within thirty (30) Business Days of receiving a complete application for approval of a Controller, Sponsor, Managing Director or Director, notify the Licensee in writing of its decision. Where the Authority cannot determine the application within that period because specified information is awaited from the applicant or an identified competent authority, it shall, before expiry of the period

(a) identify the outstanding information or matter;
(b) notify the Licensee of the reason for the delay and the revised expected decision date; and
(c) provide an updated status at least every fifteen (15) Business Days until the application is determined,

The determination shall be made as soon as reasonably practicable, and the period shall not be extended solely because of internal administrative delays.

21. Responsibilities of the Board. — (1) The Board shall have overall responsibility for the governance and oversight of the Licensee and for ensuring compliance with the Act and instruments made thereunder.

(2) Without prejudice to subsection (1), the Board shall ensure that the Licensee maintains effective arrangements for:

(a) governance, internal controls and risk management, including operational resilience and cybersecurity;
(b) AML/CFT/CPF compliance and market integrity controls;
(c) safeguarding and segregation of Customer Assets, where applicable;
(d) oversight of Outsourcing and Service Providers; and
(e) recordkeeping and regulatory reporting.

(3) The Board may delegate functions to committees or Key Individuals, provided that it retains ultimate responsibility and maintains adequate oversight, reporting lines and documentation of such delegation.

22. Board performance and training. - (1) A Licensee shall ensure that each director receives induction training and ongoing training appropriate to the director's responsibilities and the Virtual Asset Services carried on by the Licensee.

(2) A Licensee shall periodically assess the effectiveness of the Board and its committees and shall take reasonable steps to address identified gaps through training, resourcing or governance enhancements.

23. Compliance function and Compliance Officer. - (1) A Licensee shall establish and maintain an independent compliance function proportionate to its nature, scale and complexity.

(2) A Licensee shall appoint a Compliance Officer responsible for overseeing compliance with the Act and instruments made thereunder, including AML/CFT/CPF obligations, and for reporting material compliance matters to the Board.

(3) The Compliance Officer shall:

(a) be sufficiently senior and have adequate resources and access to information to perform the role effectively; and

(b) meet the fit and proper requirements under these Regulations; and

(c) be a resident in Pakistan.

(4) A Licensee shall notify the Authority of the appointment, replacement or departure of the Compliance Officer, including reasons for the change.

24. Key Individuals and management structure. - (1) A Licensee shall establish, document and maintain a management structure that clearly allocates responsibilities, authorities and reporting lines for Key Individuals.

(2) A Licensee shall ensure that Key Individuals are fit and proper and collectively have the skills and experience necessary to manage the Licensee's business, including operational risk, technology and cybersecurity, and financial crime compliance.

(3) A Key Individual, other than directors, shall act under the direction and oversight of the Board and shall manage day-to-day activities in a manner that complies with the Act and instruments made thereunder.

(4) A Licensee shall maintain and apply conflict-of-interest arrangements applicable to Key Individuals, including rules on external directorships and employment, and shall provide such information as the Authority may reasonably require.

25. Company Secretary. — (1) Where required under the Companies Act, 2017 or where directed by the Authority having regard to the nature, scale and complexity of the Licensee, the Board shall appoint a Company Secretary on terms approved by the Board.

(2) The Company Secretary shall perform the functions required under applicable company law and such additional functions as may be assigned by the Board.

26. Segregation of duties. — (1) A Licensee shall maintain organizational and procedural arrangements that ensure effective segregation between:

(a) business and revenue-generating functions; and

(b) control functions, including compliance, risk management, internal audit, and any other independent review function.

(2) A Licensee shall ensure that operational duties, including sales, dealing, order handling, accounting, settlement, reconciliation, custody or safekeeping of Customer Assets, and related recordkeeping, are appropriately segregated to reduce the risk of conflicts of interest, errors, misconduct, or abuse.

(3) The Compliance Officer and Head of Internal Audit (where appointed) shall have sufficient independence, authority, and access to the Board (or a Board committee) to discharge their duties, and shall not be involved in day-to-day revenue generation or operational decision-making.

(4) Where the nature, scale, and complexity of the Licensee does not permit full segregation by personnel, the Licensee shall implement compensating controls, including enhanced supervision, dual controls, independent checks, and increased frequency of internal review.

27. Conflicts of interest. - (1) A Licensee shall take reasonable steps to identify, prevent, manage and, where necessary, disclose conflicts of interest, and shall ensure fair treatment of Customers in all circumstances.

(2) Where a conflict of interest cannot be effectively prevented or sufficiently managed by organizational and procedural arrangements, the Licensee shall disclose the general nature and source of the conflict to affected Customers in a clear and timely manner before providing the relevant service, and shall document the basis on which Customer interests remain adequately protected.

(3) A Licensee shall establish, maintain and implement a written conflicts-of-interest policy that includes, at a minimum:

(a) identification and categorization of conflicts (including conflicts arising from proprietary trading, group structures, remuneration, listings, token issuance, and referral arrangements);

(b) governance, escalation, approval and recusal procedures;

(c) controls for gifts, hospitality, inducements and outside business interests;

(d) personal account dealing controls for directors, Key Individuals and staff; and

(e) recordkeeping and periodic review requirements.

(4) A Licensee shall maintain a conflicts register recording conflicts identified, the measures taken, disclosures made, and any residual risk accepted.

(5) Where a Board member or Key Individual has a material interest in a matter, that person shall promptly declare the interest, shall not participate in deliberations or voting on that matter, and shall not seek to influence the outcome. The Company Secretary (or equivalent) shall record the declaration and recusal in the minutes.

28. Disclosure governance. — (1) A Licensee shall establish and maintain policies and procedures to ensure that disclosures required under applicable law, these Regulations, and any instruments made under the Act are accurate, clear, not misleading, and kept up to date.

(2) A Licensee shall ensure that required public disclosures and customer-facing disclosures are made in the form and manner specified by the Authority, including through its website or other channels as applicable.

(3) The Board shall review disclosure governance periodically to ensure continued adequacy having regard to the Licensee's business model, products, and risk profile.

(4) Without prejudice to sub-regulations (1) to (3), disclosure governance shall apply to:

(a) marketing materials and promotions issued, approved, procured, facilitated or disseminated by or on behalf of the Licensee, including ensuring inclusion of required risk disclosures and compliance with conditions, standards and limitations prescribed by the Authority, in accordance with section 43(2) of the Act; and

(b) where the Licensee facilitates, approves or makes available a Virtual Asset offering to the public, the Licensee's controls to verify and retain evidence of issuer disclosures (including whitepapers and ongoing disclosures) required under section 42 of the Act and Regulations made thereunder.

29. Personal account dealing and insiders' transactions. - (1) A Licensee shall implement and enforce written policies and controls governing personal transactions in Virtual Assets by directors, Key Individuals, and relevant employees, including pre-clearance requirements, restricted lists, closed periods, and monitoring.

(2) The policies shall prohibit, in accordance with section 52 of the Act:

(a) dealing in Virtual Assets on the basis of inside information or material non-public information;

(b) recommending or inducing any Person to deal in Virtual Assets on the basis of inside information or material non-public information; and

(c) unlawful disclosure of inside information or material non-public information, and shall include procedures for identification and handling of inside information, information barriers, restricted lists and closed periods, pre-clearance, monitoring and escalation, and reporting to the Compliance Officer.

(3) The Licensee shall maintain comprehensive records of personal account dealing approvals, disclosures, breaches, and monitoring outcomes, and shall provide such records to the Authority upon request.

30. Transactions with Related Parties. - (1) A Licensee shall not enter into a material transaction with a Related Party unless:

(a) the transaction is on arm's length terms;

(b) the transaction is approved in advance by the Board (or an independent Board committee); and

(c) any conflicted person is excluded from deliberation and voting.

(2) A Licensee shall maintain a related party transactions register recording the identity of the Related Party, the nature and value of the transaction, the approval process followed, and the basis on which arm's length terms were assessed.

(3) A Licensee shall notify the Authority of any material related party transaction on quarterly basis, and shall provide supporting documentation upon request.

(4) Nothing in these Regulations shall require disclosure of confidential information to Customers or shareholders beyond what is required under applicable law; provided that the Authority may require access to records for supervisory purposes in accordance with the Act.

31. Minimum paid-up capital. - (1) A Licensee shall, at all times, maintain minimum paid-up capital in accordance with Schedule-I to these Regulations and any applicable conditions of its Licence.

(2) Where a Licensee is authorized for more than one Licence Category, the Authority may, on a risk-based basis, specify in the Licence, or by Rules or Regulations made under the Act, or by applicable direction, circular, standard, directive, guideline or other written instrument issued under the Act, the methodology for determining the applicable minimum paid-up capital and any additional prudential add-ons (including for custody exposure, operational/technology risk, market risk, or cross-border risk), provided that the Licensee is afforded an opportunity to make representations except in urgent cases.

(3) Any written direction under these Regulations shall state reasons, specify the amount and timeframe for compliance, and be proportional to the primary objectives in section 9(1) of the Act.

32. Liquid financial resources. - (1) A Licensee shall maintain at all times net liquid assets equivalent to 1.2 times of the adjusted monthly operating expenses to meet its obligations as they fall due, including during periods of stress. Paid-Up Capital maintained in assets that qualify as Eligible Liquid Assets may be counted towards satisfaction of this requirement. Where a Licensee holds more than one Licence Category, the applicable prudential floor shall be the highest requirement applicable to those Licence Categories, unless the Authority determines that an additional activity creates a separate and non-overlapping risk requiring an additional amount.

(2) A Licensee shall maintain Net Liquid Assets at or above the applicable minimum requirement specified under subsection (1). For the purposes of this section:

(a) "Net Liquid Assets" means Eligible Liquid Assets minus Current Liabilities; and
(b) "Eligible Liquid Assets" means assets that qualify as Eligible Liquid Assets under sub-regulation (3).

(3) Eligible Liquid Assets for all purposes other than capital and reserve requirements (ART/FRT) of the VASP shall comprise only assets that are readily convertible into cash within a short period and without material discount, and shall include, subject to limits, haircuts and concentration thresholds specified by the Authority:

(a) high-quality liquid assets (HQLA), including cash and cash equivalents, government securities or other instruments recognized as HQLA by the Authority;
(b) high-quality liquid fiat-referenced tokens or asset-referenced tokens approved by the Authority; and
(c) specified Virtual Assets with demonstrated deep liquidity and robust market infrastructure, as approved by the Authority.
(d) such other assets as the Authority may approve, subject to conditions.

33. Client asset safeguarding and backing. - (1) A Licensee that holds, controls, safeguards, or administers Customer Assets shall ensure that Customer Assets are properly segregated and protected in accordance with the requirements in regulations 103 to 107 (Client Money) and regulations 108 to 112 (Client Virtual Assets), the Act, any Rules or Regulations made under the Act, and any applicable direction, circular or other regulatory requirement made or issued thereunder, in each case only to the extent, and with the legal effect (if any), provided under the Act or under Rules or Regulations made thereunder.

(2) A Licensee shall not treat Customer Assets as its own assets and shall not use, pledge, encumber, lend, rehypothecate, or otherwise dispose of Customer Assets except as expressly permitted under these Regulations and with the Customer's prior informed explicit consent, and shall maintain records evidencing such consent and any permitted use.

(3) Where a Licensee owes an obligation to return Customer Assets, whether on-demand or upon specified withdrawal or settlement terms, the Licensee shall maintain arrangements ensuring that Customer Assets are available for timely return, including governance, reconciliations, controls, and safeguarding measures including periodic reconciliations and internal controls to verify the accuracy and completeness of Customer Asset holdings.

(4) Without prejudice to subsections (1) to (3), the Authority may, for specified Categories of Licence or business models, require that assets held to meet Customer withdrawal or redemption obligations including but not limited to:

(a) equal one hundred percent (100%) of the relevant Customer liabilities at all times, calculated in the manner specified at Regulations 108 to 112;

(b) be safeguarded in accordance with the custody and safeguarding requirements applicable to the Licensee; and

(c) consist of assets that mirror Customer liabilities in denomination and liquidity characteristics, subject to permitted operational tolerances.

(5) Substitute assets may be held only where operationally necessary and only in accordance with conditions specified by the Authority, including requirements that such substitute assets remain liquid, readily realizable, and available to meet withdrawal or redemption obligations.

34. Prudential requirements for token issuers. — (1) An Issuer of a Fiat-Referenced Token or Asset-Referenced Token shall, in addition to any other applicable requirements under the Act, Rules or regulation in general and these Regulations in specific, comply with the issuance requirements in sections 31 and 32 of the Act.

(2) Without prejudice to sub-regulation (1), an Issuer shall maintain reserve assets and redemption arrangements in accordance with these Regulations, including requirements relating to asset composition, custody, liquidity, valuation, segregation, audit, attestations, disclosures, and redemption timelines.

(3) Reserve assets maintained under this regulation shall, be maintained at a level equal to one hundred percent (100%) of the Issuer's outstanding redemption liabilities at all times, and shall be held as a segregated reserve.

(4) For a Fiat-Referenced Token, reserve assets under sub-regulation (3) shall comprise High-Quality Liquid Assets or such other eligible assets as may be specified, and the Issuer shall maintain mechanisms for redemption at par value without Undue Delay, in accordance with section 31 of the Act.

(5) For an Asset-Referenced Token, reserve assets under sub-regulation (3) shall comprise the underlying assets referenced by the token (or such eligible categories of underlying assets as may be specified), held in custody in accordance with Regulations, and the Asset-Referenced Token shall at all times be fully backed by the underlying assets and shall not be backed or derive its value from other Virtual Assets, in accordance with section 32 of the Act.

(6) Reserve assets shall be held with a custodian of reserve assets that complies with such requirements, oversight and inspection standards as may be prescribed by Regulations, in accordance with section 28 of the Act.

(7) The Issuer shall publish audited reserve disclosures and such other disclosures (including ongoing disclosures of material information and reserve attestations) in the manner and frequency prescribed, and shall maintain robust AML, CFT, CPF and sanctions compliance programmes, in accordance with sections 31 and 32 of the Act.

(8) The Issuer shall ensure prioritized holder protections in insolvency, including legal and operational arrangements supporting segregation and timely redemption and return of reserve assets for the benefit of holders, in accordance with sections 31 and 32 of the Act.

(9) Any permitted deviations, buffers, or operational tolerances, including the use of substitute assets, shall be specified by the Authority and shall not prejudice redemption at par value (where applicable) or timely redemption.

(10) Reserve asset requirements under this regulation shall not apply to a Licensee solely by reason of providing non-issuance Virtual Asset Services, unless otherwise specified by Regulations applicable to that Category of Licence.

(11) The Authority may grant a limited scope licence under regulation 7(5) for issuance of an FRT or ART for a limited scope including but not limited to:

(a) caps on outstanding supply, number/type of holders, and transaction volumes;
(b) limitations on distribution channels and use cases;
(c) enhanced disclosures to holders regarding pilot status and risks;
(d) redemption controls and operational safeguards; and
(e) any additional conditions necessary to protect holders and market integrity.

(12) For a limited scope license under these Regulations, the Authority may permit proportionate assurance and reporting arrangements, including attestations at intervals prescribed by Regulations made under the Act or specified by written direction issued under the Act, provided that reserves remain fully segregated and that redemption rights are protected.

(13) Nothing in these Regulations permits the Issuer to maintain reserves below one hundred percent (100%) unless expressly authorised by the Act.

34A. Significant Issuers. - (1) An Issuer shall be deemed a Significant Issuer if it meets the thresholds and criteria prescribed by Regulations, having regard to size, scale, systemic importance, market impact, number of holders, and cross-border activity, in accordance with section 33(1) of the Act.

(2) A Significant Issuer shall be registered with the Authority and shall comply with enhanced requirements, including enhanced reporting, disclosure, governance, and risk management, as prescribed in Regulations, in accordance with section 33(2) of the Act.

(3) Without prejudice to sub-regulations (1) and (2), the Authority may impose proportionate additional conditions on a Significant Issuer's Licence or registration having regard to financial stability, consumer protection, market integrity, and cross-border risks.

35. Monitoring, notification and remediation. - (1) A Licensee shall establish systems and controls to monitor compliance with these Regulations on an ongoing basis, including stress testing and contingency planning commensurate with its nature, scale and complexity.

(2) A Licensee shall notify the Authority without delay where it reasonably anticipates, or becomes aware, that it has failed or is likely to fail to meet any requirement under this Regulations, and shall provide a remedial action plan within the timeframe specified by the Authority.

(3) The Authority may require enhanced reporting, restrictions, or remedial measures where a Licensee is in breach or is likely to breach any requirement under this Regulations.

(4) The Authority may, on a risk-based basis and where necessary to advance the objectives of the Act, require a Licensee to hold and maintain additional paid-up capital, liquid financial resources, insurance, or reserve assets, having regard to the size, scope, geographic exposure, complexity and nature of the Licensee's activities and operations.

(5) A requirement under subsection (4) shall be proportionate, reasoned, and time-bound where appropriate, and shall specify the basis for the requirement, the compliance timeframe, and any reporting obligations; provided that in urgent cases the Authority may impose interim requirements subject to an opportunity to make representations as soon as reasonably practicable thereafter.

36. Insurance coverage. - (1) A Licensee shall maintain insurance arrangements, commensurate with the nature, scale, complexity, and risk profile of its Licensed Activities, to support customer protection and operational resilience.

(2) Without limiting sub-regulation (1), the Authority may specify in the Licence, or by Rules or Regulations made under the Act, or by applicable direction, circular or other regulatory requirement made or issued thereunder, minimum insurance types, coverage limits, deductibles, and other requirements, which may include but not limited to:

(a) professional indemnity insurance;
(b) crime/fidelity or commercial crime insurance covering employee dishonesty and theft;
(c) cyber risk insurance; and
(d) such other insurance as the Authority considers appropriate to the Licensee's activities and custody model.

(3) Insurance shall be obtained from an insurer licensed or authorised to provide insurance in Pakistan, unless the Authority permits otherwise in specified circumstances.

(4) The Licensee shall provide the Authority with evidence of coverage and shall promptly notify the Authority of any material change, lapse, cancellation, or non-renewal of coverage.

(5) The Licensee shall disclose insurance coverage in its audited financial statements, and shall not represent insurance as a guarantee of customer recovery

37. Outsourcing general requirements. - (1) A Licensee may outsource any activity, process or service to a Service Provider, whether within or outside Pakistan, provided that the Licensee remains fully responsible for compliance with the Act and the Regulations in relation to the outsourced activity, process or service.

(2) A Licensee shall ensure that outsourcing does not materially impair:

(a) the effectiveness of its governance arrangements, risk management, or internal controls;

(b) its operational resilience, cybersecurity, or business continuity;

(c) the safety, segregation, or timely return of Customer Assets; or

(d) the Authority's ability to obtain timely access to information reasonably required to exercise its functions under the Act.

(3) A Licensee shall designate a Key Individual as responsible for oversight of outsourcing arrangements and for coordinating regulatory engagement relating to outsourcing.

38. Material Outsourcing classification and proportionality. - (1) For the purposes of these Regulations, an outsourcing arrangement is "Material Outsourcing" where a failure, disruption, or deficiency in performance could reasonably be expected to have a significant adverse effect on:

(a) the Licensee's ability to comply with the Act or these Regulations;

(b) the security, availability, or timely return of Customer Assets;

(c) the confidentiality, integrity, or availability of customer data or critical records; or

(d) the continuity of a core Virtual Asset Service.

(2) A Licensee shall apply the requirements in regulations 37 to 43 in a manner proportionate to the nature, scale and complexity of its business and the criticality of the outsourced activity, process or service; provided that the minimum requirements in regulations 39 to 43 shall apply to all Material Outsourcing arrangements.

39. Risk assessment, due diligence and ongoing oversight. - (1) Before entering into, renewing, or materially varying an outsourcing arrangement, the Licensee shall conduct and document a risk assessment proportionate to the risks of the arrangement.

(2) The risk assessment shall consider, as relevant:

(a) the criticality of the outsourced activity, process or service and the feasibility of substitution;

(b) information security controls and incident response capabilities of the Service Provider;

(c) data access controls, confidentiality, retention and integrity safeguards;

(d) business continuity and recovery capabilities; and

(e) the Licensee's ability to monitor performance and implement exit arrangements without material disruption.

(3) The Licensee shall conduct due diligence to satisfy itself that the Service Provider is competent, capable, and reliable, and has controls appropriate to the outsourced activity, process or service.

(4) In relation to Material Outsourcing, the Licensee shall review the arrangement at least annually, and promptly following any material incident, breach, or change affecting performance, security, continuity, or compliance.

40. Outsourcing policy and register. - (1) A Licensee shall establish and maintain an outsourcing policy approved by its Board (or equivalent governing body), setting out governance, approval thresholds, monitoring, incident escalation, and exit management for outsourcing arrangements.

(2) A Licensee shall maintain an up-to-date register of Material Outsourcing arrangements in the form and manner specified by the Authority, including:

(a) the identity of the Service Provider;
(b) a description of the outsourced activity, process or service;
(c) whether the Service Provider is an intra-group entity or an external provider;
(d) the location(s) where the outsourced activity, process or service is performed and where relevant data is stored or processed; and
(e) the responsible Key Individual within the Licensee.

41. Outsourcing agreements required provisions - (1) A Licensee shall ensure each outsourcing arrangement is governed by a written agreement appropriate to the nature and risk of the arrangement.

(2) In relation to Material Outsourcing, the agreement shall, at a minimum, provide for:

(a) a clear description of the outsourced activity, process or service, service levels, and reporting;
(b) information security obligations, including incident notification to the Licensee;
(c) business continuity and disaster recovery arrangements;
(d) termination and exit assistance to support orderly transition, transfer, or insourcing; and
(e) the Licensee's ability to obtain, on a timely basis, information and records relating to the outsourced activity, process or service that are reasonably required for the Licensee to demonstrate compliance with the Act and these Regulations.

(3) Nothing in these Regulations shall require a Licensee to procure contractual rights that are unlawful or incapable of being granted under applicable foreign law; provided that the Licensee shall implement reasonable alternative measures to achieve the outcomes in subsection (2), which may include independent assurance reports, pooled audits, certifications, or other verification mechanisms acceptable to the Authority.

42. Sub-outsourcing. - (1) A Service Provider shall not sub-outsource any outsourced activity, process or service that constitutes Material Outsourcing without the Licensee's prior written consent.

(2) The Licensee shall ensure that sub-outsourcing does not reduce the Licensee's ability to meet the requirements of regulations 37 to 41, and that the Service Provider remains responsible for the performance of the outsourced activity, process or service.

43. Notifications to the Authority. - (1) A Licensee shall notify the Authority without delay upon becoming aware of:

(a) a material disruption, outage, incident, or control failure affecting a Material Outsourcing arrangement;
(b) a material breach by a Service Provider that has, or is likely to have, a significant adverse impact on Customers, Customer Assets, market integrity, or the Licensee's compliance; or
(c) termination of a Material Outsourcing arrangement where continuity of service or customer outcomes may be affected.

(2) A Licensee shall notify the Authority in advance where reasonably practicable, and otherwise without Undue Delay, of any outsourcing of a Material Function that is not a Critical Function.

(3) The notification shall include:
(a) the Function outsourced;
(b) the service provider and location(s);
(c) the risk assessment;
d) controls for data access and audit rights; and
(e) the planned implementation date.

(4) A Licensee shall, upon request, provide to the Authority information reasonably necessary to explain how the Licensee manages outsourcing risks and complies with regulations 37 to 43, including by reference to its outsourcing policy and register.

(5) Nothing in this regulation shall be construed as conferring a general veto over outsourcing decisions. This does not affect any prior approval requirement expressly set out in these Regulations or in a Licence condition.

44. ESG governance and disclosures. - (1) A Licensee shall maintain governance arrangements proportionate to the nature, scale and complexity of its business to identify and manage material environmental, social and governance risks that could reasonably affect:
(a) operational resilience, cybersecurity or business continuity;
(b) the fair treatment and protection of Customers; or
(c) the Licensee's ability to comply with the Act and these Regulations.

(2) The Authority may, by written direction or as a Licence condition, require a Licensee to make disclosures relating to material environmental or social risks only to the extent that such risks are proportionate and reasonably necessary to advance the primary objectives set out in section 9(1) of the Act, including where such risks could reasonably affect:
(a) operational resilience, cybersecurity or business continuity;
(b) the safeguarding, custody integrity or availability of Customer Assets;
(c) the fair treatment and protection of Customers;
(d) the prevention or mitigation of financial crime, fraud, market abuse or market integrity risks; or
(e) financial stability or systemic risk.

(3) Any disclosure requirement imposed under subsection (2) shall be calibrated having regard to the Licensee's nature, scale and complexity, and shall be limited to information that the Licensee can reasonably obtain and verify.

45. Scope of ESG disclosures. — (1) Where the Authority imposes ESG disclosure requirements under regulation 44(2), the Authority may specify the scope, format and frequency of such disclosures, which may include:

(a) a brief description of the Licensee's governance and accountability arrangements for ESG matters;

(b) a description of any material ESG risks identified and the steps taken to manage them; and

(c) where applicable, disclosures on workforce practices, complaints trends, and customer outcomes relevant to consumer protection and market integrity.

(2) The Authority may specify, by Regulations made under the Act or by written instrument issued under the Act, examples of proportionate ESG disclosures for different Categories of Licence.

46. Publication. - (1) Where the Authority requires a Licensee to publish ESG disclosures, the Licensee shall make such disclosures available in a prominent and accessible manner on its website, or by such other means as the Authority may specify.

(2) A Licensee shall not make ESG-related statements that are false, misleading or likely to create a misleading impression, including by omitting material information necessary to make the statements not misleading.

47. Service providers. - (1) A Licensee shall consider, as part of its outsourcing and procurement governance, whether a Service Provider's practices create material risks to the Licensee's:

(a) operational resilience, cybersecurity or business continuity; or

(b) compliance with the Act and these Regulations.

(2) Regulation 47(1) does not require a Licensee to ensure that a Service Provider complies with any particular international ESG standard, unless expressly required by applicable Pakistani law or specified by the Authority for the purpose of managing the material risks referred to in subsection (1).

48. Material changes to business and operations. - (1) A Licensee shall establish and maintain arrangements to identify, assess and manage Material changes to its business, operations, governance, risk profile, or control, and shall notify the Authority in accordance with this section.

(2) A Licensee shall seek prior approval for any material change in control or business as per Section 22(d) of the Act and shall notify the Authority of any proposed Material change as soon as practicable

(3) The application under this section shall include sufficient detail to enable supervisory assessment, including:

(a) a description of the change and expected timing;

(b) an assessment of the impact on Customers, market integrity, operational resilience, and AML/CFT/CPF controls;

(c) updates to governance, risk management, cybersecurity, outsourcing and business continuity arrangements where relevant; and

(d) mitigating measures and an implementation plan.

(4) The Authority may, on a risk-based basis and having regard to the primary objectives in section 9(1) of the Act:

(a) require the Licensee to provide additional information;

(b) require remedial measures, enhanced reporting, or restrictions;

(c) direct the Licensee to defer implementation for a reasonable period; or

(d) require the Licensee to apply for a variation of Licence or other approval under these Regulations where the change affects the scope of any Category of Licence or materially alters the Licensee's risk profile.

(e) require the Licensee to submit a remediation plan or to take specified steps to address risks arising from the Material change."

(5) For the avoidance of doubt, nothing in this section prevents a Licensee from ordinary-course treasury management, working capital facilities, or intra-group funding arrangements, provided that the Licensee remains compliant with prudential requirements and notification obligations under these Regulations.

(6) The Authority may issue non-binding guidance, or an applicable directive, guideline, circular or other written instrument issued under the Act, setting out non-exhaustive examples of Material changes and indicative notification timelines for different Categories of Licence.

49. Change of Control requirements. - (1) Every Licensee shall seek the Authority's prior written approval for any material change in control or business, in the manner prescribed.

(2) For the purposes of this section, "Material change in control" means any change in the business, operations, ownership, structure, or control of a VASP that could reasonably be expected to have a significant effect on the VASP's fitness or propriety to carry on regulated activities; the adequacy of the VASP's risk management, compliance, or governance arrangements; the interests or protection of clients, investors, or counterparties; or he integrity or stability of the virtual asset market

(3) An application for approval under subsection (1) shall be submitted by the Licensee and the proposed acquirer, and shall include information required to assess fitness and propriety, financial soundness, governance arrangements, and any other matters specified by the Authority.

(4) The Authority may approve an application under this section subject to conditions necessary to advance the primary objectives in section 9(1) of the Act.

50. Mergers and acquisitions. - (1) A Licensee shall notify the Authority in advance of any proposed merger, demerger, or acquisition involving the Licensee that constitutes a Material change.

(2) The Authority's prior written approval is required only where the transaction would result in

(a) a Change of Control; or

(b) a transfer of a Substantial Part of Assets of the Licensee.

(3) For the purposes of subsection (2)(b), "Substantial Part of Assets" means a transfer or disposition (in one transaction or a series of related transactions) that

(a) represents ten percent (10%) or more of the Licensee's total assets; or

(b) relates to assets that are critical to the Licensee's ability to provide a Category of Licence; or

(c) would reasonably be expected to materially impair the Licensee's ability to meet its obligations to Customers or to comply with these Regulations.

(4) The Authority may impose conditions to ensure orderly continuity of service, safeguarding of Customer Assets, and compliance during and after completion of a transaction under this section.

(5) A Licensee shall ensure compliance with all applicable laws in relation to any transaction under this section, including the Companies Act, 2017 and the Competition Act, 2010.

51. Recovery and wind-down planning. - (1) A Licensee shall maintain a documented Recovery and Wind-Down Plan commensurate with the nature, scale and complexity of its business and the risks of the Categories of Licence it conducts.

(2) The Recovery and Wind-Down Plan shall be designed to support the orderly cessation of regulated activities and the protection and timely return of Customer Assets, and shall include, at a minimum:

(a) governance arrangements and decision-making triggers for recovery actions and wind-down;

(b) an assessment of material impediments to orderly wind-down and mitigating measures;

(c) operational steps to safeguard, reconcile and return Customer Assets, including key dependencies on service providers and systems;

(d) communications arrangements for Customers, the Authority and other relevant stakeholders;

(e) record retention, access to systems and logs, and arrangements to maintain customer-facing channels necessary to support withdrawals and claims;

(f) staffing and key role continuity arrangements during wind-down;

(g) a plan for funding and resourcing the wind-down period; and

(h) where applicable and to the extent practicable, arrangements for any insurance, guarantee, or other risk-mitigant required under these Regulations or the Licence conditions to remain effective during wind-down, recognizing that such arrangements may be impacted by insolvency proceedings.

(3) A Licensee shall review and, where necessary, update its Recovery and Wind-Down Plan

(a) at least annually; and

(b) upon the occurrence of a Material change.

(4) Where a Licensee decides to cease carrying on all or any regulated activity, it shall notify the Authority without delay, provide its current Recovery and Wind-Down Plan, and implement the plan subject to subsection (6) and any written direction lawfully issued by the Authority under the Act and these Regulations.

(5) Where a Licensee becomes insolvent, enters into insolvency or restructuring proceedings, or becomes aware of an event that may materially impair its ability to meet obligations to Customers, it shall notify the Authority without delay and cooperate with any insolvency appointee, administrator, trustee, custodian or other competent person to support the orderly return of Customer Assets and continuity of critical customer protections.

(6) The Authority may, on a risk-based basis and where necessary to protect Customers or market integrity

(a) require the Licensee to provide progress reports, information, reconciliations, and independent assurance in such form and at such intervals as the Authority may specify;
(b) require the Licensee to propose amendments to its Recovery and Wind-Down Plan, or to implement specific remedial measures, provided that any such requirement shall be reasoned, proportionate, and limited to measures necessary to address identified risks; and
(c) where the Authority considers that an amendment is necessary and urgent, direct the Licensee to implement specified measures on an interim basis, provided that the Licensee shall be given an opportunity to make representations as soon as reasonably practicable thereafter.

CHAPTER – VI
Market Conduct

52. Client Agreements. - (1) A Licensee shall enter into a written Client Agreement with each Customer prior to providing any Virtual Asset Service to that Customer.

(2) A Client Agreement shall be fair, clear, transparent, accurate and not misleading, having regard to the nature of the service and the intended class of Customers.

(3) A Client Agreement shall, at a minimum, set out:

(a) the Virtual Asset Services to be provided and any material limitations or conditions;
(b) the fees, charges, spreads, commissions and other costs payable by the Customer, and how they are calculated;
(c) material risks relevant to the service, including custody, technology, market volatility and settlement risks;
(d) the arrangements for safeguarding Customer Assets, including segregation and any permitted use of Customer Assets (if any);
(e) the complaints handling process, including applicable steps and timelines, and the dispute resolution process, including (where applicable) the right of the Customer to refer eligible claims to any independent dispute-resolution scheme established or recognized by the Authority under section 45(2) of the Act, and how to access such scheme; and
(f) circumstances in which the Licensee may suspend, restrict or terminate the service, including where required to comply with law or to address security or market integrity risks.

(4) A Licensee shall obtain valid acceptance from the Customer in a manner compliant with applicable law, and shall provide the Customer with a copy of the Client Agreement after it is concluded.

(5) A Licensee shall notify Customers of any material change to a Client Agreement at least thirty (30) days prior to such change taking effect, except where an urgent change is required to address a legal requirement, a cybersecurity incident, a fraud risk, or a market integrity risk; provided that the Licensee shall notify Customers as soon as practicable in such cases.

(6) A Licensee shall maintain records of all versions of Client Agreements and evidence of Customer acceptance for a period of 7 years from the date of discontinuation of client

relationship unless otherwise required by any other applicable law. For the purposes of this sub-regulation, "date of discontinuation" means the later of

(a) the date on which the business relationship with the Customer is formally terminated; and

(b) the date on which the Customer's account is closed and all outstanding positions and obligations are settled.

53. Complaints handling. - (1) A Licensee shall establish and maintain internal complaint-handling procedures in accordance with the requirements prescribed by Regulations and section 45(1) of the Act.

(2) The procedures under sub-regulation (1) shall be prompt, fair, transparent, and consistently applied, and shall include, at a minimum:

(a) accessible channels for submission of complaints (including electronic channels);

(b) acknowledgement of receipt within 24 hours;

(c) investigation and resolution as soon as practicable within a reasonable time, having regard to the complexity of the complaint;

(d) where a complaint cannot be resolved within seven working days, a written update to the complainant stating reasons for delay and the expected timeframe for resolution;

(e) clear communication of outcomes, reasons, and (where applicable) remedial actions; and

(f) governance, escalation, and oversight arrangements proportionate to the Licensee's nature, scale, and risk profile.

(3) A Licensee remains responsible for complaint resolution notwithstanding the involvement of any service provider, agent, or group entity in the delivery of the service.

(4) A Licensee shall keep records of complaints received, actions taken, and outcomes and shall publish on its website clear information on how Customers may submit complaints and the steps and timelines applicable to the complaint-handling process.

(5) Where the Authority establishes or recognizes an independent dispute-resolution scheme under section 45(2) of the Act for claims below a prescribed monetary threshold, the Licensee shall:

(a) inform complainants, in writing, of their right to refer eligible complaints to such scheme once the Licensee has issued a final response or the prescribed internal timeline has elapsed without resolution;

(b) cooperate with the scheme, including by providing relevant records and information in a timely manner; and

(c) implement outcomes of the scheme to the extent required under the Act, these Regulations, or any Rules or Regulations made under the Act.

54. Public disclosures. - (1) A Licensee shall publish, in an easily accessible location on its website and kept accurate and up to date:

(a) its legal name, registered office address in Pakistan (if applicable), and contact details;

(b) its Licence number and the Categories of Licence and Virtual Asset Services for which it is authorised;

(c) the names or titles of Key Individuals or controlled functions responsible for the licensed activities, as specified by the Authority;

(d) a schedule or description of fees and charges and any material pricing methodology used for Customers; and
(e) the complaints handling process and channels for Customer support.

(2) A Licensee shall publish fair, clear and not misleading risk warnings regarding Virtual Assets and the relevant services, including:
(a) volatility and potential loss of value;
(b) liquidity risks;
(c) irreversibility of certain transfers and operational errors;
(d) technology and cybersecurity risks; and
(e) fraud, scams, manipulation and theft risks.

(3) The Authority may specify the format, prominence and minimum content of disclosures required under this section.

(4) A Licensee shall comply with any order or direction issued by the Authority under section 61 of the Act, including any direction to remove, block, or facilitate the removal or blocking of online material that promotes, operates, or relates to an unlicensed Virtual Asset Service or contravenes the Act, its Rules or Regulations.

55. Dealing controls and inside information safeguards. - (1) A Licensee shall comply with regulation 27 in relation to the identification, prevention, management and disclosure of conflicts of interest, including the maintenance of a conflicts-of-interest policy and conflicts register.

(2) Without prejudice to regulation 27, a Licensee shall establish and maintain controls to prevent misuse of inside information or material non-public information, including restricted access, need-to-know arrangements, information barriers, restricted dealing rules, watch lists and restricted lists, and escalation and reporting to the Compliance Officer.

(3) A Licensee shall establish and maintain personal account dealing controls for directors, Key Individuals and relevant Employees, including (as applicable) pre-clearance, restricted periods, monitoring and surveillance, recordkeeping, and periodic attestations.

(4) The Authority may prescribe minimum standards for controls under these Regulations (including personal account dealing controls, restricted lists, pre-clearance, and periodic attestations) proportionate to the Licensee's activities and risk profile.

56. Dealing as principal and proprietary activity. - (1) Where a Licensee deals as principal, makes markets, or trades on its own account in connection with providing Virtual Asset Services, it shall do so in a manner that is transparent, conflicts-controlled and consistent with market integrity and Customer protection.

(2) Without prejudice to subsection (1), a Licensee shall
(a) implement governance controls to approve and oversee proprietary activity, including limits, permitted purposes, and monitoring;
(b) maintain records of proprietary transactions and the rationale for such activity;
(c) ensure that proprietary activity does not misuse Customer order information or materially disadvantage Customers; and
(d) make appropriate disclosures to Customers where its role as principal may create conflicts.

(3) The Authority may specify additional restrictions for particular Categories of Licence or business models where necessary and proportionate to advance the primary objectives in section 9(1) of the Act.

57. Virtual Asset standards for admission and continued availability. - (1) A Licensee that makes a Virtual Asset available to Customers (including by listing, admitting to trading, or enabling purchase, sale or exchange) shall establish, implement and publish objective, transparent and non-discriminatory standards for the admission and continued availability of Virtual Assets.

(2) Such standards shall be proportionate to the Licensee's business model and shall address, where relevant:

(a) liquidity and market quality considerations;
(b) technology and security risks of the underlying protocol;
(c) risks of fraud, manipulation, and market abuse;
(d) legal and regulatory risks, including whether the Virtual Asset is prohibited or restricted under the Act or any other law in Pakistan, including section 53 of the Act (Prohibition on Algorithmic tokens); and
(e) conflicts of interest in relation to the Virtual Asset.

Assessments may be conducted on a risk-based basis and shall not require formal legal opinions unless otherwise specified by the Authority.

(3) A Licensee shall conduct initial and ongoing assessments against its standards and shall keep records of such assessments for three years following delisting..

(4) A Licensee shall establish clear triggers and procedures for suspension, restriction or delisting where a Virtual Asset no longer meets its standards or where continued availability presents a material and demonstrable risk of significant harm to Customers or market integrity.

(5) The Authority may direct a Licensee to suspend, restrict or cease a specified activity in relation to a Virtual Asset where the Authority has reasonable grounds to believe this is necessary to advance the objectives in section 9(1) of the Act, subject to the Licensee being afforded an opportunity to make representations as soon as practicable. While issuing such direction the Authority shall give due consideration to the specific risk identified based on the principle of proportionality. Any prohibition of a class of Virtual Assets shall be preceded by a reasoned public notice, unless urgency justifies interim restriction or other temporary measures taken in accordance with section 60 of the Act.

CHAPTER – VII
Technology

58. Technology governance and risk management framework. - (1) A Licensee shall establish, implement and maintain a technology governance and risk management framework designed to identify, assess, mitigate and monitor technology and cybersecurity risks arising from its business and licensed activities.

(2) The framework shall be proportionate to the nature, scale and complexity of the Licensee's business model, technology stack, and risk profile, including whether the Licensee

(a) holds or controls Customer Assets;

(b) operates trading, matching, settlement or wallet infrastructure;
(c) relies materially on third-party or group technology services; or
(d) provides services to a large retail customer base.

(3) The Licensee shall implement policies, procedures and controls to address identified risks, including layered security measures (defense-in-depth) where appropriate, and shall ensure that such controls are operating effectively on an ongoing basis.

(4) Without prejudice to subsections (1) to (3), the framework shall address, to the extent relevant
(a) technology governance and accountability, including Board and senior management oversight;
(b) system development and change management controls, including secure development, testing, and release procedures;
(c) operational controls, including access management, logging, monitoring, and vulnerability management;
(d) back-up, restoration and recovery controls;
(e) capacity, resilience and performance management; and
(f) periodic availability and disaster recovery testing.

(5) The Licensee shall review and update the framework and related controls periodically, and in any event following any material change to its technology, business model, threat landscape, or after a significant incident.

(6) The Authority may prescribe, by Regulations made under the Act, baseline expectations, illustrative risk parameters, assessment methodologies and minimum controls for the purposes of this regulation; and may also issue standards, directives, guidelines or other written instruments under the Act to support implementation.. Such expectations, parameters, methodologies, controls, standards, directives, guidelines or other written documents shall be proportionate and technology-neutral and shall not prescribe specific vendors, architectures or proprietary solutions unless objectively necessary.

(7) A Licensee shall designate a senior individual responsible for information security and cyber risk management ("Information Security Officer"), with appropriate authority, independence and resources; and where the Authority determines having regard to the Licensee's risk profile that a dedicated Chief Information Security Officer is required, the Licensee shall appoint a Chief Information Security Officer as may be specified by the Authority.

