SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Circular

15 August 2025

Circular to licensed virtual asset trading platform operators on custody of virtual assets

This circular elaborates on the Securities and Futures Commission's (**SFC**) expected standards for the safe custody of client virtual assets by SFC-licensed virtual asset trading platform operators and their associated entities (collectively, **Platform Operators**). To address potential platform vulnerabilities, this circular sets forth the minimum requirements that Platform Operators must meet and also provides examples of good practices to facilitate their compliance with these requirements.

Background: overseas platform incidents

According to media reports, overseas centralised virtual asset platforms have encountered multiple cybersecurity incidents over the past year, resulting in substantial financial losses. These incidents were primarily due to vulnerabilities in wallet systems and their associated controls. Specifically, these recent overseas incidents expose the following critical weaknesses:

(a) Attackers compromised a third-party wallet solution by injecting malicious code, thereby altering the platform's user interface;
(b) Inadequate access controls allowed unauthorised access to approval devices and, hence, malicious changes to approval requests;
(c) Systematic and independent transaction verifications were inadequate and, hence, failed to prevent transaction signers from manually approving fraudulent transactions;
(d) Transaction signers blindly approved forged transactions without verifying the approval content.

These incidents point to potential critical vulnerabilities in both hot and cold wallet infrastructure, platform operations, third-party management, internal controls, threat monitoring, and security awareness, regardless of the custody solutions used, such as Hardware Security Modules (HSMs), Multi-Party Computation (MPC), or Multi-Signature (Multi-Sig).

Importance of resilient custody controls and expected standards

The custody of client virtual assets demands robust security, governance, and operational controls. Under Initiative 3 in Pillar **S** (**S**afeguard) of the **ASPIRe** roadmap—"*Explore adopting a dynamic approach to custody technologies and storage ratios*"—the SFC policy direction is clearly stated as follows:

> "The SFC recognises the rapid evolution of custody technologies and the need for a forward-looking regulatory approach. Instead of mandating specific hardware solutions, the SFC will explore transitioning to more technology-neutral, outcome-based standards that prioritise the overall custody control environment. VASPs[1] may possibly adopt more innovative solutions, **provided that they demonstrate robust asset protection measures and maintain a secure, auditable control environment.** This approach highlights the need for holistic safeguards that must be put in place…"

[1] Virtual asset service providers

Earlier this year, the SFC conducted a limited-scope enquiry into Platform Operators' custody controls to evaluate their resilience against similar vulnerabilities. Whilst most Platform Operators reported having fundamental control measures in place, certain responses were deemed inadequate.

This circular aims to provide further clarification on the expectations for safeguarding virtual assets by Platform Operators. The requirements set forth in this document establish the minimum standards that Platform Operators must meet, and serve as the prerequisites for transitioning to more advanced custody technologies. Additionally, the circular includes examples of best practices which, though not compulsory, are intended to support Platform Operators in effectively implementing these standards.

Going forward, these standards will also constitute core expectations for the providers of Virtual Asset Custodian Services[2], and help to foster a consistent framework for virtual asset custody across the industry.

I. Senior management responsibilities

1. According to paragraphs 3.4 and 3.7 of the Guidelines for Virtual Asset Trading Platform Operators[3] (**Guidelines**), corporate governance, internal controls, operational review, risk management, and compliance are key elements in determining a Platform Operator's competence. Additionally, under paragraphs 5.1(c) and 5.1(k) of the Guidelines, senior management bears responsibilities for maintaining appropriate standards and ensuring that the Platform Operator effectively employs its resources and procedures for the proper performance of its business activities. Senior management should ensure that:

   (a) Effective policies, procedures and internal controls[4] are implemented; and
   (b) Adequate senior management oversight and governance by suitably qualified and experienced individuals are in place[5].

   Accordingly, a Platform Operator should designate at least one Responsible Officer or Manager-in-Charge to oversee the matters outlined in Sections II to VI below.

II. Client cold wallet infrastructure

2. According to paragraph 10.8 of the Guidelines, Platform Operators should establish and implement strong internal controls and governance procedures for private key management to ensure all cryptographic seeds and private keys are securely generated, stored and backed up. Where practicable, seeds and private keys should be generated offline and stored in a secure environment, such as an HSM, with appropriate certification for the lifetime of the seeds or private keys.

3. Given the critical role of HSMs in client asset custody, Platform Operators should perform appropriate due diligence on the HSM provider before onboarding, as well as periodic evaluation on an ongoing basis.

[2] See Public Consultation on Legislative Proposal to Regulate Virtual Asset Custodian Services
[3] Paragraph 3.4 and 3.7 of the Guidelines for Virtual Asset Trading Platform Operators
[4] Paragraph I(1) of the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission (Internal Control Guidelines)
[5] Paragraph I(5) of the Internal Control Guidelines

4. As part of the HSM vendor assessment, Platform Operators should ensure that the vendor has the capability and continuous commitment to (a) maintain security standards through effective patch management, and (b) ensure that, when patches are necessary to maintain the HSM's security, the patched HSM is validated and its certification is updated promptly.

