Annex

Updated Guidance on Expected Standards on Provision of Custodial Services for Digital Assets by Authorized Institutions

This guidance applies to custodial activities of digital assets (i.e. assets that depend primarily on cryptography and distributed ledger or similar technology), except limited purpose digital token[1], held on behalf of clients (hereafter called "client digital assets") by authorized institutions ("AIs") and subsidiaries of locally incorporated AIs[2]. As an illustration, assets covered include virtual assets ("VAs")[3], tokenised securities and other tokenised assets[4]. This guidance is not applicable to custody of proprietary assets of an AI or its group companies which are not held on behalf of clients. For the avoidance of doubt, AIs should also observe the relevant requirements[5] if they also provide dealing services in the virtual assets concerned in their custodial service.

(A) Governance and risk management

1. Prior to launching custodial services for digital assets, an AI should undertake a comprehensive risk assessment to identify and understand the associated risks. The AI should put in place appropriate policies, procedures and control measures to manage and mitigate the identified risks, taking into account applicable legal and regulatory requirements. The board and senior management of the AI should exercise effective oversight of the risk management process to ensure that the risks associated with the custodial activities are identified, assessed, managed and mitigated both before the engagement in the custodial activities and on an ongoing basis.

---

1 As defined in section 53ZR of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO).

2 For the purposes of the rest of this Annex, the term "AI" includes a subsidiary of a locally incorporated AI which provides digital asset custodial services.

3 As defined in section 53ZRA of the AMLO.

4 "Tokenised securities" and "other tokenised assets" generally refer to digital representations of "securities" as defined under the Securities and Futures Ordinance and other real-world assets respectively, using distributed ledger or similar technology to record ownership.

5 For example, in respect of third-party transfers, the relevant requirements set out in the HKMA's circular on "Virtual asset-related activities in relation to relevant stablecoins issued by licensed stablecoin issuers" issued on 27 May 2026.

2. An AI should allocate adequate resources, including the necessary manpower and expertise, for its custodial activities to ensure proper governance, operations and effective risk management. Senior management and staff engaging in the AI's custodial activities and related control functions should possess the necessary knowledge, skills and expertise to discharge their responsibilities.

3. Given the fast-evolving development in the digital asset space, an AI should ensure that sufficient training is provided to the senior management and staff involved in the custodial activities, both at the outset and on an ongoing basis. In particular, transaction signers should receive comprehensive training to fully understand verification requirements and appropriate handling procedures for exception or uncertainty concerning a transaction.

4. An AI should have appropriate accountability arrangement for the custodial activities, including setting out written and clear roles and responsibilities as well as reporting lines. There should also be adequate policies and processes to identify, manage and mitigate any potential and/or actual conflicts of interest that may arise, for example, among different activities undertaken by the AI or its affiliates.

5. An AI should establish and maintain effective contingency and disaster recovery arrangements to ensure business continuity of its custodial activities. An AI should also conduct drills to address emergency and business continuity plan ("BCP") scenarios.

(B) Segregation of client digital assets

6. An AI should hold client digital assets in separate client accounts[6] that are segregated from the AI's own assets to ensure that client digital assets are protected from claims of the AI's creditors in the event of an insolvency or resolution of the AI.

[6] Including wallet address(es) holding client digital assets on distributed ledger which should be segregated from that used for holding the AI's own assets.

7. An AI should not transfer any right, interest, ownership, legal and/or beneficial titles in the client digital assets or otherwise lend, pledge, re-pledge or create any encumbrance over the client digital assets, except for (i) the settlement of transactions, and/or fees and charges owed by the client to the AI; (ii) where prior explicit written consent of the client is obtained; or (iii) where it is required by law. The AI should have adequate and effective measures to prevent the use of client digital assets for its own account or for purposes other than those agreed with its clients.

(C) Safeguarding of client digital assets

8. An AI should put in place adequate systems and controls to ensure that client digital assets are promptly and properly accounted for and adequately safeguarded. In particular, the AI should have effective control measures to minimise the risk of loss of client digital assets due to theft, fraud, negligence or other acts of misappropriation, as well as delayed access or inaccessibility of client digital assets.

