حكومة دبي
GOVERNMENT OF DUBAI

VARA
سُلطة تنظيم الأصول الافتراضية
VIRTUAL ASSETS REGULATORY AUTHORITY

Technology and Information Rulebook

7 February 2023

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 [the **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 1.

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. Overview

1. VASPs must ensure that they implement systems and controls necessary to address the risks, including cybersecurity-related risks, to their business and VA Activities. Such systems 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.
2. VASPs must implement a technology governance and risk assessment framework which must be comprehensive and proportionate to the nature, scale, and complexity of the risks inherent in their 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 the VASP's cybersecurity objectives, including the requirements for the competency of Staff and, as relevant, end users and clients and clearly defined systems and procedures necessary for managing risks.
3. VASPs must ensure that their technology governance and risk assessment is capable of determining the necessary processes and controls that they must implement in order to adequately mitigate any risks identified. In particular, VASPs must ensure that their technology governance and risk assessment framework includes 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, such as a development, maintenance and testing process for technology systems and operations controls, back-up controls, capacity and performance planning and availability testing.
5. 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.

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 request.
4. VASPs shall ensure that they are regularly audited by independent auditors to examine their management processes for ensuring the effectiveness of their systems, controls, policies and procedures and their compliance with regulatory requirements. VASPs must provide the results of any such audit to VARA upon VARA's request.

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 adopt sufficient procedures and controls to manage the risks relating to their business, VA Activities and systems. In particular, VASPs must implement an audited risk management programme in accordance with applicable laws and regulations [including those related to cybersecurity] and the requirements of VARA from time to time. The risk management programme shall include—
   a. strategies to identify, assess, monitor and manage operational risk;
   b. procedures concerning operational risk management;
   c. an operational risk assessment methodology; and
   d. a risk reporting system for operational risk.
2. VASPs must monitor and assess operational risk management procedures on a continuous basis. In particular, VASPs must review, update and arrange for the testing of their 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.
3. 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.

4. 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 systems, controls, policies and procedures 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 an occurrence of a cybersecurity event or other 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 policies, procedures, systems 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 – 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.3 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.
"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.
"Entity"	means any legal entity or individual.
"Licence"	has the meaning ascribed to it in the Regulations.

Term	Definition
"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.
"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*.
"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.