حكومة دبي
GOVERNMENT OF DUBAI

VARA
سُلطة تنظيم الأصول الافتراضية
VIRTUAL ASSETS REGULATORY AUTHORITY

Technology and Information Rulebook

19 May 2025

varaconnect@vara.aeصندوق بريد: 9292 دبي، الإمارات العربية المتحدة - سُلطة تنظيم الأصول الافتراضية
varaconnect@vara.ae - PO Box 9292, Dubai, UAE - Virtual Assets Regulatory Authority

Contents

Introduction

The Dubai Virtual Assets Regulatory Authority ("**VARA**") was established and authorised by *Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai* ("**Dubai VA Law**") to regulate Virtual Asset Service Providers ("**VASPs**").

This Technology and Information Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time ("**Regulations**"), issued by VARA, and applies to all VASPs Licensed by VARA to carry out any VA Activity in the Emirate.

This Technology and Information Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out any VA Activity must also comply with the following Rulebooks applicable to all VASPs—

- Company Rulebook;
- Compliance and Risk Management Rulebook;
- Market Conduct Rulebook; and
- All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

Capitalised terms in this Technology and Information Rulebook have the meanings ascribed to them in the Regulations or as otherwise defined herein or provided in Schedule 2.

Unless otherwise stated, all requirements in this Technology and Information Rulebook are Rules and have binding effect.

Part I – Technology Governance, Controls and Security

A. Technology Governance and Risk Assessment Framework

1. VASPs must implement a technology governance and risk assessment framework, capable of determining defined policies underpinned by the necessary processes, procedures and controls that the VASP must implement, in order to adequately mitigate the risks identified ("**Technology Governance and Risk Assessment Framework**").

2. VASPs must ensure that they implement all policies, processes, procedures and controls necessary to address risks to the VASP's business and VA Activities covered in the Technology Governance and Risk Assessment Framework using appropriate methods, including defence-in-depth approaches for cybersecurity-related risks. Such policies, processes, procedures and controls should take into account a number of factors including, the nature, scale and complexity of the VASP's business, the diversity of its operations, the volume and size of its transactions, and the level of risk inherent with its business.

3. The Technology Governance and Risk Assessment Framework must be comprehensive and proportionate to the nature, scale, and complexity of the risks inherent in the VASP's business model and VA Activities. The Technology Governance and Risk Assessment Framework should apply to all technologies relevant to a VASP's business and VA Activities and clearly set out—
   a. the VASP's cybersecurity objectives, including the requirements for the competency of Staff and, as relevant, end users and clients; and
   b. clearly defined policies, processes, procedures and controls necessary for managing risks, including, but not limited to, consideration of international standards and industry best practice codes.

4. VASPs must ensure that their Technology Governance and Risk Assessment Framework addresses appropriate governance policies and system development controls, including but not limited to—
   a. a development, maintenance and testing process for technology systems;
   b. operations controls;
   c. back-up controls;
   d. capacity and performance planning; and

e. availability testing.

5. VASPs must monitor, assess and maintain the effectiveness of their Technology Governance and Risk Assessment Framework. In particular, VASPs must review, update and arrange for the testing of their policies, processes, procedures and controls aimed at managing risks on a periodic basis, having regard to the macroeconomic environment in which the VASP operates, as well as emerging technology risks relating to their systems and consideration of international standards and industry best practice codes.
6. VARA has provided Guidance, in Schedule 1 of this Technology & Information Rulebook, on the categories of risk, the risk mitigation measures and standards that a VASP's Technology Governance and Risk Assessment Framework should cover when complying with the Rules in this Part I of the Technology & Information Rulebook.
7. As prescribed by Rule I.I.1 of this Technology and Information Rulebook, VASPs must appoint a Chief Information Security Officer who is responsible for ensuring that the VASP complies with Part I and Part III of this Technology and Information Rulebook.

B. Cybersecurity Policy

1. VASPs must create and implement a policy which outlines their procedures for the protection of their electronic systems and client and counterparty data stored on those systems ("**Cybersecurity Policy**"). VASPs must submit their Cybersecurity Policy to VARA for assessment as part of the licensing process and at any subsequent time upon request from VARA.
2. VASPs must ensure that their Cybersecurity Policy is reviewed and updated at least annually by their CISO.
3. VASPs must ensure that their Cybersecurity Policy contains sound procedures and security mechanisms in accordance with best industry practices that will enable them to comply with all applicable information security, data protection and data privacy laws and regulations, including but not limited to Part II of this Technology and Information Rulebook and the PDPL, whilst

maintaining the confidentiality of data at all times. The Cybersecurity Policy must address the following minimum criteria—

a. information security;

b. data governance and classification;

c. access controls;

d. capacity and performance planning;

e. systems operations and availability concerns;

