中華民國虛擬通貨商業同業公會
資訊安全自律規範

中華民國虛擬通貨商業同業公會113年11月22日理監事聯席會議表決通過
金融監督管理委員會113年12月23日金管證券字第1130365997號函准予備查

第一章 總則

第一條（規範目的）
為強化會員網路及資通系統安全防護，並確保客戶資料與虛擬資產之機密性與安全性，依本會自律公約第十條特訂定本自律規範（下稱本規範）。

第二條 （定義）
本規範之用詞定義如下：
一、資通系統：係指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。
二、資通服務：係指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。
三、存取：係指存取資訊資產的各種方式，包含取得、使用、保管、查詢、修改、調整、銷毀等。
四、網路設備：係指傳輸資料、應用程式、服務和多媒體所需的網路通訊元件，如防火牆、路由器、交換器等。
五、核心系統：係指直接提供客戶虛擬資產服務或支持虛擬資產業務持續運作之必要系統（如交易系統、報價系統、帳務系統等維持交易業務之必要系統）。
六、資訊資產：係指與資訊處理相關之資產，包括硬體、軟體、資料及文件等。
七、行動裝置：一種具有資料運算處理、儲存與網路連線功能之可攜式設備，包括但不限於智慧型手機、筆記型電腦、平板電腦與 PDA 等裝置，惟本規範定義之行動裝置僅限可用於處理組織內部定義之敏感性事務且可直接連接組織網路設備、服務之行動裝置。
八、物聯網設備：指具網路連線功能之嵌入式系統設備及其周邊連網之裝置(如：感測器)。
九、深度偽造(Deepfake)：指使用電腦合成或其他科技方法製作或散布涉及真實人物實際未發生的行為舉止影像紀錄、動態圖像、錄音、電子圖像、照片及任何言語或行為等技術表現形式。

第二章 資通系統安全管理

第三條 （風險評鑑與管理）
會員應依公司業務需求，考量所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，進行適當之資訊資產風險鑑別及風險管理。

第四條 （資訊安全管理政策）
會員應依據相關法令規定及公司業務需求，考量所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，建立適當之資訊安全管理政策。

會員所訂定之資訊安全政策，應經管理階層核准，並應正式發布要求所有員工共同遵守。
會員就資訊安全政策應定期審查，以反映法令規章、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。
會員就資訊安全管理政策，應充分公告揭露於會員網站。
提供虛擬資產交易平台或虛擬資產保管商服務之會員應依其所營事業規模與性質辦理核心系統導入資訊安全管理系統，並通過公正第三方之驗證，且持續維持驗證有效性。

第五條（安全組織設立）
為確實辦理資訊安全管理事宜，會員應訂定相關人員之工作職掌與兼辦業務情形之規定，並應依規定配置適當人力資源及設備執行資訊安全管理作業，資訊處理部門與業務單位之權責，應明確劃分。
會員資訊安全人力、能力及經驗，如有不足之處，得委請外界學者專家或民間專業組織及團體，提供資訊安全顧問諮詢服務。
資訊安全人員應每年召開資訊安全管理審查會議對現有資訊安全管理依實際狀況調整。
重要資訊處理人員應簽署保密協議並定期（至少一年一次）審查保密協議內容，以確認是否重新簽署保密協議。
提供虛擬資產交易平台或虛擬資產保管商服務之會員應視資訊安全管理需要及依其所營事業規模與性質，指定專人或專責單位負責規劃與執行資訊安全工作，且資訊安全人員應取得並維持適當之資通安全專業證照，且每年應定期參加十五小時以上資訊安全專業課程訓練或職能訓練並通過評量。其他使用資訊系統之從業人員，每年應至少接受一小時以上資訊安全宣導課程。

第六條（資產分類與控制）
會員之資訊資產應列有清冊，清冊並應加以維護。
各類資訊資產之異動應由資訊資產保管者向資訊資產權責單位主管申請核准。
會員資訊資產權責單位應對資料類型之資訊資產其敏感程度，並依其敏感程度訂定資料保護措施並執行。
會員應對資訊資產之資料與文件的保存期限進行規範，並於保存期限到期後進行刪除與銷毀。