59. Cybersecurity policy and control framework. - (1) A Licensee shall establish, implement and maintain a written cybersecurity policy and supporting procedures designed to protect the confidentiality, integrity and availability of:
(a) its information systems and technology assets; and
(b) Customer Data and other confidential information processed or stored by the Licensee or on its behalf.

(2) The cybersecurity policy shall be approved by the Board (or a Board committee) and shall be reviewed at least annually, and promptly following any material change to the Licensee's technology environment, threat landscape, business model, or after a significant cyber incident.

(3) The Licensee shall submit its cybersecurity policy, and any material updates thereto, to the Authority

(a) as part of the licensing process; and

(b) thereafter, upon request, within the timeframe specified by the Authority.

(4) The cybersecurity policy shall be proportionate to the nature, scale and complexity of the Licensee's licensed activities and shall address, to the extent relevant:

(a) information security governance, roles, responsibilities and escalation;

(b) asset and data classification, access controls and authentication safeguards;

(c) secure configuration, patching, vulnerability management and malware protection;

(d) logging, monitoring and detection capabilities;

(e) incident response and recovery, including root cause analysis and remediation;

(f) business continuity, backup and restoration arrangements;

(g) third-party technology and service provider risk management; and

(h) controls for the initiation, authorization and execution of Virtual Asset transactions, including risk-based measures for high-risk or anomalous activity.

(5) The Licensee shall designate a senior individual responsible for oversight of cybersecurity risk management and implementation of the cybersecurity policy, which may be the Information Security Officer or Chief Information Security Officer designated under section 58(7).

(6) The Authority may issue standards, directives, guidelines, circulars or other written instruments under the Act specifying baseline cybersecurity controls, testing expectations, and illustrative measures for the purposes of this section; provided that any requirement intended to be mandatory and generally applicable shall be prescribed by Rules or Regulations made under the Act (or otherwise issued in a manner expressly authorised to have binding effect under the Act or under Rules or Regulations made thereunder).

60. Compliance with applicable cybersecurity and data protection requirements. - (1) A Licensee shall ensure that its technology governance arrangements, cybersecurity policy and related controls comply with all applicable laws in Pakistan relating to cybersecurity, electronic crimes, data protection and confidentiality, to the extent applicable.

(2) Where a Licensee relies on service providers to process or store Customer Data or to operate material systems supporting its licensed activities, the Licensee shall ensure appropriate contractual and operational measures are in place to meet the requirements of subsection (1).

(3) A Licensee may store or process data outside Pakistan, subject to compliance with applicable laws relating to data protection, cybersecurity, and cross-border data transfers, and subject to such safeguards as may be prescribed by Regulations, in accordance with section 39(1) of the Act.

(4) A Licensee shall implement appropriate technical, organizational, and governance measures to ensure the segregation of sensitive information from other operational data, in such manner as may be prescribed by Regulations, in accordance with section 40(1) of the Act. The Authority may prescribe, by Regulations, minimum technical standards, cybersecurity controls, storage architectures, encryption requirements, and data-governance frameworks to give effect to this regulation, in accordance with section 40(4) of the Act.

61. Cryptographic key and wallet management. - (1) A Licensee that generates, holds, controls, or otherwise can initiate or approve transactions using cryptographic keys in relation to Customer Assets shall establish, implement and maintain policies, procedures and controls for secure key and wallet management.

(2) Without prejudice to subsection (1), a Licensee shall ensure that its key and wallet management arrangements provide an appropriate level of security and operational resilience, including

(a) governance and accountability for key management, including documented roles, responsibilities and approvals;

(b) secure key generation, storage, use and backup arrangements appropriate to the custody model, including measures to minimize single points of failure and unauthorized access;

(c) robust access management and segregation of duties for any individual or system that can initiate, approve, sign, or execute Virtual Asset transactions;

(d) maintenance of auditable records of key access and key-related administrative actions, and periodic review of such records;

(e) procedures to promptly revoke or modify access where personnel roles change or employment ends, and to address key compromise or suspected compromise; and

(f) controls to manage risks arising from technology dependencies, integrations, and service providers involved in key or wallet operations.

(3) A Licensee shall regularly assess, test and review the effectiveness of its key and wallet management controls and shall remediate identified deficiencies without delay, having regard to the risk profile of the Licensee and any Customer Assets affected.

(4) Where a Licensee provides services to Customers that involve Customer-controlled wallets or self-custody, the Licensee shall provide clear information and risk warnings regarding

(a) the Customer's responsibility for safeguarding private keys, seed phrases and authentication factors; and

(b) the consequences of loss, compromise or unauthorized disclosure.

(5) The Authority may also issue standards, directives, guidelines or other instruments under the Act, specifying baseline expectations, control examples, and assurance or audit practices for secure key management and wallet operations for the purposes of this section.

62. Technology testing, assurance and audits. - (1) A Licensee shall implement a risk-based testing and assurance programme covering the technology, cybersecurity and operational resilience of the systems used to provide Virtual Asset Services, proportionate to the nature, scale, complexity and risk profile of its activities.

(2) Without prejudice to subsection (1), a Licensee shall ensure that:

(a) vulnerability assessments and penetration testing are conducted at appropriate intervals and after material changes to systems, architecture or controls;

(b) security monitoring and internal control testing are performed on an ongoing basis; and

(c) identified high-risk findings are remediated within reasonable timeframes, with escalation to the Board or senior management where material.

(3) Where a Licensee uses smart contracts or other programmable protocols that are material to the provision of its services or to the safeguarding, transfer, settlement, or issuance of Virtual

Assets, the Licensee shall ensure that such smart contracts or code are subject to independent security review and testing:

(a) prior to deployment or material upgrade; and

(b) thereafter on a periodic basis commensurate with their criticality and risk.

(4) A Licensee shall maintain appropriate documentation evidencing the tests, reviews, findings and remediation actions under this section and shall make such documentation available to the Authority upon request.

(5) The Authority may, by written direction and where necessary and proportionate having regard to the Licensee's risk profile, customer impact, custody or market infrastructure role, or credible threat indicators, require the Licensee to undertake enhanced testing, including threat-led or scenario-based testing, and to submit a remediation plan and progress updates in the timeframe specified by the Authority.

(6) Where enhanced testing under subsection (5) is required, the Authority may specify:

(a) the scope and objectives of the testing, including whether testing may be conducted on production or a representative environment;

(b) minimum competence, independence and integrity requirements for external testers; and

(c) requirements for safe handling of testing outputs, vulnerabilities, sensitive data and reporting, to minimize disruption and prevent misuse.

(7) A Licensee shall ensure that any engagement with external testers includes contractual provisions addressing confidentiality, data handling, responsible disclosure, conflict management, and secure retention and destruction of testing artefacts.

63. Controls for Virtual Asset transactions and automated activity. - (1) A Licensee shall implement systems and controls to detect, prevent and respond to market abuse, manipulation, abusive trading practices, and technology-enabled attacks or misuse, including where relevant automated or coordinated activity.

(2) Where a Licensee processes, executes, transmits, settles, or safeguards Virtual Asset transactions for Customers, it shall maintain transaction monitoring controls, including the capability to identify higher-risk transactions and addresses, and to escalate and respond in accordance with its AML/CFT/CPF policies and applicable law.

(3) The controls under subsection (2) may include the use of distributed-ledger analytics tools or equivalent measures, selected and calibrated on a risk basis having regard to the Licensee's business model, customer profile, products, and exposure to illicit finance risks.

64. Algorithm governance and controls. - (1) Where a Licensee uses algorithms that materially affect pricing, execution, risk controls, customer onboarding, transaction monitoring, safeguarding arrangements, or other regulated activities, it shall establish and maintain governance and controls to ensure effective oversight by the Board and senior management.

(2) The governance and controls under subsection (1) shall include, at a minimum:

(a) documented design objectives and intended use;

(b) testing and validation prior to deployment and following material changes;

(c) change management, including version control and approval processes;

(d) ongoing monitoring of performance and outcomes, including alerts for abnormal behaviour; and
(e) the ability to suspend or disable the algorithm promptly where necessary to protect Customers, market integrity, or operational resilience.

(3) A Licensee shall maintain adequate records to evidence compliance with this section, including key assumptions, data inputs where relevant, material limitations, and remediation actions taken.

(4) This section shall not require disclosure of proprietary algorithms, source code or trading logic, except where required under lawful investigation.

65. Business continuity and disaster recovery. - (1) A Licensee shall establish, implement, maintain and periodically test a business continuity and disaster recovery plan proportionate to the nature, scale and complexity of its activities and technology dependencies.

(2) The plan under subsection (1) shall, at a minimum, address:
(a) governance, roles and escalation procedures for disruption events;
(b) recovery objectives and priorities for material systems and services;
(c) backup, restoration and integrity controls for data and records;
(d) communications arrangements for Customers, counterparties and the Authority, where relevant; and
(e) post-incident remediation and lessons learned to reduce recurrence.

(3) Where the Licensee safeguards Customer Assets or operates technology that is material to market functioning, the Authority may require enhanced resilience measures or testing on a risk-based basis.

66. Information security officer and staff readiness. - (1) A Licensee shall designate a senior individual responsible for information security oversight, including implementation of the Technology and Information requirements under these Regulations.

(2) Where the nature, scale or risk profile of the Licensee's activities warrants, the Authority may require the appointment of a Chief Information Security Officer, and may specify role expectations, reporting lines, and independence safeguards.

(3) A Licensee shall ensure that staff receive periodic awareness training appropriate to their roles, including training on cyber risks relevant to Virtual Assets and common attack vectors, and shall maintain records of such training.

(4) Senior management shall periodically review the effectiveness of information security controls and allocate responsibilities to mitigate conflicts of interest and ensure adequate segregation between security oversight and operational delivery, where practicable.

67. Cyber incident and BCDR event notification. - (1) Where a Licensee detects:
(a) a material cybersecurity event; or
(b) an event triggering activation of its business continuity and disaster recovery plan that materially impacts its operations,
the Licensee shall notify the Authority as soon as reasonably practicable and, in any event, within twenty-four (24) hours of detection.

(2) The notification under subsection (1) shall be an initial notification and shall include, to the extent known at the time

(a) a brief description of the event and the date/time of detection;

(b) the systems, services, or customer segments likely affected;

(c) an initial assessment of impact on confidentiality, integrity, availability, and safeguarding of Customer Assets and data;

(d) immediate containment and mitigation steps taken or planned; and

(e) whether the Licensee has made, or expects to make, notifications to other competent authorities or law-enforcement agencies.

(3) The Licensee shall provide the Authority with follow-up updates in such form and at such intervals as may be specified by the Authority, and in any event

(a) a written interim update within five (5) Working Days of the initial notification (or earlier where requested), providing updated impact assessment, indicators of compromise (where relevant), and progress on remediation; and

(b) a final report within thirty (30) calendar days of detection (or such other period as the Authority may allow), setting out the root cause analysis, the full scope and impact, Customer outcomes, and corrective and preventive actions.

(4) The Licensee shall maintain records and supporting evidence relating to the event, including relevant logs and investigation outputs, and shall make such records available to the Authority upon request.

68. Personal data protection and privacy. — (1) A Licensee shall comply with all applicable data protection, data privacy and secrecy requirements in relation to Personal Data processed in connection with its licensed activities.

(2) The licensee shall be bound to provide all the requisite information to the Authority as required under the Act, Rules, Regulations or as required from time to time under applicable laws in Pakistan.

(3) Where a Licensee reasonably identifies a material conflict between applicable requirements under subsection (1) or (2) (including conflicts relating to cross-border transfers, secrecy laws, or cloud jurisdiction restrictions), the Licensee shall:

(a) document the conflict and the legal basis for its assessment;

(b) implement proportionate technical and organizational measures to mitigate associated risks; and

(c) notify the Authority immediately where the conflict materially affects the Licensee's ability to comply with these Regulations or to provide the Authority with access to information as required by the Authority.

69. Personal data protection compliance programme. - (1) A Licensee shall establish, document, implement and maintain a written programme for the governance and protection of Personal Data, proportionate to the nature, scale and complexity of its business and the sensitivity of the Personal Data processed.

(2) The programme under subsection (1) shall, at a minimum, include:

(a) assignment of responsibility and accountability for Personal Data protection;

(b) policies and procedures for lawful processing, retention, access control, security, and disposal of Personal Data;

(c) risk assessments and controls for cross-border transfers and the use of service providers;
(d) staff training and periodic awareness measures; and
(e) incident detection, response and notification arrangements aligned with these Regulations and applicable law.

(3) A Licensee shall appoint a Data Protection Officer or designate a responsible senior person to oversee compliance with subsection (1), where this is required by applicable law or where directed by the Authority on a risk-based basis.

(4) Subject to conflict-of-interest safeguards and adequacy of resources, the Authority may permit the Data Protection Officer function to be performed by the Chief Information Security Officer or another senior officer in smaller Licensees, where proportionate.

70. Provision of information to the Authority on data protection. - (1) A Licensee shall provide the Authority with information reasonably required to assess the Licensee's compliance with this Chapter, in the manner and within the timeframe specified by the Authority.

(2) The obligation under subsection (1) shall apply subject to applicable law, including data protection, banking secrecy, confidentiality, legal privilege, and restrictions arising from court orders or ongoing investigations in Pakistan or any relevant jurisdiction.

(3) Where a Licensee is unable to provide information requested under subsection (1) due to a legal restriction under subsection (2), it shall:
(a) promptly notify the Authority of the restriction and its basis;
(b) provide such information as can lawfully be provided; and
(c) propose lawful alternatives, which may include summaries, redactions, controlled access, or provision through an appropriate legal process.

71. Notification of personal data incidents. - (1) Where a Licensee becomes aware of a Personal Data breach or other incident affecting, or reasonably likely to affect, the confidentiality, integrity or availability of Personal Data, it shall notify the Authority without Undue Delay and, in any event, within seventy-two (72) hours of becoming aware of the incident, unless the Licensee demonstrates that a longer period is justified due to the circumstances and the Licensee has provided an initial notification.

(2) The notification under subsection (1) may be staged and shall include, to the extent known at the time:
(a) the nature of the incident and categories of Personal Data affected;
(b) the likely impact on data subjects and the Licensee's operations;
(c) immediate containment measures taken or planned; and
(d) the Licensee's plan and timeline for further investigation and follow-up reporting.

(3) The Licensee shall provide supplemental updates to the Authority as material information becomes available, including root cause analysis and remediation actions, within the timeline specified by the Authority.

(4) Where the Licensee is required by applicable law to notify a data regulator or data subjects, the Licensee shall inform the Authority of such notifications as soon as reasonably practicable, and shall provide copies or summaries to the extent not prohibited by applicable law.

72. Confidential information. - (1) A Licensee shall take reasonable steps to protect the confidentiality of information relating to its Customers and their affairs, and shall implement and enforce policies, procedures and controls to prevent unauthorized access, use or disclosure.

(2) Confidential information may be used only:

(a) for providing authorised Virtual Asset Services to the Customer;

(b) for compliance with applicable law and regulatory requirements; or

(c) where otherwise permitted by the Customer or applicable law.

(3) A Licensee shall ensure that access to confidential information is limited on a "need-to-know" basis and is supported by appropriate access controls, monitoring and audit trails.

(4) A Licensee shall provide training to relevant Employees on confidentiality obligations and shall require periodic attestations or acknowledgements, in the manner specified by the Licensee's governance arrangements.

(5) Neither a Licensee nor any of its Employees shall misuse confidential information, including by using such information for personal benefit or for any market abuse, fraud, or unfair dealing in relation to Virtual Assets.

73. Guidance on Technology Governance and Risk Assessment Framework. - (1) This Chapter sets out supervisory expectations to assist Licensees in designing, implementing and maintaining a Technology Governance and Risk Assessment Framework required under these Regulations.

(2) The guidance in this Chapter

(a) does not create independent legal obligations beyond those expressly set out elsewhere in these Regulations; and

(b) may be taken into account by the Authority in licensing, supervision and risk assessment, including when determining whether a Licensee's controls are proportionate and effective.

(3) A Licensee shall apply this guidance in a manner proportionate to its nature, scale and complexity, including its custody model, technology stack, use of service providers, customer base, and risk profile.

74. Risk categories to be addressed. - (1) In developing and maintaining its Technology Governance and Risk Assessment Framework, a Licensee should consider risks including, as applicable

(a) organizational and governance risks;

(b) technical and security architecture risks;

(c) detection, response and recovery risks;

(d) customer asset protection and user security risks; and

(e) operational resilience risks.

(2) The Authority may publish supplementary guidance, examples and good practices for the risk categories in subsection (1), including sector-specific expectations for custody providers, exchanges, brokers, and token issuers.

75. Organizational and governance risk considerations. - (1) A Licensee should maintain governance arrangements that allocate clear accountability for technology and security, including oversight by senior management and periodic reporting to the Board or equivalent governing body.

(2) A Licensee should adopt a documented approach to technology risk management, which may include periodic security assessments, secure development practices, workforce security controls, and controls for technology service providers, proportionate to the Licensee's risk profile.

76. Technical risk considerations. - (1) A Licensee should implement security controls that are appropriate to its custody model and threat profile, including controls for key management and wallet security where the Licensee holds or controls Customer Assets.

(2) A Licensee should adopt defense-in-depth measures, which may include segregation of duties, access controls, monitoring, secure key storage arrangements, and procedures for responding to suspected compromise.

(3) Where a Licensee deploys smart contracts or relies on smart contracts in providing services, it should implement controls for secure development, review and testing proportionate to the materiality and risk of such contracts.

77. Detection, response and recovery risk considerations. - (1) A Licensee should maintain capabilities to detect, investigate and respond to cyber threats and operational incidents, including escalation, containment and remediation processes.

(2) Where appropriate to the business model, a Licensee should maintain capabilities for transaction monitoring and analysis, including supporting fraud prevention, incident response and Customer protection, consistent with applicable law.

78. Customer asset protection and user security considerations. - (1) A Licensee should implement controls designed to reduce the risk of unauthorized access to customer accounts and loss of Customer Assets, including authentication, withdrawal controls and customer awareness measures, proportionate to its client base and service model.

(2) Where Customer Assets are held or controlled by the Licensee, it should consider concentration risk and implement appropriate operational arrangements for wallet management and diversification consistent with its safeguarding obligations.

79. Digital operational resilience testing considerations. - (1) A Licensee should establish and maintain a testing programme proportionate to its risks, including vulnerability assessments, penetration testing, and operational resilience testing.

(2) The Authority may, on a risk-based basis, require a Licensee to undertake enhanced testing by qualified independent parties, having regard to the Licensee's size, risk profile, systemic importance, custody footprint, and threat landscape.

CHAPTER – VIII
Compliance and Risk Management

80. Compliance management system. - (1) A Licensee shall establish, implement and maintain an effective compliance management system ("CMS") that is proportionate to the nature, scale and complexity of its business and the Virtual Asset Services it provides.

(2) The CMS shall be able to:

(a) cover all relevant aspects of the Licensee's operations, including policies, procedures, processes, systems, controls, training, monitoring and escalation;

(b) provide the Compliance Officer with timely access to information, records and personnel necessary to discharge the Compliance Officer's responsibilities;

(c) include arrangements to identify, assess, monitor and remediate compliance risks, including a risk-based testing and monitoring programme; and

(d) ensure that material non-compliance is escalated promptly to the Board and, where required under these Regulations, notified to the Authority.

(3) The CMS shall be documented, approved by the Board, and reviewed at least annually and following any material change to the Licensee's business, risk profile, or applicable legal and regulatory requirements.

(4) A Licensee shall establish and maintain written compliance policies and procedures that are consistent with these Regulations and any applicable Rules or Directives issued by the Authority.

(5) An employee of the Licensee who in good faith reports to the Authority a contravention of the Act or any Rules or Regulations made thereunder it shall not be subjected to any form of retaliation.

81. Appointment of Compliance Officer. - (1) A Licensee shall appoint a Compliance Officer who:

(a) is a Fit and Proper Person;

(b) has appropriate seniority, competence and relevant experience to discharge the role, commensurate with the nature, scale and complexity of the Licensee's activities and risk profile;

(c) resident in Pakistan;

(d) is a full-time employee of the Licensee or such other arrangement as may be permitted by the Authority having regard to the nature, scale and complexity of the Licensee; and

(e) reports to the Board or a Board committee with responsibility for compliance oversight.

(2) Where the Authority requires another appropriately authorised senior compliance representative to be ordinarily resident in Pakistan, such requirements shall be proportionate to the Licensee's scale, customer footprint in Pakistan, and risk profile.

(3) The Licensee shall notify the Authority of the appointment, replacement, or departure of the Compliance Officer in the manner and timeframe specified by the Authority.

82. Duties of the Compliance Officer. - (1) The Compliance Officer shall be responsible for establishing, administering and maintaining the CMS and for advising the licensee's board or relevant board committees on the Licensee's compliance with applicable legal and regulatory requirements.

(2) Without prejudice to subsection (1), the Compliance Officer shall

(a) implement and maintain compliance policies and procedures, systems and controls, including compliance training arrangements for Employees and Key Individuals;

(b) monitor and assess compliance risks, including emerging regulatory and conduct risks relevant to the Licensee;

(c) report periodically to the Board on the Licensee's compliance posture, material findings, remediation progress and significant compliance incidents; and

(d) ensure that material non-compliance is investigated, escalated and remediated, and where required, notified to the Authority.

(3) Compliance activities may be delegated to appropriately qualified personnel or service providers, provided that the Compliance Officer remains accountable for the effectiveness of the CMS.

(4) The Compliance Officer may perform additional non-client-facing roles only where this does not compromise independence, creates no material conflict of interest, and does not impair the discharge of compliance responsibilities.

83. Risk management framework. - (1) A Licensee shall establish, implement and maintain a risk management framework that is proportionate to the nature, scale and complexity of its business and the risks arising from the Virtual Asset Services it provides.

(2) The risk management framework shall include policies, procedures and methodologies to identify, measure, monitor, manage and report material risks, including financial, operational, technology and conduct risks.

(3) The Licensee's board shall approve the risk management framework and ensure it is reviewed periodically and following any material change to the Licensee's business, operations, Key Individuals, or the market conditions and legal or regulatory requirements applicable to the Licensee.

(4) Where a Licensee's nature, scale or risk profile warrants a dedicated risk function, the Licensee shall appoint a Head of Risk with appropriate authority and competence, who shall have direct access to the Board.

84. Risk reporting. - (1) A Licensee shall provide the Board with periodic risk reporting sufficient to enable effective oversight of the Licensee's risk profile and compliance with these Regulations.

(2) Risk reporting shall be provided at least quarterly, or more frequently where warranted by the Licensee's risk profile or where a material risk event occurs.

(3) Risk reporting should, as applicable, cover:

(a) financial risks (including liquidity, capital adequacy, treasury and exposures);

(b) operational and technology risks (including cybersecurity and resilience);

(c) conduct and market integrity risks (including conflicts of interest and market abuse risks where relevant);

(d) financial crime risks (including AML/CFT/CPF); and

(e) customer asset and consumer protection risks (including safeguarding arrangements).

85. Operational management. - (1) A Licensee shall establish and maintain operational policies, procedures and controls to ensure

(a) fair, honest and professional treatment of clients and market participants;

(b) safeguarding of Customer Assets in accordance with regulations 103 to 112, the Act, any Rules or Regulations made under the Act, and any applicable direction, circular, standard, directive, guideline or other written instrument issued by the Authority under the Act;

(c) integrity and reliability of records and management information; and

(d) compliance by the Licensee and its Employees with applicable legal and regulatory requirements.

(2) Where a Licensee may act on behalf of a client in relation to account operation or transactions, the Licensee shall disclose to the client the scope of its authority and the procedures and terms under which it may act, and shall act consistently with the client agreement and the client's instructions.

(3) A Licensee shall perform reconciliations and verification checks at a frequency proportionate to its business model and risks, including reconciliation of internal records against relevant third-party statements and distributed ledger records where applicable, to identify errors, omissions or misallocation of assets.

(4) A Licensee may establish committees to perform its responsibilities and to support compliance and risk oversight.

86. Books and records. - (1) A Licensee shall maintain complete, accurate and up-to-date books and records sufficient to demonstrate compliance with these Regulations and to enable effective supervision by the Authority.

(2) Records shall be retained in original form or native file format, where practicable, and shall include an audit trail of material activities and transactions, including the information necessary to support investigations, dispute resolution and regulatory reporting.

(3) Without prejudice to subsection (2), records should include, as applicable:

(a) transaction records (amount, date/time, fees/charges, relevant account or wallet identifiers, and counterparties where available);

(b) client onboarding and due diligence records;

(c) general ledger and financial records;

(d) governance records (Board minutes and committee records);

(e) complaints handling and error resolution records; and

(f) conflicts of interest registers.

(4) Records shall be retained at least for the period required under the Anti-Money Laundering Act, 2010 (VII of 2010), in accordance with section 47(4) of the Act or seven (7) years whichever is higher. Records shall be produced to the Authority in the manner required.

87. Audit. - (1) A Licensee shall appoint an external auditor, a firm of chartered accountants approved by the Division concerned that is independent under applicable law and any other requirements specified by the Authority.

(2) The external auditor shall audit the Licensee's financial statements in accordance with International Financial Reporting Standards and applicable company law requirements, and the

Licensee shall submit audited financial statements to the Authority as specified in Schedule I of these Regulations.

(3) A Licensee shall cause its operations to be audited annually and shall include a verification of the segregation of Customer Assets as required under section 24 of the Act.

(4) The Authority may, on reasonable grounds and having regard to the nature, scale and complexity of the Licensee, require the Licensee to appoint an alternative auditor or to procure additional assurance engagements relating to specified risk areas. Any additional assurance engagement shall be risk-based and proportionate and shall not duplicate existing statutory audit or assurance requirements unless justified by identified supervisory concerns.

(5) A Licensee shall establish an internal audit function that is independent of operational activities and reports to the Board or an audit committee.

(6) Internal audit shall be conducted on a risk-based plan and at a frequency proportionate to the Licensee's risks, and shall report findings, recommendations and remediation tracking to the Board.

88. Regulatory reporting. - (1) A Licensee shall submit to the Authority such returns, statements and information as may be required by the Authority, in the form, manner and frequency specified by the Authority, having regard to the nature, scale, complexity and risk profile of the Licensee and the Virtual Asset Services it provides.

(2) Without prejudice to subsection (1), the Authority may require periodic reporting to include, as applicable

(a) financial statements and prudential returns sufficient to demonstrate compliance with applicable capital, liquidity and safeguarding requirements;
(b) information on Customer Assets safeguarding arrangements and reconciliations, where relevant to the Licensee's business model;
(c) risk and compliance reporting, including key risk indicators, AML/CFT reporting as required under the AML Act, 2010 and material control findings; and
(d) such other information as the Authority considers reasonably necessary for effective supervision.

(3) The Authority shall, where practicable, specify standard templates and reporting timelines and may vary reporting frequency on a risk-based basis, including for Licensees that are newly licensed, operating under limitations, or subject to enhanced supervision.

89. Additional information. - (1) The Authority may, by written notice, require a Licensee to provide additional information or documents where necessary for supervisory purposes, including to verify compliance with these Regulations or to assess risks to customers or market integrity.

(2) A Licensee shall provide information under subsection (1) within the timeframe specified by the Authority, subject to applicable law.

90. Regulatory notifications. - (1) A Licensee shall notify the Authority without delay, and in any event within any timeframe specified in these Regulations or, where no such timeframe is specified, within the timeframe specified by the Authority, upon becoming aware of any matter that materially affects, or is reasonably likely to materially affect:

(a) the Licensee's ability to comply with these Regulations;
(b) the Licensee's financial soundness or operational resilience;
(c) the safety of Customer Assets; or
(d) the Licensee's fitness and propriety governance arrangements.

(2) Without prejudice to subsection (1), notifiable events include:
(a) commencement of Insolvency Proceedings in respect of the Licensee;
(b) any material criminal or civil proceedings, or material regulatory investigation or enforcement action, involving the Licensee, or any Controller, Board member, or Key Individual, where relevant to fitness and propriety or the Licensee's operations;
(c) any material breach of law or of these Regulations relating to the conduct of Virtual Asset Services; and
(d) cybersecurity and data incidents in accordance with the Technology chapter.

(3) A notification under this Regulation shall include such information as is reasonably available at the time, and the Licensee shall provide supplemental updates as further information becomes available.

91. Employees management and training. - (1) A Licensee shall ensure that Employees are competent, suitably qualified and appropriately supervised for the roles they perform, having regard to the nature of the Virtual Asset Services provided.

(2) A Licensee shall maintain adequate staffing and resources to operate safely and in compliance with these Regulations.

(3) A Licensee shall implement and maintain training programmes that are proportionate to roles and risks, including induction training and periodic refresher training.

(4) Without prejudice to subsection (3), a Licensee shall provide periodic training on AML/CFT/CPF, sanctions compliance, fraud risk, and conduct expectations, and shall maintain records of training completion.

(5) A Licensee shall ensure that material updates to policies and procedures are communicated to relevant Employees promptly and are readily accessible.

92. Tax reporting and compliance. - (1) A Licensee shall comply with the obligations imposed under the applicable tax laws and any Rules or Regulations issued by the relevant tax authority, in accordance with section 66 of the Act, and shall comply with all other applicable tax laws and tax reporting obligations in Pakistan that are relevant to its business and the Virtual Asset Services it provides.

(2) Where the Authority issues requirements under these Regulations relating to tax reporting, such requirements shall apply to the extent and in the manner specified by the Authority and subject to applicable law.

93. Appointment of Money Laundering Reporting Officer. - (1) A Licensee shall appoint an individual as Money Laundering Reporting Officer ("MLRO") who:
(a) is a Fit and Proper Person;
(b) has adequate knowledge and experience in AML/CFT/CPF, commensurate with the nature, scale and complexity of the Licensee's Virtual Asset Services; and

(c) is of sufficient seniority and authority to discharge the responsibilities under applicable AML/CFT/CPF laws and these Regulations.

(2) The Licensee shall ensure that the MLRO has direct access to the Board and unfettered access to relevant records, systems, and personnel necessary to perform the MLRO function.

(3) The appointment of the MLRO and the continuing suitability of the MLRO shall be reviewed periodically and, in any event, at least annually.

94. Duties of the MLRO. - (1) The MLRO shall be responsible for establishing, implementing and maintaining the Licensee's AML/CFT/CPF framework, including:

(a) AML/CFT/CPF policies, procedures and internal controls;

(b) enterprise-wide AML/CFT/CPF risk assessment and risk-based mitigation measures;

(c) oversight of customer due diligence, transaction monitoring and sanctions screening;

(d) suspicious transaction reporting and liaison with the Financial Monitoring Unit ("FMU") and other competent authorities, as applicable; and

(e) periodic reporting to the Board on the effectiveness of the AML/CFT/CPF framework, material issues, and remediation status.

(2) AML/CFT/CPF tasks may be delegated under the MLRO's oversight, provided that the Licensee remains responsible for compliance and the MLRO remains accountable for the effectiveness of the AML/CFT/CPF framework.

95. AML/CFT/CPF policies and procedures. - (1) A Licensee shall establish, implement and maintain AML/CFT/CPF policies and procedures that comply with:

(a) applicable federal AML/CFT/CPF laws of Pakistan and binding instruments issued thereunder; and

(b) such requirements, guidance, or directions, in the context, as may be issued by the competent Authority within their respective mandates.

(2) The AML/CFT/CPF policies and procedures shall be risk-based and shall, as a minimum, address

(a) prohibition of anonymous or fictitious relationships where prohibited by applicable law;

(b) targeted financial sanctions compliance, including mechanisms to implement applicable UNSCR-related measures as required under AML Act, 2010, in interpreting and applying those requirements, regard may be had to relevant FATF Standards and guidance, requirements and other applicable laws;

(c) recordkeeping and retrieval capabilities consistent with applicable law;

(d) customer due diligence (including beneficial ownership), ongoing monitoring, and enhanced due diligence for higher-risk relationships; and

(e) controls relevant to Virtual Assets, including the Travel Rule where applicable.

(3) The Authority may require a Licensee to provide copies of its AML/CFT/CPF policies and procedures, and material updates thereto, within the timeframe specified by the Authority.

96. AML/CFT/CPF systems and controls. - (1) A Licensee shall implement systems and controls proportionate to its risks, including screening and monitoring arrangements capable of

identifying suspicious activity, sanctions exposure, and other illicit finance risks relevant to its Virtual Asset Services.

(2) Where a Licensee uses distributed ledger analytics or similar tools, it shall
(a) document the rationale for selecting the tool(s), including known limitations;
(b) implement governance and quality controls over tuning, scenarios, thresholds and alerts; and
(c) periodically review the effectiveness of such tool(s) and associated controls.

97. AML/CFT/CPF risk assessments. - (1) A Licensee shall conduct and maintain an enterprise-wide AML/CFT/CPF risk assessment covering, as relevant, customer types, products/services, delivery channels, transaction patterns, geographies, and Virtual Asset-specific risk factors (including anonymity-enhancing features where applicable).
(2) The Licensee shall only permit the issuance, custody, transfer, trading, or other dealing in Virtual Assets incorporating anonymity-enhancing or privacy-enhancing features where it is able to comply with all applicable AML/CFT/CPF obligations/FATF Recommendations including customer due diligence, ongoing monitoring, record-keeping, sanctions screening, and the Travel Rule. Provided that where the Licensee is unable to comply with AML/CFT/CPF obligations and FATF recommendations, it shall not provide services in respect of such Virtual Assets

(3) The risk assessment shall be reviewed
(a) at least annually; and
(b) promptly following any material change in the Licensee's business model, products, customer base, geographic exposure, or material threat landscape.

(4) The Licensee shall ensure that the outcomes of the risk assessment inform its AML/CFT/CPF controls, resourcing, monitoring scenarios, and enhanced due diligence measures, and shall be able to demonstrate this to the Authority upon request.

98. Customer due diligence. - (1) A Licensee shall apply customer due diligence measures on a risk-based basis in accordance with section 46 of the Act and applicable federal AML/CFT/CPF laws of Pakistan, including the Anti-Money Laundering Act, 2010 (VII of 2010) and any rules, regulations or guidelines issued thereunder.

(2) A Licensee shall identify and verify customers and beneficial owners on the basis of documents, data and information obtained from the reliable source, understand the purpose and intended nature of the business relationship, and conduct ongoing monitoring.

(3) A Licensee shall apply enhanced due diligence in accordance with the internal policy compliant with AML Act, 2010 and FATF requirements in the context, for higher-risk relationships, including where the customer or beneficial owner is a Politically Exposed Person, or where anonymity-enhancing features materially elevate risk.

(4) As part of the CDD process, a Licensee shall verify customer's identity by reference to the following documents, data or information from a reliable and independent source:

(a) For individuals - full name as shown on CNIC or a passport; nationality; address; place of birth; Bank account details; and Source of fund.

(b)For legal person which are not individuals - full name of the legal person; type of legal person; constitutional documents; principle place of business; authorized person and its relationship; names and details of Ultimate Beneficial Owner of the legal person; Bank account details; and Source of fund.

(5) A Licensee shall not establish or continue a business relationship, or execute a transaction, where it is unable to complete required due diligence measures, except as otherwise permitted under applicable law.

(6) Where a Licensee relies on third parties for elements of due diligence, it shall remain responsible for compliance and shall ensure appropriate controls, oversight and information access as envisaged in these Regulation and in compliance with the FATF Recommendation 17.

(7) VASPs may apply following measures for dormant or in-operative wallets: VASP shall send prior notice to the wallet holder through any registered medium, before marking the wallet as dormant. Notices shall be sent one (1) month, seven (7) days and one (1) day prior to marking the wallet as dormant. Notice shall also include the wallet activation procedures/ channels.

(a) VASP may allow credit entries in dormant or in-operative wallets subject to compliance with other applicable AML/CFT/CPF regulations.
(b) Debit transactions/ withdrawals shall not be allowed until the wallet is activated. However, transactions e.g. debits under the recovery of any liability, any permissible charges/fee, government duties or levies and instructions issued under any law or from the court will not be subject to debit or withdrawal restriction.
(c) VASP may activate the dormant wallet upon receipt of a formal request from the customer through any authenticated medium.

(8) Unclaimed wallets/assets, which have not been operated for the last ten years except a wallet/asset in the name of a minor or a Government or a court of law, shall be surrendered to Strategic Digital Wallet Company (SDWC). The requirement to transfer unclaimed Customer Assets to the SDWC shall take effect only once an applicable regulatory procedure establishes:

(a) that the SDWC receives the assets solely in a custodial capacity and not as Government property;
(b) the transfer of responsibility and liability from the Licensee;
(c) continued segregation, safeguarding, reconciliation and recordkeeping;
(d) the treatment of forks, airdrops, staking rewards and other blockchain events;
(e) responsibility for losses occurring after transfer; and
(f) an effective and continuing right for the Customer to reclaim the assets.

Until that regulatory procedure takes effect, the Licensee shall continue to safeguard the assets for the Customer in accordance with the Act and these Regulations.

99. Suspicious transaction monitoring and reporting. - (1) A Licensee shall maintain ongoing monitoring to identify suspicious transactions and activity and shall submit reports to the FMU in the manner and form required under the AML Act, 2010 and other regulations and guidelines issued thereunder.

(2) The Licensee shall ensure internal escalation arrangements enable timely review and decision-making by the MLRO, including prompt filing to the FMU where required.

(3) The Licensee shall notify the Authority of material AML/CFT/CPF breaches, material control failures, or significant exposure events in the manner and timeframe specified by the Authority, subject to applicable law and confidentiality constraints.

(4) The Licensee shall maintain appropriate records relating to suspicious activity reviews and reports in accordance with provisions of AML Act, 2010, and shall provide information to the Authority upon request, subject to applicable law. Provided that nothing in these Regulations shall require disclosure of Suspicious Transaction Reports and related information, or any protected information, in a manner inconsistent with the AML Act, 2010.

(5) Nothing in these Regulations shall be construed as limiting or replacing the obligation of a Licensee to submit STRs, CTRs or any other reports required under the AML Act, 2010 to the Financial Monitoring Unit.

100. Travel Rule compliance. - (1) A Licensee shall comply with section 47 of the Act (Travel rule and record-keeping obligations) and the requirements applicable to "wire transfers" and "virtual asset transfers" under the Federal AML-CFT Laws, including the requirements implementing the FATF Recommendation 16 and its Interpretive Note, as updated from time to time, and any detailed procedures, standards and formats prescribed by Regulations under the Act.

(2) For the purposes of sub-regulation (1), a Licensee shall obtain, verify where required, and transmit or make available (as applicable) required and accurate originator and beneficiary information for Virtual Asset transfers meeting or exceeding the threshold of PKR equivalent of USD 1,000,. .

(3) Prior to initiating a Virtual Asset transfer at or above the applicable threshold, an ordering Licensee shall ensure that it has obtained and holds the required originator information and required beneficiary information, and is able to make such information available to the FMU, the Authority and other competent authorities upon lawful request.

(4) Prior to making Virtual Assets received through a transfer at or above the applicable threshold available to a customer, a beneficiary Licensee shall ensure that it has obtained and holds the required originator information and required beneficiary information, and is able to make such information available to the FMU, the Authority and other competent authorities upon lawful request.

(5) Subject to the Federal AML-CFT Laws, the minimum originator information shall include
(a) the originator's full name; and
(b) the originator's account number, or Virtual Asset wallet address, or other unique transaction identifier; and
(c) such additional identifiers as may be required under applicable law (which may include address, national identification number, customer identification number, or date and place of birth).

(6) Subject to the Federal AML-CFT Laws, the minimum beneficiary information shall include
(a) the beneficiary's name; and
(b) the beneficiary's account number, or Virtual Asset wallet address, or other unique transaction identifier.

(7) A Licensee shall implement risk-based controls to manage Travel Rule compliance risks relating to

(a) transfers to or from unhosted wallets and other non-obliged persons and give regard to relevant FATF Standards and guidance;

(b) deposits and withdrawals where counterparty information is incomplete, unavailable, or unreliable;

(c) transactions or patterns designed to evade thresholds or information requirements; and

(d) anonymity-enhancing features or services, where applicable.

(8) Prior to establishing a material relationship for Virtual Asset transfers with a counterparty VASP in another jurisdiction, a Licensee shall conduct risk-based due diligence on the counterparty's Travel Rule and AML/CFT controls in accordance with AML Act, 2010, in interpreting and applying those requirements, regard may be had to relevant FATF Standards and guidance, and shall review such due diligence annually and upon the occurrence of heightened risk indicators.

(9) A Licensee shall be required to demonstrate to the Authority, during licensing and on an ongoing basis, the policies, procedures, systems and controls implemented to comply with this Regulation, and shall provide evidence of their effectiveness within the timeframe specified by the Authority.

101. Compliance with targeted financial sanctions. - (1) A Licensee shall maintain policies, procedures and controls to comply with applicable targeted financial sanctions obligations under:

(a) relevant United Nations Security Council Resolutions as implemented in Pakistan; and

(b) the Federal AML-CFT Laws and any binding directions issued by competent authorities in Pakistan.

(2) The controls under subsection (1) shall be proportionate to the Licensee's risk profile and shall include, as applicable

(a) screening of customers (including beneficial owners) and relevant counterparties;

(b) screening of transfers against applicable designations;

(c) escalation and decision-making processes for potential matches; and

(d) procedures to implement freezing, blocking, rejection, or other required measures to the extent mandated by applicable law, FATF recommendation (if any) and competent authority directions.

(3) A Licensee shall maintain records of sanctions screening actions, escalations, and measures taken under subsection (2) for the period required by applicable law, and shall make such records available to the Authority upon request, subject to applicable law.