f. systems and network security, consensus protocol methodology, code and smart contract validation and audit processes;

g. systems and application development and quality assurance;

h. physical security and environmental controls, including but not limited to procedures around access to premises and systems;

i. procedures regarding their facilitation of Virtual Asset transactions initiated by a client including, but not limited to, considering multi-factor authentication or any better standard for Virtual Asset transactions that—

   i. exceed transaction limits set by the client, such as accumulative transaction limits over a period of time; and

   ii. are initiated after a change of personal details by the client, such as the address of a VA Wallet;

j. procedures regarding client authentication and session controls including, but not limited to, the maximum incorrect attempts for entering a password, appropriate time-out controls and password validity periods;

k. procedures establishing adequate authentication checks when a change to a client's account information or contact details is requested;

l. in addition to all applicable requirements in Part II of this Technology and Information Rulebook, client data privacy, including but not limited to—

   i. the security and authentication of the means of transfer of information;

   ii. the minimisation of the risk of data corruption and unauthorised access to data; and

iii. the prevention of information leakage;

m. vendor and third-party service provider management;

n. monitoring and implementing changes to core protocols not directly controlled by the VASP, as applicable;

o. incident response, including but not limited to root cause analysis and rectification activities to prevent reoccurrence;

p. supplier probity and Staff vetting procedures;

q. governance framework and escalation procedures for effective decision-making and proper management and control of risks and emergency incidents, including but not limited to responses to ransomware and other forms of cyberattacks; and

r. hardware and infrastructure standards, including but not limited to network lockdown, services/desktop security and firewall standards; and

s. sharing cyber threat information and intelligence with other VASPs and/or Entities—

i. whenever such action is in the best interests of the Virtual Asset market as a whole, to enhance operational resilience, manage the threat and, where practicable, minimise and/or mitigate the impact of such threat; and

ii. provided that, sharing such information does not increase any risks to the VASP and/or mandate the exposure of confidential information relating to the VASP sharing such information.

C. Cybersecurity – other legal and regulatory obligations

1. VASPs must ensure that their Technology Governance and Risk Assessment Framework complies with, to the extent applicable, cybersecurity laws, regulatory requirements and guidelines, including but not limited to—

a. the electronic security requirements and standards adopted by the Dubai Electronic Security Center per *Law No. (9) of 2022 Regulating the Provision of Digital Services Provided in the Emirate of Dubai*;

b. the *Federal-Decree Law No. (45) of 2021 on the Protection of Personal Data*, its executive regulations and any other cybersecurity regulatory requirements as may be imposed by the UAE Data Office from time to time; and

c. the *Consumer Protection Regulation* issued pursuant to *Central Bank Notice No. (444) of 2021* and any other cybersecurity regulatory requirements as may be imposed by the CBUAE from time to time.

D. Cryptographic keys and VA Wallets management

1. VASPs must ensure that their Technology Governance and Risk Assessment Framework addresses, to the extent necessary, the generation of cryptographic keys and VA Wallets, the signing and approval of transactions, the storage of cryptographic keys and seed phrases, VA Wallet creation and management thereof.

2. VASPs must—

a. safeguard access to Virtual Assets in accordance with industry best practices and, in particular, ensure that there is no single point of failure in the VASP's access to, or knowledge of, Virtual Assets held by the VASP;

b. adopt industry best practices for storing the private keys of clients, including ensuring that keys stored online or in any one physical location are insufficient to conduct a Virtual Asset transaction, unless appropriate controls are in place to render physical access insufficient to conduct such Virtual Asset transaction. VASPs must further ensure that backups of the key and seed phrases are stored in a separate location from the primary key and/or seed phrase;

c. adopt strict access management controls to manage access to keys, including an audit log detailing each change of access to keys. In particular, if Staff with access to a key (including a multi-signature arrangement key) leaves the employment of that VASP, the VASP must conduct an assessment to determine whether a new key must be generated;

d. adopt procedures designed to immediately revoke a key signatory's access. In particular, a VASP must—

i. ensure that the key generation process ensures that revoked signatories do not have access to the backup seed phrase or knowledge of the phrase used in the key's creation;

ii. perform internal audits on a quarterly basis concerning the removal of user access by reviewing access logs and verifying access as appropriate;

iii. implement and maintain a procedure for documenting the onboarding and offboarding of Staff;

iv. implement and maintain a procedure for documenting a VASP's permission to grant or revoke access to each role in its key management system; and

e. regularly assess the security of their information technology systems or software integrations with external parties and ensure that the appropriate safeguards are implemented in order to mitigate all relevant risks.

3. VASPs should provide information to clients on measures they can take to protect their keys and/or seed phrases from misuse or unauthorised access, and the consequences of sharing their private keys and other security information.

