VANUATU FINANCIAL
SERVICES COMMISSION

CYBERSECURITY GUIDELINES

SUPERVISION DEPARTMENT

Purpose:

As articulated in *section 59 of the Virtual Assets Services Providers Act No.3 of 2025*, this guideline is to ensure that the Virtual Asset Services Providers maintain robust cybersecurity frameworks that protect the integrity, confidentiality, and availability of virtual assets services, safeguard customer, data, and uphold Vanuatu's reputation as a secure international financial center.

1. Governance and Management

The licensee must appoint a Chief Technology Officer (CTO) or equivalent responsible:

a. for the cybersecurity oversight and incident.
b. conduct regular cybersecurity awareness and training programs for all staff.
c. establish a cybersecurity policy approved by the senior management that aligns with international best practices and relevant with the Virtual Assets Services Providers Act No.3 of 2025 (the "Act"), Regulations, and Guidelines.

2. Physical and Network Security

The licensee must maintain a controlled access to the system and sensitive data in in a secure physical office in Vanuatu including implementing firewalls, intrusion detection/prevention systems, and secure network architecture to protect against unauthorized access. In addition, he or she has to ensure encryption of data in transit and at rest, especially for virtual asset transactions and customer information.

3. System Integrity and Access Control

The licensee needs to enforce multi-factor authentication (MFA) for all critical systems and administrative access including maintaining strict access control based on the principle of least privilege for all users and systems.

4. Risk Management and Incident Response

The licensee must develop and maintain a comprehensive risk management policy that effectively identifies, assesses, and mitigate risks, particularly those associate with blockchain technology and custodian services. In conjunction with this, an established incident response plan outlining clear procedures for detecting, reporting, and responding to cybersecurity incident and breaches. Furthermore, the CTO must conduct regular internal cybersecurity audits and enables independent reviews/audits of their technology infrastructure to continuously enhance their security posture and safeguard their assets.

5. Business Continuity and Disaster Recovery

The licensee must implement and regularly test business continuity and disaster recovery plans to ensure rapid recovery from cyber incidents or other disruptions and maintain backup systems and data recovery mechanisms with secure offsite storage.

6. Third Party and Custodian Security

The licensee must ensure that any third-party service providers, including custodian, comply with equivalent cybersecurity standards, and are not subject to sanctions, and conduct ongoing due diligence and monitoring of the third-party cybersecurity practices.

7. Compliance and Reporting

The CTO must maintain a comprehensive records of cybersecurity policies, incidents, audits, and staff training for review by the Vanuatu Financial Services Commission (VFSC) and report significant cybersecurity incident promptly to the VFSC as per the regulatory requirements.

8. Insurance and Legal Compliance

The licensee must maintain adequate cyber insurance coverage for any losses including financial and legal cost associated with cyber threats and must comply with all applicable laws and regulations related to cybersecurity, data protection, and the virtual asset services provider Act.

9. Technology Infrastructure and Audits

The licensee must have adequate internal controls to continuously monitor their operations. They must regularly perform security test on their infrastructure and applications, and conduct vulnerability tests/audits on both internal and external systems. These tests must also be done when the Commissioner ask for them.

The licensee must hire a qualified and independent third-party auditor to perform vulnerability assessment and penetration test at least once a year. This also applies before launching any assessment and penetration test at least once a year. This also applies before launching any new systems, application, or products. If applicable, the audit should include a thorough review of all smart contract. The licensee must share these test results with the Commissioner when requested.

The Commissioner can require a licensee to perform advanced test called Threat-Let Penetration Testing (TLPT) if needed, based on the licensee's risk level, business importance, or other factors with the following conditions:

- TLPT must be done by a qualified external tester
- It may cover critical functions and be performed on live systems
- If third party services providers are involved, they must also be included/ participate in the testing.
- Risk from testing (Like data loss or service disruption) must be minimized.
- After testing, the summary of findings, remediate action, and proof of compliance measures must be prepared.
- All TLPT documentation must be promptly shared with the Commissioner.

The external testers must have the following:

- Be reputable and qualified.
- Have technical skills and expertise in threat intelligence and penetration testing.
- Be certified or follow recognized standards.
- Provide independent assurance about risk management and data protection.
- Have professional indemnity insurance covering misconduct and negligence.

The licensee must make sure that the contract with the external testers include proper management of TLPL results and that no additional risk is introduced to the licensee or its system as a result of the testing exercise.

