

資產管理政策

最新修訂日期：2025/06/16

第一條 依據與目的

- 一、本政策依據《虛擬資產平台及交易業務事業指導原則》第九點第四款、《提供虛擬資產服務之事業或人員洗錢防制登記辦法》第二十六條與《中華民國虛擬通貨商業同業公會會員自律公約》第十條及第十一條訂之。
- 二、為加強本公司（下稱『交易所』）虛擬資產管理，有效控管客戶資產存放風險，以確保清償能力，降低客戶資產因損失、失竊或無法使用而導致的風險，並確保保管程序的透明度與合規性，維護客戶權益，特訂定本政策。

第二條 範圍

- 一、本辦法適用於交易所內所有與用戶資產保管相關的業務操作，包含虛擬資產的保管、虛擬資產的移轉以及虛擬資產錢包管理。
- 二、本政策所規範之虛擬資產，專指交易所客戶存放於本公司冷熱錢包或第三方託管錢包之虛擬資產，不包含本公司自有之虛擬資產。

第三條 名詞定義

- 一、必要調度行為：交易所基於營運需求或風險管理，對內部或外部錢包進行資金調度的行為。這些調度可能包括但不限於：
 - (一) 熱錢包與冷錢包之間的資金調度：交易所為了安全性與符合法規要求，通常會將大部分資產存放於冷錢包，而將小部分資產存放於熱錢包，以應對用戶的提幣需求。
 - (二) 不同區塊鏈網絡間的跨鏈調度：當交易所支持多鏈資產時，可能需要在不同網絡間轉移資產，以確保流動性充足。
 - (三) 風險控制調度：當交易所發現某些地址可能面臨風險（如黑客攻擊、監管問題等），可能會進行緊急資金轉移，以保護用戶資產安全。
- 二、歸集行為：交易所為了提高資產管理效率，將分散在多個錢包地址或用戶充值地址的資金，統一歸集至特定的管理錢包（如熱提錢包或冷錢包）的行為。

第四條 權責單位

由營運部擔任虛擬資產管理的專責部門，並由執行長擔任虛擬資產管理的最高主管。

第五條 資產安全防護政策

- 一、交易所透過第三方虛擬資產託管錢包來保管交易所客戶存放的虛擬資產。
- 二、第三方虛擬資產託管錢包依其功能又可區分為「熱充錢包」、「熱提錢包」、「冷錢包」，詳細說明參下表：

錢包種類	功能
熱充錢包	交易所分配予個別客戶獨立的區塊鏈入幣地址，專門用於接收用戶充值的熱錢包，其主要功能是将用戶充值的虛擬資產快速入帳至用戶的交易所帳戶。
熱提錢包	用於處理用戶提領請求的熱錢包，須保持一定數量的虛擬資產餘額，以應付每日的提領需求。

冷錢包	指用戶所擁有之未連結網路之錢包或私鑰為離線保管之錢包。
-----	-----------------------------

(一) 虛擬資產分離與例外：

1. 用戶虛擬資產與交易所自有資產應在帳戶、技術及操作層面完全分離，不得與客戶約定與交易所自有資產混合保管，防止資金混用及濫用風險。
2. 用戶虛擬資產均須在專屬錢包中存放。
3. 本公司就其保管之客戶虛擬資產，不得與客戶約定所有權移轉於本公司。
4. 前項約定例外得混和保管之條件以《中華民國虛擬通貨商業同業公會會員自律公約》等相關規定為限。

(二) 技術安全措施：

1. 採用多層防護機制，包括防火牆、入侵偵測系統及多因子驗證，以減少網絡攻擊風險。
2. 冷錢包應完全離線運行，並使用硬體安全模組（HSM）存儲私鑰，避免私鑰外洩。

