2025 年 8 月 15 日

致持牌虛擬資產交易平台營運者的

關於虛擬資產託管的通函

本通函闡述了證券及期貨事務監察委員會（**證監會**）預期證監會持牌虛擬資產交易平台營運者及其有聯繫實體（統稱為**平台營運者**）在安全託管客戶虛擬資產方面應達到的標準。為應對潛在的平台漏洞，本通函列出了平台營運者必須符合的最低規定，並提供良好作業方式的示例，以利便它們遵守該等規定。

背景：海外平台事故

根據媒體報道，海外的中心化虛擬資產平台在過去一年遭遇多宗網絡保安事故，引致重大財務損失。這些事故主要是由於錢包系統及其相關監控措施出現漏洞所致。具體來說，這些近期的海外事故凸顯了以下重大漏洞：

(a) 攻擊者透過植入惡意程式碼，破壞第三方錢包解決方案，令平台的用戶界面遭到竄改；
(b) 針對接達的監控措施不足，導致攻擊者在未經授權下能夠接達用於批准的設備，繼而對批准請求進行惡意更改；
(c) 欠缺足夠的系統化而獨立的交易驗證，因而未能阻止交易簽署人以人手方式批准欺詐交易；
(d) 交易簽署人在沒有核對批准內容的情況下，便盲目地批准偽造交易。

無論平台營運者採用了哪類託管解決方案（例如硬件保安模組（Hardware Security Modules，簡稱 HSM）、多方計算（Multi-Party Computation，簡稱 MPC）或多重簽署（Multi-Signature ，簡稱 Multi-Sig）），這些事故都顯示了平台營運者在熱錢包及冷錢包的基礎設施、平台運作、第三方管理、內部監控措施、威脅監察及保安意識方面出現潛在重大漏洞。

穩健的託管監控措施的重要性及應達到的標準

客戶虛擬資產的託管需要穩健的保安、管治及營運監控措施。根據 **ASPIRe** 路線圖支柱 **S**（**S**afeguards 保障）下的措施 3—“*探索針對託管技術和儲存比率的動態監管方針*”—下文明確地載述證監會的政策方向：

> “證監會明白對急速發展的託管技術採取前瞻性監管框架的重要性。證監會將探索制定更技術中立、以結果為導向的標準，優先考慮整體託管內控環境，而非強制規定特定的硬件解決方案。虛擬資產服務提供者或會採用更創新的解決方案，**但前提是它們必須證明具備穩健的資產保護措施，並維持一個安全、可審計的監控環境**。這種方法強調建立全方位保障措施的必要性……”

今年初，證監會就平台營運者的託管監控措施進行了有限範圍的查詢，以評估它們對類似漏洞的抵禦能力。雖然大多數平台營運者報稱已實施基本的監控措施，但部分回應被視為有不足之處。

本通函旨在進一步闡明證監會預期平台營運者在保障虛擬資產方面應達到的標準。本文件所列的規定既是過渡至更先進的託管技術的先決條件，亦是平台營運者必須符合的最低標準。此外，本通函亦涵蓋最佳作業方式的示例，以協助平台營運者有效地落實相關標準，但這些做法並非強制性。

日後，這些標準亦將構成對虛擬資產託管服務提供者的核心要求[1]，有助在整個業界層面促進虛擬資產託管框架的統一性。

I. 高級管理層的責任

1. 根據《適用於虛擬資產交易平台營運者的指引》[2]（**該指引**）第 3.4 及 3.7 段，企業管治、內部監控、營運審查、風險管理及合規是釐定平台營運者的勝任能力的關鍵要素。此外，根據該指引第 5.1(c)及 5.1(k)段，高級管理層有責任維持適當的標準，並確保平台營運者有效地運用其資源和程序，以便適當地進行其業務活動。高級管理層應確保：

   (a) 落實有效的政策、程序和內部監控措施[3]；及
   (b) 由具備合適資格和豐富經驗的人士作出充分的高級管理層監督及管治[4]