If other third-party service providers are involved in TLPT, they may directly contract with the external tester if this helps protect service quality or data confidentiality. In this context, the licensee must still direct the testing process and the testing must cover all relevant services supporting the licensee operations. Accordingly, the test results from the third parties must fairly represents the licensee's services.

10. Risk – Based AML Framework

The licensee must develop a comprehensive AML program tailored to virtual assets, incorporating a risk-based approach (RBA) to identify, assess, and mitigate money laundering and terrorist financing risks specified to virtual asset transaction and customers. It will include continuous update and document enterprise-wide ML/TF risk assessment considering customer profiles, products, geographic exposure, and transaction types, including features like anonymity-enhancing technologies or mixers that increase risk.

11. Customer Due Diligence (CDD) and Know Your Customer (KYC).

The licensee must implement adequate and comprehensive KYC procedure to very client identities before onboarding and continuously monitor customer activities for suspicious behavior including using technological systems to automate identity verification and transaction monitoring o ensure compliance with AML requirements.

12. Compliance with the Virtual Asset Travel Rule

The licensee must ensure adherence of the FATF recommendation 16 (Travel Rule), which requiring sharing originator and beneficiary information during virtual asset transfer to enhance transparency and traceability.

13. Transaction Monitoring and Suspicious Activity Reporting

The licensee must employ advanced monitoring tools to track virtual asset transactions in real-time, flagging unusual or suspicious patterns linked to money laundering or terrorist financing and maintained a detailed record of all transactions and customer information for audit and regulatory review. Additionally, the CTO must promptly report suspicious transactions to the Commissioner.

Detection and response:

The licensee must employ the following:

Transaction monitoring

- Watch all transactions carefully to spot fraud early.
- Use behavior checks to find unusual actions and rules to catch suspicious activities.
- Use smart computer programs (machine learning) to detect any new treats.
- Get alerts immediately when something is suspicious happens.
- Regularly update its methods to stay effective.

Internal User Activity Monitoring

- Keep an eye on what employees and internal users are doing to catch problem early.
- Monitoring loging attempts, especially failures to spot insider threats.
- Watch access to important systems and any admin actions.
- Make sure the team monitoring activities is separate from the doing daily operations.

Enhanced Monitoring of Critical Systems

- Pay special attention to important system like developer tools and signing systems.
- Track when programs start or stop.
- Check network connections and changes to files.
- Control what software can be installed or run.
- Analyze use behavior to detect unusual actions.

Tactical Hardening (Quick Defense Measures)

- Be ready to quickly block hackers if a breach happens.
- Have the ability to revoke access immediately, even for single devices
- Use network segmentation and isolate systems to limit damage.
- Have pre-approved emergency procedures for quick changes.
- Test these defense measures regularly.

Assemble Incident Response Team

- Quickly gather a team including IT/security expert, legal, communications, and management to coordinate the response and handle technical, legal, and public relations aspects.

Investigation Capabilities

- Have a team of expert ready to investigate attacks right away.
- Follow strict procedures to collect and protect evidence securely.
- Keep detailed records of evidence handling.
- Use methods to find the root cause of incidents.
- Train staff regularly and test investigation skills.

Contain the Breach Immediately

- Disconnected affected devices or systems from the network to stop the hacking to spread further.
- Disable any compromised user accounts or credential right away.
- Block suspicious IP addresses or domains at your firewall.
- If needed, isolate or shut down affected servers or system temporarily.
- Use network segmentation to limit the breach's reach if available.

Assess the Impact

- Determine what systems, data, and users were affected and evaluate the risks to individuals and the entity.

On-Chain Analysis (Tracking Stolen Fund)

- Use tools to trace transactions and identify wallets involved in theft.
- Work with similar organization to track stolen funds.
- Keep training and improving these skills.

Remediation (Fixing After an Incident)

- Change all secret information like passwords and keys after an incident.
- Rebuild systems from safe backups and increase monitoring afterward.
- Confirm the attacker is fully removed.
- Review what happened and learn from the incident to improve future security.

Communicate Internally and Externally

- Keep your team informed about the breach and containment steps
- Notify affected individuals and regulatory authorities if required by law, regulation, guidelines, or policy.

14. Blockchain Analytics tools

The licensee must deploy blockchain analytic platforms (e.g., Chainalysis, Elliptic, TRM labs) to trace transactions flows, identify connections to sanctioned or high-risk wallet addresses, and visualize transaction graphs for suspicious patterns. These tools provide risk scoring for entities and wallets, helping prioritize investigations and compliance efforts.