(三) 操作安全規範：

1. 所有涉及資產操作的關鍵流程均須多重授權及多重簽名機制。
2. 定期進行資產對帳，確保記錄與實際持有資產一致。

三、法幣資產分離：

- (一) 交易所應將用戶之法幣資產與其自有之法幣分離保管，並交付信託或取得銀行十足之履約保證，除為其客戶辦理前項業務外，不得動用客戶之法定貨幣資產。
- (二) 交易所得依業務需求辦理虛擬資產交易所涉法定貨幣之收付，經客戶同意將客戶之法定貨幣留存於其於金融機構開立之相同幣別存款專戶。

第六條 用戶資產損失、失竊或無法使用風險之防免政策及程序

一、風險辨識與預防措施

- (一) 交易所應定期評估客戶資產所面臨之風險類型，包括但不限於資安攻擊、內部操作錯誤、系統異常、法規變動或第三方服務中斷等，詳參附錄客戶資產風險等級表。
- (二) 應持續檢視冷錢包與熱提錢包資產配置比例與提領頻率，確保可提流動性與長期安全性平衡。
- (三) 採行分層簽章、多重權限設計及錢包白名單等控管措施，避免因人為失誤或內部舞弊導致資產風險。

二、即時異常監控與通報機制

- (一) 若出現客戶資產異常（包括但不限於餘額不符、可疑轉出、私鑰存取紀錄異常等情形），應即時由風險控制部、營運部與資安部啟動系統鎖定機制，凍結相關錢包與交易權限。
- (二) 重大異常事件應於事件發現後6小時內由法令遵循處初步通報執行長，並於通報執行長後24小時內依主管機關規定進行公告與正式通報，包括但不限於初步調查結論、風險程度與處理計畫。
- (三) 交易所應保留異常監控之系統紀錄至少五年以上，供內部稽核與主管機關查核。

三、損失事件處理與補償原則

- (一) 對於可歸責於交易所之客戶資產損失（例如未經授權之轉出、冷錢包洩漏），應依據事件性質，啟動以下補救機制之一：
 - 1. 以同幣種或等值虛擬資產進行全額或部份賠償；
 - 2. 其他合於用戶保障與法規要求之處理方式。
- (二) 所有補償處理應由法令遵循處提報補償建議書，並經執行長核可後執行；必要時應提報董事（會）。

四、例外情境處理與客戶溝通機制

- (一) 如屬不可歸責於交易所之事件（如鏈上系統錯誤、用戶自行洩密私鑰），交易所仍應提供初步協助（如鏈上追蹤、保全證據、法律諮詢等）。
- (二) 用戶如因資產不可提領超過 48 小時，應由客服單位每日提供溝通進度，並在合理範圍內提供用戶資訊查詢權限與索償建議。

五、演練與稽核

- (一) 每年至少進行一次全所級別的資產異常事件應變演練，模擬資產失竊、系統中斷或資安入侵等場景，並檢討改進計畫。
- (二) 稽核部應每月就熱提錢包餘額異動、異常通報處理與補償流程等項目執行查核，並留存查核紀錄至少五年。

六、通報義務

本公司倘發生可能嚴重影響客戶權益之虛擬資產異常事件、資安事件或系統無法使用情形，應依主管機關之公告義務即時進行通報及公告，不得以內部流程為免責事由。

第七條 冷熱錢包部位比例

- 一、用戶虛擬資產應至少 80% 存放於冷錢包，以降低網路攻擊風險；餘下 20% 存放於熱提錢包，用於日常交易流動性需求。
- 二、交易所應定期檢視熱錢包餘額，並至少每週就上述比例進行乙次確認並就熱提錢包之超額資產轉入至冷錢包進行儲放。

第八條 虛擬資產錢包管理

- 一、冷錢包操作：
 - (一) 冷錢包操作應在物理隔離環境下進行，如無網路連接的安全設施中操作。
 - (二) 涉及冷錢包的資產轉移須經多重簽名程序，且須由至少三名授權人員共同操作。
- 二、熱錢包操作：
 - (一) 熱錢包資產應每日核對餘額，確保交易流動性需求充足但不過量暴露風險。
 - (二) 熱錢包私鑰應存放於硬體安全模組（HSM）或採用多方計算（MPC）技術進行保護。
- 三、第三方託管錢包系統由執行長、營運處主管以及營運部主管各自擁有獨立權限，權限內容如下表所列：

