SFC 證監會

Appendix 1

Expected standards of conduct for Platform Operators

This appendix sets out the expected standards of conduct for Platform Operators on cybersecurity, protection of client assets and know your client process. These standards supplement the requirements under the VATP Guidelines.

(A) Cybersecurity

Expected standard A – Network access and segmentation
Platform Operators should set their security related configurations[1] in a manner that properly segregates the network segment or security group hosting critical systems and sensitive data from other network segments or security groups which are exposed to higher hacking risk.

Expected standard B – Privileged access management
Platform Operators should develop robust privileged access management governance framework, policies and procedures and deploy a privileged access management solution to centrally and holistically manage privileged accounts at all levels, ie, system servers, workstations and network perimeters. Platform Operators should also ensure that their senior management (including Managers-in-charge of Overall Management Oversight, Key Business Lines and Information Technology): (a) have full transparency of all the privileged accounts that exist in the systems and network components in their IT environment and can properly manage all privileged access in a holistic manner, in order to strictly apply the principle of least privilege and mitigate collusion risk; (b) approve each use of the privileged accounts; and (c) are timely alerted when privileged accounts are used.

Expected standard C – Encryption
Platform Operators should (a) proactively monitor security threats and vulnerabilities which may have an impact on the secure storage of client virtual

[1] The design and implementation of network infrastructure to host systems and data in the cloud environment would be different from the network infrastructure set up in the "non-cloud" environment. Platform Operators should use cloud-native segmentation controls and adopt micro-segmentation approach to deploy the network segmentation in a granular manner, ie, access restriction between segregated network clusters, security groups and even individual system service and component.

assets; and (b) review the cryptographic algorithms used in their processes, irrespective of whether such algorithms are provided by their system vendors. These reviews should be conducted pre-deployment and on an ongoing basis to ensure that up-to-date encryption technology is used.

Platform Operators should also ensure that strong encryption algorithms are used for both the storage of data and their transmission between different systems.

Expected standard D – Security monitoring arrangement

Platform Operators should deploy sufficient resources to their security operations centre (SOC) (or equivalent function) and ensure that the SOC can properly perform continuous security monitoring and promptly identify and effectively handle security incidents in light of the Platform Operators' 24x7 operation mode.

Expected standard E – Detection of suspicious unauthorised access to client accounts

Platform Operators should implement effective automated solutions to monitor and identify suspicious unauthorised access to clients' accounts. Platform Operators should perform such monitoring in real time.

Expected standard F – Internet access control on staff workstations

Platform Operators should assess the internet access needs of each staff member, grant access based on their job duties and implement Uniform Resource Locator (URL) whitelisting control as needed, to minimise cybersecurity risks arising from potential phishing attacks.

(B) Client virtual assets

Expected standard G – Handling of client virtual assets

Platform Operators should implement adequate procedures and controls to ensure that client virtual assets are adequately safeguarded. In particular, they should ensure that (a) only their Responsible Officer(s), Manager(s)-in-charge or his/ her delegate(s) are authorised to handle and access client virtual assets; (b) no other personnel has access to any seed or private key, or holds any device or credential relating to client virtual assets; and (c) all handling and access are subject to proper oversight.

If Platform Operators store their master seed or private key in safe boxes operated by third-party service providers in Hong Kong, they (or their associated entity) should be a party to the service agreements for safe boxes with the third-party providers.

Platform Operators should implement wallet address whitelisting mechanism for all withdrawals of client virtual assets, whether to internal or external wallets, to prevent errors, omissions and potential fraudulent requests made by staff.

Expected standard H – Segregation of client virtual assets

Platform Operators should implement adequate procedures and controls to ensure no commingling of client virtual assets and the Platform Operators' (or their associated entity's) virtual assets in wallets designated for holding client virtual assets.

Expected standard I - 98/2 cold/hot wallet asset ratio

Platform Operators should implement proper procedures to ensure the proper classification of client hot and cold wallets and calculation of the amount of client virtual assets held in these wallets. In particular, Platform Operators should ensure that all client virtual assets they received are included in the calculation, regardless of whether these virtual assets have passed their internal checking and verification processes.

Platform Operators should also promptly transfer client virtual assets to the client cold wallets when the 98/2 Requirement[2] has been breached.

Expected standard J – Large withdrawals of client virtual assets

In order to minimise exposure to losses arising from a compromise or hacking of the platform, when handling large withdrawal requests (ie, those exceeding 2% of the total client virtual assets under custody), Platform Operators should implement proper procedures to ensure compliance with the 98/2 Requirement.

Expected standard K – Large deposits of client virtual assets

Platform Operators should establish, implement and enforce a real-time monitoring system to monitor client virtual assets in the hot storage. They should also (a) automatically sweep virtual assets held in the client's hot storage to cold storage upon the receipt of client virtual assets and ensure that such sweeping is conducted on a real-time basis; and (b) maintain adequate buffer below the threshold to meet the 98/2 Requirement.

Expected standard L – Storage of seeds and private keys

Platform Operators should:

(a) keep seeds and private keys in Hong Kong and in a secure environment, such as a hardware security module (HSM), with appropriate certification; and

(b) not use smart contracts in its cold wallet system as this would undermine the security of the air-gapped cold wallet and introduce an online attack surface.

