

優答台灣股份有限公司

私鑰生命週期管理要點

第壹章、私鑰之生成、使用及銷毀

第一條 私鑰之生成

本公司就所提供之服務，應個別訂有私鑰生成程序；各該服務之私鑰生成，應依各該生成程序進行。

第二條 私鑰使用之管理

本公司對於私鑰使用之管理規範如下：

- (一) 私鑰使用環境：私鑰僅得於本公司指定之隔離空間下使用。
- (二) 私鑰管理員的適合性確認：本公司將定期對私鑰管理員進行查核。
- (三) 簽名前對交易內容之覆核：有權限人員於進行簽名前，應就所涉及之交易，對其交易發起時間、目標地址、幣種與額度、目標地址之風險等級等相關資料進行審查並留存紀錄。所有交易簽名均應依據既定之授權政策執行，確保多層級控管。

第三條 本公司端私鑰之銷毀

- 一、私鑰銷毀共用通則：任何私鑰或其載具銷毀作業，均須建立「銷毀紀錄表」。
- 二、有下列情形之一者，本公司應辦理本公司端私鑰之撤銷及銷毀作業：
 - (一) 私鑰發生洩漏、疑似洩漏、遭未授權存取或有其他安全疑慮之情形。
 - (二) 私鑰之原使用目的已不達，或因業務調整、系統變更或其他原因而無繼續使用之必要。

(三) 本公司與客戶間之契約關係已終止，且已完成相關必要處置程序。

三、私鑰經撤銷及銷毀後，不得再用於存取、控制、管理或簽署任何客戶之虛擬資產交易。

第貳章、本公司端私鑰洩漏之處理流程

第四條 權責單位

部門	主要負責人	次要負責人(於主要負責人無法執行 KCP 時，作為補充性的負責人)
產品及服務營運部門	產品及服務營運部門人員	產品及服務營運部門主管
技術研發部門	技術研發人員	技術研發部門主管
法令遵循部門	法令遵循部門主管	總經理
客戶支援人員	產品及服務營運部門指定人員	技術研發部門主管
資訊安全部門	資訊安全人員	資訊安全部門主管

第五條 私鑰洩露協定基本規則

每當以下情境，資訊安全部門、產品及服務營運部門評估本公司所負責保管之私鑰已經或可能遭洩露時，應啟動私鑰洩露協定(Key Compromise Protocol，下稱「KCP」)程序。

(一) 發現置於備援私鑰上的防拆封條、存放於 Crypto Capsule 的復原種子片語，以及存放於 Crypto Zeus 的復原種子片語遭到竄改。

- (二) 發現客戶錢包出現未經授權的交易。
- (三) 本公司實體備援裝置遭竊取或損毀。
- (四) 本公司端私鑰操作者明顯失蹤，且其最親近的親友皆無法確認其行蹤；於向當地警方報案後即可啟動 KCP。
- (五) 本公司端私鑰本身所使用裝置遭洩露。
- (六) 收到可信地顯示私鑰可能面臨洩露風險的通知。
- (七) 其他本公司端私鑰疑似洩露之情境。

第六條 因本公司端私鑰洩漏所致虛擬資產遺失時之處理原則

一、受影響虛擬資產的復原流程：

- (一) 本公司於知悉虛擬資產受影響情形後，立即將受影響錢包與其他未受影響的錢包基礎設施區隔分離。
- (二) 本公司將依客戶指示將可復原虛擬資產移轉至採用全新私鑰的安全錢包。
- (三) 本公司將與區塊鏈分析供應商協調，即時追蹤遭洩露或遭竊之虛擬資產。

二、即時與受影響之客戶及利害關係人溝通：

- (一) 於確認本公司端私鑰洩漏，或因而造成重大風險後 24 小時內，通知受影響客戶及利害關係人。
- (二) 本公司秉持透明溝通原則，將指派專責人員，作為所有受影響客戶的單一聯絡窗口。

三、與執法機關及監理機關合作：

- (一) 於規定時限內向主管機關通報。
- (二) 全面配合當地及國際執法機構，包括提交可疑交易報告、稽核日誌及技術鑑識。

(三) 透過鏈上分析工具，將位址列入黑名單。

第參章、附則

第七條 核決層級

本要點經提報總經理核准後實施，修正時亦同。

版本修訂紀錄表

版次	修訂日期	修訂內容
1.0	2026.6.24	新制定