第七條（人員安全）
員工應依相關法令課予機密維護責任，並應填具保密切結書，以明責任。
會員應對異動之人員調整其資訊資產存取及使用權限。
會員應定期對全公司員工辦理資訊安全宣導講習（例如：資訊安全政策、資訊安全法令規定、資訊安全作業程序以及如何正確使用資訊科技設施等），並留存紀錄。
會員員工每年應依職務層級接受適當之資訊安全與個資保護教育訓練。

第八條（實體與環境安全）
會員應依其所營事業規模與性質制定實體與環境安全管理政策，以確保相關資訊設施之安全：

一、會員如於其營業處所有設置電腦機房者，應界定電腦機房為重要管制區域，其管理辦法應包含以下要點：

(一)機房應有門禁管制措施，並定期審查資訊機房門禁管制權限。

(二)機房應有防火設施，並應定期檢驗。

(三)會員應將地震、水災等天然災害因素列入考量。

(四)機房內各項作業情形，應設置工作日誌記錄，且應保留至少六個月。

二、制定一般設備安全管理辦法，其管理辦法應包含以下要點：

(一)辦公室應有管制措施（如門禁系統）並配備監控錄影設備，不具權限之人員不得進出。

(二)可攜式設備之使用分配應受權責主管核准後始得配發，並記錄其各項設備之保管人，及建立相關遺失通報程序。

(三)訂定設備報廢作業程序，資訊資產權責單位應確實依設備報廢作業程序移除機敏性資料後，方可進行報廢該設備。

第九條　（網路安全管理）

會員應依其所營事業規模與性質就網路系統、網路設備、網路連線及資料傳輸等網路安全事項，制定網路安全管理政策，並依風險基礎建立適當之管理機制，其中應包含以下要點：

一、網路系統安全：

(一)定期評估公司網路系統安全，並留存相關紀錄。

(二)定期或適時修補網路運作環境及作業系統之安全漏洞，並留存相關文件。

(三)各電腦主機、重要軟硬體設備應有專人負責。

(四)若為租用之公有雲端服務時應評估服務供應商對多重租戶間網路區隔管理是否符合公司日常作業以及為提供服務之需求。

(五)有關電腦網路安全（如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等）之事項應隨時對內部公告。

二、網路連線管理：

(一)應有適當網路之區隔機制，於網路控制措施制定網路存取控制列表，定期檢視防火牆規則或存取控制清單，並留存相關維護紀錄，由權責主管定期覆核。

(二)訂定遠端連線管理辦法，並進行適當防護措施，及留存相關紀錄。

三、網路設備之安全管理：

(一)應建立防火牆，並應由網路管理人員執行控管且定期檢視防火牆規則是否允當。

(二)防火牆系統之設定應經權責主管之核准，並保留相關紀錄備查。

(三)應每年定期檢視並維護防火牆存取控管設定，定期檢視 DMZ 區之防火牆規則，並留存相關檢視紀錄。

(四)應至少每年檢視一次對外網路設備規則，並留存相關紀錄。

四、網路傳輸管理：

(一)公司提供網路下單服務，應於網路下單登入時採多因子認證方式，以確保為客戶本人登入。

(二)會員及其人員利用網路傳送機密資訊，應將資料加密保護，以保護資料於公眾網路傳輸之完整性及機密。

第十條（資通系統存取控制）

會員應依其所營事業規模與性質建置與所營事業規模與性質相符之穩定與安全之資訊系統，訂定資訊系統存取控制相關規定，並以書面、電子或其他方式告知員工遵守。

會員應就各項資訊系統之權限、密碼規則、資料輸入及輸出等存取控制事項，建立適當之管理機制，並應至少包含以下要點：

一、一般權限及特權帳號管理：

（一）制定帳號之申請、建立、修改、啟用、停用及刪除之程序。

（二）定期審查資通系統帳號及權限之適切性，並視審查結果停用資通系統閒置帳號。