102. AML/CFT recordkeeping. - (1) A Licensee shall retain records relating to AML/CFT/CPF in accordance with the Federal AML-CFT Laws, including:

(a) Virtual Asset transaction records (including identifiers, wallet addresses, timestamps, and audit trails sufficient to reconstruct transactions);

(b) customer due diligence and beneficial ownership records;

(c) ongoing monitoring records, alerts, investigations and dispositions; and

(d) suspicious transaction reports and related internal analysis, to the extent permitted by applicable law.

(2) Records under subsection (1) shall be retained for the minimum period required under the AML Act, 2010 and the rules and regulations issued thereunder, and where no minimum period is specified, for a period of at least seven (7) years.

103. Client Money: application, interpretation and safeguarding. - (1) For the purposes of this Chapter, "Client Money" means money (including fiat currency) owned by a Client which is received, held or controlled by a Licensee on behalf of that Client in the course of, or in connection with, the provision of any Virtual Asset Service, excluding

(a) money that is immediately due and payable to the Licensee for its own account (including fees and charges) in accordance with the Client Agreement;

(b) money received by the Licensee as reimbursement of expenses properly incurred on behalf of the Client and due and payable to the Licensee; and

(c) any other amounts that are due and payable to the Licensee in accordance with the Client Agreement.

(2) Client Money does not include Virtual Assets held on behalf of a Client, which shall be subject to regulations 108 to 112 (Client Virtual Assets: safeguarding, segregation, reconciliations and proof of reserves).

(3) Client Money shall be treated as held or controlled by a Licensee where it is

(a) held by the Licensee;

(b) held in an account in the name of the Licensee (including an account designated for Clients); or

(c) held by a Person controlled by the Licensee, or in an account in the name of such Person, for the benefit of Clients.

(4) A Licensee that receives, holds or controls Client Money shall establish and maintain policies, systems and controls, proportionate to the nature, scale and complexity of its business, to ensure that Client Money is

(a) segregated from the Licensee's own money;

(b) identifiable and appropriately safeguarded at all times; and

(c) not used to meet obligations of the Licensee or of any other Client.

104. Client Accounts and treatment of Client Money. - (1) A Licensee that holds Client Money shall hold such Client Money in one or more segregated accounts designated for Clients (each a "Client Account") with a bank licensed by State Bank of Pakistan (a "Permitted Bank").

(2) Client Money held in a Client Account in accordance with section 24(2) of the Act, shall not be treated as the Licensee's property and shall not form part of the Licensee's estate in the event of Insolvency, subject to applicable insolvency law and any directions of the competent court or insolvency office-holder.

(3) A Licensee shall ensure that each Client Account is appropriately designated to distinguish it from the Licensee's own accounts, including through account naming conventions and internal records.

(4) A Licensee shall pay Client Money into a Client Account immediately after receipt and, in any event, no later than the end of the next Business Day, unless

(a) the money is held only temporarily for onward transmission in accordance with a Client instruction and is transmitted within the same timeframe; or

(b) the money is received in connection with a delivery-versus-payment arrangement and is settled in accordance with the arrangement within the same timeframe; or

(c) the money is held in an account in the Client's own name and the Licensee has a mandate to operate that account on behalf of the Client.

(5) A Licensee shall not pay into a Client Account any money of its own, except

(a) a minimum amount required by the Permitted Bank to open or maintain the account; or

(b) money used temporarily to meet an identified shortfall in Client Money, provided that such top-up is clearly recorded, justified, and reversed as soon as practicable after the shortfall is resolved.

(6) Withdrawals or transfers out of a Client Account shall be subject to appropriate authorization controls and shall only be made where the relevant amount is

(a) due and payable to the Licensee in accordance with the Client Agreement;

(b) payable to, or at the instruction of, the relevant Client;

(c) required to meet the payment obligations of the relevant Client in connection with the authorised service; or

(d) otherwise permitted by these Regulations or directed by the Authority.

(7) A Licensee shall not use Client Money of one Client to meet an obligation owed to another Client or to any other Person, and shall maintain controls to prevent offsetting, netting or negative balances within Client Accounts.

105. Banking arrangements for Client Accounts. - (1) A Licensee shall select one or more Permitted Banks taking into account safety, resilience, operational capability, and legal protections applicable to client asset segregation, in a manner proportionate to the Licensee's business model and risk profile.

(2) A Licensee shall take reasonable steps to ensure that the terms governing each Client Account support segregation and do not permit the Permitted Bank to apply set-off or combination of accounts in respect of the Licensee's obligations, to the extent achievable under applicable law and standard banking arrangements.

(3) Where a Licensee is unable to obtain a specific contractual acknowledgement from a Permitted Bank, the Licensee shall refrain from opening Client Account from said Permitted Bank.

106. Records, client statements and audit trail. - (1) A Licensee shall maintain accurate books and records sufficient to identify Client Money, track receipts and payments, and reconcile Client Money to Client Accounts, including

(a) date of receipt;

(b) the relevant Client identifier;

(c) payer / source where available; and

(d) transaction reference and banking value date.

(2) A Licensee shall provide Clients with periodic statements of Client Money balances and movements at a frequency appropriate to the service and Client type, and in any event:

(a) at least monthly for retail Clients; and

(b) at such other frequency as agreed with professional Clients, provided that information remains clear and accessible.

(3) Statements under subsection (2) shall be made available promptly following the statement date, and in any event within a timeframe that is reasonable having regard to the Licensee's systems and the delivery channel used.

107. Reconciliation and discrepancy notification. - (1) A Licensee shall perform reconciliations of Client Money and Client Accounts at a frequency proportionate to its activity, and in any event no less frequently than daily where the Licensee processes Client Money movements on a daily basis.

(2) Reconciliations shall compare

(a) aggregate Client ledger balances;

(b) Client Account cash book balances; and

(c) Permitted Bank statements or confirmations as at the reconciliation point.

(3) A Licensee shall investigate and resolve shortfalls, excesses and unexplained differences promptly, and where necessary may use its own funds temporarily to address a shortfall pending resolution.

(4) A Licensee shall notify the Authority without delay of any material discrepancy that is not rectified within the timeframe specified by the Authority, and shall provide a summary of cause and remediation steps.

108. Client Virtual Assets: application and interpretation. - (1) In this Chapter, "Client Virtual Assets" means Virtual Assets beneficially owned by a Client which are held, controlled, safeguarded or administered by a Licensee on behalf of that Client in the course of, or in connection with, the provision of any Virtual Asset Service, excluding Virtual Assets that are due and payable to the Licensee for its own account in accordance with the Client Agreement (including fees and charges), or properly payable as reimbursement of expenses.

(2) Client Virtual Assets are treated as held, controlled, safeguarded or administered by a Licensee where

(a) they are held in a wallet, account or other arrangement operated by or for the Licensee;

(b) they are held in a wallet or account in the name of the Licensee or a Person controlled by the Licensee; or

(c) the Licensee (or a Person acting on its behalf) holds, controls or can access the private keys, seed phrases, signing devices, authorization credentials, or other means necessary to transfer or otherwise dispose of those Virtual Assets.

109. Safeguarding and segregation of Client Virtual Assets. - (1) A Licensee shall establish and maintain policies, systems and controls, proportionate to the nature, scale and complexity of its business, to safeguard Client Virtual Assets and ensure they are identifiable, appropriately protected, and segregated from the Licensee's own assets.

(2) Client Virtual Assets are not owned by the Licensee. The Licensee shall hold or control Client Virtual Assets solely for the benefit of Clients and shall not treat Client Virtual Assets as its own assets.

(3) A Licensee shall maintain records that clearly identify which wallets, addresses, accounts or sub-accounts contain Client Virtual Assets and shall label such wallets or ledger designations accordingly (including through internal ledger tagging).

(4) A Licensee shall not use, pledge, encumber, lend, stake, rehypothecate, or otherwise dispose of Client Virtual Assets except
(a) as required to execute an instruction of the Client; or
(b) where expressly permitted under these Regulations and with the Client's prior explicit written consent, including clear disclosure of the nature of the activity, associated risks, withdrawal restrictions (if any), and how rewards/losses are allocated.

(5) Any rewards, proceeds or benefits attributable to Client Virtual Assets (including airdrops, forks, staking rewards, or similar) shall accrue to the Client unless otherwise agreed with the Client in advance in the Client Agreement and disclosed in a fair, clear and not misleading manner.

(6) A Licensee shall not take ownership of Client Virtual Assets under any Client Agreement except as expressly permitted under these Regulations.

110. Insolvency treatment and client asset protection. - (1) A Licensee shall structure its custody and safeguarding arrangements to support the segregation and protection of Client Virtual Assets in the event of Insolvency.

(2) The Licensee shall maintain records, wallet structures and reconciliation capabilities sufficient to facilitate the timely identification and return (or transfer) of Client Virtual Assets, subject to applicable insolvency law and any directions of the competent court or insolvency office-holder.

111. Reconciliations and discrepancy notification. - (1) A Licensee shall conduct reconciliations of Client Virtual Assets at a frequency proportionate to its activity, and in any event no less frequently than daily where the Licensee processes Client Virtual Asset movements on a daily basis.

(2) Reconciliations shall include, as applicable
(a) Client ledger balances per asset;
(b) on-chain balances for relevant wallets/addresses (or equivalent control evidence);
(c) pending transactions, unconfirmed deposits/withdrawals, and other timing items; and
(d) identification and investigation of breaks, shortfalls or excesses.

(3) The Licensee shall notify the Authority without delay of any material discrepancy that is not rectified within an appropriate timeframe, and shall provide a summary of cause, impact and remediation.
(4) The Licensee shall conduct a root cause analysis of any material discrepancy and implement appropriate remedial measures to prevent recurrence.

112. Proof of reserves and independent validation. - (1) Where a Licensee holds, controls, safeguards or administers Client Virtual Assets, the Licensee shall maintain procedures to demonstrate that its liabilities to Clients in respect of Client Virtual Assets held, controlled, safeguarded or administered by the Licensee are fully matched by reserve assets (or equivalent safeguarding arrangements) in accordance with the custody and safeguarding requirements in

regulations 108 to 112 and as prescribed by the Authority under the Act or these Regulations. Provided that, for the purposes of this regulation, "liabilities to Clients" shall be determined net of the following, however, the VASP shall report to the Authority both gross and net liabilities on six monthly basis

(a) authorised margin arrangements; and
(b) risk exposures and losses contractually agreed by Clients, to the extent such exposures do not constitute Client Virtual Assets held, controlled, safeguarded or administered by the Licensee.

The reporting can be at an earlier or more frequent interval required by the Authority by written notice, where reasonably necessary having regard to the Licensee's scale, custody arrangements, risk profile, any material discrepancy or another identified supervisory concern. The notice shall specify the reasons, scope, frequency and duration of the requirement and shall allow a reasonable implementation period, unless urgent action is necessary to protect Customer Assets.

(2) Proof of reserves procedures under subsection (1) may include automated or cryptographic methods, including third-party attestation and cryptographic verification, provided that such methods are capable of demonstrating, to the satisfaction of the Authority:
(a) the existence and control of the relevant reserve assets; and
(b) that Client liabilities are fully matched in accordance with this Chapter and prescribed by the Authority under the Act or these Regulations (including by Rules or Regulations made under the Act or by written instrument issued under the Act)

(3) Proof of reserves shall be subject to independent validation on six monthly basis or earlier as required by the Authority. Such validation may be carried out by
(a) an external auditor;
(b) a qualified assurance provider; or
(c) an internal assurance function that is independent of custody operations, including through methods such as third-party attestation or cryptographic verification, only where permitted by the Authority
Such validation report must be submitted to the Authority within 30 days of the end of six months period.

(4) For avoidance of doubt, compliance with this Regulation does not derogate from the Licensee's obligations to safeguard and segregate Client Virtual Assets under this Chapter, nor does it limit any other prudential or custody requirements applicable to the Licensee.

113. Anti-bribery and corruption programme. - (1) A Licensee shall establish, implement and maintain an effective anti-bribery and corruption programme that is proportionate to the nature, scale and complexity of its business and risks.

(2) The programme shall be documented in an Anti-Bribery and Corruption Policy and supporting procedures and shall be designed to prevent, detect and address bribery and corruption risks in the Licensee's operations, including in dealings with public officials and private counterparties.

(3) The programme shall be aligned with applicable anti-bribery and anti-corruption laws and regulations and may take account of internationally recognized good practices to the extent consistent with applicable law.

(4) The Board retains overall responsibility for ensuring the programme is effective. The Compliance Officer shall oversee implementation and monitoring, and shall report material findings to the Board at intervals appropriate to the Licensee's risk profile.

114. Minimum policy requirements. - (1) The Anti-Bribery and Corruption Policy shall, as a minimum:

(a) prohibit bribery and corruption in any form, including direct and indirect bribes, facilitation payments, and improper advantages;

(b) set clear rules and controls for gifts, hospitality, sponsorships, charitable contributions, political contributions (if any), and conflicts of interest;

(c) require risk-based due diligence and contractual controls for Third-Party Service Providers and other relevant counterparties;

(d) provide for escalation, investigation, remediation, and disciplinary measures that are fair, consistently applied and compliant with applicable law; and

(e) require recordkeeping sufficient to evidence compliance with this Chapter.

(2) The Policy shall permit confidential reporting, including by persons outside the Licensee, through appropriate reporting channels, and shall include measures to protect reporters from retaliation, subject to applicable law.

115. Prohibited conduct. - (1) A Licensee, and any person acting on its behalf, shall not:

(a) offer, promise, give, request, agree to receive, or accept any undue advantage in connection with the Licensee's business;

(b) make or accept facilitation payments; or

(c) use Third-Party Service Providers, intermediaries, or other arrangements to circumvent the requirements of this Chapter.

(2) The Licensee shall maintain controls designed to prevent payments for services that are not legitimate, not properly documented, or not commensurate with services actually provided.

(3) Hospitality and gifts are permitted only where they are reasonable, proportionate, transparently recorded, and consistent with the Licensee's Policy and applicable law.

116. Reporting, investigation and remediation. - (1) The Licensee shall maintain and publish (as appropriate) methods of contact for reporting suspected or actual bribery or corruption, including anonymous or confidential reporting where feasible.

(2) The Compliance Officer shall ensure that credible reports are assessed promptly, investigated where appropriate, and escalated to the Board in accordance with the Licensee's procedures.

(3) The Licensee shall document investigation steps, findings and remediation actions, and shall retain such records for at least seven (7) years or such longer period as required under applicable law.

117. Training and communication. - (1) The Licensee shall provide periodic anti-bribery and anti-corruption training to the Board, Key Individuals and Employees, and tailored training to

higher-risk roles (including those involved in procurement, third-party management, government engagement, sales, and finance).

(2) The Policy shall be made accessible to all relevant persons, and material updates shall be communicated promptly.

(3) Anti-bribery and anti-corruption training shall form part of induction for new Board members, Key Individuals and Employees.

118. Notifications to the Authority. - (1) The Licensee shall notify the Authority without delay where it becomes aware of a material bribery or corruption incident relating to the Licensee's regulated activities, including where

(a) a matter is referred to, or investigated by, a competent law enforcement authority;
(b) the incident may materially affect the Licensee's integrity, governance, financial position, or ability to comply with these Regulations; or
(c) the incident involves a Key Individual, Controller, or other person in a position of significant influence.

(2) Notifications under subsection (1) shall be made to the extent permitted by applicable law (including restrictions relating to legal privilege, confidentiality, or ongoing investigations).

FORM-I
[see regulation 6(1)]

APPLICATION FOR NO OBJECTION CERTIFICATE TO INCORPORATE A VIRTUAL ASSET SERVICE PROVIDER

The information and documents listed in Parts A–E mainly apply to the NOC stage. Part F mainly applies to the Licensing Application stage following incorporation unless otherwise specified by the Authority.

Date: _____

To
The Pakistan Virtual Asset Regulatory Authority (the Authority)
Islamabad, Pakistan

Subject: Application for No Objection Certificate to incorporate a Virtual Asset Service Provider

Dear Sir/Madam,

We, the undersigned sponsors and proposed directors (the Applicants), hereby apply for the grant of a No Objection Certificate in accordance with regulation 6 of the Pakistan Virtual Asset Services Regulations, 2026 , to incorporate a company under the Companies Act, 2017 under the proposed name * ---------- (the **Proposed VASP**) for

the purpose of undertaking the following [Category(ies) of Licence / VA Activity(ies)]: ----------.**

The information and documents required under the Annexure to this Form, duly completed, verified and signed by all Applicants, are enclosed.

We solemnly declare that the information provided in this application and in the enclosed Annexure is true, complete and correct to the best of our knowledge and belief, and that no material information has been concealed or omitted.

We undertake to keep the information and documents submitted under this application up to date and to notify the Authority in writing of any material change thereto without Undue Delay and in accordance with the requirements in these Regulations.

Evidence of payment of the prescribed processing fee in the amount of PKR [x] (receipt/reference no. [x]), paid on [x] through [bank/PSID/channel], is enclosed.

Yours faithfully, ----------

Name: [●]
CNIC/Passport No.: [●]
Signature: [●]
(On behalf of all Applicants)
Signed by all sponsors and proposed directors (Applicants)
*Proposed name of the company
**Category(ies) of Licence / VA Activity(ies) to be undertaken

ANNEXURE TO FORM-I
[see regulation 6]

INFORMATION TO BE SUPPLIED FOR OBTAINING A NO-OBJECTION CERTIFICATE (NOC) AND, WHERE APPLICABLE, FOR LICENSING READINESS

Date of Application; DD/MM/YYYY

<table>
<tr><td colspan="10">Part A – Applicant Information</td></tr>
<tr><td>1.</td><td>Name of Applicant Company (at the time of license); or name of the applicant (NOC)</td><td colspan="8"></td></tr>
<tr><td rowspan="2">2.</td><td rowspan="2">CUIN (in case already incorporated) – to be specified at the time of submission of licensing application</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="8">Date of Incorporation; ____/____/_____
DD/MM/YYYY</td></tr>
<tr><td></td><td>Application Fee:</td><td colspan="8">Application fee for the preliminary approval / NOC</td></tr>
</table>

3.		Deposit Date; ____/____/_____ DD/MM/YYYY			
		Challan #: M-_____ *(Annex the Original Challan as Annexure)*			
4.	**Legal Status (intended for business in Pakistan):**	☐ Private Limited ☐ Public Limited (Unlisted) ☐ Public Limited (Listed)			
5.	**Type of Licence applied for:**	Advisory Services Broker-Dealer Services; Custody and Administration Services; Exchange Services Lending and Borrowing Services; Virtual Asset Derivatives Services;	Virtual Asset Management and Investment Services; Virtual Asset Transfer and Settlement Services; Asset-Referenced Token Issuance Services; Fiat-Referenced Token Issuance Services; Mining Related Virtual Asset Service.		
		(Please attach a copy of /draft of memorandum and Articles of Association of the company, as an Annexure)			
6.	**Registered Office Address:**				
7.	**Contact Person Name, email and Mobile Number:**	Name & Designation:			
		Mobile Number: Email:			
8.	**Composition of Board of Directors and shareholders, including identification of the Controller of the proposed VASP:**				
	Name of Person	**Position; Shareholder /Director/CEO /Sponsor**	**Shareholding**	**Percentage (%) of Shareholding**	**Net Worth (for NOC application, related to Shareholder) Rs.**
i					
ii					
iii					
iv					
v					
	Total				
Part B – Capital & Financial Information of the proposed VASP:					

1.	**Authorised Capital:**	Authorized Capital of the Company is Rs…… divided in to ……. Shares of Rs…….. each
2.	**Paid-up Capital:**	Paid up Capital of the Company is Rs…… divided in to ……. Shares of Rs…….. each
	Capital and liquidity attestation (Regulations 31 and 32; Schedule I). (a) Does the Applicant confirm that it will meet, and maintain on an ongoing basis, the minimum paid-up capital and any applicable prudential add-ons for its intended Licence Category or Categories as set out in Schedule I and regulation 31, and will notify the Authority of any material deviation or anticipated breach in accordance with these Regulations? ☐ YES ☐ NO (b) Does the Applicant confirm that it will meet, and maintain on an ongoing basis, the minimum liquidity requirement / Net Liquid Assets requirement applicable to its intended Licence Category or Categories under regulation 32, and will notify the Authority of any material deviation or anticipated breach in accordance with these Regulations? ☐ YES ☐ NO (c) Supporting evidence attached (tick all that apply): ☐ Latest audited financial statements (if applicable) ☐ Evidence of capital sources and availability (bank letter / group support / injection plan) ☐ Capital maintenance arrangements and governance (board resolution / policy) ☐ Liquidity methodology and assumptions ☐ 12-month forward-looking capital and liquidity projection (base case and stress scenario) Certification: I, the undersigned, being duly authorised by the Applicant, certify that the statements above are true, complete and accurate to the best of my knowledge and belief. Name: _____ Title: _____ CNIC/Passport No.: _____ Signature: _____ Date: _____	

Part C - Financial projections and Business Plan of the Proposed VASP	
1.	**Business Plan (Please annex the Business Plan in detail, as an Annexure)**
i.	Financial projections: Three-year financial projections including stress and downside scenarios, with key assumptions for which licence is been sought.
ii.	Details of business model (including target market, branding, marketing strategy, distribution strategy, geographical analysis, details of proposed partners etc.) Description of proposed Virtual Asset Services; and where applicable, a high-level description of the intended custody model, including whether the Applicant will operate (i) self-custody (Applicant-controlled keys), (ii) third-party custody, or (iii) a hybrid model; and whether custody arrangements will be structured as omnibus wallets, segregated wallets, or a combination thereof, including any proposed use of sub-custodians or group entities.

2.	**Jurisdictional delivery model and channels** Provide a description of how the proposed Virtual Asset Services will be delivered, including: (a) whether services will be provided onshore in Pakistan, cross-border into Pakistan, and/or through digital channels (website, mobile application, API, affiliates, or other online distribution); (b) the proposed legal structure and jurisdictional model (including the legal entity/entities providing the services in Pakistan, and the jurisdictions in which those entities are already incorporated and/or regulated); (c) the intended target customer base by geography and customer type (retail/professional/institutional), and how geo-targeting/geo-blocking and onboarding eligibility controls will be implemented; (d) the location of key operational functions relevant to the Pakistan business (including customer onboarding, compliance, transaction monitoring, custody/key management, customer support, and complaint handling); and (e) any planned use of group entities, branches, agents, affiliates, third-party distributors, or outsourcing arrangements that support cross-border delivery.

Part D – Sponsors /CEO/Directors of the Proposed VASP

1. Details of CEO/Directors /Sponsors information:

S. No.	Name in full	CNIC/NICOP or Passport No (in case of foreigner) (Annex a copy as Annexure)	Nationality	Designation (Director/ Subscriber/ CEO) Please specify	Nature of directorship (appointed, nominee/ independent/ other)	Residential address	Contact Number	Active Tax Payer	Academic Qualification (Highest along with Annexure Reference):	Annexure Reference
i										
ii										
iii										
iv										
v										

Please provide the experience for each person in the following format as Annexure along with copies of experience certificates
(Positions held during the last 10 years along with name and address of company/ institution)
Information to be provided on the following sample format:

2. Name of CEO/Director/Sponsor/Compliance Officer

Sr. #	**Name of Organization**	**Designation**	**Period (from oldest to Current)**	
			From	**To**

i	Company A			
ii	Company B			
iii	Company C			

3.	**Details of Director/Shareholder's having 10% or more shareholding in other businesses:**			
	Name of Director/Shareholder	**Business Name**	**Address**	**Shareholding**
i.				
ii.				

4.	**Details of material legal proceedings/insolvency/bankruptcy/penal actions against Applicant/CEO/Directors/Sponsors**			
	Name of Person	**Legal Proceedings**	**Insolvency/bankruptcy**	**Penal actions**
i				

5.	**Details of the affiliation and outsourcing contracts:**			
	Name of Person	**Nature of Affiliation**	**Name and Nature of Agreement**	**Validity**
i.				

Part E – Declarations and Confirmations

We, hereby declare that:

1. The information supplied in this application and accompanying documents is true, complete, and correct to the best of our knowledge.
2. We undertake to comply with all provisions of the applicable regulatory framework.
3. We understand that any false or misleading information may result in rejection or cancellation of license.
4. We have not been associated with any illegal banking business, deposit taking or financial dealings;
5. We have not been involved in material or willful default in repayment of loans or financial obligations;
6. Neither we nor companies in which we are director or substantial shareholder have defaulted in paying taxes as on the date of application;
7. We have not been sponsor, director or chief executive or managing director of a defaulting company;
8. We have never been convicted of fraud or breach of trust or of an offence involving moral turpitude or removed from service for misconduct; and
9. We have neither been adjudged as insolvent nor have defaulted in making payments, to the creditors;
10. The directors of sponsoring company and the applicant shall inform the Authority in case of any change in the sponsors/ Controlling shareholders of the sponsoring company.
11. The applicant, its directors, sponsors, controllers, MD and Key Individuals are fit and proper and are in compliance with all the requirements for grant of a licence under the Pakistan Virtual Asset Services Regulations, 2026.
12. The applicant its directors and sponsors do not have controlling interest in any other company holding license as a VASP
13. The managing director of the applicant does not hold such office in any other company;
14. The applicant's (proposed VASP) ultimate beneficial owners have not been convicted in any predicate offences relating to AML/CFT/PF laws or any other criminal offence.
15. That the names have not been placed on the United Nations Security Council Consolidated List or any other list of banned, proscribed/designated or blacklisted, disqualified individuals or other entities maintained by the Government of Pakistan or by any foreign government or regulator/ authority.
16. We hereby authorize the person (name mentioned hereunder) as authorized representative to sign the application/documents/responses/information to the PVARA (Attach an Authority Letter/Board of Directors' resolution duly signed by all the persons, as an Annexure).

Authorized Signatory of Applicant Company

Name: _____ CNIC No.: _____

Designation: _____ Signature & Date: _____

Company Seal / Stamp

Part F - Additional Information/Documents to be Submitted along with the Licensing Application

1. Certificate of Incorporation of the Company under the Companies Act, 2017.
2. List of the Shareholders and Ultimate Beneficial Owners (UBOs).
3. List of Proposed Directors and the Key Individuals.
4. Affidavit by every sponsor, Controller, Directors and Key Individuals that they meet the fit and proper criteria as specified in these regulations. (Annexure-A)
5. Evidence of paid-up capital injected and maintained in the Applicant's bank account(s) in Pakistan, and evidence of the source of funds, in the manner specified by the Authority, subject to repatriation and availability arrangements acceptable to the Authority.
6. Documentary Evidence of Source of Funds.
7. Organizational Structure, including a list of Associated Companies, as defined in the Companies Act, 2017.
8. Official Website Address of the Person.
9. Copies of Insurance Contracts for Professional Indemnity Insurance and Commercial Crime Insurance, and shall become effective prior to commencement of regulated activity.
10. Wind-Down Plan.
11. Outsourcing Policy.
12. Anti-Bribery and Corruption Policy.
13. Conflict of Interest Policy.
14. Mechanism for the Protection of Personal Data.
15. Policy ensuring compliance with FATF Recommendations on Virtual Assets and AML/CFT/PF requirements.
16. Marketing Policy and Plan.
17. Market Conduct Policy.
18. Records Management Policy.
19. Technology Infrastructure Design.
20. Technology Governance and Risk Assessment Framework.
21. Business Continuity Management and Disaster Recovery Plan.
22. Key and Wallet Management Policy (where applicable).
23. Information Security Policy.
24. Cybersecurity Policy.
25. Complaint Handling Mechanism.
26. Insider List.
27. Compliance Manual and Mechanism for ensuring adherence to applicable laws and regulations.
28. Mechanism for the Protection and Segregation of Clients' Assets (where applicable).
29. Risk Management Framework and Methodology.
30. List of material regulatory actions, enforcement matters, or supervisory findings in the last five (5) years relating to Virtual Asset Services. (applicable if the Person or Group is already operating locally or internationally).
31. List of Regulatory Approvals for providing Virtual Asset Services in other jurisdictions (applicable if the Person or Group is operating in other jurisdictions).
32. Client Onboarding Process and Consumer Protection Policy.
33. Virtual Asset Listing Policy (where applicable).
34. Description of the Type(s) of Virtual Assets to be Managed (where applicable).
35. Any other information as may be required by the Authority.

Annexure A

Affidavit

Affidavit by every sponsor, Controller, Directors and Key Individuals

Before the Pakistan Virtual Asset Regulatory Authority

(On Stamp Paper of Appropriate Value)

I, _____ son/daughter/wife of _____ adult, resident of _____ and holding CNIC/ Passport No. _____ do hereby state on solemn affirmation as under: -

1. That I am eligible for the position of _____according to the Fit and Proper Criteria for the position of _____, annexed to the Pakistan Virtual Asset Services Regulations, 2026;

2. That I hereby confirm that the statements made, undertakings provided and the information given by me including that required under Schedule II is correct and that there are no facts which have been concealed;

3. That I have no objection if the Pakistan Virtual Asset Authority requests or obtains information about me from any third party;

4. That I undertake to bring to the attention of the Pakistan Virtual Asset Authority any matter which may potentially affect my status for the position of _____ as per the Fit and Proper Criteria annexed to the Pakistan Virtual Asset Services Regulations, 2026;

5. That all the documents provided to the Pakistan Virtual Asset Authority are true copies of the originals and I certify them to be true copies thereof;

6. That I have not availed any write off from any financial institution during the last five years;

7. That I have not defaulted against any Finance obtained from any financial institution;

8. That I have not been placed on Exit Control List (ECL);

9. That I have not been convicted from any Court of Law or any plea bargain with National Accountability Bureau (NAB);

10. I hereby confirm that the companies, firms, sole proprietorship etc. where I am a chief executive, director (other than nominee director), controller, owner or partner etc. has

no overdue loan payment and instalment outstanding towards banks or other financial institutions;

11. I have not been associated with any illegal banking business, deposit taking or financial dealings;

12. Neither I nor companies in which I am a director or controller has defaulted in paying taxes as on the date of application;

13. I have never been convicted of fraud or breach of trust or of an offence involving moral turpitude or removed from service for misconduct;

14. I have neither been adjudged an insolvent nor has defaulted in making payments, to my creditors;

15. I do solemnly declare that no investigations have been initiated against me by any Law Enforcement Agencies.

_____

DEPONENT

The Deponent is identified by me

Signature _____

ADVOCATE

(Name and Seal)

Solemnly affirmed before me on this _____ day of _____ at _____ by the Deponent above named who is identified to me by _____, Advocate, who is known to me personally.

Signature_____

OATH COMMISSIONER FOR TAKING AFFIDAVIT

(Name and Seal)]

FORM-II
[see regulation 7]

APPLICATION FOR LICENSE AS A VIRTUAL ASSET SERVICE PROVIDER

Date: _____

To
The Pakistan Virtual Asset Regulatory Authority (the Authority)
Islamabad, Pakistan

Subject: Application for License as a Virtual Asset Service Provider

Dear Sir/Madam,

We, the undersigned sponsors and directors (the Applicants), hereby apply for the grant of a License in accordance with regulation 7 of the Pakistan Virtual Asset Services Regulations, 2026, under the company name * ---------- (the **VASP**) for the purpose of undertaking the following [Category(ies) of Licence / VA Activity(ies)]: ----------.**

The information and documents required under the Annexure to Form I, duly completed, verified and signed by all Applicants, are enclosed. This application is submitted pursuant to NOC granted to the VASP on -------.

We solemnly declare that the information provided in this application and in the enclosed Annexure is true, complete and correct to the best of our knowledge and belief, and that no material information has been concealed or omitted.

We undertake to keep the information and documents submitted under this application up to date and to notify the Authority in writing of any material change thereto without Undue Delay and in accordance with requirements in these Regulations.

Evidence of payment of the prescribed processing fee in the amount of PKR [x] (receipt/reference no. [x]), paid on [x] through [bank/PSID/channel], is enclosed.

Yours faithfully, ----------

Name: [●]

CNIC/Passport No.: [●]

Signature: [●]

(On behalf of all Applicants)

Signed by all sponsors and directors (Applicants)

*Proposed name of the company

**Category(ies) of Licence / VA Activity(ies) to be undertaken

FORM -III
[see regulation 9(1)]

PAKISTAN VIRTUAL ASSETS REGULATORY AUTHORITY

Islamabad,
Date _____
Licence No. _____

LICENCE TO CARRY OUT VIRTUAL ASSET SERVICES

The Pakistan Virtual Assets Regulatory Authority (the Authority), having considered the application submitted under regulation 7 of the Pakistan Virtual Asset Services Regulations, 2026 by [Full legal name of company], a company incorporated under the Companies Act, 2017 (SECP Registration No. [x]) with its registered office at [x] (the Licensee), and being satisfied that the Licensee meets the eligibility requirements, hereby grants this Licence pursuant to regulation 9(1) of the Pakistan Virtual Asset Services Regulations, 2026 authorizing the Licensee to carry on the following Category(ies) of Licence / VA Activity(ies):

- [●]
- [●]
- …

This Licence takes effect on [effective date] and shall remain valid [until revoked/suspended], subject to the Virtual Assets Act, 2026, these Regulations and any additional conditions imposed by the Authority by written direction in accordance with the Act and these Regulations.

This Licence is issued to the Licensee only and is non-transferable.

Authorised Officer
Pakistan Virtual Asset Regulatory Authority

Official Seal and Stamp

*Authorised Virtual Asset Services / VA Activities as specified above.
**Name of the Licensee (company).

SCHEDULE-I
[See regulations 5(2), 7, 9, 10(3), and 31]

Minimum Paid-Up Capital and Prudential Conditions

S. No.	Category of Virtual Asset Service	Type of Company & Minimum Number of Directors	Minimum Paid up Capital (PKR)	Number of directors with relevant experience of at least five years at a senior management level for a particular category of Virtual Asset Services, or related field.	Submission of Financial Statements
1.	Advisory Services	A Company incorporated under the Companies Act, 2017 with minimum number of 3 Directors	15,000,000	As per regulations 20–22 and Schedule-II	As per the requirements of the Companies Act, 2017
2.	Broker-Dealer Services		75,000,000		
3.	Custody Services		200,000,000		
4.	Exchange Services		500,000,000		
5.	Lending and Borrowing Services		500,000,000		
6.	Virtual Asset Derivatives Services		500,000,000		
7.	Virtual Asset Management and Investment Services		200,000,000		
8.	Virtual Asset Transfer and Settlement Services		200,000,000		
9.	Virtual Asset Issuance Service - Fiat-Referenced Token Issuance Services		300,000,000		
10	Virtual Asset Issuance Service - Asset-Referenced Token Issuance Services		300,000,000		
11	Mining Related Virtual Asset Services		500,000,000		

Unless expressly stated otherwise, the governance conditions in this Schedule (including board composition and experience requirements) apply to all Licence Categories.

SCHEDULE-II
FIT AND PROPER CRITERIA

[see regulation 8, 9]

APPLICATION AND SCOPE

(1). The Fit and Proper Criteria in relation to the VASP is applicable to the following persons:

(a) Controller, whether Individual or Body Corporate.
(b) Directors.
(c) Key Individuals.
(d) Sponsors
(e) Managing Director/Chief Executive Officer

(2) A proposed director or managing director shall not assume the charge of office until their appointment has been approved by the Authority.

(3) The application for seeking approval of the Authority under clause (2) shall be submitted along with the requisite information as specified in Part D of ANNEXURE TO FORM-I along with requisite attachments and an Affidavit as specified in Annexure "A".

(4) The appointment of Key Individuals (other than Managing Director and Directors) does not require the approval of the Authority; however, the Virtual Asset Service Provider shall ensure at the time of appointment of Key Individual (other than CEO and Directors) that such person is compliant with the Fit and Proper Criteria.

(5) The fitness and propriety of Key Individuals shall be assessed by taking into account all the relevant factors including but not limited to the following:

(a) Integrity and track record;
(b) Financial soundness;
(c) Professional Competence and Experience; and
(d) Conflict of interest with the business of the VASP and its customers.

Provided that 5 (c) and (d) may not be considered while assessing the fitness and propriety of promotors and controllers.

Provided further that in case the Controller, being a sponsor and major shareholder, is a body corporate, in addition to the fit and proper criteria, the Authority shall assess the corporate behaviour of the said body corporate, as well as the integrity and track record of the ultimate beneficial owners of such body corporate.

Explanation: For the purpose of this clause, the term "ultimate beneficial owner" shall have the similar meaning as defined under the AML Act, 2010 and any rules, regulations, directions/guidelines issued by the competent Authority thereunder as applicable.

(6) In assessing whether an individual is a Fit and Proper Person, the Authority will:

(a) consider all relevant factors in assessing the application of the fit and proper principles contained herein on a case-by-case basis, taking into account:
    i. the conditions of the License held by the VASP;
    ii. the business model of the VASP;
    iii. the market within which the VASP operates;
    iv. the governance structure, the internal control systems and the competence of the VASP's Staff;
    v. decisions made by any other authority or regulatory body in respect of that individual, whether in Pakistan or in other jurisdictions;
    vi. the state of affairs of any other business which that the individual carries on or proposes to carry on.

(7) The Fit and Proper Criteria is perpetual in nature and the person subject to Fit and Proper Criteria shall ensure compliance with the provisions of Fit and Proper Criteria.

(8) All person's subject to Fit and Proper Criteria shall report any change with reference to their fitness and propriety to the Company Secretary of the VASP within three business days of such change taking effect and the Company Secretary subject to Fit and Proper Criteria shall within a period of seven business days from the date of receipt, report the same to the Authority.

(9) The VASP shall monitor whether any change in the status of its managing director, directors and key individuals is contrary to the requirements of the Fit and Proper Criteria. In case of any change in status, results in non-compliance with the Fit and Proper Criteria, the Board of Directors of the VASP shall immediately stop the person from performing his assigned functions, shall inform the Authority and initiate the process for replacement of the individual with a fit and proper individual.

(10) Any violations or circumvention of the Fit and Proper Criteria shall be dealt with under the provisions of the Act.

ASSESSMENT OF FITNESS AND PROPRIETY

(i) Integrity, and track record: A person shall not be considered Fit and Proper if he:

(a) has been convicted of an offence involving moral turpitude (both inside and outside Pakistan).
(b) has been convicted of any offence including mismanagement, financial or business misconduct or, fraud (both inside and outside Pakistan).
(c) has been convicted, after conducting an inquiry, by the Authority or any other regulatory or professional body or government agency.
(d) has been subject to an ongoing investigation by the Authority or any other regulatory body on matters relating to financial fraud, financial misconduct, market abuse, violation of the Virtual Asset Act or law administered by any other regulatory body or any other matter raising concerns on the integrity of the person.
(e) actively involved in the management or decision making of a company or firm whose registration or license has been revoked/cancelled or which has gone into liquidation or other similar proceedings due to mismanagement of affairs, financial misconduct or malpractice.

Provided that in case of non-executive nominee directors representing institutional interest and who otherwise do not have any personal interest, the Authority may,

after seeking explanation and if satisfied, after reasons to be recorded in writing, relax this requirement on case-to-case basis subject to such conditions as it may deem fit.

(f) Is ineligible, under the Companies Act, 2017, or any other legislation or regulation, from acting as a director or serving in a managerial capacity of a company.
(g) debarred from acting as director of the Company.
(h) has been convicted in criminal breach of trust, fraud, offences of terrorism financing or money laundering including predicate offences as provided in the Anti-Money Laundering (AML) Act, 2010, laws make thereunder, or any other AML/ CFT (Countering Financing of Terrorism) requirements notified by the Authority, and is a proscribed/designated persons, either convicted or not, "as mentioned in the notifications issued by the Ministry of Foreign Affairs on United Nations Security Councils Resolutions or intimation from National Counter Terrorism Authority/ Law Enforcement Agencies/ Home Departments of Provinces/ Ministry of Interior.
(i) entered into a plea bargain arrangement with the National Accountability Bureau
(j) entered into scheme of compromise or arrangement with its creditor.
(k) in case of Controller or major shareholder, does not have the requisite disclosed and verifiable financial resources.

(ii) Financial Soundness: In assessing financial soundness of the person, the following shall be considered:

(a) Whether the person is active tax payer and his/her name is appearing on active tax payer list of the tax authorities.
(b) whether the person has been declared by a court of competent jurisdiction as defaulter in repayment of loan or financial obligation to a financial institution;
(c) whether any instance of overdue or past due payment to a financial institution, irrespective of amount, is appearing in the overdue column of latest CIB report of the person and of the associated companies, firms, sole proprietorship etc. where the person is a managing director, director (other than nominee director), owner or partner etc.
Provided that the Authority shall provide an opportunity of making representation to the person in case of overdue or past due payment;

Provided further that the following exceptions may be granted by the Authority for the purpose of this sub-clause in case where: -

(i) Amount overdue is under litigation and the same is also appearing as amount under litigation in the CIB report; and
(ii) No overdue payment appearing in the overdue column in the subsequent latest CIB report.

(d) Whether Lender has history of multiple loans being written-off provided to the person and no write-off is appearing in CIB report of the person.
(e) Whether the person has been declared bankrupt by any court inside or outside Pakistan.
(f) Whether the person has applied to be adjudicated as an insolvent and his application is pending.
(g) whether the person is an un-discharged insolvent

(iii) Professional Competence and Experience: In assessing Professional Competence and Experience of the person, the following shall be considered:

(a) the directors should be individuals having management or business experience of at least five years at a senior level;

Provided that this condition shall not apply in case of sponsor directors.

(b) The directors shall have experience and knowledge in any related profession such as finance, banking, accounting, law, or information technology etc.

(c) The Managing Director shall possess, at a minimum, a Master's degree in business, Finance, digital finance, Information Technology, Economics, Accounting, or any other related discipline, or shall be a member of a recognized professional body such as the CFA Institute, the ICAP, the Institute of Chartered Accountants in England and Wales (ICAEW), the Association of Chartered Certified Accountants (ACCA), the Certified Public Accountants (CPA), the Global Association of Risk Professional or any other recognized professional body.

