國泰金融控股股份有限公司
區塊鏈聯盟自律公約
保險業技術暨資訊安全規範與訂定說明

中華民國　　年　　月　　日

編號	條文內容	訂定說明
一、	**技術暨資訊安全規範目的：**各參與聯盟之聯盟成員於聯盟鏈平台上進行數據交換及商業合作時，須配合本公約訂定之技術暨資訊安全內部標準，以確保聯盟成員系統具有一致性安全防護基準。	
二、	**本基準用詞定義如下：** 一、關鍵資訊系統：支持核心區塊鏈生態圈業務持續運作必要之系統或設備。 二、資料交換政策、程序及控制措施：包含但不限於區塊簽名驗證機制、多重簽名機制、告警機制等。 三、惡意攻擊：包含但不限於 51 攻擊、雜湊衝突、共識機制妥協、重入攻擊、DoS 攻擊等惡意攻擊手段。 四、資訊資產：係指軟體、硬體、文件、資料及人員等與資訊處理相關之資產皆屬於資訊資產範疇。 五、資訊安全相關認證：可為 ISO 27001 相關認證。 六、委外廠商管理規範：可包含委外廠商之人員管控、建立檢驗機制、軟、硬體維運之資通安全維護措施等。 七、委外廠商合約或協議：可包含個人資料安全防範措施及資訊安全管理責任。	
	遵循性	
三、	公約聯盟成員應確保區塊鏈生態圈所在之司法管轄區之法律、法令、法規未禁止區塊鏈及分散式帳本技術(Blockchain/ Distributed Ledger Technology)，且應確保、檢閱並避免違反區塊鏈生態圈(The Network)相關資訊安全之法律、法令、法規或契約	一、參酌 ISACA Blockchain Framework and Guidance G-1 、 G-1.01 ； ISO 27001 A.18.1.1；保險業辦理資訊安全防護自律規範第三條、第十九條。 二、各聯盟成員應遵循資訊

	義務，以及任何安全要求事項。	安全相關事項之要求，並將本文內容納入查核。
四、	公約聯盟成員應確保區塊鏈生態圈無法於高風險或受制裁之區域維運。	一、參酌 ISACA Blockchain Framework and Guidance G-1.02；ISO 27001 A.18.1.1。 二、高風險及受制裁地區應循法務部公告之「防制洗錢與打擊資助恐怖份子有嚴重缺失之國家或地區」及「其他未遵循或未充分遵循國際防制洗錢組織建議之國家或地區」。
	系統維運人員管理	
五、	公約聯盟成員區塊鏈節點角色之定義，應遵循已議定之區塊鏈協議、合約、共識機制或其他相關協議之基本要求，並指派其資訊安全責任，且衝突之角色及其權限範圍應予以區隔。	參酌 ISACA Blockchain Framework and Guidance I-1.10；ISO 27001 A.6.1.1、A.6.1.2。
六、	公約聯盟成員辦理資訊安全規範，應至少遵循下列規定： 一、應要求所聘任之員工簽署資訊安全保密切結書、雇佣契約、工作手冊，明訂員工應遵守資訊安全保密協定。 二、有委外業務者，應於委外契約中明訂資訊安全保密協定。 三、應透過每年定期、適當之教育訓練或宣導，告知內部員工應遵循之資訊安全規範。 四、管理階層應督導員工遵循公司既定之資訊安全規範。 五、員工職務異動時，應依既定程序辦理資訊資產退回與存取權限之變更或取消。	參酌 ISO 27001 A.7；保險業辦理資訊安全防護自律規範第四條。
	系統生命週期管理	
七、	公約聯盟成員應透過正式變更管理程序，以控制區塊鏈生態圈新增及變更作業(包含但不限於網路代碼、智能合約、共識機制等作業)，以確保區塊鏈	參酌 ISACA Blockchain Framework and Guidance G-3.03、G-7.02、I-1.03、I-1.11、I-2.05、SC-2.03；ISO 27001