4. VASPs must ensure that access to their systems and data may only be granted to individuals with a demonstrable business need and implement safeguards to ensure the proper identification of all individuals, including the maintenance of an access log.

E. Testing and audit

1. VASPs must engage a qualified and independent third-party auditor to conduct vulnerability assessments and penetration testing (including, to the extent relevant to the VASP's business and VA Activities, comprehensive audits of the effectiveness, enforceability and robustness of all smart contracts) at least on an annual basis and prior to the introduction of any new systems, applications and products. VASPs must provide the results of any such assessments and tests to VARA upon VARA's request.

2. VASPs should maintain effective internal functions and measures for continuous monitoring of their operations and processes. In particular, on a regular basis and on request by VARA, VASPs must perform—
   a. security testing on both infrastructure and applications; and
   b. internal system and external system vulnerability audits.
3. Evidence of tests and audits must be documented by VASPs and made immediately available by them for inspection by VARA, upon VARA's request.
4. VASPs shall ensure that they are regularly audited by independent auditors to examine their management processes for ensuring the effectiveness of their processes, procedures and controls, and their compliance with regulatory requirements. VASPs must provide the results of any such audit to VARA upon VARA's request.
5. VARA may notify a VASP that it is required to carry out advanced testing by means of TLPT, where VARA considers it necessary and proportionate to do so, taking into account the following factors–
   a. any specific risks to which a VASP is or might be exposed;
   b. the criticality of a VASP's business and/or VA Activities; and
   c. any other relevant risks.
6. All TLPTs required under Rule I.E.5 must be carried out in accordance with the following conditions—
   a. each TLPT is to be carried out by an external tester;
   b. TLPTs may be required by VARA to cover Critical or Important Functions of a VASP and, where required, be performed on live production systems, technologies and processes supporting such Functions;
   c. where it is necessary for third-party service providers of the VASP to be included in the scope of a TLPT, the VASP shall ensure the participation of such third-party service providers in the TLPT;
   d. VASPs shall mitigate the risks of testing including any potential impact on data, damage to assets, and disruption to Critical or Important Functions, services or operations at the

VASP itself or to counterparts, and with due security assurance of data and privacy of client assets;

e. at the end of the testing, the VASP (together with the external tester) shall produce a summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with all relevant requirements as stated herein; and

f. the VASP shall promptly provide all documentation relating to the TLPT to VARA, including the summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with all relevant requirements as stated herein.

7. VASPS must ensure that the external testers they use to carry out any TLPT—

a. are suitable and of good repute;

b. possess all necessary technical and organisational capabilities and demonstrate specific expertise in threat intelligence and penetration testing;

c. are certified by an accreditation body, or adhere to formal codes of conduct or ethical frameworks;

d. provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of the TLPT, including the due protection of the VASP's confidential information; and

e. are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.

8. VASPs shall ensure that contracts concluded with external testers—

a. require sound management of the TLPT results and any data processing thereof, including any generation, storage, aggregation, draft, report, communication or destruction; and

b. do not create additional risks for the VASP or any of its systems.

9. Third-party technology service providers. Where the participation of a third-party technology service provider is required in any TLPT, as referred to in Rule I.E.6.c, the VASP and the third-party technology service provider may agree that such third-party technology service provider

directly enters into contractual arrangements with the external tester appointed by the VASP under Rule I.E.6.a, if such participation is reasonably expected to have an adverse impact on—

a. the quality or security of services delivered by such third-party technology service provider to the market; or

b. on the confidentiality of the data related to such services.

10. In the event that a third-party technology service provider directly enters into contractual arrangements with the external tester appointed by the VASP for a TLPT under Rule I.E.9, the VASP notified by VARA to carry out the TLPT must ensure that—

a. the third-party technology service provider remains under the direction of the VASP;

b. the results shall cover the relevant range of services supporting Critical or Important Functions of the VASP notified by VARA; and

c. all results provided by the third-party technology service provider to the external tester must be a fair representation of, and specific to, the VASP.

F. Virtual Asset transactions

1. VASPs must implement controls that prevent the manipulation or coordinated collusion or attacks of automated systems.

2. In addition to all applicable requirements in the Compliance and Risk Management Rulebook, VASPs must implement and maintain distributed ledger tracing software to screen incoming and outgoing Virtual Asset transactions and VA Wallet addresses. How VASPs will respond to any Suspicious Transactions must be set out in their AML/CFT policies in accordance with the Compliance and Risk Management Rulebook.

G. Algorithm governance

1. If a VASP conducts VA Activities using algorithms (in whole or in part), it must establish policies and procedures that enable its Board and Senior Management to have robust oversight and control over the design, testing, performance, deployment and ongoing maintenance of such algorithms.