執行行為	可發起人	審核
------	------	----

熱充錢包轉熱提錢包	營運部主管設定參數後由系統自動執行。	初次設定之參數需經營運處主管與執行長覆核同意，後續異動亦同。
熱充錢包轉冷錢包	營運部主管設定參數後由系統自動執行。	初次設定之參數需經營運處主管與執行長覆核同意，後續異動亦同。
熱提錢包轉冷錢包	營運部主管	營運處主管
冷錢包轉熱提錢包	營運處主管	執行長

四、營運部應盤點交易所全數託管錢包，並賦予錢包固定用途，不得有除例外規定之混用或任意變更錢包用途之情形。上述盤點紀錄應以書面為之，並提交營運處主管與執行長審核後留存備查。

五、前項規定，於託管錢包增加或刪減時亦有其適用。

第九條 私鑰管理規範

詳參《私鑰管理與使用規範》之規定。

第十條 虛擬資產之移轉

- 一、除為維持交易所營運所需之必要調度或歸集行為，或依客戶之指示處分客戶之資產、抵銷客戶對其之費用債務或其他主管機關許可之事由外，交易所不得移轉或使用客戶存放於交易所託管錢包內之資產。
- 二、基於託管錢包系統限制，交易所於託管錢包間進行虛擬資產移轉僅能移轉至系統內所核可的白名單錢包地址，白名單地址的新增或刪減，應由營運處主管、執行長以及營運部主管三組錢包系統權限以相對多數決議後始得為之。
- 三、客戶若於交易所使用或購入本公司之虛擬資產理財產品，則不受第一項之限制。

第十一條 虛擬資產移轉之流程

本公司應依據下列作業流程，進行熱充錢包轉熱提錢包、熱充錢包轉冷錢包、冷錢包轉熱提錢包、熱提錢包轉冷錢包間虛擬資產之移轉：

- 一、熱充錢包轉熱提錢包：
 - (一) 系統設置歸集參數：應由營運部主管設定適當的歸集條件，就各幣別設定單筆與每日累計移轉限額、地址白名單機制及自動偵測異常交易功能。初次設定之參數需經營運處主管與執行長覆核同意，後續異動亦同。
 - (二) 操作單位：由營運部就各幣別事先設定歸集條件，由系統自動執行熱充錢包至熱提錢包之移轉操作，並依內部規範進行紀錄與監控，並確保交易資訊完整記錄，供風險控制部內部監控及法遵暨法務部與稽核部查核。
- 二、熱充錢包轉冷錢包：同前項之作業流程。
- 三、熱提錢包轉冷錢包：
 - (一) 系統設置參數：應設定熱提錢包之留存比例之最高上限，確保符合本政策第六條之規範。
 - (二) 操作單位：營運部人員應至少每週確認熱提錢包之留存比例，並由營運部主管負責執行熱提錢包至冷錢包之第一層移轉操作，並留存相關確認與移轉紀錄。

- (三) 放行簽核：前款之最終移轉需由營運處主管進行簽核放行；留存比例確認則需經由執行長簽核確認，以確保符合本政策第六條所規定之標準。
- (四) 紀錄留存：相關核准放行紀錄須完整留存，以供風險控制部內部監控及法遵暨法務部與稽核部查核。

四、冷錢包轉熱提錢包：

- (一) 系統設置參數：應設定熱提錢包之留存比例之最低水位，在符合本政策第六條規範之前提下確保交易所之流動性不受影響。
- (二) 操作單位：營運部應適時監控熱提錢包留存比例之最低水位，並由營運處主管負責執行冷錢包至熱提錢包之第一層移轉操作，並留存相關確認與移轉紀錄。
- (三) 放行簽核：前款之最終移轉需經執行長簽核放行。
- (四) 紀錄留存：經執行長核准後，相關核准放行紀錄須完整留存，以供風險控制部內部監控及法遵暨法務部與稽核部查核。