（三）定義人員角色及責任，授權應採最小權限原則，僅允許使用者(或代表使用者行為之程序)依公司部門權責及業務功能，完成作業所需之授權存取，且授權及審查記錄應留存。

二、密碼管理：

(一)使用者密碼於首次使用後應進行更改，使用者更改之密碼應符合密碼原則，系統預設之初始密碼應被停用或刪除。如初次設定密碼為使用者自行設置者，則不在此限。

(二)密碼變更時，系統應對該使用者之身分進行驗證。

(三)系統於有帳號登入異常情事時應通知相關權責單位，相關權責單位應即時了解異常原因，並留存處理紀錄。

第十一條（系統開發及維護）

自行開發或維護系統之會員應依其所營事業規模與性質建置與所營事業規模與性質相符之系統開發及資訊系統維護辦法，建立適當之管理機制，並應至少包含以下要點：

一、應用系統在規劃分析時應將資訊安全需求納入分析及規格，並應經申請單位主管核准。

二、系統開發人員應對經核准之系統開發需求申請進行可行性評估，並確認符合公司資訊安全制度。

三、應定期辦理資訊系統弱點掃描作業，針對所辨識出之潛在系統弱點，應評估其相關風險或安裝修補程式，並留存紀錄。

四、程式原始碼安全規範。

第十二條（營運持續性）

會員應就其營運之持續性，訂定相關之政策及程序，該政策及程序，應至少包括以下內容：

一、應明確訂定（例如：電腦設備、通訊設備、電力系統、資料庫、電腦作業系統等備援及回復計畫）故障復原程序，並落實執行且留存紀錄，及應包含：

(一)核心系統程式原始碼與資料備份之執行程序。

(二)核心系統從中斷後至重新恢復服務之可容忍時間要求。

(三)核心系統原服務中斷後之備援回復程序。

(四)針對重大資訊系統異常事件或天然災害之應變、備援及回復程序。

二、對故障復原程序應週期性測試，測試後應召開檢討會議，針對測試缺失謀求改進，並留存紀錄。
三、資訊安全管理單位應訂定營運持續計畫。
四、會員應訂定資通安全事件內部通報機制，包含正式之通報程序及資通安全事件通報聯絡人。
五、會員於發生影響客戶權益或正常營運之資訊服務異常事件或資通安全事件應採取適當應變程序及留存紀錄。
非提供虛擬資產交易平台或虛擬資產保管商服務之會員得僅就客戶個人資料訂定營運之持續性相關政策及程序。

第十三條（資通系統或資通服務委外辦理）
會員將其部分或全部之資通系統或服務，委由第三方辦理者，就服務供應商遴選及監督等管理事項建立適當之機制，其要點應包含：
一、會員與委外資訊服務供應商提供服務應訂定合約，合約所含內容應包含以下內容：合約期限、服務範圍、服務交付日期、服務水準要求、服務變更規範、服務驗收之標準、資通安全事件通報及應變處理作業程序、對資訊服務供應商之稽核權條款、合約轉讓或同意分包之規範、保密義務條款、罰則與損害賠償條款、爭議處理程序、違約處理條款、合約終止規範、合約終止後之處理、保固、權利及責任。
二、應定期檢查委外作業系統之安全性，且資訊服務供應商應提供安全性檢測證明（如程式資安檢測、源碼檢測、弱點掃描等），並應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過程式碼掃描或黑箱測試。
三、公司應訂定相關規範管控，與資訊服務供應商資訊委外關係於終止、解除或結束後之相關作業。
四、應管控資訊服務供應商存取權限，對於電腦通行使用權利進行適當控管。
五、應對委外廠商交付之服務系統檢查其未有植入後門程式等惡意程式，確保系統符合需求後始正式上線運作。
會員如無法符合前項要求，應採取適當評估，並依風險規劃替代措施，以確保會員對委外資訊服務供應商之最終監督義務之執行。