   因此，平台營運者應指定至少一名負責人員或核心職能主管，以監督以下第 II 至 VI 部所述的事宜。

II. 客戶冷錢包的基礎設施

2. 根據該指引第10.8段，平台營運者應在私人密鑰管理方面設立並實施嚴格的內部監控措施及管治程序，藉以確保安全地產生、儲存及備份所有加密種子及私人密鑰。在切實可行的情況下，種子及私人密鑰應以離線方式產生，以及在安全的環境（例如 HSM）中保存，並且對種子或私人密鑰的生命周期有合適的認證。

3. 鑑於 HSM 在客戶資產託管中發揮關鍵作用，平台營運者在採用 HSM 供應商前，應對其作出適當的盡職審查，以及持續地進行定期評估。

4. 作為 HSM 供應商評估的一部分，平台營運者應確保該供應商有能力並持續承諾進行以下事項：(a)透過有效的修補管理來維持保安標準；及 (b)在需要修補以維持 HSM 的保安水平時，確保經修補的 HSM 獲得驗證，而其認證亦及時予以更新。

5. 冷錢包的實施不應包含公共區塊鏈上的智能合約，以盡量減少與鏈上智能合約相關的潛在網絡攻擊媒介。

---

[1] 請參閱有關規管虛擬資產託管服務的立法建議的公眾諮詢。
[2] 《適用於虛擬資產交易平台營運者的指引》第 3.4 及 3.7 段。
[3] 《適用於證券及期貨事務監察委員會持牌人或註冊人的管理、監督及內部監控指引》（《內部監控指引》）第 I(1)段。
[4] 《內部監控指引》第 I(5)段。

III. 客戶冷錢包的操作

6. 根據該指引第10.10段，平台營運者應確保：(a)就處理客戶虛擬資產的提存要求制訂充分的程序，以防止因盜竊、欺詐及其他不誠實行為、專業上的失當行為或不作為而引致的損失；(b)實施防範措施以避免出現欺詐性要求或在威迫下作出的要求，以及設有監控措施以防止一名或多於一名高級人員或僱員將資產轉移至客戶指定錢包地址以外的錢包地址；及(c)在簽署交易及傳送至相關區塊鏈前，不能修改客戶的提取指示的目的地地址。

7. 種子或私人密鑰的產生及保護應在與網絡隔離的冷錢包設備上進行。平台營運者應保持警惕，因為攻擊會在交易生命週期的任何階段出現，並可能導致資產被挪用。客戶資產的安全程度，取決於其最脆弱的地方是否穩妥。

8. 平台營運者應(a)定期進行有關潛在攻擊媒介的全面評估，包括在實施任何重大變更（例如更改流程、系統或獲授權人士）之前進行評估；及(b)在交易流程的各個階段設立多層獨立的數據完整性檢查措施，同時從交易創建到傳送期間提供端對端完整性保護，並確保適當地劃分職責。

9. 平台營運者應實施穩健而有系統的監控措施，以防止冷錢包進行未經授權的交易，並且應採用白名單監控措施，以防止資產被轉移至未經批准的錢包地址。平台營運者應對冷錢包白名單的任何修改或增補，進行嚴格的監控及監督。每筆交易均須進行有系統的驗證，確保只有經授權的交易會獲執行，且不存在任何未經批准或非預期參數。

10. 用於批准交易的設備應屬專用性質，其功能及網路連接均需受到限制，並與通用工作設備隔離，以降低遭入侵的風險。平台營運者應使用存放於冷庫且與網絡隔離的設備，對關鍵交易數據進行完整性檢查。該等設備需透過實體接觸方可修改程式碼，以確保數據完整性的驗證流程的可靠性。