5. Cold wallet implementations should not include smart contracts on public blockchains to minimise potential online attack vectors associated with on-chain smart contracts.

III. Client cold wallet operation

6. According to paragraph 10.10 of the Guidelines, Platform Operators should ensure that (a) adequate processes are in place for handling deposit and withdrawal requests for client virtual assets to guard against losses arising from theft, fraud, and other dishonest acts, professional misconduct, or omissions, (b) safeguards are implemented to prevent fraudulent requests or requests made under duress, as well as controls to prevent one or more officers or employees from transferring assets to wallet addresses other than the client's designated wallet address, and (c) destination addresses for client withdrawal instructions cannot be modified before the transactions are signed and broadcast to the respective blockchain.

7. The generation and safeguarding of seeds or private keys should be performed on air-gapped cold wallet devices. Platform Operators should remain vigilant, as attacks can occur at any stage of a transaction's lifecycle and may result in asset misappropriation. The security of client assets is only as strong as its most vulnerable point.

8. Platform Operators should (a) regularly conduct thorough assessments of potential attack vectors, including before implementing any material changes, such as modifications to processes, systems or authorised personnel, and (b) put in place multiple layers of independent data integrity checks at various stages of the transaction process, along with an end-to-end integrity protection from transaction creation to broadcasting, and proper segregation of duties.

9. Platform Operators should implement robust systematic controls to prevent unauthorised transactions from the cold wallet. Whitelist controls should be used to prevent asset transfers to unapproved wallet addresses. Any modifications or additions to the cold wallet whitelist should be subject to stringent controls and oversight. Each transaction should undergo systematic verification to ensure that only authorised transactions proceed and no unapproved or unexpected parameters exist.

10. Devices used for transaction approval should be dedicated, with restricted functionality and limited network connectivity, isolated from general purpose workstations to reduce compromise risks. Integrity checks on critical transaction data should be conducted using air-gapped devices stored in a cold vault. These devices require physical access for code modifications, supporting the reliability of the data integrity verification process.

11. When a transaction requires manual check before signing, all its details should be displayed in a clear, human-readable format to allow signers to review the information before proceeding.

Good Practice

(a) Firm A implemented a cold wallet system, including an air-gapped HSM and a signing terminal secured within the cold wallet vault.

- Access to the area is managed through a strict multi-factor access control system that logs all entries and exits. The vault is continuously monitored and recorded by surveillance cameras. These strict physical controls minimise the risk associated with potential compromises at the signing terminal, thus enhancing confidence in the integrity of the control measure carried out at this terminal.
- Prior to signing, the signing terminal displays the complete transaction details to the signer, preventing blind signing[6] and mitigating the risk of insider attacks that could involve replacing the transaction to be signed, or supplementing it with hidden malicious parameters. If the displayed transaction does not correspond with the intended transaction details, the signing terminal will halt the process and alert the signers via a notification on the screen.
- The signing terminal implements a systematic whitelist control designed to guard against both external and insider threats that could modify destination addresses during transaction creation. For each transaction, the destination address is checked against the whitelist. If the destination address is not on the whitelist, the signing terminal will halt the operations and notify the security team.

(b) Firm B used dedicated hardware devices only for transaction review and approval. These devices are deployed exclusively for wallet operations, ensuring a clear physical separation from the approvers' ordinary activities.

(c) Firm C implemented a final stage pre-broadcast data validation check as an extra layer of end-to-end verification. Prior to broadcasting the signed blockchain transaction, the system conducts a validation process that compares the signed transaction against the original unsigned transaction. If any discrepancy is identified, the signed transaction will not be broadcast.

IV. Use of wallet solution and third-party provider

12. According to paragraphs 12.8 and 12.10 of the Guidelines, Platform Operators should ensure that any system modifications such as implementing new systems or upgrading existing ones, are thoroughly tested before deployment. Also, Platform Operators should ensure that their platforms are subject to regular review in order to maintain their integrity, reliability, security and capacity, and that robust contingency measures are established.

[6] Blind signing refers to the practice of approving or signing a transaction without reviewing its content. This behaviour is considered a poor practice in transaction management, as it increases the risk of errors.

13. Under paragraph 12.6 of the Guidelines, where a platform or any activities associated with it are provided by or outsourced to a third-party service provider, the Platform Operator should perform appropriate due diligence, engage in ongoing monitoring and make appropriate arrangements to ensure that the Platform Operator meets the requirements in the Guidelines.

14. Segregation of duties and comprehensive oversight mechanisms must be strictly enforced for wallet system code management, irrespective of whether the codebase is developed internally or externally. These controls mitigate the risk of malicious code insertion by external attackers or rogue developers, and include gatekeeping procedures such as code reviews, testing, software supply chain management, management approvals, and secure deployment practices. All of these procedures should be documented through audit trails. Administrator access to production systems—whether for deployment or upgrades—must also be tightly controlled according to the principles of least privilege, privilege separation, and recognised industry best practices.