	生態圈內進行任何變更時，皆依循已議定之共識機制並產生適當稽核軌跡紀錄。	A.12.1.2、A.12.2、A.14.1.1、A.14.1.3、A.14.2.2。
八、	公約聯盟成員辦理資訊系統維運時，應注意相關控制措施如下： 一、系統發展生命週期之維運，包含開發、測試時，須注意版本控制與變更管理。 二、應定期審核資訊系統帳號之建立、修改及刪除。 三、應制定正式之使用者註冊、註銷及存取權限配置程序，以在所有系統及服務中，對所有類型之使用者，指派或撤銷存取權限，並確保已註銷使用者無檢視或存取區塊鏈生態圈內任何交易之權限。 四、應定期檢視防火牆規則，以確保現行控制之有效性。	一、參酌 ISACA Blockchain Framework and Guidance G-5.04、ISO 27001 A.9.2.1、A.9.2.2；保險業辦理資訊安全防護自律規範第十五條。 二、已取得權限之各公約聯盟成員內部權限管理，若公約聯盟成員已具相關內部規範,可優先遵循其內部規範;如無則應符合公約條款之最低要求。 三、核發公約聯盟憑證單位應依公約聯盟相關申請作業辦法進行憑證授予，並經聯盟大會決議。
	網路管理	
九、	公約聯盟成員應依據區塊鏈生態圈現有網路協定與資源使用狀況及未來容量需求，進行以下作業： 一、 應針對資源使用狀況及容量定期分析/模擬，以確保區塊鏈生態圈系統效能可滿足目前及未來容量和雜湊需求。 二、 應確保共識機制之驗證速度滿足資料傳輸流量，以實現區塊鏈生態圈營運持續目標。 三、 應依區塊鏈生態圈業務性質及設備功能等，對關鍵資訊系統訂定相關負載量要求，以強化系統穩定性，確保業務持續運作不中斷(包含但不限於採取適當措施以限縮或封存區塊鏈生態圈)。	參酌 ISACA Blockchain Framework and Guidance G-3.02、G-4.01、G-4.03；ISO 27001 A.12.1.3、A.14.2.8、17.1.1;保險業辦理資訊安全防護自律規範第十四條。
十、	公約聯盟成員應針對區塊鏈生態圈及相關網路備妥資料交換政策、程序及控制措施，並依各公約聯盟成員內部	參酌 ISACA Blockchain Framework and Guidance G-5.01、I-2.01、I-2.02、I-2.03、

	作業程序核定，以管理及控制區塊鏈生態圈及相關網路之安全性，並防止惡意人士或未經授權節點存取已核准區塊鏈或其他聯盟鏈。	KM-2.05 ； ISO 27001 A.9.2.3、A.10.1.2、A.12.3.1、A.13.1.1、A.13.2.1、A.14.1.1。
十一、	公約聯盟成員應監控網路傳輸，以確保可滿足資料傳輸流量與共識過程速度，並實踐聯盟鏈使用效能目標。	參酌 ISACA Blockchain Framework and Guidance I-1.01；ISO 27001 A.13.1.1。
十二、	公約聯盟成員應針對網路傳輸之安全性與正確性進行風險評估，以識別區塊鏈生態圈相關威脅情境。	一、參酌 ISACA Blockchain Framework and Guidance I-1.02；ISO 27001 A.14.2。 二、依照聯盟大會訂定之風險等級相關規範進行風險評估及風險緩解措施。
	智能合約安全	
十三、	智能合約 (Smart Contracts, SC)治理：應針對智能合約之架構設計及維運作業相關固有潛在監管或法律風險，制訂對應治理目標及控管程序，以避免合規風險。	參酌 ISACA Blockchain Framework and Guidance SC-1。
十四、	公約聯盟成員應確保智能合約(包含但不限於資料傳輸技術、程式碼撰寫之已議定條款及已核准共識機制)符合直接或間接維運作業所在地之司法管轄區相關法律、法令、法規及其他要求事項；且公約聯盟成員應依據前述法律、法令、法規及其他要求事項，執行相關法令遵循作業(包含但不限於內部稽核報告、主管機關要求之報告等)。	參酌 ISACA Blockchain Framework and Guidance SC-1.01、SC-1.02、SC-1.03；ISO 27001 A.18.1。
十五、	公約聯盟成員應針對智能合約相關維運作業，指定權責單位及人員，並依前項條款執行相關法令遵循作業(包含但不限於內部稽核報告、主管機關要求之報告等)。	參酌 ISACA Blockchain Framework and Guidance SC-1.04； ISO 27001 A.18.1。
十六、	公約聯盟成員應針對智能合約設計之相關程式漏洞風險，制訂相關管理程序及處置措施(包含但不限於修復或風險緩解措施)。	參酌 ISACA Blockchain Framework and Guidance SC-2。