(d) The Managing Director shall have relevant professional experience at senior management position within the financial or information technology industry, including at least two (2) years of experience in matters relating to blockchain technology, virtual assets, virtual asset services, or related domains.

(e) the managing director should have demonstrated, through his qualification and experience, the capacity to successfully undertake the cognate responsibilities of the position; and

(f) where the Authority is not satisfied on sufficiency of the suitability criteria, it may conduct an interview of the managing director to assess his/her suitability for the position.

(g) Executive Director of a Virtual Asset Service Provider shall possess at a minimum, a Master's degree in Finance, Information Technology, Economics, Accounting, or any other related discipline, or shall be a member in good standing of a recognized professional body such as the CFA Institute, the ICAP, the Institute of Chartered Accountants in England and Wales (ICAEW), the Association of Chartered Certified Accountants (ACCA), the Certified Public Accountants (CPA), the Global Association of Risk Professional or any other recognized professional body.

(h) Executive Director shall have professional experience at senior management position within the financial or information technology industry, including at least one (1) year of experience in matters relating to blockchain technology, virtual assets, virtual asset services, or related domains.

(i) Key Individuals excluding Managing Director and Directors should possess relevant qualification and shall have relevant work experience at a senior position.

(iv) Conflict of interest

The directors, controller, sponsors, Managing Director, and Key Individuals of the Virtual Asset Service Provider shall provide an undertaking to the Board of Directors, to identify,

manage, and disclose any Conflicts of Interest, and to act at all times in the best interests of both the Customers and the VASP.

-sd-
Mariam Mumtaz
Joint Secretary (Regulatory Authorities)

The Gazette of Pakistan Extraordinary

PART II

Notification

PAKISTAN VIRTUAL ASSET REGULATORY AUTHORITY

NOTIFICATION

Islamabad,

August 21, 2026

S.R.O. 1420(I)/2026. In exercise of the powers conferred by section 68 of the Virtual Assets Act, 2026, the Pakistan Virtual Asset Regulatory Authority is pleased to make public the following

Pakistan Virtual Asset Services Activity Specific Regulations, 2026 for licensing and regulation of VASPs carrying out one or more Virtual Asset Services as stated by Schedule 1 of the Virtual Assets Act, 2026 and any other service as may be notified by the Federal Government and subsequently included in Schedule I in accordance with section 18 of the Act:

GENERAL REGULATIONS
[APPLICABLE ON ALL VIRTUAL ASSET SERVICE PROVIDERS (VASPs)]

1. Short title and commencement. — (1) This Regulation shall be applicable to all the VASP activities requiring or holding a license under the Virtual Assets Act, 2026 (the Act).

(2) These General Activity-Specific Regulations shall be read together with the Act, the Pakistan Virtual Asset Services Regulations, 2026 and each applicable individual Activity-Specific Regulation.

(3) In the event of an inconsistency

(a) the Act shall prevail over all subordinate instruments;

(b) the Pakistan Virtual Asset Services Regulations, 2026 and the Pakistan Virtual Asset Services Activity Specific General Regulations, 2026 shall prevail over an individual Activity-Specific Regulation, unless the individual Activity-Specific Regulation expressly identifies a specific provision intended to apply to that Licence Category notwithstanding the general provision.

(4) Unless otherwise expressly stated, this Regulation shall be applied by a Licensee, and administered by the Authority, in a manner proportionate to the nature, scale, complexity, risk profile, and Client base of the relevant business.

(5) A Licensee that offers margin, leveraged, derivative, lending or borrowing products or services shall establish, maintain and enforce prudent exposure, concentration, leverage and

counterparty limits proportionate to the nature, scale, complexity and risk profile of those products or services. The limits shall be reasonably designed to manage risks to Customers and the Licensee and to prevent material risks to market integrity or financial stability.

2. Licence perimeter. — (1) A Licensee shall not rely on a Licence Category to carry on any activity that falls within another Licence Category, except where such activity is expressly permitted/licensed in accordance with the Virtual Assets Act, 2026 and the Regulations and any binding direction or other instrument issued by the Authority under express authority conferred by the Act. Any binding direction or other instrument shall identify its statutory basis, binding status and effective date. Guidance may explain the Authority's supervisory expectations but shall not create a generally applicable mandatory obligation unless issued under express authority conferred by the Act.

(2) A Licensee shall not structure or operate its business in a manner that circumvents the requirements applicable to any other Licence Category under the Act or the Regulations.

(3) Where a product or service combines features falling within more than one Licence Category, the Licensee shall obtain license of that specific activity.

(4) A broader reference to Schedule 1 of the Act shall be applied when determining the scope of regulated activities.

(5) A Licence Category authorizes a Licensee to carry on an activity that is reasonably necessary or ancillary to an authorised Virtual Asset Service, provided that the activity.

(a) is subordinate to the authorised Virtual Asset Service

(b) is not separately marketed, offered or remunerated as a standalone service

(c) does not constitute a material independent business line or materially alter the Licensee's risk profile; and

(d) is conducted in accordance with the safeguarding, conduct, AML/CFT/CPF and other regulatory requirements relevant to the risks arising from that activity

A Licensee shall identify and describe any activity that it proposes to conduct in reliance on this provision in its Licence application or, where the activity is proposed after the grant of the Licence, in an application to vary the scope of its approved activities. The Licensee shall obtain the Authority's written approval before undertaking the activity. The Authority may approve an activity individually or by reference to a defined class or description of incidental activities and shall document the approval and any applicable conditions as part of the Licensee's regulatory record. Such approval shall not, by itself, require the Licensee to obtain an additional Licence Category.

The Authority may require an additional Licence Category where the scale, frequency, risk or commercial significance of the activity causes it to constitute a substantive Virtual Asset Service in its own right.

3. Multi-activity obligations. — (1) A Licensee holding more than one License Category shall comply with each applicable Activity-Specific Regulation and with the general requirements in respect of all activities carried on.

(2) All activities carried on under these Regulation shall be subject to the Client protection outcomes applicable to that activity, applied proportionately to its nature, scale and purpose, and shall not be structured or operated so as to circumvent applicable requirements.
(3) A Licensee shall not use, lend, pledge, rehypothecate, stake, encumber or otherwise dispose of Client Assets solely by virtue of its Licence. Any such use shall only be undertaken with the Client's prior written explicit and informed consent and the Licensee shall clearly disclose the nature of the activity, the associated risks, any withdrawal restrictions, and the basis on which rewards, proceeds, losses and liabilities are allocated.
(4) A Licensee carrying on multiple activities shall maintain effective controls to distinguish those activities and to manage conflicts, disclosures and conduct obligations appropriately.

4. Staff competency framework. — (1) A Licensee shall ensure that every person involved in the provision, supervision, approval, control, oversight or review of any Virtual Asset service is competent, suitably trained and appropriately supervised, having regard to the nature of the service provided and the risks of the products and activities concerned.
(2) A Licensee shall maintain a documented competency framework covering at least
(a) minimum knowledge and skills requirements for relevant roles;
(b) initial and ongoing training, including training on market conduct, conflicts of interest, AML/CFT/CPF obligations, technology and operational risks;
(c) assessment and periodic reassessment of competence; and
(d) escalation, restriction and remediation procedures where competency concerns arise.
(3) A person shall not perform a role relevant to a Virtual Asset service unless the Licensee is satisfied that the person is competent to do so and is subject to appropriate supervision and conduct controls.
(4) A Licensee shall ensure that remuneration, incentives, targets and performance management structures do not create an undue incentive to act in a manner inconsistent with the best interests of Clients or with the Licensee's obligations under the Act, the Regulations and any binding direction or other instrument issued by the Authority under express authority conferred by the Act. Any binding direction or other instrument shall identify its statutory basis, binding status and effective date. Guidance may explain the Authority's supervisory expectations but shall not create a generally applicable mandatory obligation unless issued under express authority conferred by the Act.

5. Outsourcing obligations. — (1) A Licensee shall not outsource the principal activity for which it is licensed and ensure that any outsourcing or third-party arrangement relating to its licensed activities complies with the outsourcing, governance, technology, cybersecurity and operational resilience requirements under the Regulations and any applicable guidance issued by the Authority.

(2) A Licensee may outsource any function, including a material function and on a cross-border or intra-group basis, other than core/principal activity, provided that the arrangement does not materially impair,

(a) the Licensee's ability to comply with its legal and regulatory obligations

(b) the effectiveness of its governance, risk management and internal controls

(c) the Authority's ability to supervise the Licensee or obtain timely access to relevant information, systems, premises and personnel

(d) the continuity and security of the relevant Virtual Asset Service

The Licensee shall remain fully responsible and accountable for all outsourced functions and shall conduct appropriate due diligence, maintain written outsourcing arrangements, oversee service-provider performance and maintain appropriate business-continuity and exit arrangements. Material outsourcing arrangements shall be subject to any applicable notification or prior-approval requirements prescribed by the Authority.

(3) Principal Licensed Activity means the provision by a Licensee, in its capacity as the contracting and regulated service provider, of a Virtual Asset Service specified in its Licence, together with the assumption of the corresponding legal and regulatory responsibility towards Customers and the Authority. A Principal Licensed Activity does not include each individual operational, technological, administrative, control or supporting function used in the delivery of that Virtual Asset Service, including where the function is necessary, recurring or material to its delivery, provided that the Licensee retains effective direction and control, remains fully responsible and accountable, and complies with the applicable outsourcing requirements. Where a Licensee requires clarification as to whether a proposed outsourcing arrangement involves the Principal Licensed Activity, it may seek written clarification from the Authority before entering into or implementing the arrangement. The request shall describe the function, the proposed service provider, the allocation of responsibilities and the arrangements through which the Licensee will retain effective direction, control and regulatory accountability.

(4) A Licensee shall remain fully responsible for compliance with the Act, the Regulations and any binding direction or other instrument issued by the Authority under express authority conferred by the Act. Any binding direction or other instrument shall identify its statutory basis, binding status and effective date in respect of any function, process or service outsourced to a third party, regardless of the terms of the outsourcing arrangement. Guidance may explain the Authority's supervisory expectations but shall not create a generally applicable mandatory obligation unless issued under express authority conferred by the Act.

(5) Where a third party provides material components of a licensed service, including Client interfaces, suitability tools, profiling tools, technology infrastructure, algorithmic tools, risk management systems, custody infrastructure, AML/CFT systems or other components that are material to the Licensee's regulated activities, the Licensee shall:

(a) assess the materiality of the outsourcing arrangement in accordance with criteria specified by the Authority;

(b) conduct appropriate due diligence before entry into the arrangement and on an ongoing basis;

(c) ensure that the arrangement includes appropriate rights of access, audit, oversight, information, step-in and termination; and

(d) notify the Authority of material outsourcing arrangements in accordance with the Regulations.

(6) A Licensee shall maintain and keep current a register of material outsourcing and third-party arrangements, including details of the function outsourced, the service provider, and the risk assessment conducted.

6. Operational resilience. — (1) A Licensee shall ensure that its systems, controls and infrastructure meet operational resilience, availability and recovery standards proportionate to the criticality of the services provided.

(2) A Licensee shall maintain contingency procedures for material outages, technology incidents, chain disruption, banking rail disruption, counterparty failure, routing failures, wallet disruption, chain reorganization, chain congestion, stale status information and other events that could materially affect the provision of services to Clients.

(3) A Licensee shall maintain business continuity, backup and disaster recovery arrangements sufficient to support the continuity of critical functions, consistent with the requirements of the Regulations.

(4) Material incidents that affect the provision of licensed services shall be communicated to affected Clients and to the Authority without undue delay where the incident is material, in accordance with the incident reporting requirements under the Regulations.

(5) A Licensee shall disclose material operational, technology, network, settlement, third-party and Virtual Asset infrastructure risks relevant to the services provided, including risks relating to congestion, chain reorganizations, finality, forks, validator dependencies, bridge risks, smart contract vulnerabilities and third-party service providers where applicable.

7. Reporting to the Authority. — (1) A Licensee shall notify the Authority without undue delay of any material failure, deficiency, control breach, misconduct or other event that is required to be notified under the Act, the Regulations or any applicable Regulation.

(2) The Authority may require a Licensee to provide such information, reports, management attestations, remediation plans, file reviews or thematic data as it reasonably considers necessary for supervisory purposes.

(3) A Licensee shall maintain records sufficient to demonstrate compliance with the Regulations and all applicable Activity-Specific Regulations, and shall make such records available to the Authority upon request.

(4) Records required to be maintained under any Activity-Specific Regulation shall be retained for at least seven (7) years, or such longer period as may be required under the Act, the Regulations, AML/CFT/CPF requirements, or any written direction of the Authority.

(5) A Licensee shall notify the Authority without undue delay of any material failure, deficiency, control breach or misconduct affecting the provision of the licensed activity,

including any material suitability failure, systemic mis-selling issue, major model or algorithm defect, or material conflict of interest issue.

(6) A Licensee shall document materiality assessments concerning matters potentially notifiable under the Act or these Regulations and shall make them available to the Authority upon reasonable request. The annual return shall include only matters determined to be Material, the corresponding notification and any material remediation status. Preliminary assessments of matters determined not to be Material need not be submitted routinely.

(7) The Authority may require the Licensee to provide such information, reports, management attestations, remediation plans, file reviews or thematic data as it reasonably considers necessary for supervisory purposes.

8. Breach and enforcement. — (1) A breach of these Regulations shall constitute a breach of the Licensee's obligations and shall be taken into account for licensing, conduct, prudential and supervisory purposes.

(2) Nothing in this Regulation limits the application of any other provision of the Act or the Regulations, including provisions relating to Client categorization, market conduct, disclosures, complaints handling, AML/CFT/CPF, governance, technology, operational resilience, safeguarding, reporting or enforcement.

(3) The Authority may exercise any power available to it under the Act and the Regulations in relation to a breach, including the power to impose conditions, require remediation, issue directions, restrict activities, impose penalties, or suspend or revoke a licence, as applicable.

(4) The Authority may, on application or on its own initiative, modify or waive the application of a provision of this Regulation in whole or in part in respect of a specified Licensee, class of Licensee, product, service, Client category or business model, where the Authority is satisfied that the underlying regulatory objectives remain adequately met.

(5) The Authority may, by written order recording its reasons, suspend or cancel a licence in accordance with section 23 of the Act, where it is satisfied that such action is necessary in the public interest.

Advisory Services Regulations

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Advisory Services Regulation, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026.

(2) In this Regulation:

(a) "**Advisory Services**" means the activity described in Schedule I of the Act;

(b) "**General Market Commentary**" means non-personalized information, market colour, factual material, research, education, or commentary that is not directed to the circumstances of a particular Client and does not amount to a Personalized Recommendation;

(c) "**Personalized Recommendation**" means a recommendation presented as suitable for, or based on the circumstances of, a particular Client in relation to one or more actions or transactions involving Virtual Assets, and includes such recommendation whether delivered by a natural person or generated through an automated tool, algorithm or other system; and

(d) "**Suitability Assessment**" means the assessment required under this Regulation to determine whether a Personalized Recommendation is suitable for the relevant Client.

(3) For the avoidance of doubt, General Market Commentary, factual information and educational material do not, of themselves, constitute Advisory Services unless they amount in substance to a Personalized Recommendation.

3. Nature of Advisory Services. — (1) A Licensee providing Advisory Services shall provide recommendations honestly, fairly, professionally and in the best interests of the relevant Client. VASPs shall, in the course of providing Advisory Services covering personalized recommendation, assess the range of Virtual Assets available to ensure that the client's investment objectives are met.

(2) A Licensee shall not represent that it provides independent, unrestricted, market-wide or unbiased advice unless:

(a) the scope of products, venues, issuers and counterparties considered is sufficiently broad to support that representation; and

(b) the representation is accurate, substantiated and kept under periodic review.

(3) Where the scope of the Licensee's advice is limited by product range, issuer universe, distribution arrangements, affiliated products, venue access, jurisdictional constraints, or other commercial limitations, the Licensee shall clearly disclose that limitation to the Client before the relevant recommendation is acted upon.

(4) A Licensee shall ensure that Advisory Services are clearly distinguished from execution-only services, dealing as principal, placement services, marketing communications, and general education or research.
(5) A Licensee shall not structure its Advisory Services in a manner that results in de facto execution, order routing control, or discretionary management of Client assets without the relevant Licence Category and compliance with the applicable Regulation.

4. Policies, procedures and governance. — (1) In addition to all other applicable requirements under the Regulations, a Licensee providing Advisory Services shall establish, implement, maintain and enforce written policies and procedures appropriate to the nature, scale and complexity of its business, including at least policies and procedures relating to:

(a) the basis on which advice is formulated;

(b) the collection, verification and periodic updating of Client information relevant to suitability;

(c) the approval, review and use of research, market data, third-party information, models, algorithms, scoring tools and other inputs used in the provision of advice;

(d) conflicts of interest, inducements, referral arrangements and staff personal dealing;

(e) controls to distinguish General Market Commentary from Personalized Recommendations;

(f) record-keeping and surveillance of Advisory Services activity; and

(g) review, escalation and remediation of any deficiency identified in the advisory process.

(2) The Licensee shall ensure that the advisory framework is adequately resourced, independently overseen, and subject to effective compliance monitoring.
(3) The Licensee shall review the effectiveness of its advisory policies and procedures at least annually, and more frequently where there is a material change to its business model, distribution model, Client base, products, systems, or applicable law or regulation.
(4) The Licensee shall take appropriate remedial action without undue delay where any material deficiency is identified.

5. Public disclosures. — (1) A Licensee providing Advisory Services shall publish on its website, or make available through another publicly accessible mean approved by the Authority, clear, fair and not misleading disclosures including at least the following:

(a) a description of the Advisory Services offered;

(b) whether the advice is independent, restricted, product-limited, issuer-limited, venue-limited or otherwise subject to commercial or structural limitations;

(c) a description of any material actual or potential conflicts of interest and how such conflicts are identified, managed, mitigated or disclosed;

(d) the Licensee's policies and procedures relating to data privacy, complaints handling and whistleblowing;

(e) whether the Licensee refers or introduces Clients to other Persons, including other Licensees, and if so a description of any material monetary or non-monetary benefit received in connection with such arrangements;

(f) whether any material advisory function, research input, model, data source, Client interface, or other relevant component of the service is provided or maintained by a third party; and

(g) such other information as the Authority may require.

(2) The disclosures required under sub-regulation (1) shall be kept current and reviewed whenever a material change occurs.

6. Client information and suitability assessment. — (1) Before providing a Personalized Recommendation, a Licensee shall obtain sufficient information regarding the relevant Client to enable the Licensee to assess whether the recommendation is suitable for that Client.

(2) The Suitability Assessment shall consider, at a minimum the following:

(a) the Client's knowledge and experience in relation to Virtual Assets and relevant products or services;

(b) the Client's investment objectives, including risk tolerance, expected holding period, return objectives and any relevant restrictions or preferences; and

(c) the Client's financial circumstances, including the Client's capacity to bear loss.

(3) The Licensee shall take reasonable steps to ensure that the information obtained for the Suitability Assessment is reliable, accurate, and up to date.

(4) The Licensee shall not provide a Personalized Recommendation where it lacks sufficient information to conclude that the recommendation is suitable for the Client, and shall not treat the absence of sufficient information as a basis to default to execution-only treatment without appropriate disclosure to the Client.

(5) The Licensee shall review and update relevant Client information periodically and upon becoming aware of a material change in the Client's circumstances.

(6) A Licensee shall establish procedures to ensure that Clients understand the principal risks associated with the relevant recommendation and the types of losses that may arise from acting upon it.

7. Basis of advice and methodology. — (1) A Licensee shall establish and maintain a documented methodology governing how Personalized Recommendations are formulated, approved, communicated, and reviewed.

(2) The methodology shall be reasonably designed to ensure that recommendations are based on appropriate information and analysis and are suitable for the relevant Client.

(3) Nothing in this Regulation shall require a Licensee to assess the whole market or a broad range of Virtual Assets, unless the Licensee expressly represents to the Client that its assessment does so. Where the Licensee's advisory process considers only a limited range of Virtual Assets, issuers, venues, counterparties, products, strategies or affiliated offerings, it shall clearly disclose that limitation to the Client before the recommendation is relied upon.

(4) Where a Licensee's advisory process considers only a limited range of tokens, issuers, venues, counterparties, products, strategies or affiliated offerings, the Licensee shall clearly disclose that limitation to the Client before the recommendation is relied upon.
(5) A Licensee shall not present a recommendation as suitable merely because it falls within a broad risk category or model output, unless the recommendation is in fact suitable having regard to the Client's individual circumstances.
(6) Where automated tools, algorithms or models are used to generate or support Personalized Recommendations, the Licensee shall:

(a) understand and document the methodology, assumptions, limitations and data dependencies of the tool, algorithm or model;

(b) validate the tool, algorithm or model before deployment and on an ongoing basis thereafter;

(c) maintain effective governance, oversight and change controls; and

(d) ensure that the use of automation does not diminish the Licensee's responsibility for suitability, fairness and regulatory compliance of the resulting recommendation.

8. Verification of information and fair presentation. - (1) A Licensee shall not provide advice containing any statement, promise, forecast, estimate, projection or other information which it knows, suspects, or ought reasonably to know is false, misleading, deceptive or presented in a misleading manner.
(2) Prior to making any factual statement or using any factual input material to the advisory process, the Licensee shall take reasonable steps to verify such information against appropriate and reliable source materials.
(3) Where forward-looking statements, scenario analysis or projections are used, the Licensee shall ensure that:

(a) they are fair and not misleading;

(b) their assumptions, uncertainties and limitations are appropriately disclosed; and

(c) they are not presented as certain outcomes.

(4) The Licensee shall use reasonable endeavors to verify the continued accuracy of material factual information used in an ongoing advisory relationship and shall correct any material error or outdated statement without undue delay.

9. Advice records and rationale. — (1) A Licensee shall create and maintain a contemporaneous Advice record for each Personalized Recommendation.
(2) The Advice record shall include at least the following:

(a) the Client information relied upon;

(b) the recommendation made;

(c) the principal basis on which the recommendation was assessed as suitable;

(d) any limitations in the scope of products, venues, issuers, counterparties or information considered; and

(e) the date on which the recommendation was made and the identity of the relevant adviser, approver, system or model, as applicable.

(3) Where the recommendation is generated wholly or partly through an automated process, the Advice record shall include the relevant system, model or logic used and sufficient information to permit supervisory review.

(4) A Licensee shall retain Advice records and all related suitability documentation for at least seven (7) years, or such longer period as may be required under the Act, the Regulations, AML/CFT requirements, or any written direction of the Authority.

10. Conflicts of interest, referrals and inducements. — (1) A Licensee providing Advisory Services shall identify, manage, mitigate and, where appropriate, disclose conflicts of interest arising in relation to the provision of advice.

(2) Without prejudice to the generality of sub-regulation (1), the Licensee shall maintain controls addressing at least the following:

(a) advice relating to affiliated tokens, affiliated issuers, affiliated venues or related-party arrangements;

(b) staff incentives or compensation structures linked to product distribution, Client trading volumes, or specific outcomes;

(c) personal account dealing by relevant employees;

(d) referral, introduction, distribution and reciprocal business arrangements; and

(e) receipt or payment of monetary or non-monetary benefits that may impair the objectivity of the advisory service;

(f) recommendations that directly or indirectly favour affiliated venues, products, liquidity providers or counterparties.

(3) A Licensee shall not recommend a product or transaction primarily to generate fees, commissions, spreads, trading volume or other benefit for itself or a related person.

(4) A Licensee shall disclose to the Client, before the recommendation is acted upon, any material conflict that cannot be effectively prevented or otherwise managed.

11. Outsourcing and third-party tools. — (1) A Licensee shall not outsource their core/principal activity for which it is licensed and shall ensure that any outsourcing or third-party arrangement relating to Advisory Services complies with the outsourcing, governance, technology, cybersecurity and operational resilience requirements under the Regulations.

(2) Where a third party provides research, Client interfaces, suitability tools, profiling tools, robo-advisory engines, algorithmic recommendation tools or other components material to the advisory process, the Licensee shall remain fully responsible for compliance with this Regulation.

(3) The Licensee shall ensure that any such arrangement includes appropriate rights of access, audit, oversight, information and termination, consistent with the Regulations and any applicable direction of the Authority.

Broker-Dealer Services Regulations

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Broker-Dealer Services Regulations, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026.

(2) In this Regulation:

(a) "**Broker-Dealer Services**" means the activity described in Schedule I of the Act;

(b) "**Best Execution**" means taking all reasonable steps to obtain the best possible result for a Client, taking into account price, costs, speed, likelihood of execution and settlement, size, nature and any other relevant consideration;

(c) "**Client Order**" means any instruction, indication of interest, request for quote, acceptance of quote, dealing instruction, subscription, placement instruction, or other order or direction from or on behalf of a Client relating to the purchase, sale, exchange, subscription, placement or other disposition of a Virtual Asset;

(d) "**Execution Venue**" means any exchange, trading venue, order book, market, liquidity source, counterparty arrangement, over-the-counter execution mechanism, request-for-quote system, internalization mechanism or other facility through or against which a Client Order may be executed;

(e) "**Execution Policy**" means the written policy required under regulation 10;

(f) "**Fair Pricing**" means pricing that is fair, transparent and non-discriminatory having regard to the Licensee's disclosed pricing methodology, prevailing market conditions, comparable liquidity sources and the characteristics of the relevant transaction.

(g) "**Internalization**" means execution of a Client Order against the Licensee's own account, inventory, principal book, affiliated liquidity, or another Client Order without submitting the order to an external venue;

(h) "**Proprietary Trade**" means a trade executed by the Licensee on its own account otherwise than solely for the purpose of executing, hedging or facilitating a specific Client Order; and

(i) "**Placement or Distribution Services**" means intermediary services provided in relation to the offer, sale, placement or distribution of Virtual Assets on behalf of an Issuer or offeror, where such activity falls within Broker-Dealer Services under the Regulations.

3. Nature and perimeter of Broker-Dealer Services. — (1) A Licensee shall not hold itself out as providing Broker-Dealer Services unless it is licensed for the Licence Category.

(2) A Licensee providing Broker-Dealer Services may, subject to its Licence and the Act and Regulations:

(a) receive and transmit Client Orders in relation to Virtual Assets;

(b) execute Client Orders on behalf of Clients;

(c) deal in Virtual Assets as principal or agent;

(d) trade on its own account where expressly permitted; and

(e) provide placement or distribution services for Issuers acting as intermediary.

(3) A Licensee shall not rely on a Broker-Dealer License to provide discretionary portfolio management, custodial control, transfer and settlement activity, lending and borrowing activity, derivatives and leverage activity, or issuance activity where, the relevant service falls within another Licence Category under the Regulations.

4. General conduct obligations. — (1) A Licensee providing Broker-Dealer Services shall act honestly, fairly and professionally in accordance with the best interests of its Clients.

(2) The Licensee shall comply with the Client categorization, disclosure, conflicts of interest, complaints handling and market conduct requirements under the Regulations and any binding direction, circular, standard or other instrument issued by the Authority under the Act or the Regulations.

(3) The Licensee shall ensure that its business model, remuneration arrangements, distribution arrangements, inventory management practices, and principal dealing activities do not result in the unfair treatment of Clients.

(4) Where the Licensee acts in more than one capacity, including as agent, principal, market maker, request-for-quote counterparty, placement intermediary or proprietary trader, it shall clearly identify the relevant capacity in the Client Agreement and in its disclosures, as applicable.

(5) The Licensee shall maintain effective controls to identify, manage, mitigate and, where appropriate, disclose conflicts arising from the dual role of serving Clients while also trading for its own account, warehousing inventory, supporting issuances, or routing orders to affiliated venues or liquidity providers.

5. Policies, procedures and governance. — (1) A Licensee providing Broker-Dealer Services shall establish, implement, maintain and enforce written policies and procedures appropriate to the nature, scale, complexity and business model of its activities, including such policies and procedures as are necessary to govern order handling, execution, conflicts of interest, Client disclosures, market conduct, Customer Asset handling where relevant, and operational resilience.

(2) The Licensee shall ensure that the Broker-Dealer control framework is adequately resourced, independently overseen, and subject to effective compliance monitoring, risk oversight and internal escalation.

(3) The Licensee shall review the effectiveness of its Broker-Dealer policies and procedures at least annually, and more frequently where there is a material change to its products, venues, systems, Client base, execution model, market conditions or applicable legal requirements.
(4) The Licensee shall take appropriate remedial action without undue delay where any material deficiency is identified.
(5) A Licensee may rely on group-level policies, procedures, systems, controls or assurance arrangements, provided that:

(a) they are appropriate to the Licensee's business;

(b) they are legally and operationally applicable in Pakistan;

(c) they do not impair the Authority's supervisory access, oversight or enforcement capabilities; and

(d) the Licensee maintains sufficient local oversight, governance, operational capability and access to information necessary to ensure compliance with the Act, the Regulations and any binding direction or other instrument issued by the Authority under express authority conferred by the Act. Any binding direction or other instrument shall identify its statutory basis, binding status and effective date. Guidance may explain the Authority's supervisory expectations but shall not create a generally applicable mandatory obligation unless issued under express authority conferred by the Act.

6. Public disclosures. — (1) A Licensee providing Broker-Dealer Services shall publish on its website, or make available through another publicly accessible means approved by the Authority, clear, fair and not misleading disclosures including at least:

(a) a description of the Broker-Dealer Services provided, including whether the Licensee acts as agent, principal, or both;

(b) a summary of its order handling and execution arrangements, including the types of Execution Venues or liquidity sources it may use and any material circumstances in which Client Orders may be executed on an affiliated venue, internalized, crossed, or executed over-the-counter;

(c) a summary of its Best Execution or Fair Pricing approach, as applicable to its business model;

(d) the material fees, commissions, spreads, mark-ups, mark-downs, rebates or other charges relevant to Broker-Dealer Services;

(e) a statement of the Licensee's arrangements for the safeguarding of Client Assets, where the Licensee holds or controls Client Assets;

(f) a statement of whether the Licensee refers or introduces Clients to other Persons, including other Licensees, and if so a description of any material monetary or non-monetary benefit received in connection with such arrangements;

(g) a statement of whether any Client money, Client Virtual Assets, accounts, or other material service components are maintained or performed by a third party;

(h) a link or connectivity with VASP Exchange for providing detail of the Virtual Assets for which they are providing services;

(i) the Licensee's policies relating to data privacy, complaints handling and whistleblowing; and

(j) such other information as the Authority may require.

(2) A Licensee shall be required to disclose any information expressly required by the Authority in light of the Licensee's actual business model.

(3) The disclosures required under sub-regulation (1) shall be kept current and reviewed whenever a material change occurs.

(4) A Licensee may satisfy the disclosure requirements under this Regulation in a manner proportionate to the nature, scale, and complexity of its Broker-Dealer activities, provided that all material information relevant to Clients is clearly disclosed. The extent and detail of disclosures may reflect the nature of the services actually provided by the Licensee, including whether the Licensee holds Client Assets or performs execution functions directly.

(5) A Licensee shall disclose to the Authority, within thirty (30) Business Days after the end of each quarter:

(a) the identity of any single liquidity source or affiliated venue to which twenty percent (20%) or more of the Licensee's total Client order flow was routed during that quarter, measured by volume or value; and

(b) any routing relationship that created a material conflict of interest

The disclosure shall include a description of the relevant routing practices and the measures used to identify, manage and mitigate any material conflict of interest. Nothing in this sub-regulation limits any obligation to disclose a material conflict to affected Clients.

7. Client Agreements. — (1) In addition to any general requirements under the Regulations, a Client Agreement for Broker-Dealer Services shall, at a minimum, specify:

(a) whether the Licensee will act on an execution-only, advisory, principal, agency, placement, distribution or other basis, or a combination thereof;

(b) the capacity in which the Licensee may act for each type of order, transaction or service, including agent, principal, request-for-quote counterparty, market maker or other capacity;

(c) the order types and execution methods offered;

(d) the Execution Venues and mechanisms that may be used, including any internalization, crossing or over-the-counter arrangements;

(e) the circumstances in which Client Orders may be aggregated, split, prioritized, suspended, rejected, cancelled or partially executed;

(f) the basis on which prices are determined, including any mark-ups, mark-downs, spreads or fees;

(g) the circumstances in which the Licensee may deal as principal to satisfy a Client Order, support an issuance, or manage inventory;

(h) any arrangements affecting Client Assets, collateral, margin or ancillary financing, where applicable and lawfully permitted;

(i) any special risks associated with leveraged, derivative, structured, illiquid, thinly traded or other higher-risk Virtual Asset products made available to the Client; and

(j) any other matter necessary to ensure that the Client understands the nature of the service and the material risks and conflicts associated with it.

(2) A Client Agreement shall be clear, fair and not misleading and shall be updated or supplemented where a material change occurs.

8. Order handling – general principles. — (1) A Licensee shall handle Client Orders promptly, fairly and expeditiously, in accordance with the Client's instructions, the Client Agreement and the Licensee's order handling policy.

(2) Orders for different Clients shall be treated fairly and shall not be unfairly prejudiced in favour of the Licensee, its Proprietary Trades, related parties, affiliated venues, preferred liquidity providers or other Clients.

(3) The Licensee shall maintain policies and procedures addressing at least:

(a) receipt, validation and acceptance or rejection of orders;

(b) time-stamping or other reliable sequencing of order events;

(c) priority rules where multiple Client Orders compete;

(d) the handling of partially filled, unfilled, stale, duplicate, erroneous or suspended orders;

(e) aggregation and allocation of orders;

(f) the handling of trading halts, market disruption events, system outages and severe volatility; and

(g) escalation and remediation of order handling errors.

(4) The Licensee shall ensure that its systems and controls are capable of receiving, processing and executing Client Orders in an orderly manner consistent with the scale and complexity of its business.

(5) Where a Client provides specific instructions, the Licensee shall execute in accordance with those instructions to the extent possible and lawful, and shall explain to the Client where following such instructions may limit the Licensee's ability to pursue Best Execution or Fair Pricing considerations. In the absence of such instructions, the Licensee shall execute in accordance with its Execution Policy.

9. Best Execution and Fair Pricing. — (1) Where a Licensee executes Client Orders on an agency basis, it shall comply with the Best Execution standard and take all reasonable steps to obtain the best possible result for its Clients, taking into account price, costs, speed, likelihood of execution and settlement, size, nature and any other relevant consideration.

(2) Where a Licensee executes Client Orders on a principal basis, including through request-for-quote, internalization or similar arrangements, it shall ensure that pricing is fair, transparent and non-discriminatory, consistent with its disclosed pricing policies and prevailing market conditions. No licensee shall delegate its responsibility of best execution of it's client orders.

(3) Where a Licensee executes Client Orders against its own account, inventory or through internalization, it shall ensure that:

(a) the price is consistent with prevailing market conditions across reasonably available liquidity sources; and

(b) Clients are not systematically disadvantaged as a result of such execution.

(4) A Licensee shall establish, implement and maintain an Execution Policy describing:

(a) the factors considered when determining how Client Orders will be executed;

(b) the relative importance of those factors in different circumstances;

(c) the Execution Venues or mechanisms relied upon;

(d) how the Licensee monitors execution quality or pricing quality; and

(e) how deficiencies are identified and remediated.

(5) In evaluating Best Execution and/or Fair Pricing, the Licensee shall consider, where relevant:

(a) the characteristics of the relevant market, including price levels, spreads, volatility, relative liquidity and execution resilience;

(b) the size, nature and urgency of the transaction;

(c) the number and nature of liquidity sources reasonably available;

(d) accessibility and reliability of quotes under prevailing market conditions;

(e) the costs, fees and settlement risks associated with the execution route; and

(f) the terms and conditions of the order communicated by the Client.

(6) Where a Licensee executes a Client Order off-market, over-the-counter, or against another Person outside an exchange or venue, the burden of demonstrating compliance with the applicable Best Execution or Fair Pricing standard remains with the Licensee.

(7) The Best Execution standard under this Regulation does not impose a guarantee of the best price in all circumstances, but requires reasonable steps, documented policy, ongoing monitoring and conduct consistent with the Licensee's business model and the Client's legitimate interests.

10. Selection and review of Execution Venues. — (1) A Licensee shall take reasonable steps to select and monitor Execution Venues in a manner consistent with achieving Best Execution or Fair Pricing for Clients, as applicable to its business model.

(2) Criteria for venue selection and review shall include, where relevant:

(a) price levels and spreads;

(b) available liquidity;

(c) execution reliability and settlement risk;

(d) incidental costs and fees;

(e) operational resilience;

(f) market integrity and surveillance standards of the venue; and

(g) any conflicts, ownership links or economic interests that may affect routing decisions.

(3) The Licensee shall periodically review the performance of Execution Venues used and adjust its Execution Policy, routing logic or venue list where appropriate.
(4) The Licensee shall not route Client Orders to a venue solely because the venue provides the Licensee with rebates, revenue-sharing, reciprocal business or other benefits inconsistent with the Licensee's obligations to Clients.
(5) The Licensee shall maintain sufficient records to demonstrate the basis on which venues are selected, reviewed and, where relevant, removed or restricted.

11. Routing to affiliated venues and related parties. — (1) Where a Licensee routes or executes Client Orders on an Exchange or other Execution Venue operated by itself, an Affiliate or another related party, it shall:

(a) disclose the affiliated or related-party relationship to Clients in a clear and prominent manner;
(b) ensure that Clients are not disadvantaged relative to comparable orders routed to comparable third-party venues;
(c) manage conflicts of interest arising from the dual role of venue operator and Broker-Dealer, or other related-party relationship; and
(d) maintain records sufficient to demonstrate that routing decisions remain consistent with its obligations under this Regulation.

(2) Disclosure under sub-regulation (1) shall cover, where relevant, the nature of the relationship, any shared management or ownership, and any material economic interest in order flow routed to the affiliated or related-party venue.
(3) A Licensee shall not represent routing to an affiliated venue as neutral or market-wide if, in substance, its execution model favours that venue.

12. Aggregation and allocation of orders. — (1) A Licensee may aggregate Client Orders with orders of other Clients or with Proprietary Trades only where:

(a) such aggregation is unlikely overall to disadvantage any Client whose order is to be aggregated; and
(b) the Licensee has disclosed to Clients that aggregation may occur and that it may operate to their disadvantage in certain circumstances.

(2) A Licensee shall establish and maintain fair allocation rules for aggregated orders, including rules addressing partial fills and scenarios where Proprietary Trades are aggregated with Client Orders.
(3) Allocation decisions shall be documented and shall not systematically favour the Licensee, its related parties, preferred Clients or proprietary positions.
(4) A Licensee shall not use aggregation or allocation practices to mask preferential treatment, front-running or misuse of Client Order information.

13. Dealing as principal and proprietary trading. — (1) A Licensee may deal as principal for the purpose of satisfying Client Orders, supporting placement or distribution activity, managing inventory, making markets, or otherwise as permitted by its Licence, subject to compliance with the Regulations.

(2) Where a Licensee deals as principal with a Client or against a Client Order, it shall ensure that:

(a) the capacity in which it acts is clearly disclosed;

(b) the pricing is fair, transparent and non-discriminatory;

(c) the transaction is not structured or timed so as to disadvantage the Client; and

(d) any related conflicts are effectively managed.

(3) A Licensee shall establish, implement and maintain effective controls governing Proprietary Trades, including controls to prevent:

(a) front-running of Client Orders;

(b) misuse of Client Order information or confidential Client information;

(c) unfair preference of Proprietary Trades over Client Orders; and

(d) improper inventory management practices that undermine fair treatment of Clients.

(4) Proprietary trading activity shall be subject to risk limits, monitoring, escalation and board or senior management oversight proportionate to the scale and risk of the activity.

14. Suitability and appropriateness interfaces. — (1) Where a Licensee provides investment advice or discretionary services in relation to Virtual Assets in the course of Broker-Dealer Services, it shall comply with the applicable suitability requirements under the Advisory Services Regulation, the Management and Investment Services Regulation, and other applicable Regulations, as relevant.

(2) Where a Licensee offers execution-only or non-advised services in complex or higher-risk Virtual Asset products, including derivatives, leveraged positions, structured products or similarly complex arrangements, it shall assess whether the product or service is appropriate for the Client.

(3) For the purpose of an appropriateness assessment, the Licensee shall obtain information regarding the Client's knowledge and experience in relation to the specific type of product or service concerned.

15. Placement and distribution services for Issuers. — (1) Where a Licensee provides placement or distribution services for an Issuer acting as intermediary, it shall establish and maintain controls appropriate to that role, including controls relating to:

(a) due diligence on the Issuer and the relevant Virtual Asset or offering;

(b) fair and not misleading marketing and distribution communications;

(c) allocation of offerings;

(d) management of conflicts of interest, including affiliated issuer relationships; and

(e) segregation of intermediary activities from any advisory, custody, exchange or principal trading activity that may create conflicts.

(2) A Licensee shall not distribute, place or intermediate the offer of a Virtual Asset where it knows, suspects, or ought reasonably to know that the disclosures, statements or marketing materials used are false, misleading, deceptive or materially incomplete.
(3) Where placement or distribution services are provided in connection with Issuance Services, the Licensee shall comply with any applicable Issuance Services Regulation and any conditions imposed by the Authority.

16. Client Assets, collateral and margin interface. — (1) Where Client Assets are held on an incidental basis, such holding shall be limited to temporary operational possession strictly necessary for execution, transfer, or settlement and shall not amount to ongoing custody, independent safeguarding, or unrestricted control of Client Assets.
(2) A Licensee shall not use incidental holding arrangements to circumvent the requirement to obtain a Custody Services Licence where the substance of the activity involves ongoing holding, safeguarding, administration or control of Client Assets.
(3) Client Assets held on an incidental basis shall remain subject to safeguarding, reconciliation, segregation, record-keeping and control measures appropriate to the nature, scale and duration of the activity.
(4) A Licensee shall not use, lend, pledge, rehypothecate, stake, encumber or otherwise dispose of Client Assets solely by virtue of its Broker-Dealer Licence. Any such use shall be in light of Client's prior written explicit and informed consent where required and shall clearly disclose the nature of the activity, the associated risks, any withdrawal restrictions, and the basis on which rewards, proceeds, losses and liabilities are allocated.
(5) Where a Broker-Dealer intends to offer margin, collateral or financing arrangements, it shall comply with all applicable prudential, safeguarding, conduct and disclosure requirements under the Regulations and any relevant Lending and Borrowing Services Regulation or Derivatives Services Regulation. The Broker- Dealer shall seek specific approval for offering margin products as detailed in Regulation 20 of the Exchange Services Regulations.
(6) A Broker-Dealer License shall not of itself entitle a Licensee to provide a standalone margin financing, lending, borrowing, leveraged or derivatives business.