11. 當交易在簽署前需經人手檢查時，所有交易細節都應以清晰且易於解讀的格式顯示，以便簽署人在簽署前審閱相關資料。

良好作業方式
(a) A 公司實施了一套冷錢包系統，當中包含與網絡隔離的 HSM 及在冷錢包保管庫內受保護的簽署終端機。 • 該區實施嚴格的多重因素接達監控系統，所有進出紀錄均獲保存。保管庫設置監控鏡頭，持續地進行監察及錄影。該等嚴格的實體監控措施將簽署終端機可能遭入侵的風險降至最低，從而增強對該終端機執行的監控措施的穩健性的信心。 • 在簽署前，簽署終端機會向簽署人顯示完整的交易細節，防止盲目簽署[5]的情況及降低內部攻擊風險，從而防範可能涉及替換有待簽署的交易或加入隱藏的惡意參數的行為。如顯示的交易與擬進行的交易細節不符，簽署終端機將中止流程，並透過屏幕通知向簽署人發出警示。

[5] 盲目簽署指在未經審查交易內容的情況下批准或簽署交易的行為。 由於此舉會增加出錯的風險，故被認為是交易管理中的不良作業方式。

- 簽署終端機實施有系統的白名單監控措施，旨在於交易創建期間，防範可能竄改目的地地址的外部與內部威脅。就每筆交易而言，該終端機會將目的地地址與白名單進行核對。如白名單上並無目的地地址，簽署終端機將中止操作並通知保安團隊。

(b) B 公司使用專為覆核及批准交易而設的硬件設備。這些設備只會應用於錢包操作，確保與批准人的日常活動作出明確的物理分隔。

(c) C 公司實施了傳送前的最後階段數據驗證檢查，作為多一重的端到端驗證措施。在傳送已簽署的區塊鏈交易前，該系統會執行驗證流程，將已簽署的交易與原本未簽署的交易進行比較。如發現有任何差異，已簽署的交易將不獲傳送。

IV. 使用錢包解決方案及第三方服務提供者

12. 根據該指引第12.8及12.10段，平台營運者應確保系統的任何改動（例如實施新的系統或將現有系統升級）在部署前均經過測試。平台營運者亦應確保定期對其平台進行檢視，以維持其完整性、可靠性、安全性和容量，及設有穩健的應變措施。

13. 根據該指引第12.6段，如平台或與其相關的任何活動是由第三方服務提供者提供或被外判予第三方服務提供者，平台營運者便應作出適當的盡職審查、持續的監察及適當的安排，以確保平台營運者符合該指引的規定。

14. 平台營運者必須對錢包系統程式碼的管理嚴格地執行職責劃分及全面監察機制，不論程式碼庫是由內部開發抑或外部提供的。該等監控措施包含了程式碼審查、測試、軟件供應鏈管理、管理層的批准及安全部署手法等把關程序，降低外部攻擊者或惡意開發者植入惡意程式碼的風險。所有程序均應透過審計追蹤方式記錄在案。管理員在接達編製系統時（不論是作部署或升級用途）亦須按照最小權限原則、權限分隔原則及獲認可的業界最佳作業手法，受到嚴格管控。

15. 第三方評估應包含獨立的程式碼審查，以及在建立業務關係或實施重大變更前，全面了解提供者的軟件開發和發布流程。有關評估可確保規程的穩健性，以防止被植入惡意程式碼或出現保安漏洞。

16. 如使用第三方錢包解決方案，除了在採用前對提供者進行適當的盡職審查[6]外，平台營運者亦應對提供者進行持續審查，確保完全符合該指引的規定。持續審查包括定期評估提供者的保安監控措施和營運流程，要求及時匯報事故和新冒起的風險，以及定期測試提供者的災難復原能力。平台營運者應定期進行固有風險評估，當中涵蓋第三方依賴關係和漏洞管理，並應實施緩解措施以降低剩餘風險。根據該指引第12.13段，平台營運者亦應定期對已部署的系統進行獨立的網絡保安評估。

17. 作為一項持續實施的措施，平台營運者應就處理緊急情況和業務延續計劃的情境制訂程序，並進行演練。平台營運者應與第三方解決方案提供者定期進行端到端演習，以確保業務延續計劃符合證監會設立的復原時間目標。