2. VASPs must maintain documentation and records of the design, testing, performance, deployment and ongoing maintenance of such algorithms, including but not limited to the logic

used by the algorithm, any data or assumptions upon which decisions are based and any potential or actual biases in such data or assumptions and any results produced by the algorithm.

3. VASPs must ensure that they have qualified and competent Staff to ensure the proper functioning and supervision of such algorithms on an ongoing basis.

H. Business continuity, cybersecurity events and risk

1. VASPs must implement, maintain, test and update on an annual basis an adequate Business Continuity and Disaster Recovery Plan ("**BCDR Plan**") to minimise disruption to their operations. The BCDR Plan must address, but not be limited to—
   a. events that may trigger the implementation of the BCDR Plan, such as cybersecurity events and technical failures, and procedures to be taken to assess the nature, scope and impact of the event;
   b. resource requirements, including but not limited to Senior Management and Staff, systems and other assets;
   c. recovery priorities for the VASP's operations, including but not limited to the preservation of essential data and critical functions and the maintenance of those data and functions;
   d. communication arrangements for affected internal and external parties;
   e. processes to validate the integrity of information affected by any interruption;
   f. procedures to mitigate operational impact and/or to transfer operational functions including, but not limited to, escalation of response and recovery activities to designated personnel and management;
   g. an alternative site sufficient to recover and continue operations for a reasonable period; and
   h. procedures to remediate identified and/or exploited vulnerabilities or upgrade relevant protocols once stable operations are resumed to prevent similar events.
2. The BCDR Plan should take into consideration and address factors and issues specific to Virtual Assets and DLT including, but not limited to, network malfunction, loss of data or compromise in data integrity, and key storage and maintenance of authorisation layers.

I. Chief Information Security Officer and management

1. VASPs must appoint a Chief Information Security Officer ("**CISO**") who is responsible for ensuring that the VASP complies with Part I and Part III of this Technology and Information Rulebook. The CISO must be a separate individual from the CO however the CISO may also take on the responsibilities of the Data Protection Officer under Rule II.B.2 of this Technology and Information Rulebook.
2. The CISO must be of sufficiently good standing and appropriately experienced.
3. Senior Management must regularly assess and review the effectiveness of the VASP's processes, procedures and controls in relation to the VASP's compliance with this Technology and Information Rulebook and all applicable laws and regulatory requirements, as well as allocate duties and apportion roles and responsibilities within the VASP to prevent conflicts of interests.

J. Staff competency

1. In addition to relevant requirements in the Compliance and Risk Management Rulebook, VASPs must ensure that all Staff are aware of the latest cybersecurity risks and developments (including those specific to Virtual Assets and DLT), taking into account the type and level of cyber risks that they may face in their respective roles.

K. Notification to VARA

1. In addition to relevant requirements in the Compliance and Risk Management Rulebook, upon the detection of any occurrence of (i) a material cybersecurity event or (ii) an event triggering the implementation of the BCDR Plan that materially impacts a VASP's business operations, the VASP shall report such event to VARA as soon as reasonably practicable, and in any event no later than seventy-two (72) hours from detection, with all relevant details of the nature, scope and impact of such event and the steps the VASP is or will be taking to mitigate such impact including, but not limited to, whether any notifications or reports have been made to authorities other than VARA.

Part II – Personal Data Protection

A. Compliance with applicable data protection law

1. VASPs must comply with all applicable data protection and data privacy requirements in all relevant jurisdiction(s) as follows—
   a. within the UAE, including the PDPL and any sectoral or free zone laws and regulations that may apply to the VASP; and
   b. any data protection laws outside of the UAE that may apply to the VASP's activities wheresoever conducted.
2. Compliance with all applicable data protection and data privacy requirements under Rule II.A.1 of this Technology and Information Rulebook shall include, but not be limited to, where data may be stored or located and how such data is transferred.

B. Compliance programme

1. VASPs shall produce and implement a written compliance programme to protect the privacy of Personal Data, in accordance with all applicable data protection laws.
2. Notwithstanding the requirements of any applicable data protection laws, VASPs shall at a minimum comply with the following VARA requirements—
   a. appoint a Data Protection Officer who has the appropriate competencies and experience to perform the statutory duties and responsibilities associated with this role under applicable data protection laws (including under Article 11 of the PDPL) ("**Data Protection Officer**"). The Data Protection Officer can be the same individual as the CISO of the VASP; and
   b. establish a function in their organisation that is responsible for the management and protection of Personal Data in accordance with all applicable law and is appropriate for the level of risk involved with such Personal Data, including responsibility for implementing and maintaining appropriate processes, procedures and controls.

C. Provision of information to VARA

1. Notwithstanding any other requirement elsewhere in the Regulations, Rulebooks or Directives, VASPs shall take all steps, including where applicable provide all notifications, contractual provisions and obtain all consents, that are necessary to enable VARA to have access to any information relating to the VASP's compliance with this Part II of this Technology and Information Rulebook, regardless of where such information is stored. Access to such information shall be provided by VASPs in the manner and within the timelines communicated by VARA to the VASP.