十七、	公約聯盟成員應確保所有於區塊鏈生態圈中運作之智能合約已經共識機制核准，且具適當資料傳輸大小限制，以預防潛在超量資料傳輸或未被檢測到之資料遺失。	參酌 ISACA Blockchain Framework and Guidance SC-2.02；ISO 27001 A.17.1。
十八、	公約聯盟成員應確保智能合約符合資訊安全相關要求事項(包含但不限於存取權限控管)，並針對惡意攻擊建立適當風險緩解及處置措施。	參酌 ISACA Blockchain Framework and Guidance SC-3.01、SC-3.02、SC-3.03、SC-3.04、SC-3.06、SC-4、SC-4.05；ISO 27001 A.8.2.3、A.9.2、A.14.1、A.18.1。
十九、	公約聯盟成員應針對智能合約建立確保資料完整性與不可否認性之機制，以避免相關風險。	參酌 ISACA Blockchain Framework and Guidance SC-4.02；ISO 27001 A.8.2.3、A.13.2、A.18.1。
二十、	公約聯盟成員應明確定義智能合約程式碼函式之存取權限，包含但不限於透過適當加密保護措施，以防止外部人員未經授權之存取。	參酌 ISACA Blockchain Framework and Guidance SC-4.03；ISO 27001 A.8.2.3、A.18.1。
	節點安全	
二十一、	公約聯盟成員應確保區塊鏈生態圈之資料格式與系統架構符合公約聯盟成員相關資訊安全要求事項或標準，且資料上傳至聯盟鏈應符合聯盟鏈開發者所制定之相關規定，以達到區塊鏈生態圈之互通性。	一、參酌 ISACA Blockchain Framework and Guidance G-3.05、D-1.05；ISO 27001 A.13、A.14.1.1；保險業辦理資訊安全防護自律規範第五條。
	作業安全	
二十二、	公約聯盟成員應針對區塊鏈生態圈相關關鍵資訊系統產生之稽核紀錄(內容包含但不限於事件類型、發生時間、發生位置、使用者身分識別等資訊)應有保留機制及存取管理。	參酌 ISACA Blockchain Framework and Guidance G-6.01、G-6.02；ISO 27001 A.12.4.1、A.12.7.1；保險業辦理資訊安全防護自律規範第十七條。
二十三、	公約聯盟成員應確保區塊鏈之架構設計或網路協定已遵循資料傳輸時間順序，以防止網路效能或完整性毀損。	參酌 ISACA Blockchain Framework and Guidance I-1.05；ISO 27001 A.12.6.1。
二十四、	公約聯盟成員應針對區塊鏈生態圈相關關鍵資訊系統進行校時，以確保生	參酌 ISACA Blockchain Framework and Guidance I-