第十四條（新興科技應用）
會員應事先評估使用雲端運算服務之風險，若雲端運算服務涉及關鍵性系統、資料或服務者，應訂定雲端運算服務相關運作安全規範，其內容包含下列項目：
一、為雲端服務使用者時，應訂定雲端服務提供者之遴選機制、查核措施、備援機制、服務水準（含資訊安全防護）、復原時間及服務終止措施要求等，如有不符需求之處，需有其它補償性措施。
二、如公司為雲端服務提供者時，應訂定雲端運算服務安全控管措施，應包含法律遵循、權限控管、權責歸屬及資訊安全防護等項目。如涉及敏感性資料之傳遞，應使用超文字傳輸安全協定（HTTPS）、安全檔案傳輸協定（SFTP）等加密之網路協定。

三、終止雲端服務時資料處置方式，包括但不限於刪除、將資料移回會員資通系統自行處理，或將其移轉至其他雲端服務業者等。
四、應設置一定程序確保終止使用雲端服務時，刪除雲端服務業者留存之資料，並留存刪除或銷毀之紀錄。前述資料包括但不限於客戶之個人資料、電子資料、應用程式及備份資料等。

會員得依據公司內部業務單位性質，訂定公務用行動裝置之申請、使用、更新、繳回與審核等相關資訊安全規範與管理辦法，其內容應包含行動裝置儲存機密資料之限制與管理方式。

會員得依據公司內部業務單位性質，訂定員工自攜行動裝置之資訊安全規範與管理辦法，其內容應包含裝置使用用途、限制內部裝置私接存取網際網路及行動裝置儲存機密資料之限制與管理方式等。

會員應制定物聯網相關資訊安全規範與管理辦法，須包含下列項目：
一、應建立物聯網設備管理清冊並至少每年更新一次。
二、物聯網設備應具備安全性更新機制且定期更新，如存在已知弱點無法更新時，應建立補償性管控機制。
三、應關閉物聯網設備不必要之網路連線及服務，避免使用對外公開的網際網路位置。
四、採購物聯網設備時，宜優先採購取得資安標章之物聯網設備。
五、定期辦理物聯網設備使用及管理人員資安教育訓練。
六、應建立物聯網設備存取權限控管措施。

會員如使用影像視訊方式進行身分驗證時，應強化驗證並搭配其他驗證因子（如上傳身分證件、手機簡訊 OTP）。

第三章 個人資料保護

第十五條（個人資料保護）

會員應針對資通系統所保有之個人資料進行風險評估及控管。

為維護所保有個人資料資通系統之安全，應採取下列資料安全管理措施：
一、訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，應採取防範資料洩漏之適當措施。
二、針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。
三、作業過程有備份個人資料之需要時，對備份資料予以適當保護。

為維護保有個人資料資通系統安全，應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員約定保密義務。

保有個人資料之資通系統應建置留存個人資料使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況。

保有個人資料之資通系統應建立個人資料外洩防護機制，管制個人資料檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁或網路檔案等方式傳輸，並應留存相關紀錄、軌跡及證據。

資通系統如刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：
一、刪除、停止處理或利用之方法、時間。

二、將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

第十六條（個人資料保護法之遵循）
會員應依《個人資料保護法》，妥善處理客戶及公司內部人之個人資料，並遵守下列規定：
一、會員應依《個人資料保護法》妥善處理公司保有之個人資料，並定期或不定期稽核依 《個人資料保護法》定義之個人資料管理情形。
二、前揭個人資料之更新、更正或註銷均應將更新、更正、註銷之內容、作業人員及時間詳實記錄。
會員應留存個人資料使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況。

附則 其他

第十七條 （除外情形）
第十三條之事項，除另有規定外，應於本規範發布施行起一年內實施。

第十八條（適用範圍）
若無明文排除，本規範相關條文於所有類型之會員原則上應一體適用。但業務種類或形態本質上不適用者，不在此限。
本規範之解釋，應考量規範目的及風險控管之實效性。

第十九條（違規處理程序）
會員違反本自律規範，依本公會會員自律公約及其他有關之規定辦理。

第二十條（本規範施行程序）
本規範經本會理事會會議通過，並報請主管機關備查後施行，修正時亦同。