17. Technology, resilience and continuity of execution. — (1) A Licensee shall maintain systems, controls and business continuity arrangements sufficient to support the orderly receipt, routing, execution, confirmation and recording of Client Orders, including during periods of high uncertainty, severe volatility, market disruption, cyber incident or operational stress.
(2) This Regulation is without prejudice to the broader technology, cybersecurity, incident reporting and operational resilience requirements under the Act and the Regulations.

18. Record-keeping. — (1) A Licensee shall keep, for at least the minimum period required under AML Act, 2010, AML Rules, applicable AML/CFT Regulations and any other applicable law, and the Regulations, records sufficient to:

(a) evidence compliance with this Regulation;

(b) reconstruct individual transactions and Client Orders; and

(c) support investigations into suspected misconduct, execution failures, pricing anomalies or misuse of Client Order information.

(2) Records shall include, at a minimum:

(a) Client Orders and any amendment, rejection, suspension, cancellation or execution event;

(b) time-stamped records or equivalent sequencing records of order receipt, routing and execution;

(c) allocation decisions and rationales;

(d) suitability or appropriateness assessments and warnings, where applicable;

(e) execution quality, pricing quality and venue review reports;

(f) records of Proprietary Trades and monitoring outcomes; and

(g) communications with Clients relating to orders, execution issues, pricing issues and complaints.

(3) Records shall be sufficiently complete, accessible and reliable to permit supervisory review, internal investigation, reconstruction of events and effective remediation.

19. Management information, oversight and reporting to the Authority. — (1) A Licensee shall produce regular management information on matters relevant to Broker-Dealer Services, including at least:

(a) execution quality and venue performance;

(b) order handling statistics, including error rates, rejects, partial fills and material exceptions;

(c) complaints related to execution, pricing, routing or order handling; and

(d) incidents involving market abuse, front-running, misuse of Client Order information, execution system failures or conflicts incidents.

(2) The Licensee's board shall review such information at a frequency commensurate with the scale and risk of the business and shall direct remedial action where necessary.

(3) A Licensee shall report to the Authority, in the manner and frequency determined by the Authority:

(a) material breaches of this Regulation or the relevant market conduct provisions of the Regulations;

(b) serious or systemic execution failures;

(c) material pricing control failures;

(d) incidents of suspected market abuse or misuse of Client Order information involving the Licensee, its staff or its Clients; and

(e) any other matter which the Authority may reasonably require for supervisory purposes.

Provided further that reporting to the Authority under this Regulation shall not relieve a VASP of its obligation to submit STRs and other reports to the FMU in accordance with the AML Act, 2010.

(4) The Authority may require the Licensee to provide additional information, management attestations, file reviews, remediation plans or thematic data, and may direct the Licensee to take specific remedial measures.

Custody Services Regulations

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Custody Services Regulations, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026.

(2) In this Regulation:

(a) "**Custody Services**" means the activity described in Schedule I of the Act;

(b) "**Custody Wallet**" means any wallet, address, account, sub-account or similar arrangement used to hold, control or evidence Client Virtual Assets;

(c) "**Segregated Wallet**" means a Custody Wallet designated for a single Client or clearly identified Client group, which remains subject to the Custodian's control, governance, safeguarding, monitoring and compliance framework

(d) "**Key Management**" means the generation, distribution, storage, backup, access, use, rotation, recovery and destruction of private keys, seed phrases, signing devices, authorization credentials or other means of control over Client Virtual Assets; and

(e) "**Proof of Reserves**" means the procedures, controls and validation mechanisms used to that liabilities to Clients in respect of Client Virtual Assets held, controlled, safeguarded or administered by a Licensee are fully matched by reserve assets or equivalent safeguarding arrangements, as required by the Regulations.

(f) **Sovereign Client"** means

- the Federal Government;
- a Provincial Government;
- the State Bank of Pakistan;
- the Authority; or
- any public sector entity specifically designated by the Authority.

(g) "**Third-Party Custodian**" means a Person appointed by a Licensee to support the holding or control of Client Assets on behalf of the Licensee;

(3) For the avoidance of doubt:

(a) references in this Regulation to Clie[1]nt Assets include Client Virtual Assets and, where applicable, Client Money relevant to custody arrangements; and

(b) nothing in this Regulation alters the legal treatment of Client Assets as set out in the Act and the Regulations.

3. Nature and perimeter of Custody Services. — (1) A Licensee shall not hold itself out as providing Custody Services unless it is authorised for that Licence Category or is otherwise permitted to hold or control Client Assets on an incidental basis under the Regulations.

(2) A Licensee providing Custody Services shall perform the safekeeping or administration, on behalf of customers and pursuant to their instructions, of: Virtual Assets; or private cryptographic keys seed phrases, signing devices, authorization credentials or other means of access that allow the customer to transfer or dispose of Virtual Assets independently but excludes the mere provision of software, hardware or infrastructure that enables a customer to retain exclusive control over their own private keys.

(3) A Custody authorization does not, of itself, authorize the Licensee to lend, stake, pledge, rehypothecate, transfer, settle, manage, invest, issue, or otherwise deploy Client Assets except with prior written explicit consent.

(4) Where a custody arrangement forms part of another licensed activity, the Licensee shall comply with this Regulation to the extent applicable to the holding, control, safeguarding or administration of Client Assets in connection with that activity, and such arrangement shall not be structured or operated in a manner that circumvents the requirements applicable to any other Licence Category under the Act or the Regulations.

4. Custody governance and accountability. — (1) The Licensee shall be responsible for the oversight of custody arrangements and the protection of Client Assets.

(2) The Licensee shall ensure the effective implementation of custody policies, procedures and controls approved by the Licensee's board.

(3) The Licensee shall establish clear segregation and appropriate independence between custody operations, trading activities, compliance, risk, and technology functions, commensurate with the nature, scale and complexity of its activities.

(4) The Licensee shall approve and periodically review, at a minimum:

(a) custody models and wallet architecture;

(b) safeguarding and segregation arrangements;

(c) Key Management and access-control standards;

(d) reconciliation and discrepancy management arrangements;

(e) incident response and recovery arrangements;

(f) policies governing any permitted use of Client Assets; and

(g) outsourcing and Third-Party Custodian arrangements.

(5) The Licensee shall maintain adequate governance, committee structures, reporting lines and management information to enable effective oversight of custody risks, technology risks, operational risks and Client protection risks.

(6) The Licensee shall, at a frequency proportionate to the scale and risk of its activities, obtain independent assurance over its custody controls, including safeguarding, reconciliation and

Key Management arrangements, and shall make such reports available to the Authority on half yearly basis.

5. Safeguarding and segregation of Client Assets. — (1) A Custodian shall safeguard Client Assets in a manner that ensures they are segregated from the Custodian's own assets and from the assets of other Persons, in accordance with the Act, the Regulations and this Regulation.
(2) Client Virtual Assets are not owned by the Custodian. The Custodian shall hold or control Client Virtual Assets solely for the benefit of Clients and shall not treat Client Assets as its own assets.
(3) The Custodian shall maintain records that clearly identify which wallets, addresses, accounts, sub-accounts or ledger designations contain Client Assets, including through internal ledger tagging where appropriate.
(4) Segregation shall be implemented in wallet structures, account structures and internal ledgers and records, including by jurisdiction where relevant.
(5) The Custodian shall structure its arrangements so as to support the identification, protection and return of Client Assets in accordance with the insolvency and Client asset protection requirements under the Act and the Regulations.

6. Insolvency protection and legal treatment of Client Assets. — (1) A Custodian shall structure its custody arrangements to support the legal protection afforded to Client Assets under the Act and the Regulations, including protection from:

(a) claims of the Custodian's creditors; and

(b) inclusion in the Custodian's insolvency estate, to the extent permitted by applicable law.

Notwithstanding anything to the contrary contained in any other law for the time being in force, Customer Assets held by a Licensee shall not form part of the Licensee's estate in the event of its insolvency or liquidation.
(2) The Custodian shall maintain records, wallet structures, Client agreements and reconciliation capabilities sufficient to facilitate the timely identification and return, or transfer, of Client Assets, subject to applicable insolvency law and any directions of a competent court or insolvency officeholder.
(3) The Custodian shall assess and document any material legal uncertainty affecting the enforceability or practical effectiveness of its custody structure, including cross-border insolvency issues where relevant, and shall disclose material residual risk to Clients in a fair, clear and not misleading manner.
(4) Where custody arrangements involve cross-border structures or legal uncertainty, the Custodian shall obtain and maintain legal analysis or opinions sufficient to support its assessment of Client Asset protection.

7. Control, access and wallet management. — (1) A Custodian shall establish and maintain effective controls governing access to Client Assets, including the management of private keys, seed phrases, signing devices, account credentials and other means of control.

(2) Access controls shall ensure, as appropriate to the custody model and risk profile:

(a) segregation of duties;

(b) secure key generation, storage, backup and recovery;

(c) multi-factor, multi-approval or multi-signature arrangements where appropriate;

(d) controlled and auditable transaction approval processes; and

(e) timely revocation of access rights where no longer required.

(3) The Custodian shall maintain documented wallet architecture standards, including the basis for using hot, cold and warm Wallets, and the methodology for transferring assets between wallets.

(4) The use of Segregated Wallets shall not, of itself, require or permit direct independent control of Client Virtual Assets by the Client unless otherwise expressly approved by the Authority.

(5) The Custodian shall identify, assess and mitigate risks of collusion, single points of failure, credential compromise, insider misuse and unauthorized access.

(6) The Custodian shall ensure that manually executed core/principal custody functions are performed only by authorised personnel under controlled procedures.

(7) A Custodian shall implement a risk-based wallet allocation framework that:

(a) limits the proportion of Client Assets held in hot or online environments to levels commensurate with operational needs and risk appetite;

(b) ensures that the majority of Client Assets are held in secure offline or equivalent environments where appropriate; and

(c) is approved by the Licensee's board and subject to periodic review.

8. Key generation, storage, backup and recovery. — (1) A Custodian shall generate seeds, private keys and related cryptographic mechanisms using secure generation practices appropriate to industry standards and the Custodian's risk profile.

(2) The Custodian shall apply secure storage and encryption controls to primary and backup keys and shall avoid any arrangement that creates a single point of access enabling a transaction without further control.

(3) Key and seed backups shall be stored separately from primary keys and protected by controls at least equivalent to those applied to primary keys.

(4) The Custodian shall establish and maintain effective policies and procedures to respond where any seed, private key, signing device or other credential is lost, stolen, corrupted or otherwise compromised.

(5) Such procedures shall address, where relevant:

(a) recovery or protection of affected Client Assets;

(b) timely communication with affected Clients, counterparties and the Authority;

(c) cooperation with law enforcement and other competent authorities; and

(d) activation of wind-down or emergency migration arrangements where necessary.

(6) Key Management arrangements shall, where appropriate to the scale and risk of the custody model:

(a) incorporate multi-party computation, multi-signature or equivalent distributed control mechanisms;

(b) ensure that no single individual or system can unilaterally transfer Client Assets;

(c) implement geographic, organizational and logical separation of key components; and

(d) be subject to periodic independent testing and validation.

9. Reconciliations and discrepancy notification. — (1) A Custodian shall conduct reconciliations of Client Assets at least daily, and more frequently where appropriate having regard to transaction volumes, asset values and risk profile.

(2) Reconciliations shall include, as applicable:

(a) Client ledger balances per asset;

(b) on-chain balances for relevant wallets or addresses, or equivalent control evidence;

(c) Client Money balances and Client Accounts where relevant to the custody model;

(d) pending transactions, unconfirmed deposits or withdrawals, and other timing items; and

(e) identification and investigation of breaks, shortfalls, excesses or unexplained differences.

(3) Discrepancies shall be identified, investigated and resolved promptly.

(4) The Custodian shall notify the Authority without delay of any material discrepancy that is not rectified within twenty-four (24) hours and shall provide a summary of cause, impact and remediation based on information then available. The Custodian shall provide material updates as further information becomes available and a final report as soon as reasonably practicable and, in any event, within thirty (30) days, unless the Authority permits a longer period for reasonable cause.

(5) The Custodian shall maintain a register or equivalent record evidencing each Client's position and the reconciliation basis supporting that position.

(6) Where a shortfall in Client Assets is identified:

(a) the Custodian shall take immediate steps to make good the shortfall from its own resources or other available arrangements;

(b) the Custodian shall not allocate losses to Clients except where expressly permitted under the Act, the Regulations and the Client Agreement; and

(c) the Custodian shall notify the Authority and affected Clients without delay.

10. Proof of reserves. — (1) A Custodian shall maintain proof-of-reserves or equivalent assurance procedures sufficient to demonstrate on an ongoing basis that liabilities to Clients in respect of Client Virtual Assets are fully matched by safeguarded holdings or other equivalent arrangements.

(2) Proof of Reserves procedures may include automated or cryptographic methods, including third-party attestation and cryptographic verification.

11. Use of Client Assets. — (1) A Custodian shall not use, sell, transfer, assign, pledge, loan, stake, rehypothecate, encumber or otherwise dispose of Client Assets solely by virtue of its Custody Licence.

(2) Client Assets may be used only where:

(a) such use is expressly permitted under the Act and the Regulations;

(b) the Client has provided explicit, prior, informed consent within the limits clearly defined by the client where required under law or regulation;

(c) the relevant Client Agreement clearly discloses the nature of the activity, the associated risks, withdrawal restrictions, and how rewards, proceeds, losses and liabilities are allocated; and

(d) the Licensee holds any additional Licence Category required for the substance of the relevant activity.

(3) Nothing in this Regulation permits the use of Client Assets other than as expressly allowed under the Act, the Regulations and applicable law.

(4) Where consent-based use of Client Assets is permitted, the Custodian shall operate within clearly defined limits approved by the Licensee's board and shall maintain additional risk-management controls and, where required, capital or liquidity buffers.

(5) Any rewards, proceeds or benefits attributable to Client Virtual Assets, including airdrops, forks, staking rewards or similar benefits, shall accrue to the Client unless otherwise agreed in advance in the Client Agreement and disclosed in a fair, clear and not misleading manner.

12. Account statements and Client reporting. — (1) A Custodian shall provide Clients with periodic statements at intervals appropriate to the nature of the custody service and, in any event, not less frequently than monthly unless otherwise agreed with Professional Clients or Institutional Clients or otherwise permitted by the Authority.

(2) Statements shall include, at a minimum, as applicable:

(a) all Virtual Asset transactions specific to the Client account during the reporting period;

(b) the dates and transaction amounts of corresponding transactions;

(c) balances and value for each type of Virtual Asset held for the Client; and

(d) such other information as is necessary for the Client to understand its holdings, movements and material restrictions.

(3) Statements shall be made available promptly following the statement date and within a timeframe that is reasonable having regard to the Custodian's systems and delivery channel.

(4) Nothing in this Regulation limits any requirement under the Regulations to provide more frequent or more detailed reporting for particular Client categories, products or business models.

13. Client disclosures and custody agreements. — (1) A Custodian shall disclose to Clients material information relating to custody arrangements in a clear, fair and not misleading manner.

(2) Such disclosures shall include, at a minimum:

(a) the nature of the custody service and the custodial framework applied;

(b) wallet arrangements, including use of Omnibus versus Segregated Wallets and hot versus cold and warm storage, where relevant;

(c) the principal custody risks applicable to the service;

(d) the treatment of Client Assets in the event of insolvency or wind-down;

(e) whether and on what terms Client Assets may be used, pledged, rehypothecated, staked or otherwise deployed;

(f) the Custodian's outsourcing arrangements and any use of Third-Party Custodians; and

(g) the cybersecurity, incident response and reimbursement framework applicable to the custody service, where relevant.

(3) Client agreements for Custody Services shall state clearly that ownership of Client Assets remains with the Client, unless otherwise expressly permitted under the Regulations for a separately regulated service.

(4) Client agreements shall, at a minimum, address—

(a) the circumstances, timing and process for the return or transfer of Client Assets;

(b) the treatment of material changes to supported Virtual Assets, including forks or protocol changes;

(c) settlement finality, including when a transfer is deemed complete and when the Custodian's obligations cease in relation to that transfer;

(d) frequency and content of account statements;

(e) the party responsible for safeguarding Client Assets; and

(f) policies and controls governing access to Client Assets.

(5) Custody Services shall be provided pursuant to a contractual arrangement under which the Client transfers control of a Virtual Asset to the Custodian solely for the purpose of receiving Custody Services, without transferring beneficial ownership or discretionary authority except as expressly authorised under the Client Agreement and the Regulations.

14. Public disclosures. — (1) In addition to any disclosure requirements under the Regulations, a Custodian shall publish in a prominent place on its website, or via other accessible means approved by the Authority:

(a) a description of material conflicts of interest arising from custody activities and how they are managed;

(b) policies on data privacy, whistleblowing and handling of Client complaints; and

(c) any additional information the Authority may require.

(2) Public disclosures under this regulation shall be kept current and reviewed whenever a material change occurs.

15. Outsourcing. — (1) A Custodian shall not outsource or delegate the principal custody activity for which it is licensed. The Custodian shall at all times retain effective control, governance, oversight, and responsibility in respect of Client Assets and custody operations.

(2) For the purposes of this regulation, core/principal custody activity includes:

(a) ultimate responsibility for safeguarding Client Assets;

(b) governance and oversight of custody arrangements;

(c) approval and control of wallet architecture and custody models;

(d) provision of Key Management arrangements;

(e) reconciliation and Client asset recordkeeping; and

(f) control and supervision of access to Client Assets.

(3) A Custodian may utilize wallet infrastructure providers, technology service providers in a limited support capacity only, and only to the extent that:

(a) such arrangements do not result in the transfer of ultimate responsibility and/or effective control over custody functions;

(b) the Custodian retains effective oversight, governance and supervisory access;

(c) the arrangement does not impair the Authority's ability to supervise Client Asset protection arrangements; and

(d) the arrangement complies with this Regulation, the Regulations and any conditions imposed by the Authority.

(e) the arrangement does not result in the transfer of beneficial ownership of Client Assets except as otherwise expressly permitted under the Act and the Regulations.

(4) A Custodian shall not outsource or delegate custody arrangements in a manner that:

(a) materially impairs its ability to safeguard Client Assets;

(b) results in the Custodian ceasing to exercise effective oversight, governance or control over Client Assets or core/principal custody functions; or

(c) prevents the Custodian or the Authority from obtaining timely access to records, systems, controls or information necessary for supervisory, safeguarding or recovery purposes.

(5) Where a Custodian outsources its function in light of this Regulation, the Act or applicable regulatory framework, it shall:

(a) conduct due diligence on the regulatory status, financial strength, operational resilience, controls and reputation;

(b) enter into a written agreement specifying responsibilities, segregation standards, reporting obligations and audit rights; and

(c) monitor performance and risk on an ongoing basis.

(6) The Authority shall have access, audit and information rights in respect of outsourced arrangements to the extent permitted by law and the relevant contractual framework.

(7) A Custodian shall apply documented selection criteria designed to ensure that any appointed wallet infrastructure provider possesses the operational capability, security standards,

governance arrangements, and regulatory standing appropriate to the protection of Client Assets. Such criteria shall include, at a minimum, that the provider:

(a) demonstrates institutional-scale operational capability and experience in Virtual Asset custody or wallet infrastructure services;

(b) operates under, or is subject to, regulatory oversight in a jurisdiction acceptable to the Authority;

(c) maintains recognized independent security certifications, including SOC 2 Type II or equivalent standards acceptable to the Authority;

(d) maintains arrangements relating to segregation, operational resilience, business continuity and, where applicable, insurance, consistent with the requirements of this Regulation; and

(e) is capable of supporting the Custodian's reconciliation, audit and supervisory reporting obligations.

(8) A Custodian shall ensure that any wallet infrastructure arrangement:

(a) preserves the Custodian's ability to comply with the Act, the Regulations and this Regulation;

(b) provides the Authority with appropriate audit, inspection, access and information rights;

(c) maintains appropriate safeguards over Client Assets, including segregation and reconciliation controls; and

(d) does not result in Client Assets being held in individually controlled wallets or structures outside the custody and control framework approved by the Custodian and the Authority.

(9) The Authority may, by policy, Regulation, circular, directive, or other written instrument issued under the Act or the Regulations, prescribe additional requirements, standards, eligibility criteria or evidential requirements applicable to wallet infrastructure providers, and compliance with such instrument shall be deemed compliance with the relevant requirements of this Regulation.

16. Operational resilience and incident management. — (1) A Custodian shall ensure that custody systems and controls meet operational resilience and availability standards appropriate to the criticality of custody services, in accordance with the Regulations.

(2) The Custodian shall maintain incident response, escalation and recovery arrangements appropriate to wallet infrastructure, key-management processes, reconciliation processes and Client asset protection.

(3) Material custody incidents, including loss of keys, cyber breaches, misallocation of Client Assets or significant delays in returning Client Assets, shall be reported to the Authority as soon as practicable and, in any event, within any timeframe specified by the Authority under the Regulations or by supervisory notice.

(4) The Custodian shall maintain an incident log recording near misses as well as actual losses, to support lessons learned, remediation and supervisory engagement.

(5) The Custodian shall maintain business continuity, backup and disaster recovery arrangements sufficient to support the continuity of critical custody functions.

17. Staking and yield-generating activities from custody. — (1) A Licensee shall not provide staking-related, protocol participation, yield-generating or similar activities in connection with Custody Services except with explicit prior written informed consent of the client.
(2) Where a Licensee is permitted to provide such activities, the Licensee shall comply with all applicable safeguarding, disclosure, governance, technology, operational resilience, conflict management and conduct requirements under the Act, the Regulations and this Regulation.
(3) The Authority may impose restrictions, conditions or prohibitions on staking-related or yield-generating activities involving Client Assets.

18. Sovereign Clients and permissible yield-related activities. — (1) The Authority may issue a policy Regulation or other guidance setting out prudential, operational and risk-management requirements applicable to any yield-related activities conducted in respect of Virtual Assets held for a Sovereign Client by Strategic Digital Wallet Company, licensed in light of Section 38 of the Act.
(2) A Licensee holding license for conducting activities under Section 38 of the Act may facilitate limited yield-related activities in respect of Virtual Assets held for a Sovereign Client, including staking or other arrangements specifically approved by the Authority, subject to:

(a) the Act;
(b) the Regulations;
(c) any applicable policy Regulation, guidance or direction issued by the Authority; and
(d) the express written mandate of the relevant Sovereign Client.

(3) Such Licensee shall not engage in any yield-related activity involving Virtual Assets held for a Sovereign Client unless:

(a) the activity has been expressly authorised in writing by the relevant Sovereign Client;
(b) the Licensee has conducted and documented an assessment of the associated operational, custody, liquidity, counterparty and technology risks;
(c) the activity complies with the safeguarding, segregation, reconciliation and disclosure requirements of this Rulebook; and
(d) beneficial ownership of the relevant Client Assets remains identifiable at all times.

(4) Unless otherwise expressly approved by the Authority in a specific case, such Licensee shall not:

(a) engage in unsecured lending of Sovereign Client assets;
(b) transfer Sovereign Client assets under arrangements involving rehypothecation or unrestricted onward use by counterparties; or
(c) deploy Sovereign Client assets through structures that materially impair custody control, transparency or recoverability.

(5) Nothing in this Rule alters the legal character of the underlying holdings as Client Assets, or limits the obligations of the Licensee under the Act, the Regulations or this Regulation to safeguard, segregate, and properly account for Client Assets held for a Sovereign Client.

Exchange Services Regulations

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Exchange Services Regulations, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026.

(2) In this Regulation:

(a) "**Exchange Services**" means the activity described in Schedule I of the Act;

(b) "**Exchange**" means a Licensee authorised to provide Exchange Services;

(c) "**Listed Virtual Asset**" means a Virtual Asset admitted, listed, enabled, or otherwise made available for trading, exchange or market access on the Exchange;

(d) "**Matching System**" means any order book, algorithm, crossing engine, request-for-quote arrangement, swap facility or other mechanism by which buying and selling interests are brought together or executed on the Exchange;

(e) "**Market Abuse**" includes fraud, manipulation, wash trading, spoofing, layering, abusive self-trading, dissemination of false or misleading information, misuse of material non-public information, and any other abusive practice prohibited under the Act, the Regulations or applicable law;

(f) "**Participant**" means a Client, member, user, market participant, intermediary, market maker or other Person permitted by the Exchange to access or use the trading venue, whether directly or indirectly;

(g) "**Trading Halt**" means a temporary suspension, pause, restriction or interruption of trading, matching, order entry, cancellation, or other market activity on the Exchange, whether venue-wide or asset-specific; and

(h) "**Trading Rules**" means the rules, protocols, procedures and standards governing access to, participation in, and operation of the Exchange.

3. Nature and perimeter of Exchange Services. —

(1) A Licensee shall not hold itself out as providing Exchange Services unless it is authorised for that Licence Category.

(2) A Licensee providing Exchange Services may, subject to its Licence and the Act and Regulations—

(a) operate a trading venue, order book, Matching System, swap facility, or similar arrangement for the trading or exchange of Virtual Assets;

(b) set and enforce Trading Rules governing access, participation, matching, suspension, delisting and market integrity; and

(c) perform operational, administrative, technological, control or support functions that are directly connected with, and necessary for, the operation of the Exchange.

4. Exchange governance and accountability. — (1) The Exchange shall be responsible for the oversight of exchange operations, market integrity and compliance with the Act, the Regulations and this Regulation.

(2) The Licensee shall be responsible for the day-to-day management of exchange activities, including implementation of the policies, procedures and controls approved by the Licensee's board.

(3) The Licensee shall establish clear segregation and appropriate independence between trading operations, market surveillance, compliance, risk management and technology functions, commensurate with the nature, scale and complexity of its activities.

(4) The Licensee shall approve and periodically review, at a minimum:

(a) Trading Rules;

(b) listing and delisting standards;

(c) market surveillance and escalation arrangements;

(d) proprietary trading policies, if any;

(e) business continuity and trading disruption arrangements; and

(f) conflicts of interest controls relevant to Exchange Services.

(5) The Exchange shall maintain adequate governance, committee structures, reporting lines and management information to enable effective oversight of venue risks, technology risks, abuse risks and Client protection risks.

5. Policies, procedures and governance framework. — (1) In addition to all other applicable requirements under the Regulations, an Exchange shall establish, implement, maintain and enforce written policies and procedures appropriate to the nature, scale and complexity of its business, including at least policies and procedures relating to:

(a) admission and ongoing participation of Participants;

(b) listing, suspension, restriction and delisting of Virtual Assets;

(c) market operations, Trading Rules, order types and matching logic;

(d) market surveillance and abuse prevention;

(e) conflicts of interest management, including related-party listings, affiliated trading activity and proprietary trading;

(f) Client protection, including disclosures, treatment of Client Assets and handling of Client instructions where relevant;

(g) handling of system outages, disruptions, Trading Halts, market stress and venue-wide or asset-specific suspension events;

(h) settlement, delivery, reconciliation and post-trade processing;

(i) use of market data, reference prices and price-formation methodologies; and

(j) such other matters as the Authority may reasonably require.

(2) The Exchange shall assess and, in any case, at least annually review the effectiveness of its policies and procedures and take appropriate measures to address any deficiency.

(3) The Exchange shall maintain records sufficient to demonstrate compliance with its policies and procedures and the basis for material exchange decisions.

(4) A Licensee may rely on group-level policies, procedures, systems, controls or assurance arrangements, provided that:

(a) they are appropriate to the Licensee's business and risk profile;

(b) they are legally and operationally applicable in Pakistan;

(c) the Licensee retains full responsibility for compliance with the Act, the Regulations and this Regulation; and

(d) the Authority is able to obtain access, directly or indirectly, to relevant records, systems, personnel and information necessary for supervisory purposes.

6. Public disclosures. — (1) An Exchange shall publish on its website, trading interface or another publicly accessible means approved by the Authority, clear, fair and not misleading disclosures including at least:

(a) the Trading Rules, including order types, matching priority, market sessions and any special trading conditions;

(b) fee schedules, including trading, listing and ancillary fees;

(c) eligibility criteria for Participants and access arrangements;

(d) policies for handling outages, system disruptions, Trading Halts, suspensions, reopenings and other material market events;

(e) procedures for suspension, restriction or delisting of Listed Virtual Assets;

(f) a summary of the Exchange's standards for admission and continued availability of Virtual Assets;

(g) a description of how Client Assets relevant to Exchange activity are safeguarded, where the Exchange holds or controls such assets;

(h) a summary containing the following information pertaining to each Virtual Asset offered for exchange by the VASP:

i). name and symbol;

ii). date of issuance;

iii). market capitalization and fully diluted value;

iv). circulating supply, including as a percentage of maximum total supply (if applicable);

v). whether the Virtual Asset has been subject to an independent smart contract audit and the date of the most recent audit; and

vi). largest reduction in price from high to low stated as both an absolute amount and a percentage change, including when it occurred;

(i) the Exchange's policies relating to data privacy, complaints handling and whistleblowing; and

(j) such other information as the Authority may reasonably require.

(2) The Exchange may publish factual information regarding Listed Virtual Assets, including asset identifiers, circulating supply, audit status, and other neutral descriptive information, provided that such disclosures are presented in a fair, clear and not misleading manner and do

not amount to financial promotion, endorsement or recommendation activity inconsistent with the Act or the Regulations.

(3) The Exchange shall keep disclosures under this regulation current and update them promptly where a material change occurs.

7. Admission and participation criteria. — (1) An Exchange shall establish objective, transparent and non-discriminatory criteria for the admission and ongoing participation of Participants.

(2) Admission criteria shall address, at a minimum the following:

(a) eligibility and onboarding requirements;

(b) access to trading systems and market interfaces;

(c) ongoing compliance obligations;

(d) operational, financial and technical conditions for participation, where relevant; and

(e) grounds for refusal, suspension, restriction or termination of access.

(3) The Exchange shall apply admission criteria consistently and shall not grant or maintain access on terms that materially prejudice market integrity or Client protection.

(4) The Exchange shall maintain adequate records of admission, refusal, suspension and termination decisions and the basis for such decisions.

8. Participant rules and code of conduct. — (1) An Exchange shall publish and enforce a code of conduct or equivalent Participant rules governing conduct on the trading venue.

(2) The code of conduct or equivalent rules shall include, at a minimum the following:

(a) compliance with the Act, the Regulations, this Regulation and applicable market conduct obligations;

(b) prohibitions on Market Abuse and abusive trading practices;

(c) obligations to provide accurate information to the Exchange;

(d) cooperation with surveillance, compliance and investigative processes; and

(e) sanctions or disciplinary consequences for breach of applicable rules.

(3) An Exchange shall ensure that Participants are fairly informed of the rules applicable to them and that relevant Clients or Participants validly accept those rules through contractual, platform or other lawful means.

(4) Nothing in this regulation limits the powers of the Authority to impose supervisory, disciplinary or enforcement measures directly under the Act or the Regulations.

9. Virtual Asset admission and continued availability. — (1) An Exchange shall establish, implement and publish objective, transparent and non-discriminatory standards for the admission and continued availability of Virtual Assets on its venue.

(2) Such standards shall be proportionate to the Exchange's business model and shall address, where relevant, the following

(a) liquidity and market quality considerations;

(b) technology and security risks of the underlying protocol;

(c) risks of fraud, manipulation and Market Abuse;

(d) legal and regulatory risks, including whether the Virtual Asset is prohibited or restricted under the Act or any other law in Pakistan;

(e) issuer disclosures and transparency, where relevant; and

(f) conflicts of interest in relation to the Virtual Asset.

(3) The Exchange shall conduct initial and ongoing assessments against its standards and shall keep records of such assessments.

(4) The Exchange shall establish clear triggers and procedures for suspension, restriction or delisting where a Virtual Asset no longer meets its standards or where continued availability presents a material and demonstrable risk of significant harm to Clients or market integrity.

10. Listing procedures and notification. — (1) Subject to the Act, the Regulations andthis Regulation and any direction of the Authority, an Exchange may admit or list a Virtual Asset without prior product approval by the Authority, provided that:

(a) the Virtual Asset is not subject to any explicit restriction or prohibition by the Authority or by law;

(b) the Virtual Asset complies with the Exchange's internal listing policies and due diligence standards;

(c) where the Virtual Asset has previously been launched or admitted to trading in another jurisdiction, the Exchange has considered any available regulatory, market integrity and trading history information relevant to its assessment; provided that prior launch or admission to trading on another venue shall not be a condition for listing in Pakistan; and

(d) the Exchange complies with any notification or information requirement specified by the Authority in relation to listing decisions.

(2) Any notification made to the Authority in connection with a listing shall not constitute approval of the Virtual Asset by the Authority, and the Exchange remains fully responsible for its listing decision.

(3) The Authority may, by direction, notice or supervisory requirement, require prior notification, accelerated notification, delayed notification, additional information, or risk-based escalation for particular classes of Virtual Assets, Exchanges or business models.

(4) An Exchange shall not admit for trading any derivative, leveraged or synthetic product unless permitted under its Licence and consistent with the Derivatives Services framework and any applicable conditions imposed by the Authority.

11. Market operations and fair trading. — (1) An Exchange shall operate its trading systems in a fair, orderly and transparent manner.

(2) The Exchange shall take reasonable steps to ensure fair and non-discriminatory access to trading information for Participants, subject to lawful and transparent differentiation based on access type, technical connectivity, market model, or Participant category, provided that such differentiation does not result in unfair advantage or undermine market integrity.

(3) Trading Rules shall be applied consistently and without undue preference.
(4) The Exchange shall establish and disclose rules governing at least the following:
(a) market sessions and trading hours;
(b) order entry, modification and cancellation;
(c) matching logic and priority;
(d) treatment of partially filled, unfilled, stale, erroneous or duplicate orders;
(e) Trading Halts, suspensions and reopenings; and
(f) circumstances in which the Exchange may reject, cancel, bust, reverse or otherwise remediate trades or orders.
(5) The Exchange shall maintain systems and controls reasonably designed to prevent disorderly trading, unfair discrimination and systemic operational disruption.

12. Pricing methodology and market data integrity. — (1) Where the Exchange determines, calculates, publishes or uses prices, indices, reference rates, market data or valuation metrics in connection with Exchange Services, it shall establish documented methodologies designed to support integrity, reliability and resistance to manipulation.
(2) Such methodologies shall address, where relevant, the following:
(a) data sources and eligibility criteria;
(b) handling of outliers, stale data and anomalous prints;
(c) fallback arrangements for unavailable or unreliable data;
(d) governance over methodology changes; and
(e) controls to prevent conflicts of interest affecting price determination.
(3) An Exchange shall disclose in clear terms the basis on which prices quoted or displayed to Participants are determined, to the extent necessary for Participants to understand execution, pricing outcomes and the operation of the market.
(4) The Exchange shall not present price information in a misleading manner and shall maintain controls appropriate to the integrity of any benchmark-like or reference pricing process it operates.

13. Market surveillance and abuse prevention. — (1) An Exchange shall establish and maintain effective market surveillance arrangements to detect, deter and escalate Market Abuse, manipulation and other misconduct.
(2) Surveillance arrangements shall be proportionate to the nature and scale of trading activity and shall include monitoring of trading behaviour, order activity, participant conduct and other relevant market signals.
(3) The Exchange shall have procedures for investigating suspicious activity and taking appropriate action, including referral, restriction, suspension, escalation to the Authority, and preservation of relevant records.
(4) Surveillance arrangements shall be supported by adequate staffing, systems, escalation protocols and management oversight.

(5) An Exchange shall share information relevant to surveillance, disciplinary and supervisory purposes with the Authority in accordance with the Act, the Regulations and any lawful request or reporting requirement of the Authority.
(6) Where the Exchange suspects potential abuse affecting the market, it shall notify the Authority without undue delay and provide such information as is relevant and reasonably available to the Exchange at the time of the report, including, where applicable, information relating to positions, exposures, order activity, inventory levels, delivery mode, margin changes or other actions taken by the Exchange.

14. Conflicts of interest, related-party listings and proprietary activity. — (1) An Exchange shall identify, prevent, manage and disclose conflicts of interest relevant to Exchange Services and shall not allow such conflicts to materially prejudice Clients, Participants or market integrity.
(2) Without prejudice to the generality of sub-regulation (1), the Exchange shall maintain policies and procedures addressing at least:

(a) related-party or affiliated listings;

(b) affiliated Participants or connected trading activity;

(c) proprietary trading by the Exchange or any group entity;

(d) economic interests in listed assets, venues, issuers, market makers, or liquidity providers; and

(e) decision-making conflicts affecting surveillance, listing or disciplinary outcomes.

(3) Where an Exchange or any group entity trades on its own account, such activity shall be subject to strict controls to prevent conflicts of interest and unfair advantage.
(4) Proprietary trading policies shall be approved by the Licensee's baord, disclosed to the Authority, and supported by controls to prevent misuse of Client or Participant order information and unfair preference over other market users.
(5) The Exchange shall maintain a record of material conflicts identified and the measures taken to manage, mitigate or disclose them.

15. Client Assets and custody interface. — (1) Where an Exchange holds or controls Client Virtual Assets or Client Money, whether on a standalone or incidental basis, it shall comply with the applicable safeguarding, segregation, reconciliation, record-keeping and disclosure requirements under the Regulations and, where applicable, the Custody Services Regulation.
(2) An Exchange shall not use, lend, pledge, encumber, rehypothecate, stake or otherwise dispose of Client Assets solely by virtue of its Exchange Licence. Any such use shall require Client's prior written, explicit and informed consent.
(3) Where reserve assets are held in respect of Client liabilities arising from Exchange activities, such assets shall be maintained and safeguarded in accordance with the applicable prudential, safeguarding and reserve requirements under the Regulations.

16. Settlement and settlement finality. — (1) An Exchange shall establish, document and maintain settlement arrangements designed to achieve timely, accurate and orderly settlement of transactions executed on its venue, having regard to the product, settlement model, underlying distributed ledger or other infrastructure used, and the associated operational, liquidity, counterparty and market risks.

(2) The Exchange shall disclose to Participants:

(a) the applicable settlement cycle;

(b) the point at which a trade is treated as final under the Exchange's rules and operational procedures; and

(c) the circumstances in which settlement may be delayed, suspended, cancelled, reversed, or subject to close-out or default procedures.

Such disclosure shall not be taken as determining the legal finality of settlement under applicable law.

(3) Settlement arrangements shall be supported by appropriate reconciliations, exception management, participant communications, and default-management controls, and shall not expose Clients or the market to undue and avoidable settlement risk.

(4) Where settlement is dependent on third-party infrastructure, on-chain confirmation standards, banking rails, custodial movement, or other external dependencies, the Exchange shall maintain procedures for handling delays, failures and exceptions and shall communicate material settlement disruptions to affected Participants and to the Authority without undue delay.

(5) Where an Exchange's ordinary settlement model requires a settlement cycle longer than twenty-four (24) hours because of infrastructure dependencies, market conditions, product design or another objectively justified factor, the Exchange shall notify the Authority before implementing that settlement model and shall disclose the applicable settlement cycle to Participants. A material and unexpected failure to meet the applicable settlement cycle shall be notified to the Authority without undue delay. Other settlement exceptions shall be documented and may be reported on an aggregated quarterly basis.

(6) An Exchange shall complete final settlement within twenty-four (24) hours of execution, or within an alternative settlement cycle notified under sub-regulation (5), to the extent settlement is within its reasonable control. Where settlement is delayed by external infrastructure, distributed-ledger conditions, counterparties, custodians, banking rails or necessary compliance controls, the Exchange shall take reasonable steps to complete settlement and communicate any material delay to affected Participants.

17. Trading systems continuity, resilience and controls. — (1) In addition to the broader technology, cybersecurity and operational resilience requirements under the Regulations, an Exchange shall have in place effective systems, procedures and arrangements to ensure that its trading systems:

(a) are resilient;

(b) have sufficient capacity to ensure orderly trading under conditions of high uncertainty and extreme volatility;

(c) are able to reject orders that exceed pre-determined volume and price thresholds or are clearly erroneous, where appropriate to the market model;

(d) are fully tested to ensure that applicable conditions and controls are met; and

(e) are subject to effective business continuity arrangements, including backup and disaster recovery systems, facilities and sites, to ensure continuity of services and reporting capability in the event of system failure.

(2) The Exchange shall maintain and disclose procedures for handling outages, connectivity failures, Trading Halts, system degradations and resumptions of trading.

(3) The Exchange shall maintain escalation and decision-making arrangements for venue-wide disruption, including criteria for halting, suspending, reopening or restricting trading.

18. Market disruption, suspension and delisting powers. — (1) An Exchange shall have documented powers and procedures to suspend, restrict or halt trading in a Virtual Asset or on the venue where necessary to preserve orderly markets, protect Clients, or respond to operational, legal or market integrity risks.

(2) The Exchange shall also maintain documented procedures for the lifting of a suspension or restriction, including any conditions that must be satisfied before trading resumes.

(3) The Authority may, where it has reasonable grounds to believe that a Virtual Asset, market function, or specified activity gives rise to a material risk to market integrity, Client protection, financial stability, compliance with applicable law, or any other objective of the Act, direct the Exchange to suspend, restrict, delist or cease the relevant activity.