	態圈之時間戳記與相關關鍵系統時間之誤差不超過議定範圍，並防止時間戳記誤差值導致區塊鏈生態圈內之濫用與詐欺行為。	1.09；ISO 27001 A.12.4.4、A.12.6.1;保險業辦理資訊安全防護自律規範第十七條。
二十五、	公約聯盟成員應確保無論是直接或間接操作情境下，區塊鏈生態圈維運人員無法變更區塊時間戳記，以避免惡意人士對區塊鏈進行濫用或詐欺，並確保資訊安全。	參酌 ISACA Blockchain Framework and Guidance I-2.04、D-1.04；ISO 27001 A.13、A.14.2。
	個人資料保護	
二十六、	公約聯盟成員應確保區塊鏈生態圈維運作業所在司法管轄區客戶個人可識別資訊之隱私符合相關法律、法令、法規中之要求。	一、參酌 ISACA Blockchain Framework and Guidance G-1.04、SC-1.06、SC-4.09;ISO 27001 A.8.2.3、A.9.2、A.13.1.3、A.18.1.2、A.18.1.4、A.18.1.5;保險業辦理資訊安全防護自律規範第六條。 二、建議公約聯盟成員可同時依據「保險業辦理電腦系統資訊安全評估作業原則」辦理各項資訊安全評估作業，以改善並提升網路與資訊系統安全防護能力。 三、客戶個人可識別資訊可參酌「個人資料保護法」第2條第1款針對「個人資料」之定義：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
	加密及金鑰管理	
二十七、	公約聯盟成員應建立金鑰管理程序，	一、參酌 ISACA Blockchain

	且應包含但不限於以下要求： 一、應確保金鑰設計及產製具有適當複雜度。 二、應防止並針對加密金鑰外洩事件或潛在情境進行應變。 三、應針對加密金鑰擁有者建立並實施適當權限授予與移除之相關程序。 四、應針對加密金鑰及種子制訂相關存取控制及備份程序，並定期針對其備份資料進行測試。 五、應確保加密金鑰及種子之備份儲存位置，應與主加密金鑰存放於不同伺服器或地理位置。 六、應避免加密金鑰及種子之備份之環境風險，包含但不限於火災、洪水、盜竊及其他不可抗力因素。	Framework and Guidance KM-1、KM-1.01、KM-1.02、KM-1.03、KM-2.01、KM-2.02、KM-2.03、KM-3.02、KM-3.03；ISO 27001 A.9.2.3、A.10.1.2、A.11.1、A.12.3.1、A.17.1。 二、公約聯盟成員已具相關內部規範，可優先遵循其內部規範；如無則應符合公約條款之最低要求。
	實體安全	
二十八、	公約聯盟成員應訂定硬體設備報廢作業程序，報廢前應將機密性、敏感性資料及授權軟體予以移除、實施安全性覆寫或實體破壞，應確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄，若委託第三者銷毀時，應簽訂保密合約。	一、參酌 ISO 27001 A.11.2.7;保險業辦理資訊安全防護自律規範第十一條。 二、公約聯盟成員已具相關內部規範，可優先遵循其內部規範；如無則應符合公約條款之最低要求。
二十九、	公約聯盟成員於非公司職場實施異地辦公或遠端工作時，應評估相關作業風險，以強化遠端作業之安全： 一、針對營運環境調整、資料傳輸及加密機制、機敏資料防護、稽核軌跡留存、異常行為監控及對外遠端存取設備進行評估及強化，系統及設備如有重大漏洞應立即處理及因應，降低業務運作風險並確保穩定及安全。 二、針對使用之視訊會議系統、VPN及 VDI 等設備，應訂定相關使用規範並落實各項安全管控作業。	參酌保險業辦理資訊安全防護自律規範第十二條。
	事件與營運持續管理	
三十、	公約聯盟成員應確保區塊容量大小	參酌 ISACA Blockchain