第十二條 客戶資產權益事件處理原則

一、透明性與即時性：

涉及客戶資產權益的重大事件（包括但不限於交易失敗、資產遺失）應於一個工作日內即時以書面或電話聯繫之方式通知相關用戶，並提供處理進度更新。

二、權益保障：

在事件處理期間，用戶資產應受到充分保障，任何可歸責於交易所之損失須以幣本位之計算方式採取賠償措施。

第十三條 客戶資產權益事件處理程序

一、事件分類：

- (一) 根據事件性質（包括但不限於資產操作失敗、資產異常）分為「一般事件」與「重大事件」處理。
- (二) 重大事件因於事件發生後當日起算三個工作日內上報董事（會）及相關監管機構。

二、調查與補救：

- (一) 啟動內部調查，確定事件原因與責任歸屬，並根據調查結果提供補救措施。
- (二) 補救措施應包括損失資產的追償、補償方案或其他替代處理方式。

三、報告與記錄

(一) 內部報告：

每次事件處理完成後，應向董事（會）提交完整報告，包括事件原因、處理過程與後續改進建議。

(二) 外部報告：

根據監管要求，向相關機關提交事件處理報告，並配合後續調查需求。

第十四條 稽核與更新

一、內部稽核：

每月對冷熱錢包管理、私鑰保管與資產異常處理進行稽核，確保符合內控要求。

二、外部稽核：

本公司就所保管之客戶資產，應設置定期性與經常性之對帳措施，且至少每年委任會計師出具報告並公告。

三、政策更新：

本辦法應每年至少修訂一次，或根據監管要求及實務需求進行調整。

第十五條 紀錄保存

- 一、交易所應確保就所有保管之客戶資產，應確實記錄個別客戶之姓名、錢包地址、資產金額、數量與轉入及轉出等處分情形，並留存且提供客戶相關鏈上紀錄，以便查詢，除其他法律另有規定外，紀錄之保存年限應至少五年以上；倘遇有爭議者應保存至爭議消除為止。
- 二、交易所應至少每日檢核客戶帳上虛擬資產與託管錢包內虛擬資產數量，並確保託管用戶資產之錢包內虛擬資產扣除本公司自有虛擬資產後須大於等於客戶帳上虛擬資產總和，並由稽核部將上述檢核紀錄提交執行長審核後留存備查。
- 三、交易所應至少每日檢核客戶之法幣數額以及所有客戶之法幣總額，並由稽核部將上述檢核紀錄提交執行長審核後留存備查。

第十六條 生效日期

本辦法自 2025/02/18 起生效，由法令遵循處負責解釋與執行。

附錄一：客戶資產風險等級表

風險等級	定義	常見情境	對應應變處理措施
等級一（重大風險）	高度可能造成用戶資產無法提領、交易全面中止或大規模損失。	- 錢包系統遭入侵且資產已被轉出 - 冷錢包私鑰外洩 - 鏈上大規模異常或智能合約漏洞被利用	- 即時凍結錢包操作權限 - 於內部通報後24小時內通報主管機關全體客戶 - 啟動補償與事後復原機制
等級二（中度風險）	對部分用戶造成資產異常、資金延遲提領或交易行為異常。	- 熱提錢包提領量異常 - 客戶資產餘額短暫不符帳 - 系統升級或轉帳誤操作	- 限縮提領與轉帳功能 - 啟動內部資安調查程序 48小時內完成初步處置與公告進度
等級三（一般風險）	對個別客戶帳務造成暫時性影響，未產生實質損失。	- 個別地址提領延誤 - 系統顯示錯誤未影響實際資產 - 資產追蹤中但尚未發生轉出風險	- 客服即時回報與進度追蹤 - 內部通報並追蹤改善紀錄 - 不需對外公告
等級四（潛在風險）	尚未產生實質影響但具警訊性或重複發生之潛在操作/系統弱點	- 用戶多次誤觸資產操作流程 - API 接口異常觸發錯誤訊息 - 資安監控偵測異常登入行為	- 通知營運與資安單位追蹤 - 建議列入內稽稽核範圍 - 納入月報與改善追蹤