[6] 盡職審查應包括評估該提供者是否具備穩健的業務延續計劃及定期進行災難復原能力測試。

V. 持續進行實時威脅監控

18. 根據該指引第 12.12(f)和 12.14 段，平台營運者應：(a)對平台的基礎設施實施足夠的保安監控措施，包括建立保安運作中心（Security Operations Centre，簡稱 SOC）或具有足夠資源的同等職能，負責所有保安監察程序及技術，並擔當協調人的角色，以有效地進行有關事故的偵測工作；及(b)訂立書面政策及程序，訂明懷疑或確實的網絡保安事故應以何種方式上報。

19. 平台營運者應將鏈上客戶資產與分類帳餘額進行實時對帳。如任何非預期交易導致出現差異，平台營運者應立即通知 SOC 或具備同等職能的監控團隊，並與相關團隊合作採取適當的措施。

20. SOC 應與錢包管理、營運及技術等領域的網域專家密切合作，定期評估並完善警報及其參數。高級管理層應監察該流程，確保有效地校正警報門檻，以便及時偵測潛在問題。

21. 平台營運者應建立穩健的機制，以偵測未經授權而接達或入侵關鍵錢包基礎設施的情況，當中包括冷錢包保管庫、簽署設備、數據庫、生產環境軟件及程式碼庫。

22. 鑑於託管系統在本質上既複雜而重要，平台營運者的監控流程應涵蓋託管系統及其依賴關係，包括供應商、技術、區塊鏈規程、加密程式及可能影響客戶資產安全的常用函式庫。

23. 監控框架應涵蓋對重大行業事故及公開保安漏洞的考量，而它們可能威脅託管系統和相關組件的穩健性。

24. 鑑於虛擬資產平台和區塊鏈活動是無間斷地運作的，平台營運者應全天候進行保安監控，包括在假日期間。平台營運者應分配充足資源以應對突發問題，並制訂程序，以調配額外資源處理在正常營業時間以外發生的事故。

25. 平台營運者應制訂有系統的架構，按嚴重程度處理保安警報和應對事故，並分配相應的對策規程。

良好作業方式
一些公司實施了有效的全天候監控功能，能夠在某宗行業事故於社交媒體出現後立即識別出來，即使當時是香港的午夜時分。雖然該事故沒有直接影響該公司的託管系統，但其嚴重性足以令保安團隊立即將此事上報至高級管理層。一支由合適的專業人士、高級管理層、技術和保安人員組成的應對團隊迅速成立，除了全面評估其可能對本身託管系統所帶來的影響外，還密切監察該行業事故的事態發展。

VI. 培訓與意識

26. 根據該指引第 12.5 段，平台營運者需為平台的設計、開發、部署、運作及改動調配具備足夠資格的職員，以及充足的專業知識、技術資源和財政支援。此外，《內部監控指引》第 III(3)段訂明，管理層應確保職員獲提供充分的入職及持續培訓，以配合職員執行特定職責。

27. 平台營運者尤其應確保交易簽署人接受全面培訓，以充分了解驗證規定，以及在交易出現任何例外或不確定情況時的適當處理程序。

28. 平台營運者應採取穩健的措施，以防止盲目簽署的情況，並確保有效地以人手方式審查或批准交易。

良好作業方式
除了定期的保安意識培訓外，C 公司還為員工提供有關交易驗證的培訓，特別聚焦於防止在以人手方式驗證時出錯的程序。 由於大多數網絡攻擊都是來自社交工程攻擊手法，尤其是釣魚攻擊，故 B 公司每月為全體員工進行釣魚攻擊模擬演習，以強調保安的重要性。

未來路向

本通函所列明的規定即時生效。平台營運者應對其虛擬資產託管框架、程序及監控措施進行嚴格評估，以確保符合預期應達到的標準。平台營運者對有關規定的遵守情況，應成為其年度外部合規及技術評估的一部分。

如對本通函有任何疑問，請聯絡你的個案主任。

證券及期貨事務監察委員會
中介機構部

完

SFO/IS/025/2025