	(Block size)、區塊高度(Block height)和區塊間隔時間(Block interval time)符合區塊鏈生態圈目前及未來資源需求，以實現區塊鏈生態圈營運持續目標，並維持其運算完整性及穩定性。	Framework and Guidance G-4.02、I-1.06、 I-1.07；ISO 27001 A.12.6.1、A.17.1.1。
三十一、	一、公約聯盟成員應加強資訊安全事件管理。 二、公約聯盟成員應依資訊安全事件通報應變作業實施原則，若發生資訊安全事件時，應儘速回報公約聯盟，並採取適當處理措施，以控制資安事件影響範圍之擴大。	參酌 ISO 27001 A.12.4；保險業辦理資訊安全防護自律規範第十三條。
	脆弱性管理	
三十二、	公約聯盟成員應確防止區塊鏈生態圈傳輸之資料(包含但不限於客戶資料)，遭受未經授權揭露、修改，或透過區塊鏈生態圈進行惡意攻擊。公約聯盟成員亦應進行預防性分析、實施安全功能性之測試及驗收測試計畫及準則、網路服務安全監控及分析等，以降低區塊鏈中演算法之存取漏洞，並避免區塊鏈生態圈損害之惡意行為。	參酌 ISACA Blockchain Framework and Guidance G-5.02、I-3.01、I-3.02、I-4.02、I-4.03、I-5.01、SC-4.06；ISO 27001 A.8.2.3 、 A.9.2 、 A.12.6.1、A.13.1.2、A.14.1.1、A.14.1.2、A.14.2.8、A.14.2.9、A.18.1。
三十三、	公約聯盟成員應針對區塊鏈技術之脆弱性實施預防性控制措施，並採取適當措施以因應相關風險，以確保區塊鏈生態圈每一區塊之資料傳輸量總和不超過議定之區塊大小，以防止網路效能或完整性毀損。	參酌 ISACA Blockchain Framework and Guidance I-1.04；ISO 27001 A.12.6.1。
	供應商管理	
三十四、	公約聯盟成員應針對區塊鏈生態圈相關關鍵資訊系統委外作業，進行資訊安全評估以強化資訊安全，並遵循下列事項： 一、應確保委外廠商應具備資訊安全相關認證或已有資通安全維護之相關措施。 二、應審核作業委外廠商資格：	一、參酌 ISO 27001 A.15；保險業辦理資訊安全防護自律規範第十六條、第十八條。 二、第三方服務供應商由各公約聯盟成員遵循其內部規範自行管理與監督。 三、產品交付和驗收或維運係指委外廠商提供之交付標

	1. 公約聯盟成員應制定有關審核委外廠商資格之內控機制，並就委外作業進行廠商評選審查作業。 2. 公約聯盟成員之廠商評選審查作業，應包含作業委外廠商遴選機制、合約或協議簽訂、作業委外廠商管理要項、產品交付和驗收或維運等項目。 3. 公約聯盟成員應將資訊安全或個人資料隱私管理納入委外廠商評估項目。 三、作業委外廠商管理要項： 1. 公約聯盟成員應建立委外廠商管理規範。 2. 公約聯盟成員應針對委外作業內容重大變更或重大事件，審查是否影響相關關鍵資訊系統及區塊鏈生態圈之資訊安全管理制度或依循標準之要求並評估其風險，採取適當控制措施。 3. 作業委外廠商簽訂合約或協議，應遵循相關安全管理措施。 四、委外稽核： 1. 公約聯盟成員應依據各成員內部相關規範，針對委外廠商進行委外查核作業。 2. 公約聯盟成員應於執行委外查核作業後，保留相關稽核紀錄之文件。	的物或產品，需具備合法性且不得違反智慧財產權之規定或侵害第三人合法權益。
資訊資產		
三十五、	公約聯盟成員應依據區塊鏈生態圈之作業流程，識別人員、表單、設備、軟體、系統等資產，並建立資產清冊、作業流程、網路架構圖、組織架構圖及負責人，並定期清點以維持其正確性。	