2. VASPs shall notify VARA as soon as possible and in any event within twenty-four (24) hours following notification by them to either—

   a. any data regulator, including in the UAE; or

   b. a Data Subject

   of any incident affecting, or potentially affecting, Personal Data and shall provide VARA with a summary of such report and, where the relevant data regulator is located in the UAE, a copy of such report, unless and to the extent prohibited by applicable law as demonstrated by the VASP to VARA's satisfaction.

Part III – Confidential Information

A. Use and protection of confidential information by VASPs

1. VASPs shall take all reasonable steps to protect the ongoing confidentiality of all information related to their clients and all related properties and records. Such steps shall include implementing and enforcing appropriate policies, procedures and mechanisms to protect the confidential nature of any information shared with them, whether under the terms of a confidentiality agreement or otherwise.
2. Such policies, procedures and mechanisms shall require that use of any information related to a VASP's clients is only made for the purposes for which the information is provided and in compliance with relevant confidentiality agreements which shall be consistent with applicable laws and regulatory requirements, including with respect to acceptance of such agreements.
3. VASPs shall—
    a. familiarise Staff with—
        i. their internal policies on the collection and processing of confidential information; and
        ii. requirements in this Part III of this Technology and Information Rulebook as applicable to relevant Staff; and
    b. periodically certify their Staffs' compliance with such internal policies.
4. Staff must not share confidential information within the VASP or with any other Entities unless it is absolutely necessary for the purposes of conducting VA Activities related to such confidential information.
5. Neither VASPs nor their Staff shall use or share confidential information for the purpose of the trading of Virtual Assets by any Entity.

Schedule 1 – Guidance on Technology Governance and Risk Assessment Frameworks

Introduction

All VASPs are required to implement a Technology Governance and Risk Assessment Framework under Rule I.A.1 of this Technology and Information Rulebook. This Schedule 1 is provided by VARA as Guidance to VASPs, to assist them in creating effective Technology Governance and Risk Assessment Frameworks.

VASPs should consider all categories of risk and the risk mitigation standards (as may be applicable), set out in this Schedule 1 of the Technology & Information Rulebook, when creating their Technology Governance and Risk Assessment Frameworks.

Nothing in this Schedule 1 of the Technology & Information Rulebook shall limit, reduce or otherwise amend any Rules, or other requirements, with which VASPs must comply, under any applicable laws or regulations, Regulations, Rules or Directives, including but not limited to in respect of Personal Data protection.

A. Risk category 1: Organisational

1. Comprehensive security framework standard: VASPs are expected to utilise a balanced approach to ensure that security resources are allocated appropriately across their entire organisation, preventing security gaps and minimising single points of failure that attackers can exploit. VASPs are expected to implement a documented security framework that addresses both wallet infrastructure and enterprise security. The framework is expected to include, but not be limited to —
    a. regular security assessments of all system components;
    b. formal risk assessment methodology, including risks inherent in both centralised and decentralised structures;
    c. governance structure with clear security accountability; and
    d. adoption of best in class standards.
2. Secure development lifecycle standard: To ensure that security is integrated throughout the development process, reducing the accumulation of security debt even in rapid development

environments, VASPs are expected to establish and adhere to a formal secure development lifecycle methodology that incorporates security at every stage, from requirements gathering to deployment and maintenance. This methodology is expected to include, but not be limited to—

a. defining security requirements and mandatory security review gates before deployment;

b. threat modelling for new features and secure coding standards; and

c. post-implementation validation of the efficacy of the measures deployed.

3. Workforce security management standard: To address the unique challenges of the distributed workforce model common in the VA space, and to reduce the risk of compromised developer workstations leading to system intrusions, VASPs are expected to implement comprehensive workforce security controls, including but not limited to—

a. mandatory endpoint protection for all devices with access to any systems, including but not limited to production systems;

b. regular security awareness training specific to common threats;

c. background checks for all personnel with access to sensitive or critical systems;

d. formalised onboarding and offboarding procedures for all staff, including contractors; and

e. minimum security requirements for personal devices used for work purposes.

4. Infrastructure management standard: To ensure visibility across dispersed infrastructure, reducing security gaps at environment boundaries and enabling effective security monitoring, VASPs are expected to maintain comprehensive infrastructure documentation and controls, including but not limited to—

a. comprehensive asset inventories across all environments;

b. network diagrams and data flow mappings;

c. centralised configuration management and formal change control processes; and

d. regular infrastructure security assessments.