9. In developing the systems and controls to safeguard client digital assets, an AI may adopt a risk-based approach, taking into account the nature, features and risks of the digital assets held in its custody. Risks may be dependent on, for example, the type of distributed ledger technology ("DLT") network used (such as private-permissioned, public-permissioned and public-permissionless) as well as the mitigation measures in place. For instance, client digital assets held as permissionless tokens on a public-permissionless DLT network may be exposed to heightened cybersecurity risks, and recovery of lost assets may be difficult in the event of theft, hacking or other cyberattacks, compared with public-permissioned and private-permissioned DLT networks where there may be controls of access to the DLT networks. Client digital assets held as permissioned tokens with access controls on the smart contract may enable recovery of lost assets.

10. Systems and controls to safeguard client digital assets include, among others, written policies and procedures for:

- authorising and validating access to effecting deposit, withdrawal and transfer of client digital assets, including the access to the devices storing seeds and private keys. A robust mechanism should be established to detect unauthorised access or intrusions to critical wallet infrastructure, including the cold wallet vault, signing devices, databases, production binaries, and code repositories;
- robust systematic controls to prevent unauthorised transactions from the cold wallet. Whitelist controls should be used to prevent asset transfer to unapproved wallet address, with stringent controls and oversight on any change to the cold wallet whitelist. Each transaction should undergo systematic verification to ensure authorisation;
- managing and safeguarding seeds and private keys of client digital assets, covering key generation, distribution, storage, use, destruction and backup; and
- handling security alerts and managing incidents according to severity levels, and assign corresponding response protocols.

11. In particular, an AI is expected to adopt relevant industry best practices and follow applicable international security standards in safeguarding client digital assets in a way that is commensurate with the nature, features and risks of the assets being held. While the procedures and controls set out below are not intended to be prescriptive or one-size-fits-all, they are generally required for an AI which holds client VAs. For other digital assets, an AI may adopt a risk-based approach in the implementation of the following procedures and controls commensurate with the risks posed but if such digital assets are in the form of permissionless tokens on a public-permissionless DLT network, an AI also should exercise extra caution and critically assess the implementation:

(a) generating and storing seeds and private keys, including their backups, in secure and tamper-resistant environment and devices, such as hardware security module ("HSM"). Where practicable, seeds and private keys should be generated offline with an appropriate lifetime limit. Given the critical role of HSMs in client asset custody, AIs should perform appropriate due diligence on the HSM provider before onboarding, as well as periodic evaluation on an ongoing basis. As part

of the assessment, AIs should ensure that the vendor has the capability and continuous commitment to (i) maintain security standards through effective patch management, and (ii) ensure that, when patches are necessary to maintain the HSM's security, the patched HSM is validated and its certification is updated promptly;

(b) securely generating, storing and backing up seeds and private keys in Hong Kong[7];

(c) cold wallet implementations should not include smart contracts on public blockchains to minimise potential online attack vectors associated with on-chain smart contracts;

(d) implementing measures to ensure that any smart contract used in the custody process is not subject to any contract vulnerabilities or security flaws to a high level of confidence;

(e) assessing potential attack vectors on a regular basis, including before any material changes to processes, systems, or authorised personnel, and putting in place multiple layers of independent data integrity checks across the transaction lifecycle with an end-to-end integrity protection and proper segregation of duties;

(f) 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 include gatekeeping procedures such as code reviews, testing, software supply chain management, approvals, and secure deployment practices, and should be documented through audit trails. Administrator access to production systems should be tightly controlled according to the principles of least privilege, privilege separation, and recognised industry best practices;

(g) in client cold wallet operation, devices used for transaction approval

[7] Subject to the HKMA's consent, a HKMA-licensed stablecoin issuer may be appointed by an AI (e.g. by entering into a delegation or outsourcing arrangement) to provide custody services for specified stablecoins it issues, provided the issue of such is authorized by a licence granted under the Stablecoins Ordinance, and that the seeds and/or private keys are safeguarded and backed-up in Hong Kong or a location acceptable to the HKMA.