(4) Any direction under sub-regulaiton (3) shall be lawful, necessary and proportionate to the risk identified and shall specify the scope of the direction and, where practicable, the reasons for it.

(5) The Exchange shall comply with any lawful direction issued under this Regulation.

(6) The Exchange shall immediately communicate material suspension, restriction, halt, reopening or delisting decisions to the Authority, to affected Participants and to Clients.

19. Margin, leverage and derivatives interface. — (1) An Exchange shall not offer, list, facilitate or otherwise make available margin trading, leveraged spot products, futures, options, perpetual contracts, contracts for difference, leveraged tokens or other derivatives or leveraged products unless the Licensee holds the relevant Licence Category or the applicable and relevant permissions within such Categories required under the Act and the Regulations and such permission is expressly stated in its Licence.

(2) Where an Exchange facilitates any margin or leveraged activity, it shall maintain rules, controls and disclosures addressing at least:

(a) eligibility of Participants and Clients;

(b) collateral and margin methodologies;

(c) liquidation, close-out and default handling;

(d) position limits, concentration risk and market integrity controls; and

(e) Client risk disclosures and appropriateness controls, where applicable.

(3) An Exchange shall not treat authorization to operate a trading venue as sufficient authority to conduct a standalone margin financing, lending, or derivatives business where, in substance, the relevant activity falls within another Licence Category.

(4) Detailed rules on margin methodologies, collateral standards, liquidations and leveraged or derivatives products may be specified by the Authority in the applicable Regulation or by licence condition.

(5) VASPs must ensure that they have sufficient assets to provide Margin Trading services in order that they can fully satisfy client obligations, at all times.

20. Authority approval and powers -

(1) Authority may approve an application for the provision of Margin Trading services, provided that the VASP can demonstrate, to the Authority's satisfaction, compliance with the following requirements

a) the VASP has submitted for the Authority's approval details of the terms and conditions upon which it proposes to offer Margin Trading services to clients, including a copy of the template Margin Trading Agreement to be used by the VASP, together with information relating to the VASP's financial condition and compliance with all Capital and Prudential Requirements applicable to the VASP;

b) the VASP has established, and is able to demonstrate the Authority, appropriate policies and procedures as well as systems and controls with regards to Margin Trading services, which shall include but not be limited to

i). the Margin which may be called, the applicable Margin rates and the method of calculating the Margin;

ii). the acceptable methods of Margin payment and forms of collateral;

iii). the circumstances under which a client or counterparty may be required to provide Margin and additional Margin, and the consequences of a failure to meet a Margin call, including the actions which the VASP may be entitled to take; and

iv). applicable escalation procedures where a client or counterparty fails to meet Margin calls; and

v). the VASP ensures, and is able to demonstrate to the Authority that Virtual Assets collected as collateral for Initial Margin and Maintenance Margin purposes are liquid and can be liquidated within a reasonable timeframe.

(2) The Authority may require to inspect the Margin Trading system of the VASP used to calculate clients' Margin Trading positions and Margin and, prior to granting approval, request any other clarifications, information or documents it deems necessary.

(3) Notwithstanding a VASP having approval from the Authority for the provision of Margin Trading, the Authority may instruct VASPs to take any of the following actions

which shall be lawful, necessary and proportionate to the risk identified and shall specify the scope of the direction and, where practicable, the reasons for it, in its sole and absolute discretion from time to time, and VASPs must comply with such instructions

a) suspend Margin Trading services for specified Virtual Assets or clients;
b) close existing client positions; and
c) increase Initial Margin and/or Maintenance Margin requirements.

21. Record-keeping. — (1) An Exchange shall keep, for at least the minimum period required under AML Act, 2010, AML Rules, applicable AML/CFT Regulations and any other applicable law, and the Regulations, records sufficient to:

(a) evidence compliance with this Regulation;

(b) reconstruct market events, trading decisions, surveillance escalations and exchange actions; and

(c) support investigations into suspected misconduct, listing decisions, disruption events or participant breaches.

(2) Records shall include, at a minimum:

(a) Trading Rules and amendments thereto;

(b) listing, suspension and delisting assessments and decisions;

(c) participant admission, refusal, suspension and termination decisions;

(d) order, trade and market event data sufficient to support surveillance and reconstruction;

(e) records of Trading Halts, outages, system incidents and remedial actions;

(f) surveillance alerts, investigations and escalations; and

(g) records relating to proprietary trading, related-party activity and conflict management decisions, where applicable.

(3) Records shall be sufficiently complete, accessible and reliable to permit supervisory review, internal investigation, reconstruction of events and effective remediation.

22. Management information, reporting and board oversight. — (1) An Exchange shall produce regular management information on matters relevant to Exchange Services, including at least:

(a) trading volumes, concentration and market quality indicators;

(b) listing, suspension and delisting activity;

(c) surveillance alerts, investigations and outcomes;

(d) system performance, outages, Trading Halts and operational incidents;

(e) participant disciplinary actions and serious rule breaches; and

(f) Client or participant complaints relevant to Exchange operations.

(2) The Licensee's board shall review such information at a frequency commensurate with the scale and risk of the business and shall direct remedial action where necessary.

(3) An Exchange shall report to the Authority, in the manner and frequency determined by the Authority:

(a) material breaches of this Regulation or applicable market conduct requirements;
(b) serious or systemic trading, surveillance, technology or settlement failures;
(c) material changes to listing standards, Trading Rules or market structure;
(d) significant incidents of suspected Market Abuse; and
(e) any other matter that the Authority may reasonably require for supervisory purposes.

(4) The Authority may require the Exchange to provide additional information, management attestations, remediation plans, file reviews or thematic data, and may direct the Exchange to take specific remedial measures.

Lending and Borrowing Services Regulations

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Lending and Borrowing Regulations, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026.

(2) In this Regulation:

(a) "**Borrower**" means any Client or counterparty that receives Virtual Assets under a Lending Arrangement;
(b) "**Collateral**" means Virtual Assets, or other assets provided to secure obligations under a Lending Arrangement;
(c) "**Lender**" means any Client, Licensee or counterparty that provides Virtual Assets under a Lending Arrangement;
(d) "**Lending Arrangement**" means a contractual arrangement under which a Client lends Virtual Assets to, or borrows Virtual Assets from, a Licensee or a third-party counterparty via a Licensee;
(e) "**Lending and Borrowing Services**" means the activity described Schedule I of the Act;
(f) "**Liquidation Even**t" means any event under a Lending Arrangement that gives rise to a right to liquidate, close out, enforce or otherwise realize Collateral or terminate relevant positions; and
(g) "**Re-use**" includes lending, pledge, rehypothecation, transfer, staking or other deployment of Client Assets as per explicit, written prior consent of the client as specified under the Act.

3. Nature and perimeter of Lending and Borrowing Services. — (1) A Licensee shall not hold itself out as providing Lending and Borrowing Services unless it is authorised for that Licence Category.

(2) A Licensee providing Lending and Borrowing Services may, subject to its Licence and the Act and Regulations:

(a) facilitate or enter into collateralized or uncollateralized Lending Arrangements involving Virtual Assets;

(b) provide borrowing, lending, margin lending, or similar financing arrangements linked to Virtual Assets; and

4. Governance and risk oversight. — (1) The Licensee's board shall approve and oversee the Lending and Borrowing business, including the following:

(a) product design, approval, review and eligibility criteria for Clients;

(b) risk appetite and limits for credit, concentration, liquidity, market and operational risks;

(c) collateral, margin and liquidation policies;

(d) target-market determinations, where applicable; and

(e) governance over any Re-use of Client Assets, if lawfully permitted.

(2) Senior management shall implement policies, procedures and controls to manage risks arising from Lending and Borrowing Services, including credit, concentration, liquidity, market, technology, operational and legal enforceability risks, and shall ensure that those risks are reflected in the Licensee's prudential, capital and liquidity planning under the Regulations.

(3) A Licensee shall maintain adequate governance, reporting lines, escalation procedures and management information to enable effective oversight of asset sufficiency, collateral adequacy, withdrawal obligations, counterparty exposure, concentration risk and Client asset protection.

(4) The Licensee's board shall review the Lending and Borrowing business at a frequency commensurate with its scale and risk and shall direct remedial action, where required.

5. Policies, procedures and control framework. — (1) In addition to all other applicable requirements under the Regulations, a Licensee providing Lending and Borrowing Services shall establish, implement, maintain and enforce written policies and procedures appropriate to the nature, scale and complexity of its business, including at least policies and procedures relating to:

(a) product design and approval;

(b) Client onboarding and eligibility;

(c) credit assessment and counterparty due diligence;

(d) collateral eligibility, valuation, margining and liquidation;

(e) liquidity management and asset sufficiency;

(f) withdrawal rights and restrictions;

(g) the use, holding, safeguarding and any permitted Re-use of Client Assets;

(h) valuation, reporting and record-keeping;

(i) stress-testing and contingency planning;

(j) outsourcing and third-party arrangements; and

(k) such other matters as the Authority may reasonably require.

(2) A Licensee shall assess and, in any event, at least annually review the effectiveness of those policies and procedures and take appropriate measures to address any deficiency.

(3) A Licensee may rely on group-level policies, procedures, systems, controls or assurance arrangements, provided that they are appropriate to the Licensee's business, legally and operationally applicable in Pakistan, and sufficient to ensure compliance with the Act, the Regulations and this Regulation.

6. Product governance and target market. — (1) A Licensee shall not offer a Lending Arrangement unless it has assessed the nature, legal character, risks, collateral profile, liquidity profile and operational dependencies of the arrangement and is satisfied that the arrangement is consistent with the Act, the Regulations, this Regulation and the terms of its Licence.
(2) A Licensee shall identify the target market, if any, for each material type of Lending Arrangement and shall ensure that the arrangement is distributed only to those categories of Clients for whom it is appropriate.
(3) A Licensee shall not design, market or distribute a Lending Arrangement in a manner that obscures the legal character of the arrangement, the use of Client Assets, the existence of lock-ups or notice periods, or the order in which losses may be borne.
(4) The Licensee shall periodically review each material product type and suspend, restrict or withdraw it where it no longer remains appropriate or where it presents material and unmanaged risks to Clients or to the Licensee.

7. Client disclosures and agreements. — (1) A Licensee providing Lending and Borrowing Services shall disclose to Clients, in a clear, fair, timely and not misleading manner, material information including at least the following:

(a) the nature and terms of the Lending Arrangement;

(b) whether the arrangement is pooled, bilateral, principal-based, agency-based, margin-based or otherwise;

(c) interest, fees and charges, including whether interest is simple or compound, fixed or variable, and how it is calculated, adjusted and paid;

(d) collateral requirements, valuation methodologies, loan-to-value ratios, margin calls and liquidation triggers;

(e) withdrawal rights, notice periods, lock-ups, gates, delays or other restrictions;

(f) risks associated with price volatility, liquidity mismatch, counterparty default, rehypothecation or other Re-use, liquidation, operational failure and legal enforceability; and

(g) whether and on what terms Client Assets may be Re-used, including the categories of counterparties to whom assets may be exposed.

(2) Client Agreements shall be clear, fair and not misleading and shall comply with the market conduct requirements under the Regulations.
(3) In addition to general Client Agreement requirements under the Regulations, a Client Agreement for Lending and Borrowing Services shall, to the extent applicable, set out clearly the following:

(a) the nature of the Lending Arrangement;

(b) descriptions of the assets lent, borrowed or used as Collateral sufficient to identify them;

(c) rights of the parties with respect to custody, use and return of lent assets and Collateral;

(d) interest basis, rate determination, payment frequency and adjustment mechanisms;

(e) withdrawal rights, applicable notice periods and any lock-ups;

(f) defaults, Liquidation Events and associated recovery mechanisms, including the order of application of Collateral and any shortfall allocation, and a clear statement that the relevant arrangement is not equivalent to custody or safekeeping arrangements;

(g) whether and on what terms the Licensee may Re-use Client Assets and the Client's explicit consent thereto where required;

(h) termination rights and consequences of termination; and

(i) the Licensee's complaints procedure and escalation channels.

8. Liquidity and asset sufficiency. — (1) A Licensee offering Lending and Borrowing Services shall at all times maintain sufficient Virtual Assets and/or fiat to meet its contractual obligations to Clients when due, taking into account the following:

(a) the maturity profile of Lending Arrangements;

(b) agreed withdrawal rights;

(c) haircut, margin and Collateral requirements;

(d) potential stressed outflows; and

(e) any concentration in counterparties, assets, maturities or funding sources.

(2) A Licensee shall not operate a Lending and Borrowing business model that results in a structural or persistent mismatch between its obligations to Clients and the assets available to meet those obligations.

(3) The Licensee shall implement governance controls, monitoring frameworks and usage-tracking mechanisms capable of:

(a) identifying emerging shortfalls in assets, Collateral or liquidity; and

(b) triggering escalation to senior management and the Authority where a shortfall arises or is reasonably foreseeable.

(4) The Licensee shall notify the Authority without undue delay where it is, or is likely to be, unable to meet its obligations to Clients in respect of Lending Arrangements.

(5) A Licensee shall not represent a Lending Arrangement as withdrawable on demand, or as low-risk or equivalent to custody, unless that representation is accurate having regard to the legal terms, liquidity profile and use of assets within the arrangement.

9. Withdrawal rights and restrictions. — (1) Clients' contractual rights to withdraw Virtual Assets or fiat from Lending Arrangements must be clearly documented in the Client Agreement, including the following:

(a) whether assets are redeemable on demand, subject to notice, or locked up;

(b) any minimum or maximum withdrawal amounts;

(c) any fees or penalties for early withdrawal; and

(d) the circumstances in which withdrawals may be delayed, gated, suspended or otherwise restricted.

(2) Where withdrawal rights are restricted as part of a Lending Arrangement, the Licensee shall:

(a) disclose such restrictions clearly before the Client enters the arrangement; and

(b) ensure that marketing and communications are consistent with those restrictions and are not misleading.

(3) Where withdrawals are permitted, the Licensee shall ensure that transfers out are executed in accordance with the Transfer and Settlement Services Regulation and the Custody Services Regulation, except where delayed due to factors outside the Licensee's control, in which case the Licensee shall promptly inform affected Clients.

10. Collateral management. — (1) A Licensee shall establish and maintain written policies governing the acceptance, valuation, monitoring and liquidation of Collateral, ensuring such policies remain prudent, transparent and appropriate to the nature, scale and complexity of the activity.

(2) Collateral policies shall address, at a minimum:

(a) eligible Collateral types and any concentration limits;

(b) valuation methodologies, frequency of revaluation and application of haircuts;

(c) initial and variation margin requirements and triggers, including automated triggers where operationally feasible;

(d) Collateral liquidation processes, including priority of application of proceeds; and

(e) governance over exceptions, overrides and non-standard Collateral.

(3) Where Collateral consists of Client Virtual Assets or Client Money, the Licensee shall ensure that Collateral arrangements are consistent with the safeguarding requirements in the Regulations and any applicable Custody Services Regulation requirements.

(4) Eligible Collateral shall consist of assets that are liquid, readily realizable and capable of valuation using observable market data or otherwise conservative methodologies appropriate to the relevant risk. High-quality Collateral may include cash, cash equivalents, short-term government securities of high credit quality, high-quality liquid Fiat-Referenced Tokens and Asset-Referenced Tokens, and specified Virtual Assets with deep and demonstrable liquidity, subject to appropriate haircuts.

(5) Collateral shall only be used in accordance with governing agreements and the terms of the relevant Lending Arrangement.

11. Use and Re-use of Client Assets. — (1) Client Assets, including lent assets and Collateral, shall not be Re-used, lent on, pledged, rehypothecated, staked or otherwise deployed for the Licensee's own benefit or for third parties unless:

(a) such use is permitted by applicable law and the Pakistan Virtual Asset Services Regulations, 2026;

(b) the Client's explicit, prior, informed consent has been obtained and should be utilized within the limits clearly defined by the client; and

(c) the scope, risks, withdrawal implications and counterparties or categories of counterparties relevant to such use are clearly set out in the Client Agreement.

(2) Where Re-use is permitted, the Licensee shall maintain:

(a) Prior, explicit written consent of the clients for the re-use of such assets;

(b) records of which assets are Re-used, with whom and under what terms;

(c) additional risk management and, where required, capital or liquidity buffers to reflect the increased risk to Clients; and

(d) a clear understanding and documentation of the resulting exposure of Clients to counterparty, liquidity and market risks arising from such re-use.

(3) A Lending and Borrowing authorization does not disapply or dilute the safeguarding standards applicable to Client Money and Client Virtual Assets under the Regulations.

(4) The Licensee shall not obscure Re-use of Client Assets by describing the arrangement as "custody", "safekeeping" or other language suggesting that the assets remain fully insulated from lending counterparty risk where that is not the case.

12. Counterparty due diligence and credit assessment. — (1) A Licensee shall conduct comprehensive due diligence on Borrowers and lending counterparties on a periodic basis, including:

(a) identity verification and beneficial ownership;

(b) business purpose and economic rationale of the Lending Arrangement;

(c) financial strength, liquidity and leverage;

(d) market, concentration and country risk; and

(e) any other information that a prudent lender would require to assess the risks associated with the arrangement.

(2) Risk profiles shall be updated periodically and whenever a material change occurs in a counterparty's risk profile.

(3) The Licensee shall integrate such assessments into its credit-risk limits, Collateral requirements, pricing, tenor limits and exposure management.

(4) Before providing any Lending and Borrowing Services on behalf of a third party, the Licensee shall ensure that sufficient steps are taken on behalf of that third party to meet applicable requirements.

13. Risk management framework and stress-testing. — (1) In addition to the governance and prudential requirements under the Regulations, a Licensee shall maintain a risk-management framework for Lending and Borrowing Services covering, at a minimum:

(a) credit risk, including Borrower default and counterparty failure;

(b) market risk, including price volatility of lent assets and Collateral;

(c) liquidity risk, including the ability to meet withdrawals and obligations;

(d) operational and technology risk; and

(e) legal and enforceability risk, including Collateral realization and close-out risk.

(2) The Licensee shall ensure that liquidity risk and market risk are each monitored and tested regularly, and that appropriate measures are put in place to address such risk promptly.

(3) The Licensee shall conduct periodic stress-tests tailored to its Lending and Borrowing portfolio, including scenarios involving:

(a) sharp market declines in Collateral and lent asset values;

(b) concentrated Borrower defaults;

(c) spikes in withdrawal demands; and

(d) combined scenarios of market, liquidity and counterparty stress.

(4) Stress-test results shall be reported to the Licensee's board and used to adjust limits, Collateral requirements and contingency plans.

14. Liquidation, close-out and default management. — (1) A Licensee shall maintain documented policies and procedures governing margin calls, top-up requirements, Liquidation Events, close-out and enforcement of Collateral.

(2) Such procedures shall be transparent, non-discriminatory, consistent with Client disclosures and reasonably designed to minimize disorderly liquidation and avoidable harm to Clients.

(3) Procedures shall address at least:

(a) triggers for margin calls and Liquidation Events;

(b) notice, where commercially and operationally appropriate;

(c) methods for valuing Collateral during stressed conditions;

(d) priority and sequence of asset liquidation;

(e) treatment of shortfalls, excess proceeds and fees; and

(f) communication with Clients and the Authority where material disruption or deficiency arises.

(4) A Licensee shall not rely on discretionary or opaque liquidation powers that are materially inconsistent with its Client Agreement or disclosures.

15. Client reporting and valuation. — (1) A Licensee shall furnish to each Client, at least monthly and more frequently where necessary having regard to the product or risk profile, statements showing:

(a) total asset holdings of the Client subject to Lending Arrangements;

(b) lending and borrowing transactions executed during the period;

(c) interest accrued or payable;

(d) Collateral posted, required and any margin calls; and

(e) any liquidations, forced close-outs, defaults or other material events affecting the Client's positions.

(2) Statements shall be clear, timely and accessible and retained for at least the minimum period required under applicable law and the Regulations.

(3) Where market prices are not readily observable, the Licensee shall:

(a) use conservative valuation techniques; and

(b) disclose to Clients the limitations and uncertainties in such valuations.

(4) The Licensee shall have comprehensive and documented valuation policies and procedures sufficient to support prudent risk management, accurate Client reporting and supervisory review.

16. Public disclosures and transparency. — (1) A Licensee offering Lending and Borrowing Services shall, in a prominent place on its website or via other accessible means approved by the Authority, disclose at least:

(a) the principal risks to Client assets, including volatility, counterparty and liquidity risk;

(b) the Licensee's use-of-funds policy, including whether Client assets are on-lent and, if so, to what categories of counterparties;

(c) Collateral policies, including acceptable Collateral types, haircuts and margin practices;

(d) material concentrations of counterparty exposure, in aggregated and appropriately anonymized form; and

(e) governance, reporting and assurance arrangements relating to assets and liabilities, updated at a frequency appropriate to the business model and, in any event, not less frequently than quarterly where the Authority so requires.

(2) A Licensee shall also publish a clear explanation of:

(a) its Lending and Borrowing Services;

(b) which services are available to which Client types; and

(c) any licensing and regulatory restrictions on such services.

(3) A Licensee shall not be required to publish a fixed-format public asset-and-liability report every three months in all cases, unless the Authority specifically requires such publication. Instead, the Authority may specify the form, content and frequency of any public prudential or transparency disclosure having regard to the Licensee's business model and risk profile.

17. Record-keeping. — (1) A Licensee shall keep complete and accurate records of all Lending Arrangements, including:

(a) Client agreements and consents;

(b) transaction histories;

(c) Collateral movements and valuations;

(d) margin calls and responses; and

(e) defaults, restructurings, recoveries, liquidations and other material events.

(2) The Licensee shall maintain records sufficient to confirm and identify all Client positions and to demonstrate compliance with this Regulation and the Regulations.

(3) Records shall be retained for at least the minimum period required under AML Act, 2010, AML Rules, applicable AML/CFT Regulations and any other applicable law and the regulations and shall be made available to the Authority upon request.

18. Outsourcing and third-party arrangements. — (1) Where a Licensee relies on third parties for credit assessment, Collateral management, valuation, servicing, technology, wallet infrastructure, collection or recovery functions, the Licensee shall remain fully responsible for compliance with this Regulation and the Regulations.

(2) Such arrangements shall comply with applicable outsourcing and third-party risk requirements under the Regulations and shall include appropriate rights of access, audit, oversight, information and termination.

(3) The Licensee shall monitor third-party performance, conflicts, concentration risk and dependency risk on an ongoing basis.

Management and Investment Services Regulations

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Management and Investment Services Regulations, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026.

(2) In this Regulation:

(a) "**Discretionary Management**" means Management and Investment Services under which the Licensee has authority to make investment or portfolio decisions on behalf of the Client without obtaining a separate instruction for each transaction;

(b) "**Management and Investment Services**" means the same as defined Schedule 1 of the Act.

(c) "**Mandate**" means the contractual investment objectives, constraints, risk limits, asset universe and other terms agreed between a Licensee and a Client for the provision of Management and Investment Services;

(d) "**Model Portfolio**" means a model, strategy, allocation framework or similar structure used by a Licensee as a basis for managing one or more Client Portfolios; and

(e) "**Non-Discretionary Management**" means Management and Investment Services under which the Client retains decision-making authority and the Licensee acts on the basis of the Client's instructions or approvals;

(f) "**Performance Fee**" means any fee calculated by reference to the performance, appreciation, return or other investment outcome of a Portfolio or part of a Portfolio; and

(g) "**Portfolio**" means the Virtual Assets, positions, cash or other assets managed, administered or otherwise dealt with by a Licensee for or on behalf of a Client under a Mandate.

(3) For the avoidance of doubt, Management and Investment Services may include responsibility for staking on behalf of Clients where such staking is performed on a discretionary basis or forms part of a broader investment management Mandate. Where the relevant staking structure also falls within another regulated activity, the Licensee shall comply with the applicable Regulation and any related licence condition to the extent relevant.

3. Nature and perimeter of Management and Investment Services. — (1) A Licensee shall not hold itself out as providing Management and Investment Services unless it is authorised for that Licence Category.

(2) A Licensee providing Management and Investment Services may, subject to its Licence and the Act and Regulations:

(a) act in a fiduciary, agency or similar capacity for the purpose of managing or administering another Customer's Virtual Assets;

(b) carry out portfolio management services for one or more identified Customers;

(c) provide discretionary or non-discretionary portfolio or investment management involving Virtual Assets;

(d) operate, manage or administer a managed investment arrangement involving Virtual Assets, to the extent permitted under applicable law; and

(e) undertake ancillary functions necessary for the operation of such services, subject to compliance with all applicable safeguarding, prudential, technology and conduct requirements, and provided that such functions do not constitute a separate regulated activity requiring an additional Licence Category under the Regulations.

(3) Where a Portfolio includes derivatives, leverage, lending, liquidity provision, or other features requiring another Licence Category, the Licensee shall hold the relevant Licence Category and comply with the applicable Regulation and any related Licence condition to the extent relevant. Where a Portfolio includes staking, the Licensee shall determine the applicable regulatory treatment having regard to whether the staking is discretionary, non-discretionary, custodial or otherwise structured, and further having regard to the fact that prior written informed, explicit client consent has been obtained and kept on record, and shall comply with any applicable Regulation and licence condition accordingly.

4. Governance and fiduciary responsibility. — (1) The Licensee's board shall approve and oversee the provision of Management and Investment Services, including:

(a) investment strategies;

(b) risk appetite and limits;

(c) conflicts of interest arrangements;

(d) Mandate structures and target-market determinations; and

(e) valuation, reporting and Client asset use controls.

(2) A Licensee shall ensure that Management and Investment Services are conducted in accordance with approved policies, procedures and applicable regulatory obligations.

(3) A Licensee providing Discretionary Management shall act in the best interests of Clients and exercise due skill, care and diligence in carrying out its responsibilities.
(4) The Licensee shall maintain adequate governance, reporting lines, escalation procedures and management information to enable effective oversight of strategy risk, liquidity risk, market risk, operational incidents, concentration risk, valuation risk, Client asset use risk and Client protection issues.

5. Policies, procedures and control framework. — (1) In addition to all other applicable requirements under the Regulations, a Licensee providing Management and Investment Services shall establish, implement, maintain and enforce written policies and procedures appropriate to the nature, scale and complexity of its business, including at least policies and procedures relating to:

(a) Mandate design, approval and review;
(b) portfolio construction, rebalancing and monitoring;
(c) asset selection criteria and any listing or delisting triggers relevant to managed strategies;
(d) risk limits, including concentration, leverage, liquidity and counterparty limits;
(e) order handling, execution and trading venue selection;
(f) suitability, appropriateness and Client onboarding;
(g) conflicts of interest, inducements and personal account dealing;
(h) valuation and performance measurement;
(i) use of Client Assets, including any permitted staking, lending, liquidity provision or other yield strategies;
(j) periodic reporting and public disclosures;
(k) outsourcing and third-party dependencies; and
(l) such other matters as the Authority may reasonably require.

(2) The Licensee shall assess and, in any event, at least annually review the effectiveness of those policies and procedures and take appropriate measures to address any deficiency.
(3) A Licensee may rely on group-level policies, procedures, systems, controls or assurance arrangements, provided that they are appropriate to the Licensee's business, legally and operationally applicable in Pakistan, and sufficient to ensure compliance with the Act, the Regulations and this Regulation.

6. Public disclosures. — (1) A Licensee providing Management and Investment Services shall publish on its website, or make available through another publicly accessible means approved by the Authority, clear, fair and not misleading disclosures, including at least:

(a) a description of the services offered, including whether the service is discretionary, non-discretionary, model-based, mandate-based or otherwise;
(b) broad investment strategies and asset classes in scope;
(c) material risk factors, including market, liquidity, protocol, custody, operational, leverage and concentration risks, where relevant;

(d) fee structures, including Performance Fees where applicable;

(e) whether Client Assets may be used in connection with staking, lending, liquidity provision, leverage or similar strategies, and the principal risks of such use;

(f) high-level information on order execution and venue selection practices, where relevant;

(g) historical quarterly and annual performance of VASP in relation to managing different funds and/or investment portfolios;

(h) a statement as to how liquidity risk is managed

i) the Licensee's policies relating to data privacy, complaints handling and whistleblowing; and

(j) such other information as the Authority may reasonably require.

(2) A Licensee shall not represent in any marketing material that its Management and Investment Services are:

(a) risk-free or capital-guaranteed; or

(b) equivalent to staking-only, custody-only or yield-only services, where the service involves active management, market exposure or investment discretion.

(3) Where a service includes staking or protocol-based rewards as part of a broader Mandate, marketing shall fairly describe that component and the associated risks, including slashing, lock-up, unbonding, liquidity and protocol risks.

(4) Disclosures under this regulation shall be kept current and reviewed whenever a material change occurs.

7. Client onboarding, suitability and appropriateness. — (1) A Licensee shall establish and maintain processes to assess the suitability or appropriateness of Management and Investment Services for each Client, having regard to:

(a) the Client's investment objectives;

(b) risk tolerance;

(c) financial circumstances; and

(d) knowledge and experience relating to Virtual Assets and relevant strategies.

(2) Where a service is assessed as not suitable or not appropriate, the Licensee shall:

(a) provide a clear warning to the Client; or

(b) refrain from providing the service, where doing so would be inconsistent with law, regulation, Licence conditions, internal risk policies or the Licensee's duties to act fairly and professionally.

(3) The Licensee shall collect all necessary information from Clients for the purpose of assessing relevant factors depending on the nature of the service and shall take reasonable steps to ensure such information is accurate and up to date.

(4) The Licensee shall maintain procedures for periodic review of Client information and Mandate suitability, particularly where there is a material change in strategy, risk profile, market conditions or the Client's known circumstances.

(5) The Licensee shall maintain records of suitability and appropriateness assessments for at least the minimum period required under applicable law and the Regulations.

8. Mandate definition and approval. — (1) A Licensee shall not provide Management and Investment Services to a Client unless a documented Mandate has been agreed with that Client.

(2) The Mandate shall set out, at a minimum:

(a) the Client's investment objectives, risk tolerance and time horizon;

(b) whether the service is discretionary or non-discretionary;

(c) the types of Virtual Assets, strategies, products or protocols in scope;

(d) any restrictions, including whether derivatives, leverage, staking, lending, liquidity provision, yield strategies or unlisted tokens are permitted;

(e) any diversification, concentration, liquidity, custody or counterparty limits;

(f) the basis on which fees and charges are calculated; and

(g) the circumstances in which the Mandate may be varied, suspended or terminated.

(3) The Licensee shall maintain procedures for approving, monitoring and reviewing Mandates and any material amendment to a Mandate.

(4) The Licensee shall not depart materially from a Mandate unless—

(a) the departure is necessary to protect the Client or preserve the Portfolio in exceptional circumstances;

(b) the departure is consistent with the Client Agreement and applicable law; and

(c) the reasons for the departure are documented, recorded, and communicated to the Client.

9. Portfolio construction, execution and portfolio management. — (1) A Licensee providing Discretionary Management shall establish policies and procedures governing:

(a) portfolio construction;

(b) execution and order handling;

(c) portfolio monitoring; and

(d) rebalancing.

(2) Investment and execution decisions shall be taken in the best interests of Clients and on the basis of fair, reasonable and consistently applied criteria.

(3) The Licensee shall establish documented rules or methodologies for portfolio allocation, rebalancing, risk monitoring and deviations from Model Portfolios or strategy guidelines.

(4) Where Client Orders are routed or transmitted to a trading venue, Broker-Dealer or other intermediary, the Licensee shall ensure prompt and proper transmission of those instructions and shall maintain controls over venue selection, execution quality and allocation fairness.

(5) The Licensee shall not receive any remuneration, discount or other benefit for routing Client Orders to a particular trading platform or service provider unless that arrangement is disclosed in the Client Agreement, managed as a conflict of interest, and consistent with the Licensee's duty to act in the best interests of Clients.

10. Conduct and Client first duty. — (1) A Licensee providing Management and Investment Services shall act honestly, fairly and professionally in accordance with the best interests of its Clients.

(2) In assessing a Client's best interests, the Licensee may take into account factors including, but not limited to, Client suitability, price of Virtual Assets, costs, speed, likelihood of execution and settlement, transaction size, custody arrangements, liquidity profile and any other relevant conditions, provided that the Licensee shall act in accordance with any specific instructions provided by the Client where the service is non-discretionary.

(3) The Licensee shall not:

(a) misuse information relating to Clients' Virtual Assets, Portfolios, positions, strategies or orders; or

(b) allow proprietary trading or related-party dealings to improperly benefit from knowledge of Client positions or orders.

(4) The Licensee shall maintain policies on personal account dealing by relevant staff that prohibit front-running, misuse of confidential information and other abusive conduct.

11. Conflicts of interest and inducements. — (1) A Licensee shall identify, prevent, manage and, where appropriate, disclose conflicts of interest arising in the provision of Management and Investment Services.

(2) Such conflicts shall include, where relevant:

(a) simultaneous management of multiple Client Portfolios;

(b) management of proprietary or related-party Portfolios alongside Client Portfolios;

(c) receipt of fees, rebates or other benefits from trading venues, counterparties, issuers, validators or protocol operators;

(d) allocation of limited investment opportunities among Clients or between Clients and proprietary accounts; and

(e) any interest in assets, protocols, issuers or service providers included in a Client Portfolio.

(3) Inducements, commissions or other benefits shall be structured and managed in a manner that does not impair the Licensee's obligation to act in the best interests of Clients.

(4) Where a material conflict cannot be effectively prevented or otherwise managed, it shall be disclosed to the Client clearly and before the relevant action is taken.

12. Use of Client Assets in management services. — (1) Whether or not Client Virtual Assets used by a Licensee in the course of Management and Investment Services are held on behalf of the Client shall be clearly stated in the Client Agreement.

(2) Where the use, lending, staking, rehypothecation, liquidity provision, leverage deployment or other deployment of Client Virtual Assets requires the Client's consent under the Act or the Regulations and within the limits clearly defined by the Client, the Licensee shall obtain the Client's explicit, prior and informed consent and shall clearly disclose the nature of the activity,

the associated risks, any withdrawal restrictions, and the basis on which rewards, proceeds, losses and liabilities are allocated.

(3) The Licensee shall clearly explain the increased risks where Client Assets are used, including:

(a) the likelihood and severity of potential losses; and

(b) the impact on the Client's ability to withdraw or realize those assets.

(4) The Licensee shall not use, lend, stake, pledge, encumber or otherwise deploy Client Assets except:

(a) as required to execute an instruction of the Client or implement an agreed Mandate in accordance with the Client Agreement and the Regulations; or

(b) where expressly permitted under the Act or the Regulations and, where applicable, supported by the Client's consent in accordance with sub-regulation (2).

(5) Any rewards, proceeds or benefits attributable to Client Virtual Assets, including gains, rewards, interest, airdrops, forks or staking rewards, shall accrue to the Client unless otherwise agreed with the Client in advance in the Client Agreement and disclosed in a fair, clear and not misleading manner.

(6) A Licensee shall not take ownership of Client Virtual Assets under any Client Agreement except as expressly permitted under the Regulations.

13. Client Agreements – minimum content. — (1) In addition to all general Client Agreement requirements under the Regulations, Client Agreements for Management and Investment Services shall set out the following, to the extent applicable:

(a) a description of the Virtual Assets in scope of the Mandate sufficient to identify them;

(b) the respective rights of the Licensee, the Client and any other relevant Person in respect of the Portfolio and any staking or yield components;

(c) how and when any proceeds, gains, rewards or interest are paid or payable and, in the case of variable proceeds, how they are calculated and communicated;

(d) whether Client Virtual Assets shall be held on behalf of the Client and in what form;

(e) the Client's explicit, informed, written prior consent for any use of Client Virtual Assets by the Licensee and shall clearly disclose the nature of the activity, the associated risks, any withdrawal restrictions, and the basis on which rewards, proceeds, losses and liabilities are allocated;

(f) any right of the Client to withdraw Virtual Assets during the Mandate, including any notice, lock-up or gating provisions;

(g) any rights of the Licensee to vary the terms of the Client Agreement;

(h) any rights of the Licensee and the Client to terminate the Mandate and the consequences of termination, including settlement, unwinding and treatment of open positions or staked assets;

(i) any terms relating to fluctuation in the value of Virtual Assets to which the Mandate relates;

(j) consequences of any event of default;

(k) an explanation of the risks to which the Client may be exposed;

(l) full details of the Licensee's Client complaints procedure; and

(m) whether the Licensee receives any remuneration, discount or other benefit for routing Client Orders to a particular trading platform or service provider.

(2) Client Agreements shall be clear, fair and not misleading and shall be updated or supplemented where a material change occurs.

14. Valuation and pricing. — (1) A Licensee shall establish and apply reasonable and consistently applied methodologies for determining the value of Virtual Assets and managed Portfolios for the purposes of Client reporting, performance calculation, fee calculation, risk management and record-keeping.

(2) Where reliable and observable market prices are available, the Licensee shall ordinarily use such market prices or pricing derived from reasonably available market sources.

(3) Where market prices are not readily observable, are materially unreliable, or do not reasonably reflect the value of the relevant Virtual Asset or Portfolio position, the Licensee shall apply prudent and consistently applied alternative valuation methodologies and document the basis for doing so.

(4) Valuation methodologies, pricing sources and any material assumptions shall be documented and applied consistently.

(5) A Licensee shall not use valuation methodologies in a manner that materially misrepresents Portfolio value, performance, risk or fees.

15. Client reporting, performance measurement and transparency. — (1) A Licensee shall provide Clients with periodic reports relating to:

(a) portfolio performance;

(b) fees and charges;

(c) Portfolio composition and valuation;

(d) transactions during the reporting period; and

(e) changes affecting the managed Portfolio.

(2) Reports shall be clear, accurate and provided at appropriate intervals, and in any event not less frequently than quarterly unless a more frequent reporting period is required by the nature of the service, the Mandate, the Client category or a direction of the Authority.

(3) Where the service involves higher frequency trading, leverage, derivatives, liquidity risk or use of Client Assets, the Licensee shall provide more frequent reporting where necessary for fair and effective Client understanding.

(4) Periodic reports shall include, where applicable:

(a) the total value of Virtual Assets in the Client's account or Portfolio;

(b) all transactions entered into during the reporting period;

(c) changes in amount and valuation of assets during the reporting period;

(d) any fees, Performance Fees, expenses or charges deducted; and

(e) any material operational, protocol, custody, liquidity or counterparty event affecting the Portfolio.

(5) Performance measurement methodologies shall be documented, consistently applied and not presented in a misleading manner.

16. Fees and charges. — (1) No payment may be made, or benefit given, to the Licensee out of any Virtual Assets under its management, whether by way of fees for its services, reimbursement of expenses or otherwise, unless:

(a) it is permitted by the Client Agreement; and

(b) the Client Agreement specifies how it will be calculated and accrued, and when it will be paid.

(2) A Licensee shall not introduce any new category of fees, nor increase the rate or amount of existing fees payable out of assets under management, unless the Licensee has provided Clients with prior written notice of such introduction or increase and its effective date.

(3) The Authority may prescribe minimum notice standards for fee changes by direction, circular or other written instrument.

(4) Performance Fees, where used, shall be structured and disclosed in a fair, clear and not misleading manner and shall not incentivize conduct inconsistent with the best interests of Clients.

17. Risk management and due diligence. — (1) In addition to requirements under the Regulations and all other applicable instruments of the Authority, a Licensee shall ensure that liquidity risk and market risk in respect of Management and Investment Services are monitored and tested regularly, and that appropriate measures are put in place to address such risks promptly.

(2) The Licensee shall maintain a risk-management framework covering, at a minimum:

(a) market risk;

(b) liquidity risk;

(c) custody and safeguarding risk;

(d) counterparty and venue risk;

(e) valuation risk;

(f) leverage and derivatives risk, where relevant; and

(g) operational and technology risk.

(3) Due diligence on assets, venues, counterparties, validators, protocols or other service providers used within Client Portfolios shall be proportionate to the nature of the strategy and documented appropriately.

(4) Risk-management and due-diligence arrangements shall be subject to periodic internal assurance, compliance, risk, internal audit or external review appropriate to the nature, scale and complexity of the business.

(5) The Licensee shall provide such risk-management and due-diligence materials to the Authority upon request.

18. Record-keeping. — (1) A Licensee shall keep complete and accurate records of all Management and Investment activities, including:

(a) Client Agreements and Mandates;

(b) suitability and appropriateness assessments;

(c) Portfolio allocations, transactions, rebalancing and performance records;

(d) valuation methodologies, valuation records and pricing sources;

(e) conflict management decisions and inducement records;

(f) consents relating to Client Asset use;

(g) fee calculations and deductions; and

(h) complaints, incidents, remediation actions and communications with Clients relating to material matters.

(2) Records shall be retained for at least the minimum period required under AML Act, 2010, AML Rules, applicable AML/CFT Regulations and any other applicable law and regulations and shall be made available to the Authority upon request.

(3) Records shall be sufficiently complete, accessible and reliable to permit supervisory review, internal investigation and reconstruction of events.

Transfer and Settlement Services Regulations

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Transfer and Settlement Services Regulations, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026, and Schedule 1 of the Act.

(2) In this Regulation:

(a) "**Failed Transfer**" means a transfer, settlement or related instruction that is not executed, is defectively executed, is materially delayed, or is otherwise incomplete relative to the relevant Transfer Instruction or disclosed service conditions.

(b) "**Recipient Licensee**" means the Licensee that receives a Transfer Instruction or Virtual Asset for the benefit of a Client;

(c) "**Sender Licensee**" means the Licensee that originates or initiates a Transfer Instruction on behalf of a Client;

(d) "**Settlement Finality**" means the point, determined in accordance with the Licensee's documented arrangements and disclosed to Clients, at which a transfer or settlement is treated as final for the purposes of the relevant service;

(e) "**Third-Party Settlement Arrangement**" means any arrangement involving a payment service provider, bank, wallet infrastructure provider, blockchain infrastructure provider, custodian, correspondent, agent, or other third party used to support transfer or settlement functions; and

(f) "**Transfer and Settlement Services**" means the activity as defined in schedule I of the Act; and

(g) "**Transfer Instruction**" means any instruction from or on behalf of a Client to send, transmit, transfer, settle, redeem, burn or otherwise move a Virtual Asset or related obligation.