5. Third-party technology service provider standard: To ensure risks arising from the use of third-party technology services are incorporated as part of the VASP's framework, VASPs are expected to implement appropriate standards and controls for each third-party technology

service provider, which are proportionate to the nature, scale, complexity and importance of the services provided, including but not limited to—

a. conducting comprehensive due diligence on all such service providers;

b. having in place written contractual arrangements with all such service providers; and

c. adopting multi-vendor strategies where possible and/or practicable.

B. Risk category 2: Technical

1. Key generation standard: To reduce the risk of weak or predictable keys that could be exploited by attackers, VASPs are expected to generate cryptographic keys using industry-approved methods with sufficient entropy, including but not limited to—

   a. hardware security modules ("**HSMs**") for key generation, where possible;

   b. formal validation of key generation routines;

   c. best in class security processes for all cryptographic keys, including minimum standards for encryption;

   d. separation of duties during key generation; and

   e. comprehensive audit logging of all generation activities.

2. Wallet creation standard: To ensure that wallets are created in a controlled, secure environment with appropriate oversight, VASPs are expected to implement a secure wallet creation process that includes, but is not limited to—

   a. formal wallet creation procedures with separation of duties;

   b. multiple levels of approval for new wallet creation;

   c. tamper-evident processes for all creation activities;

   d. comprehensive logging and monitoring of wallet creation; and

   e. physical security controls for creation environments.

3. Key storage security standard: To reduce the risk of key compromise, which is the most direct path to asset theft, VASPs are expected to store cryptographic keys using defence-in-depth approaches, including but not limited to—

   a. HSMs for critical key storage;

b. appropriate separation of key components for keys-at-rest including both physical decentralisation and encryption/cryptographic methods;

c. restricted physical and logical access to key storage mechanisms; and

d. regular testing of key backup and recovery procedures.

4. Smart contract security standard: To reduce the risk of vulnerabilities in smart contract code that could be exploited to manipulate transactions or extract funds, VASPs are expected to implement formal smart contract review and testing processes, including but not limited to—

a. static and dynamic code analysis;

b. independent third-party audits before deployment and formal verification where applicable;

c. comprehensive penetration testing; and

d. regular re-assessment of deployed contracts.

5. Multi-signature security standard: To eliminate single points of failure in wallet security and ensure resilience against compromise of individual signers, VASPs are expected to implement robust multi-signature requirements, including—

a. minimum multi-signatures for high-value operations, where the minimum number of signers (M) is greater than the total number of signatories (N) divided by two (2) (i.e. $M > N/2$);

b. geographic distribution of signing authorities;

c. diverse authorisation mechanisms and separation of duties between signers; and

d. regular testing of signature processes.

6. Transaction verification standard: To reduce the risk of authorising fraudulent transactions, VASPs are expected to implement comprehensive transaction verification processes, including but not limited to—

a. mandatory multi-level verification;

b. automated detection of anomalous transactions in real-time triggering immediate notifications;

c. clear procedures for signers to verify and validate transactions;

d. formal process for addressing verification anomalies; and

e. immediate halting of the signing process when errors are reported.

7. Key compromise response standard: To ensure organisations can respond effectively to suspected or confirmed key compromises and to limit potential damage, VASPs are expected to develop and maintain a formal key compromise response plan that includes, but is not limited to—

   a. clear triggers for activation, with pre-authorised emergency response procedures and formal communication protocols;

   b. rapid key rotation capabilities; and

   c. regular testing and simulation.

8. Key holder management standard: To reduce the risk of unauthorised access to cryptographic keys through proper lifecycle management of key holders, VASPs are expected to implement comprehensive key holder management processes, including but not limited to—

   a. just-in-time access provisioning;

   b. regular access reviews and immediate revocation processes;

   c. segregation of duties; and

   d. secure backup key holder procedures.

9. Authentication control standard: To reduce the risk of unauthorised access through comprehensive authentication requirements, VASPs are expected to implement strong authentication controls, including but not limited to—

   a. multi-factor authentication for all access to systems with cryptographic keys;

   b. hardware-based authentication for critical operations, with biometric verification where appropriate;

   c. time-based restrictions on authentication attempts; and

   d. continuous validation of session authenticity.

10. Developer workstations standard: To address a common initial access vector for attackers by securing the development environment, VASPs are expected to implement strict controls for developer workstations, including but not limited to—

    a. endpoint protection and monitoring;

    b. network segmentation;

c. prohibition of direct production access;

d. secure secret management solutions; and

e. regular security assessments.

11. Security testing standard: To ensure ongoing identification and remediation of vulnerabilities before they can be exploited, VASPs are expected to conduct appropriate security tests regularly, and in all events prior to any update to a production system. Such security test should include, but not be limited to—

a. annual penetration testing by qualified third parties;

b. quarterly vulnerability assessments;

c. continuous automated security scanning;

d. regular best practice security exercises for high-value systems; and

e. formal remediation tracking for identified vulnerabilities.