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, and these devices require physical access for code modifications, supporting the reliability of the data integrity verification process;

(h) strictly restricting access to cryptographic devices or applications on a need-to-know basis to authorised personnel with appropriate screening and training; maintaining up-to-date documentation of how the access is authorised and validated as well as the access rights allocated; using strong authentication method, such as multi-factor authentication, to authenticate access to seeds and private keys; maintaining audit trail of the access to the cryptographic devices or applications;

(i) implementing robust controls to avoid any "single point of failure" by way of, for example, using key sharding or similar technology to split and distribute a private key among multiple personnel authorised by the AI for distributed storage so that no single party holds the entirety of the key. Generally, a certain number of key shard holders are required to act collectively to sign a transaction to ensure that no single person possesses full access, while preventing operation interruption when a single shard is lost, unavailable or stolen. To prevent "single point of failure", the use of multiple wallets, instead of one single wallet, to hold client digital assets may also be considered. Robust measures should be implemented to prevent blind signing and ensure effective manual transaction review or approval. All details of a transaction which requires manual check should be displayed in a clear, human-readable format to allow signers to review before signing;

(j) putting in place controls to prevent and mitigate the risk of collusion among authorised personnel with access to the seeds and private keys;

(k) having adequate offsite backups and contingency arrangements for seeds and private keys, which should be subject to the same security controls as the original seeds and private keys. Backed up seeds and private keys should be kept offline in a secure physical location that is separate from

and will not be affected by any event at the primary location where the original seeds and private keys are stored;

(l) storing a substantial portion[8] of client digital assets in cold storage unconnected to the internet, unless otherwise justified;

(m) allowing deposit and withdrawal of client digital assets only through wallet addresses that belong to clients[9] (e.g. through proof of ownership test, such as message signing or micropayment test) and are whitelisted, except for transfers to support payment services or to execute client's settlement instructions where third-party transfers will be allowed provided that effective risk controls in respect of third-party transfers are in place; and

(n) being liable to its clients for the loss of client digital assets as a result of an incident that is attributable to the AI, and ensuring adequate financial resources (which may include suitable insurance arrangement) to cover potential losses.

12. Where an AI offers a user interface or portal for clients to manage their digital assets held by the AI, effective client authentication and notification controls should be put in place, following relevant guidance set out by the HKMA from time to time.

13. An AI should closely monitor the trends and developments in emerging security threats, vulnerabilities, attack and fraud risks as well as technological solutions; evaluate periodically the adequacy and robustness of the security risk controls having regard to the emerging threats and technological advancements; and put in place measures to keep the technology to safekeep client digital assets in line with relevant industry best practices and applicable international standards. The wallet storage technology used for keeping client digital assets should be tested before deployment to ensure reliability.

---

[8] Where client digital assets under custody are VAs, an AI should store 98% of the client digital assets in cold storage.

[9] "clients" also refer to clients of another AI, a licensed corporation or virtual asset trading platform operator ("VA trading platform") licensed by the Securities and Futures Commission which holds digital assets on their behalf in an account maintained with the AI.

(D) Delegation and outsourcing

14. As a general principle[10], as far as VAs are concerned, an AI may only delegate or outsource its custody function to (i) another AI (or a subsidiary of a locally incorporated AI); (ii) a VA trading platform[11] licensed by the SFC; or (iii) an HKMA-licensed stablecoin issuer that has obtained the HKMA's consent to provide custody for specified stablecoins it issues, provided the issue of which is authorized by the licence granted under the Stablecoins Ordinance). For digital assets other than VAs, if they are in the form of permissionless tokens on a public-permissionless DLT network, the AI should exercise extra caution and critically assess whether it is appropriate to delegate or outsource its custody function.

15. Where an AI enters into a delegation or outsourcing arrangement in the provision of digital asset custodial services, the AI should perform appropriate due diligence before selecting and appointing the delegate or service provider. The AI should assess and be satisfied with, among others, the delegate or service provider's financial soundness, reputation, managerial skills, technical and operational capability (e.g. incorporating independent code reviews and understanding of the provider's software development and release process before onboarding or implementing material changes) and capacity to ensure compliance with the expected standards set out in this Annex and other applicable legal and regulatory requirements, as well as the ability and capacity to keep pace with the technological developments on the digital asset front. The due diligence assessment and its result should be documented with proper record keeping. The AI should have effective controls in place to monitor and review the performance of the delegate or service provider on an ongoing basis to ensure regulatory compliance. This ongoing review should include regular evaluation of the delegate's or service provider's security controls and operational processes, mandating timely reporting of incidents and

[10] See Part X paragraph 10.1 of "Guidelines for Virtual Asset Trading Platform Operators" (June 2023) and paragraph 20 of "Circular on SFC-authorised funds with exposure to virtual assets" (Revised on 27 May 2026), both issued by the Securities and Futures Commission, for reference.

