虛擬通貨產業資安標準要點

第一章	**總則**
第一點	本辦法之目的在於規範比特幣及虛擬通貨發展協會（下稱「本會」）團體會員（下稱「會員」）從事虛擬通貨相關業務活動中資訊安全管理的基本準則。 前項所指虛擬通貨相關業務之定義範圍如下： 一、 虛擬通貨與新臺幣、外國貨幣及大陸地區、香港或澳門發行之貨幣間之交換。 二、 虛擬通貨間之交換。 三、 進行虛擬通貨之移轉。 四、 保管、管理虛擬通貨或提供相關管理工具。 五、 參與及提供虛擬通貨發行或銷售之相關金融服務。
第二點	各會員應明確規範資訊安全管理政策和維運資訊安全管理系統。
第二章	**資訊安全管理政策**
第三點	會員應制定資訊安全管理政策，應包含： 一、 資訊安全之定義、目標及範圍，其範圍應包含核心系統（如：交易平台、錢包系統等）。 二、 資訊安全之原則及標準。 三、 資訊安全管理相關工作應設立之組織、該組織之最高負責人及組織職責等。 四、 員工應遵守之相關準則及規定 。 五、 資訊安全之緊急事件通報相關規定及說明。
第四點	資訊安全管理政策應參考相關法令與實際業務執行需求訂定。
第三章	**資訊安全管理組織之建立**
第五點	資訊安全管理政策應明訂資訊安全管理組織之建立、權責及分工，並應指定高階管理人員負責資訊安全管理事項的協調與推動，並成立跨單位之資訊安全推行小組並統籌資訊安全政策、計畫、資源調度等事項。
第四章	**資訊安全管理與維運**
第六點	會員應根據資訊系統安全管理政策訂定相關管理與維運計畫，並定期檢視計畫的有效性。
第七點	會員應針對資訊系統進行獨立地定期或是不定期查核，包含但不限於內部自行查核，並依查核結果進行改善。
第五章	**風險管理**
第八點	資訊安全管理應以風險評估方式進行資訊安全風險管理，並採取有效的控制措施。
第九點	風險管理的標準應包含風險容忍度及資訊風險評估實施標準。
第十點	針對虛擬通貨資產，會員應做成清冊或其他可識別資產之表單，且定期檢視該項目內容是否足以重建公司虛擬通貨資產全貌。 且項目至少應包含以下：

	一、 資產項目。 二、 資產重要性或價值。 三、 資產管理人及負責人。
第十一點	會員應對風險發生之可能性及發生後的結果進行分析，並應採取以下方法處理及對應： 一、 降低： 制定並採取控制措施降低風險。 二、 避免： 停止該業務運作。 三、 接受： 尋求業務委外或外部保險。
第十二點	針對風險應規劃管理政策及執行實施計畫。
第六章	**虛擬通貨資產安全管理**
第十三點	針對虛擬通貨資產，應建立保管、權限控管與額度管理機制。
第十四點	應針對虛擬通貨資產其屬性及組織運作需求規劃熱錢包和冷錢包架構。
第十五點	錢包系統的管理應考量以下控制措施： 一、 系統存取權限管理與控制。 二、 多簽章技術。 三、 分層授權管理。 四、 交易監控。
第十六點	冷錢包系統應離線並妥善保存，並留下相關存取紀錄供查核。
第十七點	錢包系統的虛擬通貨數量應定期進行檢視，減少錢包系統額度過高增加的風險。
第十八點	虛擬通貨於冷/熱錢包的移轉應建立有效的管理流程或機制，並留下相關紀錄供查核。
第七章	**系統開發安全管理**
第十九點	當進行資訊系統開發與強化，應在規劃的需求階段，將安全需求納入考量。
第二十點	資訊系統應保護其機密性，防止洩漏或被竄改，同時應使用加密技術保護。
第二十一點	資訊系統應具備以下安全相關功能： 一、 驗證資料輸入真確性。 二、 驗證內部資料的完整性。 三、 資料在傳輸或儲存過程中以加密方法保護。 四、 利用訊息鑑別技術，檢測資料內容是否遭受未經授權的竄改或破壞。
第二十二點	資訊系統應建立與生產環境分離的測試環境和驗證環境，防止發生未授權的存取。
第二十三點	資訊系統應建立生產環境變更程序且考量授權流程並嚴格執行，以確保生產環境的安全性不被破壞。
第八章	**人員安全管理與教育**
第二十四點	對可存取機密性與敏感性資訊或系統的員工，於工作指派前應進行適當的安全評估程序，例如： 一、 工作記錄。 二、 犯罪記錄。 三、 信用記錄。

	四、 資歷查核。
第二十五點	針對不同工作類別之需求，應定期辦理資訊安全教育訓練及宣導，以提高員工資訊安全意識。
第二十六點	資訊安全教育及訓練的內容應包含資訊安全政策、資訊安全法令、緊急事件通報程序及如何正確使用資訊技術/工具等。
第九章	**網路安全管理**
第二十七點	應建立多層次網路安全措施且相結合的縱深防禦（如： 應用程式防火牆、入侵防禦/偵測系統系統、雙因子認證、內部存取控制等）。
第二十八點	應建立網路安全管理機制，以確保資料透過網路傳輸的安全性，並防止未經授權的存取行為。
第二十九點	對於跨公司/組織的網路系統，應加強網路安全管理，並協議相關網路安全規定。
第三十點	應定期檢視網路系統的安全弱點，並採取適當的防護措施。
第三十一點	透過網際網路傳送敏感性資料時，應使用虛擬專用網路（VPN）傳輸，以確保資料的機密性。
第十章	**資料安全管理**
第三十二點	資料應根據機密性與風險程度進行分級，並以此分級並採取妥善的管理措施。
第三十三點	各會員應根據資料分級結果將資料機密性較高或風險等級較高的資料，於傳輸與儲存時，使用加密技術保護。
第三十四點	資料存取權限應分級，僅供職務上有需求的人存取，且應留存相關存取權限紀錄，避免未經授權的存取行為。
第三十五點	應建立異地備援機制，以保護重要資料的可用性。
第三十六點	建立異地備援機制時，應考量復原時間目標（RTO）和復原點目標（RPO）指標，且依照建置成本、軟/硬體需求、通訊需求、建置時間等面向評估後，使用以下架構擇一執行： 一、 冷備援站。 二、 暖備援站。 三、 熱備援站。 四、 鏡像備援站。
第十一章	**緊急事件管理**
第三十七點	應制定緊急事件管理規定、通報管道、通報程序與處理流程，並定期演練。
第三十八點	關於緊急事件演練的情境，應根據實際情況制定，且應包含： 一、 網路攻擊。 二、 內部導致的系統故障。 三、 外部導致的系統故障。 四、 資料洩漏。 五、 自然災害。 六、 傳染病。

第三十九點	緊急事件發生時，應遵照事前制定的通報管道、通報程序與處理流程通知負責單位和權責機關。
第十二章	**資訊安全管理政策聲明**
第四十點	會員得依本會指定之文件、資料及方式，提交包含本辦法第三點所定範圍之資訊安全管理政策在內之相關文件，向本會提交完成資訊安全管理政策之聲明。 本會對會員提交之聲明文件進行書面查核，聲明程序經本會通知限期補正，而屆期不補正者，本會將不為第三項之公告。 本會將公告完成資訊安全管理政策聲明之業者名單於本會網站。
第十三章	**其他**
第四十一點	本辦法自中華民國一百十一年十月一日公告，中華民國一百十二年一月一日實施。