(3) For the avoidance of doubt, this Regulation applies to transfer and settlement activity whether conducted on-chain, off-chain, through internal ledgers, through banking rails, or through hybrid arrangements.

3. Nature and perimeter of Transfer and Settlement Services. — (1) A Licensee shall not hold itself out as providing Transfer and Settlement Services unless it is authorised for that Licence Category or is otherwise permitted under the Act or Regulations to perform such activity in connection with another licensed activity.

(2) A Licensee provides Transfer and Settlement Services where, as a business or service for or on behalf of another person, it initiates, routes, transmits, processes, settles or completes the movement of Virtual Assets or related obligations between Clients, between a Client and a third party, or as part of another Virtual Asset Service.

(3) A Transfer and Settlement authorization does not, of itself, authorize the Licensee to operate an exchange, provide discretionary management, provide standalone custody, provide lending and borrowing, provide derivatives, or conduct issuance activity other than the transfer and settlement elements of those activities to the extent separately authorised or otherwise permitted under the Act or Regulations.

(4) Where transfer and settlement functions are provided as part of Exchange Services, Broker-Dealer Services, Custody Services, Issuance Services, or other licensed activities, the Licensee shall comply with this Regulation in addition to the Regulation applicable to the primary activity.

4. Governance and oversight. — (1) The Licensee's board shall approve and oversee arrangements for the licensed services, including the following:

(a) settlement models and cycles;

(b) risk controls for operational, liquidity, counterparty and settlement risk;

(c) participant or user access criteria, where the Licensee operates or administers settlement arrangements; and

(d) escalation and incident-management frameworks for transfer and settlement failures.

(2) A Licensee shall implement policies, procedures and controls to ensure the safe, timely and accurate execution of transfers and settlements in accordance with the Act, the Regulations and this Regulation.

(3) A Licensee shall maintain adequate governance, reporting lines and management information to enable effective oversight of transfer and settlement risks, third-party dependencies, settlement failures, Client protection issues and operational incidents.

5. Policies, procedures and control framework. — (1) In addition to all other applicable requirements under the Regulations, a Licensee providing Transfer and Settlement Services shall establish, implement, maintain and enforce written policies and procedures appropriate to the nature, scale and complexity of its business, including at least policies and procedures relating to:

(a) receipt, validation and execution of Transfer Instructions;

(b) routing logic and destination verification;

(c) settlement cycles, cut-off times and Settlement Finality;

(d) reconciliation between internal records and on-chain, off-chain or account balances;

(e) handling of Failed Transfers, delayed transfers, erroneous transfers and disputed transfers;

(f) communication with Clients and counterparties in relation to transfer status, failures and exceptions;

(g) safeguarding and treatment of Client Assets used in transfer and settlement processes;

(h) Travel Rule and other AML/CFT/CPF controls relevant to transfers;

(i) outsourcing and Third-Party Settlement Arrangements;

(j) default, close-out, suspension and termination procedures where the business model includes participant obligations, prefunding, collateral, netting or similar arrangements; and

(k) such other matters as the Authority may reasonably require.

(2) A Licensee shall assess and, in any case, at least annually review the effectiveness of its policies and procedures and take appropriate measures to address any deficiency.

(3) A Licensee may rely on group-level policies, procedures, systems, controls or assurance arrangements, provided that they are appropriate to the Licensee's business, legally and operationally applicable in Pakistan, and sufficient to ensure compliance with the Act, the Regulations and this Regulation.

6. General prudential and legal compliance requirements. — (1) A Licensee providing Transfer and Settlement Services shall comply with all applicable laws of Pakistan relevant to transfer, settlement, remittance, payments, foreign exchange, sanctions, AML/CFT/CPF, consumer protection and related matters, to the extent such laws apply to the Licensee or the relevant activity.

(2) Nothing in this Regulation shall be construed as deeming the Licensee subject to every legal regime of every foreign jurisdiction connected to a transfer or settlement.

(3) Where a transfer or settlement has a cross-border element, the Licensee shall identify and manage the resulting legal, sanctions, AML/CFT/CPF, operational, and settlement risks on a risk-based basis in compliance with applicable AML framework.

(4) A Licensee shall not market or represent its service as able to complete a transfer or settlement in circumstances where it knows, or ought reasonably to know, that the relevant

transfer route, network, bank rail, counterparty arrangement or destination infrastructure is materially constrained or unavailable.

7. Integrity and accuracy of transfers. — (1) A Licensee shall establish controls to ensure the integrity and accuracy of transfers and settlements, including at least:

(a) pre-execution validation of Transfer Instructions;

(b) verification of destination details, including wallet addresses, account identifiers or equivalent routing details;

(c) reconciliation between internal records and on-chain or account balances; and

(d) error-prevention measures, including limits, validation checks and other controls appropriate to the business model.

(2) A Licensee shall maintain documented procedures for handling Failed Transfers, delayed transfers, erroneous transfers and disputed transfers, including:

(a) identification and escalation;

(b) timely communication with affected Clients and counterparties;

(c) remediation; and

(d) where appropriate, compensation arrangements.

(3) The Licensee shall not process a Transfer Instruction where available information gives rise to a material concern that the destination is invalid, incomplete, inconsistent with the Client's instruction, or otherwise gives rise to a material risk of error, fraud, sanctions breach or loss, unless the issue is first resolved.

8. Authorization and Client instructions. — (1) A Licensee shall have procedures for ensuring that all Transfer and Settlement Services carried out for a Client are authorised by the relevant Client or other person lawfully entitled to give the relevant instruction, and that the Licensee acts in accordance with that instruction at all times.

(2) A Licensee shall keep records of all Client instructions and any material amendment, cancellation, rejection, failure or execution event for at least the minimum period required under applicable law and the Regulations.

(3) A Licensee shall implement controls to authenticate the origin of instructions, prevent unauthorized execution, and detect anomalies, fraud indicators or suspicious activity.

(4) Where the Licensee receives conflicting, ambiguous or incomplete instructions, it shall suspend execution until the issue is clarified or otherwise resolved in accordance with documented procedures.

9. Responsibility for execution and failed transfers. — (1) A VASP shall be responsible for executing the Transfer Instruction in accordance with the Client's instructions and its disclosed service conditions.

(2) Where a transfer or settlement is not executed, is defectively executed, or is incomplete due to a failure attributable to the Licensee, the Licensee shall take prompt remedial action,

including tracing, correction, reversal, restoration or compensation, as appropriate to the circumstances and applicable law.

(3) A Licensee shall not be required under this Regulation to guarantee settlement outcomes that depend wholly on factors outside its control, including the functioning of public distributed ledger networks, third-party banking rails or recipient-side infrastructure, provided that the Licensee:

(a) has acted in accordance with the Client's instructions and its disclosed procedures;

(b) has taken reasonable steps to trace and remediate the failure; and

(c) has communicated the position to the Client without undue delay.

(4) Where the Recipient Licensee is the point of failure, responsibility shall be allocated according to the facts, contractual arrangements, and applicable law, and the Sender Licensee shall cooperate in tracing and resolution.

(5) Nothing in this regulation prevents the Authority from requiring a Licensee to make a Client whole where Client protection considerations and the facts of the case justify such outcome under the Act or the Regulations.

10. Settlement Finality and execution arrangements. — (1) A Licensee shall establish arrangements to ensure the timely, reliable and accurate execution of transfers and settlements.

(2) Transfer and settlement processes shall be designed to minimize operational, liquidity and counterparty risks, taking into account the characteristics of the underlying Virtual Asset networks and any off-chain settlement mechanisms used.

(3) A Licensee shall clearly disclose to Clients, and document in its internal procedures, the point at which a transfer or settlement is considered final and the conditions under which a transfer may be reversed or cancelled, if at all.

(4) Settlement arrangements shall be supported by appropriate reconciliations, exception management and Client communications and shall not expose Clients or the market to undue and avoidable settlement risk.

(5) Where a Licensee's ordinary settlement model requires a settlement cycle longer than twenty-four (24) hours because of infrastructure dependencies, market conditions, product design or another objectively justified factor, the Licensee shall notify the Authority before implementing that settlement model and shall disclose the applicable settlement cycle to Customers. A material and unexpected failure to meet the applicable settlement cycle shall be notified to the Authority without undue delay. Other settlement exceptions shall be documented and may be reported on an aggregated quarterly basis

(6) A Licensee providing Transfer and Settlement Services shall complete final settlement within twenty-four (24) hours of execution, or within an alternative settlement cycle notified under sub-regulation (5), to the extent settlement is within its reasonable control. Where settlement is delayed by distributed-ledger congestion or malfunction, counterparty or custodian performance, banking or payment rails, Travel Rule requirements, sanctions or fraud-prevention controls, or another factor outside the Licensee's reasonable control, the

Licensee shall take reasonable steps to complete settlement and communicate any material delay to affected Customers.

11. Client disclosures and transparency. — (1) A Licensee shall disclose to Clients, in a clear, fair and not misleading manner, material information relating to Transfer and Settlement Services, including at least:

(a) processing times and settlement cycles, including any cut-off times;

(b) fees and charges;

(c) risks associated with transfers and settlement, including network congestion, chain reorganizations, finality risk, counterparty dependencies and reliance on third-party providers;

(d) procedures for handling Failed Transfers, delayed transfers or disputed transfers;

(e) the point of Settlement Finality and the circumstances in which a transfer may be reversed, rejected, delayed or cancelled; and

(f) any material restriction affecting the Licensee's ability to process a transfer, including sanctions, Travel Rule, screening or destination-related limitations.

(2) Where the service includes exchange, trade or conversion as part of the transfer or settlement flow, the Licensee shall disclose all material terms associated with such exchange, trade or conversion, including applicable fees, rates, spreads and material execution assumptions.

(3) Disclosures under this regulation shall be consistent with the Licensee's obligations under the market conduct provisions of the Regulations.

12. Wallet controls and transfer restrictions. — (1) A Licensee shall establish and maintain controls governing transfers involving external wallet addresses, including controls relating to wallet verification, sanctions screening, Travel Rule compliance, transaction monitoring, source and destination checks, and risk-based restrictions.

(2) A Licensee shall not permit transfers of Client Virtual Assets to or from self-hosted, unverified, or otherwise non-compliant wallet arrangements except in accordance with controls, conditions, restrictions or approvals specified by the Authority.

(3) The Authority may restrict, prohibit, or impose conditions on transfers involving self-hosted wallets, privacy-enhancing technologies, anonymizing protocols, mixers, cross-chain bridge arrangements, or other arrangements that materially impair regulatory visibility, AML/CFT/CPF compliance, or transaction traceability.

13. Receipts, confirmations and status notifications. — (1) A Licensee shall provide the Client with an acknowledgement or receipt after receiving a Transfer Instruction, containing, where applicable:

(a) confirmation of receipt or initiation status;

(b) date and time of receipt of the instruction;

(c) amount and type of the relevant Virtual Asset or related obligation;

(d) destination or recipient reference details, where appropriate and lawful;

(e) a breakdown of fees paid or payable;

(f) transaction identification details or reference; and

(g) contact details for enquiries or complaints.

(2) Following completion or final determination of the relevant transfer or settlement event, the Licensee shall provide the Client with a completion confirmation or status update containing, where applicable:

(a) date and time of completion or other final status;

(b) amount and type of the relevant Virtual Asset transferred or settled;

(c) transaction identification details or reference; and

(d) where relevant, details of any exchange, trade or conversion completed in the course of the transfer or settlement.

(3) A Licensee may comply with this regulation through platform notifications, account statements, receipts, electronic confirmations or other durable medium appropriate to its business model, provided the information is available to the Client in a timely and intelligible manner.

(4) A Licensee shall retain all such acknowledgements, confirmations and receipts for at least the minimum period required under applicable law and the Regulations.

14. Client Assets used in transfer and settlement. — (1) A Licensee shall not use, lend, pledge, convert, encumber or otherwise dispose of Client Assets for the purposes of Transfer and Settlement Services except to the extent strictly necessary to execute the Client's instructions or otherwise as expressly permitted.

(2) A Transfer and Settlement authorization does not, of itself, permit the Licensee to rehypothecate, lend or otherwise deploy Client Assets for yield, liquidity management, treasury or proprietary purposes.

(3) Where a transfer or settlement arrangement requires temporary holding, prefunding, buffering or movement of Client Assets, the Licensee shall ensure that such arrangements comply with the safeguarding, segregation, disclosure and record-keeping requirements under the Regulations and, where applicable, the Custody Services Regulation.

(4) Any consent given by a Client for a particular settlement-related movement of assets shall not be treated as blanket consent for unrelated use of Client Assets.

15. AML/CFT/CPF, Travel Rule and sanctions interface. — (1) Transfer and Settlement Services shall be conducted in compliance with applicable AML/CFT/CPF obligations, including requirements relating to the transmission of originator and beneficiary information under the Regulations and applicable law.

(2) A Licensee shall ensure that systems and processes supporting Transfer and Settlement Services, can

(a) collect, transmit and receive required originator and beneficiary information;

(b) implement counterparty screening and risk controls; and

(c) support the retention and retrieval of records for the periods required under applicable AML/CFT/CPF laws and the Regulations.

(3) A Licensee shall implement controls to identify and manage sanctions risks, high-risk jurisdictions, high-risk counterparties, typologies of illicit finance, and other indicators relevant to transfer and settlement activity.

(4) Where required originator or beneficiary information cannot be obtained, transmitted, received or verified in accordance with applicable requirements, the Licensee shall apply risk-based escalation, restriction, rejection, suspension or reporting procedures, as appropriate.

16. Outsourcing and Third-Party Settlement Arrangements. — (1) A Licensee shall maintain sufficient operational capability, systems, personnel, and control over Transfer and Settlement Services to perform the regulated activity on a substantive and ongoing basis and shall not operate as a mere intermediary, booking entity, or pass-through arrangement for an unlicensed or third-party operator.

(2) A Licensee shall not outsource the core/principal operational responsibility for Transfer and Settlement Services.

(3) Where Transfer and Settlement functions rely on outsourcing or Third-Party Settlement Arrangements, the Licensee shall retain full responsibility for compliance with this Regulation and with its obligations to Clients.

(4) Outsourcing and third-party arrangements shall:

(a) comply with applicable outsourcing and third-party risk requirements under the Regulations;

(b) provide the Licensee with adequate audit, access and information rights; and

(c) allow the Authority, where applicable, to obtain information and to conduct or commission reviews of relevant arrangements.

(5) The Licensee shall conduct due diligence on material third-party providers and monitor their performance, legal risk, operational resilience and dependency risk on an ongoing basis.

(6) Where a material third-party dependency creates a risk of interruption or disorderly failure of transfer or settlement services, the Licensee shall maintain contingency arrangements and escalation procedures appropriate to that risk.

17. Default, prefunding and participant-failure procedures. — (1) Where a Licensee's actual business model includes participant obligations, prefunding, collateral, netting, close-out, or similar settlement mechanisms, it shall maintain documented default-management procedures proportionate to that business model and risk profile.

(2) Nothing in sub-regulation (1) shall be construed as permitting settlement netting, offsetting or similar arrangements in a manner inconsistent with applicable foreign exchange, payment-system, or banking laws, including requirements relating to routing, reporting or settlement of fiat currency transactions through authorised channels.

(3) Such procedures may include suspension, cancellation, reversal, close-out, use of collateral, restriction of further activity, or other remedial measures, but shall not require a default fund,

portability regime, or central-counterparty style structure unless the Licensee in fact operates such a model or the Authority specifically requires it.

(4) Default procedures shall clearly define:

(a) the circumstances constituting financial or operational default;

(b) how different types of default may be treated;

(c) decision-making authority and escalation processes; and

(d) communication with affected Clients, Participants, counterparties and the Authority.

(5) A Licensee shall be able to demonstrate, upon request, the rationale for its default-management arrangements, including how any such arrangements correspond to the specific risks arising from its activities.

18. Record-keeping and audit trail. — (1) A Licensee shall keep, for at least the minimum period required under AML Act, 2010, AML Rules, applicable AML/CFT Regulations and any other applicable law, and the Regulations, records sufficient to:

(a) evidence compliance with this Regulation;

(b) reconstruct individual transfers, settlements and related events; and

(c) support investigations into failed execution, fraud, sanctions concerns, Travel Rule issues or other misconduct.

(2) Records shall include, at a minimum:

(a) Transfer Instructions and any amendments, cancellations, rejects or exceptions;

(b) time-stamped records or equivalent sequencing records of receipt, routing and execution;

(c) screening results and Travel Rule transmission data, where applicable;

(d) communications with Clients and counterparties relating to material transfer or settlement events;

(e) reconciliations, discrepancy investigations and remediation actions; and

(f) records of use of Third-Party Settlement Arrangements and any material incident affecting them.

(3) Records shall be sufficiently complete, accessible and reliable to permit supervisory review, internal investigation and reconstruction of events.

19. Public disclosures. — (1) In addition to any disclosure requirements under the Regulations, a Licensee providing Transfer and Settlement Services shall publish on its website, or make available through another publicly accessible means approved by the Authority:

(a) a description of material conflicts of interest arising from its transfer and settlement activities and how they are managed;

(b) its policies relating to data privacy, complaints handling and whistleblowing;

(c) whether it refers or introduces Clients to other Persons in connection with Transfer and Settlement Services and whether it receives any material monetary or non-monetary benefit from such arrangements;

(d) whether any accounts, funds, Virtual Assets or other material service components are maintained or performed by a third party;

(e) a statement in terms of Travel Rule compliance; and

(f) such other information as the Authority may reasonably require.

(2) Public disclosures under this regulation shall be kept current and reviewed whenever a material change occurs.

Issuance Services Regulation

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Issuance Services Regulation, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026.

(2) In this Regulation:

(a) "**Asset-Referenced Token**" or "**ART**" means as defined in Schedule I of the Act.

(b) "**Fiat-Referenced Token**" or "**FRT**" means as defined in the Act.

(c) "**Issuance Services**" means Asset-Referenced Token Issuance Services or Fiat-Referenced Token Issuance Services, as applicable;

(d) "**Issuer**" means a Licensee authorised to provide one or both categories of Issuance Services;

(e) "**Reserve Assets**" means the segregated assets maintained by an Issuer to support the value and redemption of an ART or FRT in accordance with the Act, the Regulations and this Regulation;

(f) "**Reference Asset**" means the fiat currency, asset or basket of assets to which an ART or FRT refers for the purpose of its value representation;

(g) "**Significant Issuer**" means an Issuer that meets the thresholds and criteria prescribed under the Regulations or otherwise determined by the Authority in accordance with the Act; and

(h) "**Whitepaper**" means the primary public disclosure document relating to an Issuance prepared in accordance with this Regulation.

(3) For the avoidance of doubt, an Issuer authorised for one category of Issuance Services shall not issue, market, administer or manage a token of the other category unless separately authorised to do so or expressly permitted by the Authority in writing.

3. Nature and perimeter of Issuance Services. — (1) A Person shall not hold itself out as providing Issuance Services unless it is authorised for the relevant Licence Category.

(2) An Issuer may, subject to its Licence and the Act and Regulations:

(a) create, issue, offer, redeem, administer for an ART or FRT;

(b) manage the issuance, burning, circulation, reserve management, redemption and disclosure arrangements associated with ART or FRT issuance that programme; and

(c) perform ancillary functions that are integral to the operation of such services, subject to compliance with all applicable safeguarding, conduct, prudential and disclosure requirements, and provided that such functions do not constitute a separate regulated activity requiring an additional Licence Category unless permitted.

(3) Nothing in this Regulation limits the types of assets that may be tokenized, provided that the resulting Virtual Asset is not otherwise prohibited by applicable law and complies with the applicable issuance, disclosure, prudential and conduct requirements.

4. Issuance authorization and approval. — (1) An Issuer shall not issue an ART or FRT unless the relevant Issuance has been notified to, or approved by, the Authority in accordance with the risk-based approach. The Authority may require prior approval for specified categories of Issuance, including restricted, retail-facing, complex or systemically significant issuance.

(2) An application for approval of an Issuance shall include, at a minimum:

(a) a description of the token structure, stabilization mechanism and intended use cases;

(b) proposed reserve composition, custody and valuation arrangements;

(c) redemption modalities and any conditions or limitations;

(d) key risk factors and mitigation measures;

(e) the proposed Whitepaper and related disclosure materials; and

(f) such other information as the Authority may require.

(3) The Authority may grant approval, grant approval subject to conditions, or refuse approval, having regard to:

(a) the adequacy and quality of Reserve Assets;

(b) governance and operational arrangements;

(c) the effect on holders, markets and financial stability; and

(d) consistency with applicable law and regulatory policy.

(4) The Authority may impose conditions on approval, including conditions relating to reserve management, disclosures, redemption rights, issuance limits, distribution restrictions, operational controls, or enhanced reporting, and may vary such conditions over time.

(5) Notwithstanding subregulaion (2) above, an application or notification for an Issuance shall include such information as is proportionate to the nature, scale, complexity and risk profile of the relevant Issuance. The Authority may specify simplified requirements for pilot, restricted, professional-only or low-risk programmes

5. Governance and accountability of issuers. — (1) The Licensee's board shall approve and oversee:

(a) the design and operation of each Issuance;

(b) reserve, liquidity and risk-management policies for each issuance;

(c) redemption policies, including any gating, suspension or limitation mechanisms; and

(d) disclosure and reporting frameworks to token holders, the public and the Authority.

(2) Senior management shall be responsible for:

(a) implementing policies, procedures and controls approved by the Licensee's board;

(b) ensuring that issuance, reserve management, custody, transfer and redemption processes are operated in accordance with the Act, the Regulations, notices, directives, circulars, guidelines issued thereunder; and

(c) ensuring adequate resources, including treasury, legal, risk, compliance and technology, to support safe and continuous operation of each Issuance.

(3) An Issuer shall establish clear segregation, proportionate to the nature, scale and complexity of its activities, between:

(a) token issuance and lifecycle management;

(b) reserve management and treasury;

(c) custody and safekeeping of Reserve Assets as specified by the Authority;

(d) compliance, risk and internal audit; and

(e) technology, including smart-contract management and supporting systems.

6. Reserve assets and full backing. — (1) An Issuer shall maintain Reserve Assets sufficient at all times to support the value and redemption of issued tokens in accordance with the terms disclosed to token holders and approved by the Authority.

(2) Reserve Assets shall:

(a) be appropriately valued on a regular basis using robust and transparent methodologies;

(b) be segregated from the Issuer's own assets and clearly identified as backing the relevant Issuance;

(c) be held and structured so as to provide, to the extent permitted by applicable law, protection from claims of the Issuer's creditors in the event of insolvency; and

(d) be composed in accordance with standards specified by the Authority, including any requirements on asset quality, maturity, currency, diversification and concentration limits.

(3) Reserve Assets shall be maintained at a level sufficient to support the Issuer's outstanding redemption liabilities in accordance with the Act and the Regulations. The Authority may prescribe, by direction, the timing, methodology, and operational tolerances applicable to reserve maintenance and remediation of temporary mismatches.

(4) Nothing in this Rulebook permits the Issuer to maintain Reserve Assets below one hundred percent (100%). Any temporary deviation that may arise from bona fide operational or settlement timing differences shall be promptly identified, monitored, and rectified in accordance with standards specified by the Authority.

(5) The Issuer shall maintain policies and procedures for regular calculation of outstanding token liabilities and for monitoring reserve adequacy at a frequency proportionate to the nature, scale, complexity and redemption profile of the Issuance, and in accordance with any minimum frequency specified by the Authority.

7. ART-specific reserve requirements. — (1) For an Asset-Referenced Token, Reserve Assets shall comprise the underlying assets referenced by the token or such eligible categories of underlying assets as may be prescribed by the Authority.
(2) An ART shall at all times be fully backed by the relevant underlying assets and shall not be backed by, or derive its value from, other Virtual Assets.
(3) The Issuer shall ensure that the composition of Reserve Assets for an ART is appropriate to the reference structure, disclosed to holders, and capable of supporting the redemption arrangements of the issuance.
(4) Where the ART refers to more than one underlying asset, the Issuer shall maintain and disclose a methodology for allocation, valuation and rebalancing of Reserve Assets consistent with the disclosed stabilization mechanism.

8. FRT-specific reserve requirements. — (1) For a Fiat-Referenced Token, Reserve Assets shall comprise High quality liquid assets as defined in Pakistan Virtual Assets Services Regulations, 2026 or such other eligible assets as may be specified or approved by the Authority.
(2) Reserve Assets for an FRT shall, unless otherwise approved by the Authority, be exclusively denominated in the reference fiat currency.
(3) Reserve Assets for an FRT shall be unencumbered and freely available to meet redemption obligations.

9. Custody and safeguarding of reserve assets. — (1) Reserve Assets shall be held with a Custodian licensed under the Custody Services framework or with another entity that is regulated, supervised, as specified and agreed by the Authority for this purpose, having regard to the nature of the Reserve Assets and the risk profile of the Issuance.
(2) Custody arrangements shall ensure:

(a) legal and operational segregation of Reserve Assets from the Issuer's own assets;

(b) appropriate control over movements of Reserve Assets, including segregation of duties and multi-level approvals; and

(c) auditability and timely reconciliation between reserve records, custodial records and the outstanding token supply.

(3) Reserve Assets shall be held in a manner that provides effective protection for holders in the event of the Issuer's insolvency, including legal and operational arrangements that support segregation and bankruptcy remoteness and the timely redemption or return of assets for the benefit of holders.
(4) Reserve Assets shall not be rehypothecated, pledged, encumbered, subjected to set-off or otherwise made unavailable for redemption obligations, except to the extent expressly permitted by law and approved by the Authority.

10. Redemption rights and mechanisms. — (1) An Issuer shall provide clear, enforceable and transparent rights for holders to redeem ARTs or FRTs:

(a) in the case of an FRT, at par value; and

(b) in the case of an ART, in accordance with the valuation and redemption basis approved under these Regulations and disclosed in the Whitepaper.

(2) A redemption request shall be executed without undue delay and ordinarily within twenty-four (24) hours of receipt of a complete and valid request. A longer period may apply where reasonably necessary because of non-Business Days, banking or settlement hours, the nature or liquidity of the Reference Asset, distributed-ledger conditions, third-party infrastructure, fraud-prevention controls, sanctions screening or another factor outside the Issuer's reasonable control, provided that the applicable timeframe and material conditions are clearly disclosed to holders. The Issuer shall notify the Authority without undue delay of any material or recurring failure to meet the applicable timeframe. Other exceptions and the reasons for them shall be documented and included in the Issuer's quarterly regulatory report.

(3) Redemption processes shall be accessible to eligible holders and executed within the timelines disclosed in advance, subject to the nature of the product, distribution model, Client category, applicable law and any operational, fraud-prevention or sanctions-related controls that are reasonably necessary.

(4) Any proposed temporary suspension, gating or limitation of redemptions shall:

(a) be permitted under the terms and conditions disclosed to holders;

(b) be objectively justified on risk, operational or prudential grounds; and

(c) be promptly notified to the Authority and disclosed to holders, including the reasons and expected duration.

(5) An Issuer shall maintain documented redemption procedures and shall ensure that marketing and other communications do not misrepresent the speed, certainty or conditions of redemption.

(6) The Authority may specify, by rule, regulation, direction or condition, more detailed redemption timelines, operational procedures or permissible exceptions for specified categories of token or Issuer.

11. Whitepaper and primary disclosure obligation. — (1) An Issuer shall prepare, publish and maintain a Whitepaper or such other principal disclosure document as may be specified by the Authority for the relevant category of Issuance before the relevant token is offered, marketed or otherwise made available to the public, unless otherwise exempted by the Authority.

(2) A Whitepaper shall be clear, accurate, fair and not misleading and shall contain the information necessary for an informed assessment of the Issuance, the token, the rights of holders and the principal risks associated with holding, using or redeeming the token.

(3) The Issuer shall be fully responsible for the accuracy, completeness and ongoing maintenance of the Whitepaper.

(4) The Whitepaper shall be updated without undue delay where a material change occurs in relation to the Issuance, the token, the reserve structure, redemption rights, key risks, or any other information the omission or misstatement of which would make the Whitepaper materially misleading.
(5) The Authority may prescribe the form, content, timing, language, publication method and update process for Whitepapers by implementation Instrument issued under this Regulation.

12. Minimum content of Whitepaper. — (1) A Whitepaper shall include the contents as specified in the Schedule 1 of these Regulations.
(2) Notwithstanding the content specified above, the Authority may issue templates or simplified disclosure requirements for restricted, pilot, professional-only or otherwise lower-risk issuances.

13. Ongoing disclosures and public transparency. — (1) An Issuer shall disclose to token holders and the public, in a prominent and accessible manner, information, including, but not limited to:

(a) the nature and structure of the token, including Reference Assets, stabilization mechanism and intended use cases;

(b) Reserve Assets, reserve composition and custody arrangements;

(c) redemption rights, processes and any limitations or conditions;

(d) key risks associated with the token, including legal, operational, liquidity, custody and market risks; and

(e) fees and charges, where applicable.

(2) Disclosures shall be:

(a) clear, accurate, fair and not misleading;

(b) consistent with obligations under the market conduct framework and any applicable marketing rules; and

(c) updated on a timely basis where material changes occur.

(3) An Issuer shall publish, at a frequency and in a form specified by the Authority, information on reserve composition, reserve adequacy and token liabilities, including any assurance or attestation reports where required.
(4) For an FRT, the Issuer shall disclose on its website, or through another public channel approved by the Authority, information on tokens in circulation, Reserve Assets and reserve sufficiency at the frequency specified by the Authority, taking into account the size, scale, risk profile, holder base and systemic relevance of the Issuer or the token.
(5) The Authority may require more frequent or more granular public disclosures where warranted by the size, scale, risk profile or systemic relevance of the Issuer or the token.
(6) The Authority may differentiate public reporting, assurance and disclosure frequency between Significant Issuers and other Issuers, and between retail-facing issuances and professional-only or restricted issuances.

14. Audits, attestations and assurance. — (1) An Issuer shall ensure that its Issuance is subject to independent external audit or assurance to the extent and at the frequency required by the Authority, having regard to the nature, scale and risk profile of the programme.

(2) The Issuer shall obtain, at the intervals prescribed by the Authority, independent assurance in relation to at least the following, but not limited to:

(a) the number and value of tokens in circulation;

(b) the composition and value of Reserve Assets; and

(c) such other matters as the Authority may reasonably require, having regard to the materiality and risk profile of the relevant Issuance.

(3) The form, scope, methodology and frequency of any audit, attestation or assurance exercise shall be determined by the Authority having regard to the nature, scale and risk profile of the relevant Issuance.

(4) A restricted or pilot Issuance may be subject to proportionate assurance and reporting arrangements specified by the Authority, provided that Reserve Assets remain fully segregated and redemption rights remain protected.

(5) An Issuer shall submit to the Authority the results of any assurance exercise immediately after completion.

15. Stabilization and risk management. — (1) An Issuer shall establish and maintain arrangements to identify, measure, monitor and manage risks affecting the stability of ARTs or FRTs, including market, liquidity, credit, operational, technology and legal risks.

(2) Stabilization mechanisms, including where applicable creation and redemption procedures, use of market makers and rebalancing of reserves, shall be:

(a) clearly documented and disclosed;

(b) subject to governance oversight; and

(c) operated in a manner that is consistent with disclosed terms and does not unduly disadvantage holders.

(3) The Issuer shall conduct stress testing and contingency planning at a frequency and level of sophistication commensurate with the nature, scale and complexity of the Issuance and any specific requirements imposed by the Authority.

(4) Where a material risk to programme continuity, reserve adequacy or redemption integrity is identified, the Issuer shall take prompt remedial action and notify the Authority without delay.

16. Outsourcing and third-party arrangements. — (1) Where an Issuer relies on third parties for reserve management, custody, technology, transfer and settlement, redemption processing, Whitepaper preparation, assurance or other material functions, the Issuer shall remain fully responsible for compliance with the Act, the Regulations and this Regulation.

(2) Such arrangements shall comply with applicable outsourcing and third-party risk requirements under the Regulations and shall provide the Issuer with adequate rights of access, audit, oversight, information and termination.
(3) The Issuer shall conduct due diligence on material third parties and monitor their performance, resilience, legal risk, conflicts and dependency risk on an ongoing basis.
(4) The Authority shall have access, audit and information rights in respect of material outsourced arrangements to the extent permitted by law and contract.

17. Significant Issuers. — (1) A Significant Issuer shall comply with enhanced requirements, including enhanced reporting, disclosure, governance and risk-management requirements, as prescribed by the Regulations or otherwise imposed by the Authority in accordance with the Act.
(2) An Issuer shall be deemed "significant" where:
(a) the total market capitalization of the fiat referenced or Asset-Referenced token exceeds five billion Pakistani Rupees (PKR 5,000,000,000); or
(b) the number of users based in Pakistan holding the fiat referenced or Asset-Referenced token exceeds five million (5,000,000); or
(c) such other thresholds as may be Prescribed by the Authority.
(3) Significant Issuers shall be required to maintain additional own funds equivalent to at least three percent (3%) of reserve assets, capped at PKR 3 billion (or such lower or higher cap as the Authority may prescribe in Regulations) and shall submit enhanced risk assessment and governance.
(4) Without prejudice to sub-regulation (1), the Authority may impose proportionate additional conditions on a Significant Issuer's licence or registration having regard to financial stability, consumer protection, market integrity and cross-border risks.
(5) The Authority may require a Significant Issuer to maintain enhanced monitoring, testing, wind-down planning, operational resilience measures, redemption controls, reserve governance arrangements or additional disclosures.

18. Limited Scope Issuance. — (1) The Authority may grant a limited scope licence for issuance of an ART or FRT on a pilot basis, subject to:
(a) caps on outstanding supply, number or type of holders, and transaction volumes;
(b) limitations on distribution channels and use cases;
(c) enhanced disclosures to holders regarding pilot status and risks;
(d) redemption controls and operational safeguards; and
(e) any additional conditions necessary to protect holders and market integrity.
(2) A limited scope issuance shall remain subject to the core requirements on reserve segregation, programme governance, clear disclosures and protection of redemption rights, except to the extent the Authority expressly modifies specific requirements on a proportionate basis.

19. Monitoring, notification and remediation. — (1) An Issuer shall establish systems and controls to monitor compliance with this Regulation on an ongoing basis, including stress testing and contingency planning commensurate with the nature, scale and complexity of the Issuance.

(2) An Issuer shall notify the Authority without delay where it reasonably anticipates, or becomes aware, that it has failed or is likely to fail to meet any requirement under this Regulation, and shall provide a remedial action plan within the timeframe specified by the Authority.

(3) The Authority may require enhanced reporting, restrictions, programme modifications, redemption controls or other remedial measures where an Issuer is in breach or is likely to breach any requirement under this Regulation.

(4) The Authority may, on a risk-based basis and where necessary to advance the objectives of the Act, require an Issuer to hold and maintain additional paid-up capital, liquid financial resources, insurance, reserve assets or operational safeguards, having regard to the size, scope, geographic exposure, complexity and nature of the Issuer's activities and operations.

20. Record-keeping. — (1) An Issuer shall keep complete and accurate records relating to each Issuance, including the following:

(a) programme approvals and related conditions;

(b) Whitepapers and all material updates;

(c) reserve calculations, reserve holdings and reconciliations;

(d) assurance reports, attestations and audit materials;

(e) redemption requests, processing times, restrictions and outcomes;

(f) disclosures to holders and the public;

(g) complaints, incidents, remediation actions and communications with the Authority; and

(h) material outsourcing and third-party arrangements.

(2) Records shall be retained for at least the minimum period required under AML Act, 2010, AML Rules, applicable AML/CFT Regulations and any other applicable law, and the Regulations and shall be made available to the Authority upon request.

(3) Records shall be sufficiently complete, accessible and reliable to permit supervisory review, internal investigation and reconstruction of events.

Derivatives Services Regulation

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Derivatives Services Regulation, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026.

(2) In this Regulation:

(a) "**Derivatives Services**" means as defined in Schedule 1 of the Act;

(b) "**Derivative Contract**" means a futures contract, perpetual contract, option, swap, contract for difference or other contract whose value is derived from a Virtual Asset or other permitted underlying or reference;

(c) "**Eligible Collateral**" means collateral that the Licensee has determined, in accordance with its documented policies, to be acceptable for Margin purposes having regard to liquidity, volatility, concentration, legal certainty and realizability;

(d) "**Funding Payment**" means any periodic payment, adjustment or transfer associated with a perpetual or similar contract;

(e) "**Initial Margin**" means the Margin required to establish a Derivative Contract or Leverage Arrangement;

(f) "**Leverage Arrangement**" means any arrangement under which a Client obtains a leveraged, margined or synthetic exposure to a Virtual Asset or related market movement, whether through a Derivative Contract, leveraged token, financing mechanism or similar structure;

(g) "**Liquidation**" means the forced reduction, close-out, or termination of a Derivative Contract or Leverage Arrangement due to insufficient Margin, breach of risk limits, or other event specified in the relevant Regulation or the Client Agreement;

(h) "**Maintenance Margin**" means the minimum Margin that must be maintained to keep a Derivative Contract or Leverage Arrangement open; and

(i) "**Margin**" means collateral posted by a Client or Licensee in support of an open Derivative Contract or Leverage Arrangement;

(3) For the avoidance of doubt, Derivatives Services may be cash-settled, fiat-margined, coin-margined, physically settled or otherwise settled, provided the structure is lawful and permitted under the Act, the Regulations and the terms of the Licence.

3. Eligibility for authorization. — (1) A Person shall not be eligible to apply for, obtain or hold a licence to provide Derivatives Services unless that Person:

(a) holds a valid Broker-Dealer Services licence or Exchange Services licence; or

(b) otherwise satisfies such operational, prudential, conduct and client-protection requirements as the Authority may specify for a Derivatives Services licence, including where services are limited to Professional Clients or Institutional Clients.

(2) Where a Licensee holding Derivatives Services ceases to hold the underlying Broker-Dealer Services licence or Exchange Services licence referred to in sub-regulation (1), the Licensee shall:

(a) notify the Authority immediately; and

(b) cease offering new Derivatives Services unless otherwise directed by the Authority.

(3) The Authority may impose such restrictions, wind-down requirements or other licence conditions as it considers necessary where a Licensee no longer satisfies the requirement in sub-regulation (1).

4. Nature and perimeter of Derivatives Services. — (1) A Licensee shall not hold itself out as providing Derivatives Services unless it is authorised for that Licence Category and provided explicit approval of the Authority to deal with institutional, professional and/or retail clients.

(2) A Licensee providing Derivatives Services may, subject to its Licence and the Act and Regulations, and in compliance with Regulation 3 (Eligibility for authorization):

(a) offer, arrange, deal in, or facilitate Derivative Contracts;

(b) offer margin or leveraged arrangements, including leveraged spot products, leveraged tokens, synthetic exposures and similar products;

(c) provide margining, liquidation, risk management and default-management arrangements that are integral to such services; and

(d) perform ancillary functions that are integral to the operation of such services, subject to compliance with all applicable safeguarding, conduct, prudential and disclosure requirements, and provided that such functions do not constitute a separate regulated activity requiring an additional Licence Category under the Regulations

(3) Where there is doubt whether a product, arrangement or instrument falls within the mandate of the Securities and Exchange Commission of Pakistan or the State Bank of Pakistan, the Licensee shall not offer the product until regulatory clarity has been obtained in accordance with the Act and the Regulations.

(4) The Authority may approve a modified or lighter application of specified conduct, disclosure, reporting or appropriateness requirements for Derivatives Services offered exclusively to Professional Clients or Institutional Clients, provided that prudential, market integrity and Client asset protection objectives remain adequately met.

5. Governance and risk oversight. — (1) The Licensee's board shall approve and oversee the Derivatives business, including:

(a) product design, approval and review;

(b) risk appetite and limits for market, credit, liquidity, counterparty, settlement and operational risks;

(c) Margin, collateral and Liquidation policies;

(d) Client eligibility and target-market determinations; and

(e) conflicts of interest arrangements relevant to derivatives and leveraged products.

(2) Senior management shall implement policies, procedures and controls to manage the risks arising from Derivatives Services and shall ensure that those risks are reflected in the Licensee's prudential, capital and liquidity planning.

(3) The Licensee shall ensure that Derivatives activities are subject to effective governance, risk oversight and control by Key Individuals and staff with competence appropriate to the scale, complexity and risk profile of the business.

(4) The Licensee shall maintain adequate governance, reporting lines, escalation procedures and management information to enable effective oversight of exposures, margin sufficiency, liquidation events, concentration risk, operational incidents and Client protection issues.

6. Policies, procedures and control framework. — (1) In addition to all other applicable requirements under the Regulations, a Licensee providing Derivatives Services shall establish, implement, maintain and enforce written policies and procedures appropriate to the nature, scale and complexity of its business, including at least policies and procedures relating to:

(a) product approval and classification;

(b) Client onboarding, eligibility and appropriateness;

(c) Margin methodologies and collateral standards;

(d) leverage limits and exposure controls;

(e) valuation, mark-to-market and price-source controls;

(f) Funding Payments and contract adjustment mechanisms, where applicable;

(g) Liquidation, close-out and default management;

(h) handling of market disruption, trading suspension, system outage and severe volatility;

(i) safeguarding and treatment of Client Assets used as Margin or collateral;

(j) management of conflicts of interest, including proprietary trading and related-party activity;

(k) stress-testing, model validation and back-testing; and

(l) such other matters as the Authority may reasonably require.

(2) The Licensee shall assess and, in any event, at least annually review the effectiveness of those policies and procedures and take appropriate measures to address any deficiency.