[11] Which may hold VAs through its Associated Entity.

emerging risks, and regular testing of the delegate's or service provider's disaster recovery capabilities. AIs 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.

16. When engaging a delegate or service provider in the provision of digital asset custodial services, an AI should have the technical expertise to assess the effectiveness of the solutions deployed in safeguarding clients' digital assets, and whether it introduces any single point of failure. The AI should also fully understand the terms and conditions under which the delegate or service provider holds the client digital assets, and assess whether it will materially affect the legal rights of the client, including in the event of insolvency of the delegate or service provider. It is the AI's responsibility to ensure that the delegate or service provider segregates client digital assets properly in accordance with paragraphs 6 and 7 of this Annex.

17. An AI's contingency and disaster recovery arrangements should cover the scenario of disruption to the delegated or outsourced digital asset custodial services. The AI should also assess the delegate or service provider's resilience capabilities, including their contingency plans and procedures, to ensure availability of the custodial service. End-to-end rehearsals should be conducted regularly with the delegates or service provider to ensure the BCP meets the recovery time objectives.

18. An AI is reminded to also maintain relevant systems and controls as in delegation or outsourcing arrangements for traditional financial activities.

19. The ultimate responsibility and accountability for any delegated or outsourced activities rest with an AI.

(E) Disclosure

20. An AI should provide its clients with full and fair disclosure of the custodial arrangements in a clear and easily comprehensible manner including:

- the respective rights and obligations of the AI and its clients, including the clients' rights of ownership to their assets in the event of the AI entering insolvency or resolution;

- the custodial arrangement, including how client digital assets are stored and segregated, the procedures and the time taken to deposit and withdraw client digital assets, and any applicable fees and costs;

- the insurance / compensation arrangement to cover potential loss of client digital assets caused by, for example, security incidents or misappropriation;

- any existence of client digital assets commingled with assets of other clients, and the risks involved;

- the circumstances and the arrangement where the AI will take legal and/or beneficial title to the client digital assets, or otherwise transfer, lend, pledge, re-pledge or create any encumbrance over the client digital assets, and the risks involved;

- the treatment of client digital assets and their respective rights and entitlements in events such as voting, hard forks and airdrops; and

- the existence and the nature of any potential and/or actual conflicts of interest associated with the custodial activities of the AI.

(F) Record keeping and reconciliation of client digital assets

21. An AI should maintain appropriate books and records for each customer to track and record ownership of client digital assets, including the amount and the kind of assets owed to the client as well as the movement of the assets to and from the client's account. Regular and frequent reconciliation of client digital assets should be conducted on a client-by-client basis, taking into account both relevant off-chain and on-chain records. Any discrepancies noted should be addressed and escalated to senior management as appropriate in a timely manner.

22. An AI should have systems and controls in place to keep and safeguard all records relevant to the custodial activities, which shall be provided to the HKMA in a timely manner upon request.

(G) Ongoing monitoring

23. An AI should regularly review its policies and procedures and conduct independent audit on its systems and controls and its compliance with the applicable requirements in respect of custody of client digital assets. Any system modifications such as implementing new systems or upgrading existing ones, should also be thoroughly tested before deployment. Security monitoring should be conducted on a 24/7 basis, with adequate resources and established procedures to address contingency issues and incidents occurring anytime, including holidays.

24. In view of the inherent complexity and significance of custody systems, AIs' 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.

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

(H) Provision of staking services for VAs from custodial services

26. The HKMA has issued guidance on "Provision of staking services[12] for VAs from custodial services" on 7 April 2025. The HKMA would like to remind AIs that in complying with the relevant requirements, AIs should also have due regard to the requirements set out in the terms and conditions

[12] Staking services refer to any arrangements which involve the process of committing or locking client VAs for a validator to participate in a blockchain protocol's validation process based on a proof-of-stake consensus mechanism, with returns generated and distributed for that participation.

for providing staking services as imposed by the SFC to SFC-licensed VA trading platform providing staking services as per the Appendix to its circular issued on 7 April 2025.