12. Unauthorised recovery standard: To reduce the risk of unauthorised recovery of cryptographic keys from disposed media, VASPs are expected to implement comprehensive data sanitisation policies and procedures that ensure—

a. secure disposal of all media containing sensitive information;

b. cryptographic erasure or physical destruction of media containing cryptographic keys;

c. formal chain of custody documentation for media disposal;

d. regular assessment of sanitisation effectiveness; and

e. secure decommissioning procedures for all systems.

13. Audit logging standard: To enhance visibility into system activities and support effective investigation of security incidents, VASPs are expected to implement comprehensive monitoring and logging systems that—

a. capture all security-relevant events and store logs securely with tamper-evidence, maintaining logs for a minimum of one year;

b. include all wallet and key operations; and

c. implement real-time alerting for security events.

C. Risk category 3: Detection and response

1. Transaction monitoring standard: To enable early detection of fraudulent activities, VASPs are expected to implement comprehensive transaction monitoring, including but not limited to—
   a. behavioural analysis to detect anomalous patterns, and rule-based monitoring for known suspicious activities;
   b. machine learning capabilities for advanced threat detection;
   c. real-time alerting for Suspicious Transactions; and
   d. regular review and refinement of detection methodologies.
2. Internal user activity monitoring standard: To enhance the ability to identify compromised accounts or insider threats early, VASPs are expected to implement monitoring of internal user activities, including but not limited to—
   a. authentication attempts and failures and pattern analysis to detect insider threats;
   b. access to sensitive or critical systems and administrative activities; and
   c. segregation of monitoring from operational teams.
3. Enhanced monitoring standard: To provide visibility into activities on critical systems, enabling early detection of any compromises, VASPs are expected to implement enhanced monitoring of developer and signing systems, including but not limited to—
   a. process creation and termination monitoring;
   b. network connection analysis and file system change detection;
   c. software installation and execution control; and
   d. user behaviour analytics.
4. Tactical hardening standard: To enable organisations to limit attacker access once a compromise is detected, VASPs are expected to maintain capability to rapidly implement tactical hardening measures, including but not limited to—
   a. emergency access revocation, including individual end-points;
   b. network segmentation capabilities and system isolation procedures;
   c. pre-approved emergency change procedures; and
   d. regular testing of hardening capabilities.

5. Investigation capability standard: To enhance the ability to identify attack vectors and compromised assets during incidents, VASPs are expected to maintain comprehensive investigation capabilities, including but not limited to—
   a. dedicated forensic resources (internal or contracted) deployable and responsive in real-time and/or on immediate notice;
   b. secure evidence collection and handling procedures;
   c. chain of custody documentation;
   d. root cause analysis methodologies; and
   e. regular training and capability testing.
6. On-chain analysis standard: To improve the ability to trace stolen funds and identify potential recovery opportunities, VASPs are expected to develop and maintain on-chain analysis capabilities, including but not limited to—
   a. transaction tracing tools and wallet attribution capabilities;
   b. collaboration with other VASPs for fund tracing; and
   c. regular training and capability development.
7. Remediation standard: To reduce the risk of re-exploitation, VASPs are expected to implement comprehensive remediation procedures, including but not limited to—
   a. complete rotation of all secret components (including but not limited to passwords, keys and key shards) after incidents;
   b. system rebuilding from secure baselines and enhanced monitoring post-incident;
   c. formal verification of attacker removal; and
   d. post-incident review and lessons learned.

D. Risk category 4: Customer VAs

1. Customer authentication standard: To reduce the risk of any customer account compromises, VASPs are expected to implement robust customer authentication, including but not limited to—
   a. strong multifactor authentication;
   b. prohibition of instant messaging verification for high-risk operations;

c. risk-based authentication challenges and biometric authentication where appropriate; and

d. suspicious login detection and alerting.

2. Withdrawal control standard: To limit potential losses from compromised accounts through structured withdrawal controls, VASPs are expected to implement comprehensive withdrawal controls, including—

a. tiered withdrawal limits;

b. cooling periods for large transactions;

c. verification for high-value withdrawals outside of prescribed limits and/or 'bands';

d. verification for critical transactions;

e. behavioural analysis to detect anomalous withdrawal patterns; and

f. graduated approval requirements based on transaction value.

3. User education standard: To reduce customer vulnerability to social engineering and other attacks through improved awareness, VASPs are expected to implement comprehensive user education programmes, including but not limited to—

a. security best practices;

b. common attack vector awareness and secure account management guidance; and

c. regular security notifications.