(3) A Licensee may rely on group-level policies, procedures, systems, controls or assurance arrangements, provided that they are appropriate to the Licensee's business, legally and operationally applicable in Pakistan, and sufficient to ensure compliance with the Act, the Regulations and this Regulation.

7. Product governance and scope notification. — (1) Before offering a new type of Derivative Contract or Leverage Arrangement, a Licensee shall assess the nature, legal character, settlement model, leverage features, target market, risk profile, valuation methodology, margin methodology, operational dependencies and market-abuse risks of the product.

(2) The Licensee shall not offer a Derivative Contract or Leverage Arrangement unless it is satisfied that the product is consistent with the Act, the Regulations, this Regulation and the terms of its Licence.

(3) The Licensee shall maintain internal records identifying, for each material product type:

(a) the type of contract or arrangement;

(b) whether it is made available to Retail Clients, Professional Clients or any other category of Client recognized under the Act, the Regulations or a direction of the Authority;

(c) the settlement model;

(d) the underlying Virtual Asset or other permitted reference; and

(e) the principal conduct, risk and operational controls applicable to the product.

(4) The Authority may require the Licensee to provide prior notification, additional information, restrictions, or enhanced controls in relation to particular classes of Derivative Contracts or Leverage Arrangements.

8. Client categorization, onboarding and appropriateness. — (1) A Licensee shall not provide Derivatives Services to a Client unless it has assessed the Client's eligibility and, where applicable, the appropriateness of the relevant product or service for that Client.

(2) In assessing appropriateness, the Licensee shall obtain sufficient information regarding the Client's knowledge and experience in relation to derivatives, leverage, margining, liquidation risk and relevant Virtual Asset markets.

(3) If the Licensee concludes that a product or service is not appropriate for a Retail Client, it shall warn the Client clearly of that assessment and record that the warning has been provided.

(4) If the Client does not provide sufficient information to enable an appropriateness assessment, the Licensee shall warn the Client that such a determination cannot be made.

(5) Nothing in sub-regulations (3) and (4) requires the Licensee to proceed with the transaction where doing so would be inconsistent with law, regulation, Licence conditions, internal risk policies or the Licensee's duties to act fairly and professionally.

(6) A Licensee shall maintain procedures for heightened onboarding and suitability-related review where it offers particularly complex, high-leverage or high-volatility products.

9. Client disclosures and risk warnings. — (1) A Licensee providing Services shall disclose to Clients, in a clear, fair, timely and not misleading manner, material information including at least:

(a) the nature of the Derivative Contract or Leverage Arrangement;

(b) the extent and effect of leverage, including the potential for amplified losses and total loss of Margin;

(c) Margin requirements, margin-call processes, top-up obligations and Liquidation triggers;

(d) fees, charges, spreads, commissions and Funding Payments;

(e) settlement model and, where relevant, delivery mechanics;

(f) outage, system disruption, trading suspension and market-dislocation risks;

(g) the basis on which prices, marks, indices, reference rates or valuations are determined;

(h) any rights of the Licensee to amend Margin requirements, risk limits, settlement parameters or other product terms; and

(i) conflicts of interest, including proprietary trading, internalization, related-party liquidity and liquidation arrangements.

(2) A Licensee shall not market a leveraged or derivative product as low-risk, capital-protected, or suitable for all Clients unless that representation is accurate and substantiated.

(3) Risk disclosures shall be tailored to the nature of the product and the category of Client to whom it is offered.

10. Client Agreements. — (1) In addition to general Client Agreement requirements under the Regulations, a Client Agreement for Derivatives Services shall, to the extent applicable, set out clearly:

(a) the nature of the Derivative Contract or Leverage Arrangement;

(b) Initial Margin and Maintenance Margin requirements and how they are determined;

(c) the circumstances in which Margin requirements may be changed;

(d) acceptable forms of collateral and applicable haircuts;

(e) margin calls, timing, permitted methods of satisfaction, and consequences of failure to meet a margin call;

(f) Liquidation and close-out rights, including when and how the Licensee may reduce or terminate a position;

(g) settlement terms, including whether the product is cash-settled, physically settled, fiat-margined or coin-margined;

(h) Funding Payments, financing charges, commissions, fees and other costs;

(i) any rights of the Licensee to suspend trading, reject orders, restrict positions, amend risk limits or otherwise intervene in exceptional circumstances;

(j) any rights of the Client to withdraw excess Margin or terminate positions and the consequences of doing so; and

(k) the Licensee's complaints procedure and escalation channels.

(2) The Client Agreement shall be clear, fair and not misleading and shall be consistent with the market conduct requirements under the Regulations.

11. Margin framework. — (1) A Licensee shall establish and maintain a documented Margin framework that is prudent, risk-sensitive, transparent and appropriate to the nature, scale and complexity of its Derivatives business.

(2) The Margin framework shall address, at a minimum:

(a) Initial Margin and Maintenance Margin methodologies;

(b) eligible forms of Margin and collateral;

(c) valuation methodologies and application of haircuts;

(d) concentration limits and wrong-way risk;

(e) frequency of margin calculation and revaluation;

(f) margin-call processes and escalation procedures; and

(g) treatment of exceptional volatility, illiquidity or other stressed market conditions.

(3) Margin requirements shall be designed to reflect the risk profile of the product, the Client, the underlying market, the settlement model and any operational or liquidity constraints.

(4) A Licensee shall not rely on a fixed leverage cap alone as a substitute for a prudent Margin framework.

12. Eligible collateral and safeguarding of margin assets. — (1) A Licensee shall establish and maintain documented policies governing the acceptance, valuation, monitoring and liquidation of collateral used for Derivatives Services.

(2) Where a Licensee holds, controls, safeguards or administers Client Assets as Margin or collateral in connection with Derivatives Services, it shall ensure that such arrangements achieve an outcome equivalent to the safeguarding, segregation, reconciliation, disclosure and Client protection standards applicable under the Act, the Regulations and, where relevant, the Custody Services framework, having regard to the nature, scale and risk profile of the relevant activity.

(3) Eligible Collateral shall consist only of assets that are sufficiently liquid, readily realizable, capable of prudent valuation and legally available for enforcement.

(4) Where Client Assets are held, controlled or applied as Margin or collateral on an incidental basis, the Licensee shall have requisite license and achieve Client protection outcomes equivalent to those applicable to standalone Custody Services, applied proportionately to the nature, scale and purpose of the activity, and shall not use such arrangements to circumvent applicable custody requirements.

(5) Client Margin and collateral must be fully segregated and safeguarded, or otherwise protected by equivalent safeguarding arrangements, to the extent required under the Regulations and shall not be treated as the Licensee's proprietary assets.

(6) The Licensee shall not use, lend, pledge, stake, rehypothecate or otherwise deploy Client Margin or collateral except with client's prior written explicit and informed consent and shall clearly disclose the nature of the activity, the associated risks, any withdrawal restrictions, and the basis on which rewards, proceeds, losses and liabilities are allocated.

13. Leverage limits and exposure controls. — (1) A Licensee shall implement leverage limits proportionate to its risk profile, Client base, product characteristics and operational capacity.

(2) Leverage limits shall be supported by exposure controls at Client level, product level and firm level and shall address, where relevant:

(a) concentration risk;

(b) wrong-way risk;

(c) correlation risk;

(d) liquidity stress;

(e) intraday and overnight exposure; and

(f) contagion between products, Clients or venues.

(3) The Licensee shall have the ability to reduce leverage, require additional Margin, restrict new positions or close existing positions where necessary to protect Clients, preserve market integrity or manage prudential risks.

(4) The Licensee shall document the basis on which leverage limits are set, reviewed and amended.

14. Valuation, mark-to-market and pricing controls. — (1) A Licensee shall establish documented methodologies for valuing Derivative Contracts, Leverage Arrangements, Margin and collateral.

(2) Such methodologies shall address, where relevant, including but not limited to:

(a) pricing sources and hierarchy;

(b) mark-to-market frequency;

(c) handling of stale prices, outliers and anomalous prints;

(d) fallback arrangements where primary data is unavailable or unreliable; and

(e) controls to prevent conflicts of interest affecting valuations.

(3) Valuation methodologies shall be subject to governance review and periodic validation commensurate with the nature, scale and complexity of the Licensee's business.

(4) A Licensee shall not use a valuation methodology that materially understates risk, overstates collateral value, or otherwise distorts Client positions or the Licensee's prudential picture.

15. Liquidation, close-out and default management. — (1) A Licensee shall maintain documented policies and procedures governing margin calls, Liquidation, close-out and default management.

(2) Such procedures shall be transparent, non-discriminatory, consistent with Client disclosures and reasonably designed to minimize disorderly Liquidation and avoidable harm to Clients and the market.

(3) Procedures shall address at least:

(a) triggers for margin calls and Liquidation;

(b) timing, notice and escalation, where operationally appropriate;

(c) methods for valuing positions and collateral during stressed conditions;

(d) partial liquidation, full close-out and staged reduction mechanisms;

(e) treatment of shortfalls, excess proceeds and fees;

(f) default management and communication with affected Clients; and

(g) communication with the Authority where material disruption or deficiency arises.

(4) A Licensee shall not rely on opaque or unlimited discretionary liquidation powers that are materially inconsistent with its Client Agreement or disclosures.

(5) Where the business model includes default funds, guarantee funds, insurance arrangements or similar buffers, the Licensee shall disclose their function and limitations clearly and shall not represent them as eliminating Client risk.

16. Stress-testing, model validation and back-testing. — (1) A Licensee shall conduct periodic stress-testing of its Derivatives and Leverage exposures, including stress-testing of Margin sufficiency, collateral values, concentrated positions, liquidation capacity and liquidity under severe but plausible scenarios.

(2) A Licensee shall ensure that any risk model, valuation model, margin model or liquidation model used in connection with Derivatives Services is subject to appropriate validation, testing, governance and change control.
(3) Back-testing and benchmarking shall be conducted where appropriate to the model and business model concerned.
(4) Stress-test and validation results shall be reported to the Licensee's board or an appropriate committee and used to adjust risk limits, Margin methodologies, collateral standards and contingency arrangements.

17. Market conduct and conflicts of interest. — (1) A Licensee providing Derivatives Services shall act honestly, fairly and professionally in accordance with the best interests of its Clients.
(2) The Licensee shall maintain effective controls to identify, prevent, manage and, where appropriate, disclose conflicts of interest arising from:
(a) proprietary trading;
(b) internalization or principal dealing;
(c) market making or liquidity provision;
(d) related-party counterparties, venues or liquidity sources;
(e) liquidation arrangements; and
(f) the use of Client Order information or position information.
(3) A Licensee shall prohibit front-running, abusive self-trading, manipulation of mark prices, abusive liquidations, misuse of Client information, or any other abusive practice prohibited under the Act, the Regulations or applicable law.
(4) Where the Licensee also operates an Exchange or Broker-Dealer business, it shall maintain effective information barriers and conflict management controls proportionate to the scale and complexity of the integrated model.

18. Exchange and Broker-Dealer interface. — (1) Where Derivatives Services are offered through an Exchange, the Exchange shall maintain policies, procedures, systems, controls, and disclosures appropriate to leveraged and derivatives activity, including those relating to participant eligibility, collateral, Liquidation, concentration limits and market integrity.
(2) Where Derivatives Services are offered through a Broker-Dealer, the Broker-Dealer shall comply with the relevant appropriateness, order handling, Fair Pricing, conflict management and Client disclosure requirements in addition to this Regulation.
(3) A Licensee shall not continue to provide Derivatives Services if it ceases to hold a valid Broker-Dealer Services licence or Exchange Services licence on which premise the Derivatives Services were authorised, except to the extent necessary to close out, transfer or otherwise wind down existing positions in accordance with a direction of the Authority.

19. Technology, operational resilience and trading continuity. — (1) A Licensee shall ensure that systems supporting Derivatives Services are resilient, secure and capable of orderly operation under conditions of high uncertainty and extreme volatility.

(2) The Licensee shall maintain contingency procedures for system outages, pricing failures, order-routing failures, margining failures, liquidation system failures, stale market data, chain disruption, banking rail disruption and other events that could materially affect derivatives or leveraged positions.

(3) Material incidents affecting derivatives or leveraged products shall be communicated to affected Clients and to the Authority immediately.

(4) The Licensee shall maintain business continuity, backup and disaster recovery arrangements sufficient to support the continuity of critical derivatives and leverage functions.

20. Client reporting and statements. — (1) A Licensee shall furnish to each Client periodic statements at intervals appropriate to the nature, scale and risk profile of the relevant product and Client category and, in any event, not less frequently than monthly for Retail Clients unless otherwise required by the Authority.

(2) Statements shall be clear, timely and accessible and retained for at least the minimum period required under applicable law and the Regulations.

(3) The Licensee shall provide additional information promptly where a material event significantly affects the Client's position, margin status or exposure.

21. Public disclosures. — (1) A Licensee offering Derivatives Services shall, in a prominent place on its website or via other accessible means approved by the Authority, disclose at least:

(a) the categories of derivatives or leveraged products offered;

(b) the categories of Clients to whom such products are made available;

(c) material risk warnings relating to leverage, Margin, Liquidation and volatility;

(d) high-level information on collateral standards and pricing methodology;

(e) whether the Licensee acts as principal, agent, venue operator, or in more than one such capacity; and

(f) such other information as the Authority may reasonably require.

(2) A Licensee shall keep public disclosures under this regulation current and review them whenever a material change occurs.

22. Record-keeping. — (1) A Licensee shall keep complete and accurate records of all Derivatives and Leverage activities, including:

(a) Client Agreements and risk acknowledgements;

(b) product approvals and reviews;

(c) Client categorization and appropriateness assessments;

(d) orders, trades, positions, valuations, Margin movements and Liquidation events;

(e) model validation, back-testing and stress-testing results;

(f) conflict management decisions and proprietary trading controls; and

(g) defaults, incidents, complaints and remediation actions.

(2) Records shall be retained for at least the minimum period required under AML Act, 2010, AML Rules, applicable AML/CFT Regulations and any other applicable law, and the Regulations and shall be made available to the Authority upon request.

(3) Records shall be sufficiently complete, accessible and reliable to permit supervisory review, internal investigation and reconstruction of events.

Mining Services Regulation

1. Short title, scope and hierarchy. — (1) This Regulation may be cited as the Mining Services Regulation, 2026.

2. Definitions. — (1) Unless the context otherwise requires, words and expressions used but not defined in this Regulation shall have the meanings assigned to them in the Act and the Pakistan Virtual Asset Services Regulations, 2026.

(2) In this Regulation:

(a) "**Client Mining Assets**" means Client Assets or Client Money provided to, held by, controlled by, or otherwise exposed to the Licensee in connection with Mining Services;

(b) "**Hosted Mining Arrangement**" This License Category shall apply to a Person who, as a business, establishes, maintains, and operates Mining Infrastructure and provides Hosted Mining Arrangements by housing, managing, maintaining, or operating mining equipment on behalf of Clients, including arrangements involving Client Mining Assets or Client Money for mining-related activities;

(c) "**Mining Infrastructure**" means the hardware, software, firmware, facilities, energy systems, connectivity, wallets, operational processes and related infrastructure used for Mining Services;

(d) "**Mining Pool**" means any arrangement under which computational resources, validator resources or similar participation resources are pooled for the purpose of mining, validation, block production, transaction ordering, reward generation or similar activity;

(e) "**Mining Rewards**" means block rewards, transaction fees, protocol rewards, validator rewards or any other proceeds arising from Mining Services; and

(f) "**Mining Services**" means mining-related virtual asset activities requiring a licence under the Pakistan Virtual Asset Services Regulations, 2026 because the activity involves services to third parties involving Client Assets or Client Money.

(3) For the avoidance of doubt, Mining Services under this Regulation include only licensed mining-related activities involving third-party service provision and do not include purely proprietary mining falling outside the licensing perimeter.

3. Nature and perimeter of Mining Services. — (1) A Person shall not hold itself out as providing Mining Services unless it is authorised for that Licence Category.

(2) A Licensee providing Mining Services may, subject to its Licence and the Act and Regulations:

(a) operate Mining Infrastructure or Hosted Mining Arrangements for or on behalf of Clients;

(b) pool, administer, route or otherwise manage mining or validation participation for Clients;

(c) receive, hold, allocate or distribute Mining Rewards for Clients; and

(d) perform ancillary functions that are integral to the operation of such services, subject to compliance with all applicable safeguarding, conduct, prudential and disclosure requirements, and provided that such functions do not constitute a separate regulated activity requiring an additional Licence Category under the Regulations

(3) Where a Mining Services business model includes custody, transfer, pooling of Client Mining Assets, reward distribution, staking, validator activity, or any other function that falls within another Licence Category, the Licensee shall hold the relevant Licence Category and comply with the applicable Regulation.

(4) For the avoidance of doubt, staking, validator activity or similar protocol-participation activity performed on behalf of Clients shall be assessed on a substance-over-form basis and may constitute Custody Services, Management and Investment Services, or another regulated activity depending on the nature of the authority exercised, the treatment of Client Assets, the degree of discretion involved, and the overall structure of the arrangement.

(5) The Authority may require a Person conducting large-scale proprietary mining, even where licensing is not otherwise required, to register or make declarations in accordance with any registration or declaration framework established under the Act or the Regulations, or as may be prescribed by the Authority.

4. Governance and oversight. — (1) The Licensee's board shall approve and oversee the provision of Mining Services, including:

(a) business model and service scope;

(b) operational and technology risk appetite;

(c) custody and safeguarding arrangements for Client Mining Assets;

(d) reward allocation methodology;

(e) outsourcing and Mining Pool arrangements; and

(f) conflict management arrangements.

(2) Senior management shall ensure that Mining Services are conducted in accordance with approved policies, procedures and applicable regulatory obligations.

(3) The Licensee shall maintain adequate governance, reporting lines, escalation procedures and management information to enable effective oversight of operational uptime, service

continuity, reward allocation, energy and infrastructure dependency, concentration risk, Client protection issues and incident management.

(4) The Licensee shall identify the Key Individuals responsible for Mining Services, including responsibility for operations, technology, safeguarding, compliance and risk management.

5. Policies, procedures and control framework. — (1) In addition to all other applicable requirements under the Regulations, a Licensee providing Mining Services shall establish, implement, maintain and enforce written policies and procedures appropriate to the nature, scale and complexity of its business, including at least policies and procedures relating to—

(a) Client onboarding and eligibility;

(b) operation, maintenance and security of Mining Infrastructure;

(c) uptime, resilience, failover and business continuity;

(d) treatment, safeguarding and reconciliation of Client Mining Assets;

(e) reward generation, calculation, allocation and distribution;

(f) fees, expenses, deductions and charges;

(g) Mining Pool participation or other third-party participation arrangements;

(h) incident management, outage handling and Client notification;

(i) conflicts of interest, including proprietary mining alongside Client mining;

(j) outsourcing and third-party dependencies; and

(k) such other matters as the Authority may reasonably require.

(2) The Licensee shall assess and, in any event, at least annually review the effectiveness of those policies and procedures and take appropriate measures to address any deficiency.

3) A Licensee may rely on group-level policies, procedures, systems, controls or assurance arrangements, provided that they are appropriate to the Licensee's business, legally and operationally applicable in Pakistan, and sufficient to ensure compliance with the Act, the Regulations and this Regulation.

6. Client disclosures and transparency. — (1) A Licensee providing Mining Services shall disclose to Clients, in a clear, fair, timely and not misleading manner, material information including at least:

(a) the nature of the Mining Services provided;

(b) whether the service involves hosted mining, pooled participation, validator operation, reward administration, or another structure;

(c) the treatment of Client Mining Assets and any role of the Licensee in holding, controlling or administering those assets;

(d) the basis on which Mining Rewards are calculated, allocated and distributed;

(e) fees, deductions, operating costs, energy charges, pool charges and any other amounts that may reduce Client proceeds;

(f) operational, technology, protocol, downtime, slashing, maintenance, regulatory and counterparty risks relevant to the service;

(g) any lock-up, withdrawal, unbonding, payout timing or distribution restrictions; and

(h) the circumstances in which the Licensee may suspend, restrict, terminate or materially modify the service.

(2) A Licensee shall not market Mining Services as guaranteed, risk-free, or capable of producing a fixed level of rewards or returns unless that representation is accurate and substantiated.

(3) Where the service involves a Mining Pool, third-party node operator, external infrastructure provider or similar arrangement, the Licensee shall disclose the role of that third party and the principal risks associated with that dependency.

7. Client Agreements. — (1) A Licensee shall not provide Mining Services to a Client unless a written Client Agreement has been agreed with that Client.

(2) In addition to general Client Agreement requirements under the Regulations, a Client Agreement for Mining Services shall, to the extent applicable, set out clearly:

(a) the nature and scope of the Mining Services;

(b) the respective rights and obligations of the Licensee, the Client and any third party materially involved in the service;

(c) whether Client Mining Assets or Client Money are transferred to, held by, controlled by, or otherwise exposed to the Licensee;

(d) the basis for calculation, timing and distribution of Mining Rewards;

(e) all fees, deductions, charges and expenses payable by the Client or deductible from rewards;

(f) any lock-up, unbonding, maintenance, withdrawal, payout or termination conditions;

(g) service levels, uptime commitments if any, and the consequences of outages or performance failures;

(h) any right of the Licensee to modify, suspend or terminate the service and the consequences of doing so;

(i) the treatment of Client Assets and Mining Rewards on termination or insolvency; and

(j) the Licensee's complaints procedure and escalation channels.

(3) The Client Agreement shall be clear, fair and not misleading and shall be consistent with the market conduct requirements under the Regulations.

8. Treatment of Client Assets and Client Money. — (1) A Licensee shall not receive, hold, control, safeguard or administer Client Mining Assets except in accordance with the Act, the Regulations, this Regulation, and any other applicable Regulation.

(2) Where a Licensee holds or controls Client Mining Assets or Client Money in connection with Mining Services, it shall comply with the safeguarding, segregation, reconciliation, record-keeping and disclosure requirements under the Regulations and, where applicable, the Custody Services Regulation.

(3) A Mining Services licence does not, of itself, permit the Licensee to use, lend, pledge, stake, rehypothecate, encumber or otherwise deploy Client Mining Assets for its own benefit or for third parties. Any such use shall require Client's prior written, explicit, and informed consent and shall clearly disclose the nature of the activity, the associated risks, any withdrawal restrictions, and the basis on which rewards, proceeds, losses and liabilities are allocated.
(4) The Licensee shall structure its arrangements so that Client Mining Assets are identifiable, segregated from the Licensee's own assets, and capable of timely return, transfer or payout in accordance with the Client Agreement and applicable law.

9. Reward calculation, allocation and distribution. — (1) A Licensee shall establish and maintain a documented methodology for the calculation, allocation and distribution of Mining Rewards.
(2) The methodology referred to in sub-regulation (1) shall be fair, transparent, consistently applied and disclosed to Clients in an understandable manner.
(3) The methodology shall address, where relevant, including but not limited to:
(a) how rewards are attributed to individual Clients or groups of Clients;
(b) treatment of pool fees, third-party fees, infrastructure costs, slashing losses, penalties, downtime losses and other deductions;
(c) timing and frequency of distributions;
(d) treatment of rounding, dust balances and residual amounts; and
(e) treatment of forks, airdrops, protocol changes, restatements or retroactive adjustments affecting Mining Rewards.
(4) A Licensee shall not change its reward allocation methodology in a way that materially disadvantages Clients without prior notice consistent with the Client Agreement and any applicable requirements under the Regulations.
(5) The Licensee shall maintain records sufficient to demonstrate the basis on which Mining Rewards were calculated, allocated and distributed.

10. Mining infrastructure, operational integrity and maintenance. — (1) A Licensee shall establish, operate and maintain Mining Infrastructure in a manner consistent with the technology, cybersecurity and operational resilience requirements under the Regulations.
(2) The Licensee shall maintain documented standards and procedures relating to:
(a) hardware and software maintenance;
(b) patching, upgrades and configuration management;
(c) physical security and environmental controls where relevant;
(d) uptime monitoring, performance monitoring and fault detection; and
(e) failover, backup and recovery arrangements.
(3) A Licensee shall ensure that Mining Infrastructure is fit for purpose, reasonably resilient, and capable of supporting the service levels and reward expectations disclosed to Clients.

(4) A Licensee shall not continue to accept new Clients or additional Client Mining Assets where it is aware, or ought reasonably to be aware, that its Mining Infrastructure is materially inadequate to support the relevant service safely and effectively.

11. Protocol, pool and network due diligence. — (1) Before supporting a protocol, Mining Pool, validator framework or other network arrangement in connection with Mining Services, a Licensee shall conduct due diligence appropriate to the nature, scale and complexity of the activity.

(2) Such due diligence shall address, where relevant:

(a) technology and security characteristics;

(b) protocol governance and operational history;

(c) reward mechanism and sustainability of reward generation;

(d) slashing, penalty, downtime or similar risk;

(e) degree of concentration, centralization or dependency on a limited number of operators;

(f) legal and regulatory risks; and

(g) the Licensee's ability to operate or support the relevant arrangement in a compliant and resilient manner.

(3) The Licensee shall actively monitor supported protocols, pools and network arrangements on an ongoing basis.

(4) Where the Licensee becomes aware that a protocol, pool or network arrangement no longer meets its risk standards or presents a material risk to Clients, the Licensee shall:

(a) cease accepting new Client Mining Assets or new participation in the affected arrangement where appropriate;

(b) notify affected Clients and the Authority without undue delay where the matter is material; and

(c) determine and implement an appropriate remediation, migration, suspension or wind-down plan.

12. Outsourcing and third-party arrangements. — (1) Where a Licensee relies on third parties for hosting, colocation, power supply, pool participation, validator operation, reward administration, custody, payout processing, software, monitoring or other material functions, the Licensee shall remain fully responsible for compliance with the Act, the Regulations and this Regulation.

(2) Such arrangements shall comply with applicable outsourcing and third-party risk requirements under the Regulations and shall provide the Licensee with adequate rights of access, audit, oversight, information and termination.

(3) The Licensee shall conduct due diligence on material third parties and monitor their performance, resilience, legal risk, conflicts and dependency risk on an ongoing basis.

(4) The Authority shall have access, audit and information rights in respect of material outsourced arrangements to the extent permitted by law and contract.

13. Conflicts of interest. — (1) A Licensee shall identify, prevent, manage and, disclose conflicts of interest arising in the provision of Mining Services.

(2) Such conflicts shall include, where relevant, including but not limited to:

(a) proprietary mining or validation activity conducted alongside Client-facing Mining Services;

(b) preferential allocation of infrastructure capacity, rewards or service quality between proprietary and Client activity;

(c) related-party participation in pools, infrastructure providers or counterparties; and

(d) fee or reward structures that may distort the Licensee's treatment of Clients.

(3) A Licensee shall not allocate Mining Rewards, infrastructure capacity or operational priority in a manner that unfairly disadvantages Clients.

(4) Material conflicts that cannot be effectively prevented or otherwise managed shall be disclosed to Clients clearly and before the relevant service is provided or continued.

14. Reporting to Clients. — (1) A Licensee shall furnish to each Client, at least monthly and more frequently where necessary having regard to the service model or Client Agreement, statements showing, including but not limited to:

(a) Client Mining Assets or Client Money held or used in connection with the service;

(b) Mining Rewards generated, allocated and distributed during the reporting period;

(c) fees, charges, costs or deductions applied;

(d) any material outages, slashing events, penalties, pool failures, protocol issues or similar events affecting the service; and

(e) any material changes to the service, reward methodology or operational arrangements.

(2) Statements shall be clear, timely and accessible and retained for at least the minimum period required under applicable law and the Regulations.

(3) The Licensee shall provide additional information promptly where a material event significantly affects the Client's participation, assets or expected rewards.

15. Public disclosures. — (1) A Licensee providing Mining Services shall publish on its website, or make available through another publicly accessible means approved by the Authority, clear, fair and not misleading disclosures including at least:

(a) a description of the Mining Services provided;

(b) broad categories of supported protocols, pools or infrastructure arrangements;

(c) the principal risks relevant to the service;

(d) fee structures and reward allocation principles;

(e) whether Client Assets or Client Money are held by the Licensee or a third party in connection with the service;

(f) the Licensee's policies relating to data privacy, complaints handling and whistleblowing; and

(g) such other information as the Authority may reasonably require.

(2) Public disclosures under this regulation shall be kept current and reviewed whenever a material change occurs.

16. Operational resilience and incident management. — (1) A Licensee shall ensure that systems, controls and infrastructure supporting Mining Services meet operational resilience, availability and recovery standards proportionate to the criticality of those services.

(2) The Licensee shall maintain contingency procedures for material outages, Mining Infrastructure failures, software or firmware failures, power disruption, cooling failure, cyber incidents, protocol changes, pool failures, payout failures and other events that could materially affect Mining Services.

(3) Material incidents affecting Mining Services shall be communicated to affected Clients and to the Authority without undue delay where the incident is material.

(4) The Licensee shall maintain business continuity, backup and disaster recovery arrangements sufficient to support the continuity of critical Mining Services functions.

17. Record-keeping. — (1) A Licensee shall keep complete and accurate records of all Mining Services activities, including:

(a) Client Agreements;

(b) onboarding and service eligibility records;

(c) Client Mining Assets and Client fund records;

(d) reward calculations, allocations and distributions;

(e) protocol, pool and network due-diligence records;

(f) outage, incident, slashing, penalty and remediation records;

(g) outsourcing and third-party arrangements; and

(h) complaints, communications and material disclosures to Clients.

(2) Records shall be retained for at least the minimum period required under AML Act, 2010, AML Rules, applicable AML/CFT Regulations and any other applicable law, and the Regulations and shall be made available to the Authority upon request.

(3) Records shall be sufficiently complete, accessible and reliable to permit supervisory review, internal investigation and reconstruction of events.

Schedule 1 – VA Whitepaper Requirements

Not all of the information listed herein will be applicable for every Virtual Asset. At such time, Issuers and/or their Licensed Distributors must exercise professional judgement, acting in accordance with the regulatory requirements at all times, when determining if the information listed herein is applicable for the purposes of inclusion in a Whitepaper of a specific Virtual Asset. Issuer shall be fully responsible for the accuracy and completeness of all Whitepapers.

A. Information about the Issuer

1. Issuer's name, legal structure, registered address, and head office location (if different);
2. Issuer's date of incorporation or registration;
3. Identity of the Issuer's parent company;
4. Identities, business addresses, and functions of the Issuer's owners, management and/or members;
5. whether any individual involved in the issuance, including the Issuer's owners, management and/or members, has been convicted of any offence of dishonesty, fraud, financial crime or an offence under laws relating to companies, banking, insolvency, money laundering and insider dealing, and, to the extent permissible under applicable laws, whether any individual is subject to ongoing inquiries or investigations in respect of such offences;
6. business, business related and/or professional activities of the Issuer, including any regulatory authorizations or Licenses, and its group;
7. Issuer's financial condition over the past three (3) years, or since registration if the Issuer has existed for less than three years
8. an assessment based on a fair review of the development, performance, and position of the Issuer's business over the past three (3) years, or since registration if the Issuer has existed for less than three (3) years, including the causes of any material changes. The assessment should be a balanced and comprehensive analysis of the Issuer's business development, performance, and position, and should be consistent with the size and complexity of the business;
9. a detailed description of the Issuer's governance arrangements;
10. if the Issuer issues other Virtual Assets or undertakes other Virtual Assets Activities, this should be clearly stated;
11. if there is any connection between the Issuer itself and the Entity or organization that has control of the DLT used to issue the Virtual Assets, including if the DLT is run, managed or controlled by an Entity closely connected to the Issuer or other project participants; and
12. details of all Entities (including businesses addresses or company domiciles) involved in the issuance and/or operation of the Virtual Asset, such as advisors, development teams, and/or VASPs.

B. Information about the Virtual Asset

1. name, abbreviation or ticker handler of the Virtual Asset;
2. description of the characteristics of the Virtual Asset and all features and uses
3. information about the plans for the Virtual Asset and all related projects, including a description of the past and future milestones and resources already allocated;
4. an explanation of the target market of the Virtual Asset, including any restrictions as regards the type of owners;
5. the name of any trading platform for Virtual Assets where admission to trading is or will be sought, and information about how investors can access such trading platforms and the costs involved;
6. information about technical requirements necessary to own and/or hold the Virtual Asset, including but not limited the types of VA Wallets with which the Virtual Asset is compatible;
7. a detailed description of the issuance structure of the Virtual Asset, in particular the number that will be issued, the issuance schedule, when all of the supply of the Virtual Asset will be made available and how many will be allocated or retained by any party, including but not limited to the Issuer, its investors and/or advisors; and
8. the planned use of any proceeds or consideration received by the Issuer, in any form, related to issuing the Virtual Asset

C. Information about the rights and obligations attached to the Virtual Asset

1. description of the characteristics and functionality of the Virtual Asset being issued, including information about whether the functionality will change, and if so when such changes will take place;
2. description of the rights and obligations, if any, of the owner, and the procedure and conditions for the exercise of those rights;
3. whether the rights represented by the Virtual Asset may differ depending on what DLT or platform the Virtual Asset is acquired or used;
4. description of the conditions under which the rights and obligations may be modified;
5. information on subsequent issuances or offers that may have a dilutive effect on the Virtual Asset being issued, and the number of units of the Virtual Asset retained by the Issuer itself;
6. information on how and where the Virtual Asset can be purchased or sold after the issuance;
7. any restrictions on the transferability, or additional steps required to give legal effect to a transfer of ownership, of the Virtual Asset that is being issued;
8. description of protection schemes protecting the value of the Virtual Asset or any initial investments in the Virtual Asset;

9. information on the nature and enforceability of rights, including permanent rights of redemption and any claims that owners may have against the Issuer;
10. information on any rights an owner of the Virtual Asset will have in the event the Issuer is Insolvent, including in the context of any scheme of arrangement or recovery plan;
11. information on whether different rights are allocated to different owners, and the non-discriminatory reasons for such different rights;
12. information on the arrangements put in place by the Issuer to ensure the liquidity of the Virtual Asset, including the name of the Entities in charge of ensuring such liquidity;
13. the contact details for submitting complaints, and a description of the complaints-handling procedures and any dispute resolution mechanism or redress procedure established by the Issuer of the Virtual Asset;
14. detailed information on any rights of redemption and how the Virtual Asset is redeemed, including whether the owner will be able to choose the form of redemption, the form of transference, or the official currency of redemption;
15. any material legal or regulatory considerations applicable to owning, storing, transferring, or otherwise using the Virtual Asset, including to give legal effect to a transfer of ownership; and
16. the law applicable to the Virtual Asset, as well as the competent court.

D. Information about underlying technology

1. information on the technology used, including DLTs, as well as protocols and technical standards, allowing for the holding, storing, and transfer of Virtual Assets;
2. information on the consensus mechanism used by the DLT on which the Virtual Asset is issued including, where the Virtual Asset is issued on more than one DLT whether any variances in mechanisms used by different DLTs give rise to a variance in the rights of owners of the Virtual Asset;
3. incentive mechanisms to secure transactions and any applicable fees;
4. if the Virtual Asset is issued, transferred, and stored using DLT that is operated by the Issuer or a third-party acting on the Issuer's behalf, a detailed description of the functioning of such DLT and information on the outcome of any audits, if such an audit was conducted, including what Entity carried out the audit; and
5. a statement on the environmental and climate-related impact of the Virtual Asset.

E. Information about any initial offer to the public of the Virtual Asset

1. the reasons for any offer to the public;
2. the amount that the offer to the public intends to raise denominated in PKR, including any minimum and maximum target subscription goals set for the offer to the public of the Virtual Asset;
3. whether oversubscriptions are accepted and how allocations will be determined in the event of oversubscription;

4. a specific notice that purchasers participating in the offer to the public of Virtual Asset will be reimbursed if the minimum target subscription goal is not reached at the end of the offer to the public, or if the offer is cancelled, and a detailed description of the refund mechanism, including the expected timeline of when such refunds will be completed;
5. the issue price of the Virtual Asset being offered to the public, denominated in both PKR and/or any other Virtual Assets;
6. the total number of Virtual Assets to be offered to the public, and the percentage of the total supply in circulation (i.e. supply available prior to the intended new issuance) of the Virtual Asset that the offer to the public represents;
7. an indication of the prospective owners targeted by the offer to the public, including any restriction as regards the type of owners for such Virtual Assets;
8. information about the various phases of the offer to the public of Virtual Assets, including information on discounted purchase prices for early purchasers of Virtual Assets (pre-public sales). In the case of discounted purchase prices for some purchasers, an explanation why purchase prices may be different, and a description of the impact on the other investors;
9. for time-limited offers, the subscription period during which the offer to the public is open;
10. arrangements to safeguard funds or other Virtual Assets during the time-limited offer to the public or during the withdrawal period;
11. methods of payment to purchase the Virtual Assets offered, and methods of transfer of the value to the purchasers when they are entitled to be reimbursed;
12. information on any rights the Issuer has to withdraw or cancel the offer to the public;
13. information on the manner and time schedule of transferring the purchased Virtual Assets to the owners and/or holder;
14. expenses to be incurred by purchasers of the Virtual Asset related to the offer to the public of the Virtual Asset, including any applicable subscription fee or the method in accordance with which the offer price will be determined;
15. potential conflicts of interest of the persons involved in the offer to the public arising in relation to the offer; and
16. the law applicable to the offer to the public of Virtual Assets, as well as the competent court.

F. Information about Virtual Asset – ART

1. clear and accurate description of the rights and/or value that the Asset Referenced Virtual Assets (ART) grants, or purports to grant, owners and/or holders of the ART and a clear and detailed policy on how the VASP ensures the ART derives and maintains its value;
2. the types and composition of Reference Assets, and criteria for how such Reference Assets were identified;

3. Where the value of a Reference Asset cannot be established by reference to a reliable and observable market price, the Whitepaper shall
    a) describe the methodology used to determine its value; and
    b) include or be accompanied by an independent valuation report, or other independent valuation evidence approved by the Authority, with a valuation date not more than three (3) months before submission of the Whitepaper

    The valuation report or evidence shall identify, where available
        i). the name, qualifications and independence of the valuer
        ii). the valuation date
        iii). the methodology, material assumptions and principal data sources
        iv). the resulting value or valuation range
        v). any material limitation, uncertainty or conflict of interest.

    Where a material change occurs between the valuation date and issuance, the Issuer shall update the valuation or explain the effect of that change before issuance. The Authority may permit alternative evidence where an independent valuation report would not be meaningful or proportionate having regard to the nature of the Reference Asset.
4. whether the types of Reference Asset will change and, if so, the circumstances in which any such changes may take place;
5. whether the ART represents, or purports to represent, a direct right of ownership of the Reference Assets, or a fractional proportion thereof, and if so, a detailed description of how the right of ownership is established and/or such fractionalisation is structured;
6. if transactions in the Reference Assets are subject to legal or regulatory requirements relating to their settlement and/or transfer of title, a detailed description of how such requirements will be met and an explanation of how the VASP will respond to transactions in the ART not resulting in corresponding transactions in the Reference Asset being legally settled, completed and/or transferred, and any mitigation employed by the VASP to address such risks;
7. whether the ART maintains, or purports to maintain, a stable reference to the value of the Reference Assets, and if so, a detailed description of how such stable reference is maintained and the weighting of each type of Reference Asset in the unit value of the ART;
8. whether the VASP will maintain Reserve Assets in respect of the ART;
9. the types and composition of Reserve Assets, and criteria for how such Reserve Assets were identified;
10. whether the types of Reserve Asset may be subject to change and, if so, the circumstances in which any such changes may take place, including a detailed description of the VASP's investment policy for the Reserve Assets;
11. a clear and detailed policy on the procedure for the creation and destruction of the ARTs in public circulation and the consequence of such creation or destruction on the increase and decrease of the Reserve Assets;
12. full details of the rights of owners and/or holders of the ART to redeem the value of the ART, including but not limited to the requirements under these Regulations and the procedures and timeline for owners and/or holders of the ART to redeem such value;

13. the custody arrangement of the Reference Asset and/or Reserve Assets, including but not limited to, the custodians involved and how the VASP ensures it has timely access to Reserve Assets to process redemption requests;
14. detailed assessments of risks relevant to the management, custody, investment and/or liquidation of the Reference Asset and/or Reserve Assets, including but not limited to, credit risk, market risk, counterparty risk and liquidity risk, and policies and procedures to manage such risks for the purpose of processing redemption requests; and
15. any other relevant information as may be determined by the Authority.

G. Information about Fiat Asset – FRT

1. Type(s) and composition of Reference Currency(ies);
2. whether the type(s) and composition of Reference Currency(ies) may change and, if so, the circumstances in which any such changes may take place and the consequential effect of such changes;
3. clear and detailed policy on the creation and redemption of FRTs in circulation and the consequence of such creation or redemption on the increase and decrease of the Reserve Assets;
4. type(s) and composition of Reserve Asset(s), and methodology for valuing such Reserve Assets;
5. criteria for how Reserve Asset(s) are or will be identified;
6. the custody arrangement of the Reserve Assets including, but not limited to, the custodian(s) involved and how the VASP Licensed to issue FRTs ensures it has timely access to Reserve Assets to process redemption requests in compliance with these Regulations;
7. detailed description of how Reserve Assets are maintained, with reference to the requirements of these Regulations;
8. detailed description of how they will comply with Regulations relating to the handling of redemption requests in these Regulations, and all relevant risks which may affect their compliance;
9. the procedures and timeline for holders of FRTs to redeem such FRTs at par;
10. prominently state whether having a valid Client Agreement with the VASP Issuer is a condition for redemption of the FRT directly from the VASP Issuer;
11. detailed assessments of risks relevant to the management, custody, investment and/or liquidation of the Reserve Assets, including, but not limited to, credit risk, market risk and liquidity risk, and policies and procedures to manage such risks for the purpose of processing redemption requests; and
12. any other relevant information as may be determined by the Authority.

-sd-
Najia Ubaid
Additional Director