15. Suspicious Activity Reporting (SAR)

The licensee must maintain comprehensive records of transactions and flagged activities to support timely and accurate suspicious activity reports to the VFSC and the Vanuatu Financial Intelligent Unit (FIU), including relevant blockchain-specific data in reports, such as wallet addresses, transaction hashes, and device identifiers, to facilitate effective regulatory assessment.

16. Cryptographic keys and VA Wallets management.

The licensee must have clear rules and control for creating cryptographic keys and virtual assets wallets, approving and singing transactions, safely storing cryptographic keys and seed phrases, and properly managing virtual assets wallets.

The licensee must perform these following tasks in the course of his duties:

- protect virtual assets carefully by using best industry practices to protect access and avoid having a single point of failure (no one person or system should control everything).

- store the private keys safely by using best practices for storing clients' private keys and do not keep all keys online or in one physical place without strong controls.

- Procedure to immediately revoke access from people who shouldn't have it anymore and make sure revoked people cannot access back up seed phrases.

- Do quarterly audit to check access logs and confirms only authorized people have access and keep records of staff joining or leaving and who can grand or remove access.

Key Generation

- Use trusted industry methods to create strong, unpredictable cryptographic keys.
- Using hardware security modules (HSMs) where possible.
- Validate key creation processes formally.
- Follow top security practices, including minimum encryption standards.
- Separate duties among staff during key generation.
- Keep details logs of all key generation activities.

Wallet Creation

- Create wallets in a secure, controlled environment.
- Have a formal procedure with clear separation of duties.
- Require multiple approvals before making new wallets.
- Use tamper-evidence methods to detect unauthorized changes.
- Log and monitor all wallet creation actions.
- Ensure physical security of the wallet creation area.

Key storage area

- Protect keys using multiple layers of defense.
- Store critical keys in HSMs.
- Keep key part separate physically and cryptographically.
- Limit who can access key storage, both physically and digitally.
- Regularly test backup and recovery keys.

Smart Contract Security

- Review and test smart contract code carefully.
- Use static and dynamic code analysis tools.
- Get independent third-party audits before deployment.
- Conduct penetration testing.
- Reassess contracts regularly after deployment.

Multi Signature Security

- Use multi-signature wallets to avoid single points of failure.
- For important transactions, require more than half of signers to approve.
- Distribute signer across different locations.
- Use different authorization methods and separate signer duties,
- Test signature process regularly.

Transaction Verification

- Verify transaction at multiple level before approval.
- Use automated systems to detect unusual transactions an alert immediately.
- Provide clear steps for signers to check transactions.
- Have a formal process to handle verification issues.
- Stop the signing process immediately if errors are found.

Key Compromise Response

- Have a clear plan to respond to suspected or confirmed key breaches.
- Define when to activate the plan with pre-approved emergency steps.
- Be able to quickly replace compromised keys.
- Test the response plan regularly with drills.

Key Holder Management

- Give access to keys only when needed (just-in-time access).
- Review access rights regularly and revoke immediately if necessary.
- Separate duties among key holders.
- Have secure backup procedures for key holders.

Developer Workstations

- Protect developer computers with endpoint security and monitoring.
- Separate developer networks from production systems.
- Do not allow direct access to production from developer machines.
- Use secure methods to manage secrets (passwords, keys).
- Perform regularly security checks on developer environments.

Unauthorized Recovery Prevention

- Safely dispose of all media containing sensitive data.
- Use cryptographic erasure or physically destroy media with keys.
- Keep records of media disposal.
- Regularly Check how effective data sanitization with keys.
- Follow Secure procedures when retiring systems.

Audit logging

- Record all important security events and keep logs secure and tamper-proof.
- Keep logs for at least 7 years.
- Log all wallet and keys-related operations.
- Set up real-time alerts for security incidents.

17. Usage of Algorithms

If a licensee uses algorithms to do their work, they must have a clear rules and processes. These rules help the licensee management to carefully watch and control how algorithm are created, tested, work, are put into use, and kept running properly.

The licensee must keep detailed records and documents about these algorithms, this includes how the algorithm works, the data and assumptions it uses to make decisions, any possible biases in the data or assumptions, and the results the algorithm produces.

The licensee must have skilled and trained staff to make sure the algorithms work correctly and are supervised all the time.

Branan Karae
Commissioner

COMMISSION DES AFFAIRES FINANCIERES
VANUATU
FINANCIAL SERVICES COMMISSION