[2] Platform Operators are required to store 98% of the client virtual assets in cold storage (referred to as "98/2 Requirement")

Expected standard M – Access to seeds and private keys

Platform Operators should:

(a) store backups of seeds or private keys in secure locations, other than the primary site of the seeds/ private keys, to mitigate the risk of a single point of failure in case of disruptions at the primary site;

(b) ensure that the access control for the backup of seeds or private keys is as stringent as that for their originals;

(c) implement adequate procedures to ensure prompt retrieval of the backups of seeds or private keys and restoration of their custody system upon any system failure or outage at the primary site; and

(d) properly identify and mitigate any key man risks and establish appropriate back-up arrangements.

Expected standard N – Segregation of duties and rights of persons authorised to access the seeds and private keys

Platform Operators should implement appropriate measures to segregate the duties and rights of personnel authorised to access the seeds and private keys. They should also conduct proper assessments and implement adequate controls to identify and mitigate collusion risk and ensure the secure storage of client virtual assets. Before making any material changes to the custody control matrix, such as altering control personnel or processes, Platform Operators should conduct a proper collusion analysis[3] to identify any potential risks.

Expected standard O – Contingency plan

Platform Operators should implement a comprehensive contingency plan which sets out all material disruptive scenarios (including major operational breakdown or insolvency of third-party service providers) and the procedures for handling these scenarios. Platform Operators should also conduct proper operational risk evaluation and implement adequate mitigation measures to respond to potential disruptions caused by failure of third-party service providers.

Expected standard P – Recovery of custody system

Platform Operators are required to have adequate procedures and resources to restore their custody services in a timely manner. They should also test their contingency plans at least annually to ensure they could restore services within 12 hours.

[3] Collusion analysis should assess whether two authorised persons, with the authority granted to them, can transfer client virtual assets, assuming that one or both authorised persons may not follow the Platform Operator's procedures and controls.

Expected standard Q – Backup facility
Platform Operators should implement adequate procedures to minimise and appropriately manage the risk of interruptions or other operational or control failures. They should also ensure their backup site is fully functional and maintain a security level equivalent to that of their primary site, to allow them continued access to client virtual assets in case of disruptions at the primary site.

Expected standard R – Insurance arrangement
Platform Operators should conduct adequate analysis to ensure that the insurance policy in place is sufficient to cover the Compensation Amount (ie, 50% of client virtual assets in cold wallets and 100% of client virtual assets in hot wallets held by their associated entity), including potential loss arising from fraud or default on the part of the Platform Operators or their associated entities. Amongst other things, Platform Operators should assess the potential impact of the occurrence of an exclusion event specified under the insurance policy, the likelihood of receiving a claim upon an insured event, and the potential impact of Event Deductibles[4].

Expected standard S – Monitoring of compensation arrangement
Platform Operators should implement adequate procedures to ensure the value of Compensation Amount is properly calculated to ensure the sufficiency of the compensation arrangement. In particular, they should include the value of all client virtual assets received and held by themselves (and their associated entities) when calculating the Compensation Amount.

Expected standard T – Handling of client money
Platform Operators should arrange for their clients to directly deposit funds into the segregated bank accounts of the Platform Operators' associated entity to reduce the exposure of client funds to unnecessary risks.

Expected standard U – Operation of bank accounts
Platform Operators should ensure that only persons who are involved in the day-to-day management of the Platform Operators' or their associated entity's operations are authorised to operate the associated entity's segregated bank account, and the authorised signatory arrangements of all bank accounts comply with the standards set out under the answer to question 5 of the Client Money FAQs[5]. Platform Operators should also implement adequate procedures and controls to prevent and detect potential fraud and omissions and ensure that client money is appropriately protected. If a dual signatory is not required for effecting payments

4 Event Deductible referred to the amount the Platform Operator is responsible for paying towards an insured loss.

5 Frequently Asked Questions on Client Money issued on 31 May 2023 (Client Money FAQs)

from the Platform Operators' bank accounts, they should ensure that adequate compensating controls are in place.

(C) Access to Platform Operators' services

Expected standard V – Access to services

Platform Operators should conduct adequate due diligence and assessment on the functionality of the geolocation, VPN and proxy detection features in third-party solutions as well as the accuracy and completeness of the databases maintained by external vendors both before deployment and on a regular basis. This is to ensure that the Platform Operators can leverage these databases and tools to (a) identify persons with IP addresses from Restricted Jurisdictions[6] and prevent them from accessing the operators' services; and (b) identify IP addresses associated with VPNs and proxies. Platform Operators should also maintain proper documentation on the assessments and due diligence conducted.

If Platform Operators allow clients to access their services using VPNs and proxies, they are required to implement adequate procedures to detect and prevent access to their services by persons attempting to circumvent the relevant jurisdictions' ban on trading virtual assets. For example, Platform Operators should implement clear and adequate monitoring procedures and take appropriate follow-up actions to address irregularities in client behaviour or VPN/ proxy usage and changes in clients' circumstances.

[6] Restricted Jurisdictions referred to locations related to (a) sanctioned jurisdictions; and (b) jurisdictions which have banned trading in virtual assets.