15. Third-party assessments should incorporate independent code reviews, as well as comprehensive understanding of the provider's software development and release processes before onboarding or implementing material changes. These assessments ensure the robustness of protocols to prevent the introduction of malicious code or security vulnerabilities.

16. In case a third-party wallet solution is utilised, in addition to conducting appropriate due diligence[7] on the provider before onboarding, Platform Operators should maintain ongoing review of the provider to ensure full compliance with the Guidelines. This ongoing review includes regular evaluation of the provider's security controls and operational processes, mandating timely reporting of incidents and emerging risks, and regular testing of the provider's disaster recovery capabilities. Platform Operators should regularly conduct inherent risk assessments covering third-party dependencies and vulnerability management, and implement mitigation measures to reduce residual risks. They should also perform independent cybersecurity assessments of the deployed system periodically, in accordance with paragraph 12.13 of the Guidelines.

17. As an ongoing measure, Platform Operators should establish procedures and conduct drills to address emergency and business continuity plan (BCP) scenarios. End-to-end rehearsals should be conducted regularly with third-party solution providers to ensure the BCP meets the recovery time objectives set by the SFC.

V. Ongoing real-time threat monitoring

18. According to paragraphs 12.12(f) and 12.14 of the Guidelines, Platform Operators should (a) employ adequate security controls over platform infrastructure, including establishing a Security Operations Centre (SOC) or equivalent function with sufficient resources to take charge of all security monitoring processes and technologies and act as a coordinator for efficient incident detection, and (b) establish written policies and procedures specifying how a suspected or actual cybersecurity incident should be escalated.

[7] The due diligence should include assessing whether the provider has a robust business continuity plan and conducts regular testing of its disaster recovery capabilities.

19. Platform Operators should implement real-time reconciliation of on-chain client assets with the ledger balance. Should any unexpected transactions cause discrepancies, the SOC or an equivalent monitoring team should be promptly alerted and take appropriate actions with relevant teams.

20. The SOC should work closely with domain experts in areas such as wallet management, operations, and technology to regularly assess and refine alerts and their parameters. Senior management should oversee this process to ensure that alert thresholds are effectively calibrated for the timely detection of potential issues.

21. Platform Operators should establish robust mechanisms to detect unauthorised access or intrusions to critical wallet infrastructure, including the cold wallet vault, signing devices, databases, production binaries, and code repositories.

22. In view of the inherent complexity and significance of custody systems, Platform Operators' monitoring processes should cover both the custody system and its dependencies, including vendors, technologies, blockchain protocols, encryption algorithms, and common libraries that may impact the safety of client assets.

23. The monitoring framework should incorporate consideration of significant industry incidents and the publicly identified security vulnerabilities that may threaten the integrity of the custody system and related components.

24. Given the continuous operation of virtual asset platforms and blockchain activities, security monitoring should be conducted on a 24/7 basis, including during holidays. Platform Operators should allocate adequate resources to address contingency issues and establish procedures to mobilise additional resources for incidents occurring outside regular business hours.

25. Platform Operators should develop a structured framework for handling security alerts and managing incidents according to severity levels, and assign corresponding response protocols.

Good Practice
A few firms implemented an effective 24/7 monitoring function, which successfully identified an industry incident immediately after its emergence on social media, even though it was around midnight in Hong Kong. Although the incident did not directly impact the firm's custody system, it was significant enough to prompt the security team to escalate the matter to senior management without delay. A response team, comprising the right mix of expertise, senior management, technology, and security personnel, was quickly assembled to thoroughly assess any potential impact on their own custody systems whilst closely monitoring the developments of the industry incident.

VI. Training and awareness

26. In accordance with paragraph 12.5 of the Guidelines, Platform Operators are required to allocate appropriately qualified personnel, as well as sufficient expertise, technological resources, and financial support to the design, development, deployment, operation, and modification of their platforms. Furthermore, Section III(3) of the Internal Control Guidelines stipulates that management must ensure staff receive adequate training tailored to their specific roles, both at the outset and on a continuous basis.

27. In particular, Platform Operators are expected to ensure that transaction signers receive comprehensive training to fully understand verification requirements and the appropriate handling procedures in case of any exception or uncertainty concerning a transaction.

28. Platform Operators should implement robust measures to prevent blind signing and ensure effective manual transaction review or approval.

Good Practice
In addition to regular security awareness training, Firm C implements training on transaction validation for staff, focusing specifically on procedures to prevent errors when performing manual verification. Firm B conducts monthly phishing simulations for all staff to emphasise the importance of security, as the majority of cyber-attacks stem from social engineering tactics, especially phishing.

Way forward

The requirements outlined in this circular take immediate effect. Platform Operators should critically assess their virtual assets custody framework, procedures, and controls to ensure compliance with the expected standards. Adherence to these requirements should form part of Platform Operators' annual external compliance and technology assessment.

Should you have any queries regarding this circular, please contact your case officers-in-charge.

Intermediaries Division
Securities and Futures Commission

End

SFO/IS/025/2025