4. VA Wallet concentration risk standard: To reduce the risk of concentration of Client VAs in a single or small number of VA Wallets, VASPs are expected to implement controls for the safe diversification of Client VAs across VA Wallets, including but not limited to—

a. cold storage VA Wallets;

b. VARA Licensed VASPs providing Custody Services; and

c. physical distribution of servers storing information through which VA Wallets can be accessed and/or controlled.

E. Risk category 5: Digital operational resilience

1. Digital operational resilience test standard: To achieve a high level of digital operational resilience, VASPs are expected to carry out digital operational resilience testing including, but not limited to—
   a. establishing and maintaining a sound and comprehensive digital operational resilience testing programme, including a range of assessments, tests, methodologies, practices and tools as set out below in paragraph 2;
   b. identifying weaknesses, deficiencies and gaps in digital operational resilience and promptly implementing corrective measures;
   c. when conducting the digital operational resilience testing programme, VASPs should follow a risk-based approach taking into account any specific risks to which the VASP is or might be exposed, the criticality of assets and of services provided by or to the VASP, as well as any other material risk factor;
   d. ensuring that tests are undertaken by independent external parties;
   e. classifying and remedying all issues revealed throughout the performance of the tests and establishing internal validation processes to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed; and
   f. ensuring that appropriate tests are conducted at least yearly on all systems and applications supporting Critical or Important Functions.
2. The digital operational resilience testing programme referred to in paragraph 1 should provide for testing of tools and systems through the execution of appropriate tests, including but not limited to—
   a. vulnerability assessments and scans;
   b. open source analyses;
   c. network security assessments;
   d. gap analyses;
   e. physical security reviews;
   f. questionnaires and scanning software solutions;
   g. source code reviews;

h. scenario-based tests;

i. compatibility testing;

j. performance testing;

k. end-to-end testing; and

l. penetration testing.

Schedule 2 – Definitions

Term	Definition
"AML/CFT"	has the meaning ascribed to it in the Regulations.
"BCDR Plan"	has the meaning ascribed to it in Rule I.H.1 in this Technology and Information Rulebook.
"Board"	has the meaning ascribed to it in the Company Rulebook.
"CBUAE"	means the Central Bank of the United Arab Emirates.
"Chief Information Security Officer" or **"CISO"**	has the meaning ascribed to it in Rule I.I.1 of this Technology and Information Rulebook.
"Compliance and Risk Management Rulebook"	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
"Compliance Officer" or **"CO"**	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
"Critical or Important Function"	has the meaning ascribed to it in the Company Rulebook.
"Cybersecurity Policy"	has the meaning ascribed to it in Rule I.B.1 in this Technology and Information Rulebook.
"Data Protection Officer" or **"DPO"**	has the meaning ascribed to it in Rule II.B.2 of this Technology and Information Rulebook.
"Data Subject"	has the meaning ascribed to it in the PDPL.
"Distributed Ledger Technology" or **"DLT"**	has the meaning ascribed to the term "Distributed Ledger Technology" in the Dubai VA Law.
"Dubai VA Law"	means *Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai*, as may be amended from time to time.
"Emirate"	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.

Term	Definition
"Entity"	means any legal entity or individual.
"Function"	has the meaning ascribed to it in the Company Rulebook.
"Guidance"	has the meaning ascribed to it in the Regulations.
"HSM"	means a hardware security module.
"Licence"	has the meaning ascribed to it in the Regulations.
"Licensed"	means having a valid Licence.
"PDPL"	means the *Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data*.
"Personal Data"	has the meaning ascribed to it in the PDPL.
"Regulations"	means the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time.
"Rule"	has the meaning ascribed to it in the Regulations.
"Rulebook"	has the meaning ascribed to it in the Regulations.
"Senior Management"	has the meaning ascribed to it in the Company Rulebook.
"Staff"	has the meaning ascribed to it in the Company Rulebook.
"Suspicious Transactions"	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
"Technology and Information Rulebook"	means this Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
"Technology Governance and Risk Assessment Framework"	has the meaning ascribed to it in Rule I.A.1 of this Technology and Information Rulebook.
"Threat Led Penetration Testing" or **"TLPT"**	means a framework that mimics the tactics, techniques and procedures of real- life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the VASP's critical live production systems.
"UAE"	means the United Arab Emirates.
"UAE Data Office"	means the UAE Data Office established by virtue of *Federal Decree-Law No. (44) of 2021 Establishing the UAE Data Office*.

Term	Definition
"VA Activity"	means the activities listed in Schedule 1 of the Regulations, as may be amended from time to time.
"VA Wallet"	has the meaning ascribed to the term “Virtual Asset Wallet” in the Dubai VA Law.
"VARA"	means the Dubai Virtual Assets Regulatory Authority.
"VASP"	means an Entity Licensed by VARA to conduct VA Activity(ies) in the Emirate.
"Virtual Asset" or **"VA"**	has the meaning ascribed to it in the Dubai VA Law.