國泰金融控股股份有限公司
區塊鏈聯盟自律公約
電動車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、	一、本基準用詞定義如下： 二、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。 三、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。 四、電動車駕駛行為原始資料：透過電動車原廠API串接取得之駕駛行為資料(包含但不限於行車速度、經緯度等)。 五、獨立單位：可為內部稽核單位或外部顧問。 六、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。 七、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。 八、物件：蒐集電動車駕駛行為原始資料之設備及相關元件(包含但不限於車上診斷系統，On-Board Diagnostics)。 九、數位證據：包含但不限於車輛黑盒子中記錄之急加速、急轉彎、胎壓驟變等。 十、網路安全事件處置計畫：因應重大或攻擊事件預計實施之處置措施。	

	十一、網路安全目標：包含但不限於確保資訊資產之完整性、機密性、可用性，且針對內、外部惡意之威脅、破壞行為採取預防措施。 十二、網路安全聲明：包含但不限於以簡單扼要且符合前述之網路安全目標，訂定公約聯盟成員之聲明，如「個資不外洩、服務不間斷、資料不流失」等。 十三、網路安全目標績效報告：依據網路安全目標，出具對應目標指標衡量結果。	
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、法規或契約義務，以及任何安全要求事項。	參酌 ISACA Blockchain Framework and Guidance G-1、G-1.01；ISO 27001 A.18.1.1。
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	參酌 ISACA Blockchain Framework and Guidance I-1.10、ISO 27001 A.6.6.1、

	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。	A.6.6.2。
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。
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。	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 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，對所有型式之使用者，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。	一、參酌 ISACA Blockchain Framework and Guidance G-5.04；ISO 27001 A.9.2.1、A.9.2.2。 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，並實踐組織使用者之使用效能目標。	參酌 ISACA Blockchain Framework and Guidance I-1.01；ISO 27001 A.13.1.1。
十、	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 及 G-4.03；ISO 27001 A.12.1.3、A.14.2.8 及 A.17.1.1。
十一、	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，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。	一、參酌 ISACA Blockchain Framework and Guidance G-5.01、I-2.01、I-2.02、I-2.03、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；ISO 21434 RQ-10-01、RQ-10-03、WP-10-01 及 WP-10-02。 二、公約聯盟成員建立正式網路安全政策、程序及控制措施，應符合以下事項： (1)應分配單位、人力並劃分責任歸屬，以完成執行網路安全之各項活動。 (2)應透過資源提供及各項

		控管措施之協調，以強化網路安全執行度。 (3)應透過維運人員能力管理、網路安全意識強化及持續改善，以建立符合網路安全的組織文化。 (4)應執行組織層面的網路安全稽核。 (5)應針對網路安全相關之資訊交流實施控管作業。 (6)應透過管理系統進行網路安全活動管控作業。 三、公約聯盟成員應針對區塊鏈生態圈相關網路設備，建立資訊資產清冊並定期盤點。 四、公約聯盟成員應確保網路安全稽核由獨立單位執行(例：內部稽核單位或外部顧問)。 五、公約聯盟成員應針對區塊鏈生態圈及電動車相關關鍵系統開發、串接後期階段，擬定相關網路安全需求。
十二、	一、公約聯盟成員應針對區塊鏈生態圈訂定網路安全計畫，計畫中應包含以下項目： 1. 區塊鏈生態圈網路安全計畫之目標； 2. 區塊鏈生態圈之網路安全，與其他關鍵資訊系統或資訊傳輸之相依性； 3. 區塊鏈生態圈之網路安全權責單位與人員； 4. 區塊鏈生態圈之網路安全活動所需資源清單(包含但不限於防火牆設備、入侵防禦系統、網	一、參酌 ISO 21434 RQ-06-02、RQ-06-03、RQ-06-04、RQ-06-05、RQ-06-06、RQ-06-07、RQ-06-09、RQ-06-10、RQ-06-11、RQ-06-12、RQ-06-14。 二、公約聯盟成員所訂定之網路安全計畫，應適用於整體區塊鏈生態圈(含已串接之相關關鍵資訊系統)。 三、如公約聯盟成員已具

	路流量監控系統等)； 5. 區塊鏈生態圈相關資訊資產清冊(包含但不限於電動車駕駛行為原始資料)。 二、前述網路安全計畫，應於區塊鏈生態圈及相關關鍵資訊系統發生重大變更時，進行網路安全計畫之調整與更新。如非因重大變更而進行網路安全計畫之調整，則應另載明緣由，並依據公約聯盟成員內部簽核流程進行核准。 三、應將網路安全計畫納入資訊資產管理作業。	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。
十三、	一、公約聯盟成員應針對區塊鏈生態圈，建立相關網路安全事件清單及對應網路安全目標層級，並透過獨立單位進行網路安全風險評估，並應作成網路安全風險評估報告。 二、網路安全風險評估之評估範圍應包含： 1. 網絡安全計劃及與其相關之資訊資產(包含但不限於區塊鏈生態圈相關關鍵資訊系統)； 2. 網絡安全風險處置措施； 三、網路安全風險評估報告應包含評估之風險結果、是否接受該風險(含原因)及改善建議。	一、參酌 ISO 21434 RQ-06-23、RQ-06-24、RQ-06-25、RQ-06-26、RQ-06-27、RQ-06-28、RQ-06-29、RQ-06-30、RQ-06-31、RQ-06-32、WP-06-02、WP-06-03、WP-06-04。 二、公約聯盟成員可依循 ISO 21434 之 Threat Analysis and Risk Assessment (TARA) 評估框架，進行網路安全風險評估作業，以利詳列網路安全事件對應之安全目標。 三、網路安全風險評估作業應符合以下： (1)由獨立單位執行(包含但不限於內部稽核單位或外部顧問)。 (2)評估執行人員應具備適當專業能力及工具。
十四、	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。
十五、	一、公約聯盟成員應於網路安全之	一、參酌 ISO 21434 RQ-

	範疇下，定義電動車相關物件(item)之資訊、運作環境以及與其他物件交互關係。 二、公約聯盟成員應依據網路安全風險評估結果，確定風險處置措施；訂定網路安全目標及網路安全聲明，並產出網路安全目標績效報告。 三、公約聯盟成員應確保各電動車相關物件及其運作環境，已符合公約聯盟訂定之網路安全目標及要求。	09-01、RQ-09-02、RQ-09-03、RQ-09-04、RQ-09-05、RQ-09-06、RQ-09-07、RQ-09-08、RQ-09-09、RQ-09-10、RQ-09-11、WP-09-01、WP-09-02、WP-09-03、WP-09-04、WP-09-05、WP-09-06、WP-09-07。 二、公約聯盟成員可依循ISO 21434 之 Threat Analysis and Risk Assessment (TARA)評估框架，進行網路安全風險評估作業，以利詳列網路安全事件對應之安全目標。
智能合約安全		
十六、	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。
十七、	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。
十八、	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。
十九、	公約聯盟成員應針對智能合約設計	參酌 ISACA Blockchain

	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)。	Framework and Guidance SC-2。
二十、	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，且具適當交易大小限制，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。
二十一、	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。
二十二、	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。
二十三、	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		
二十四、	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。	參酌 ISACA Blockchain Framework and Guidance G-3.05 及、D-1.05；ISO 27001 A.13、A.14.1.1。
作業安全		
二十五、	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。
二十六、	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	參酌 ISACA Blockchain Framework and Guidance I-1.05、ISO 27001 A.12.6.1。

	損。	
二十七、	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。	參酌 ISACA Blockchain Framework and Guidance I-1.09；ISO 27001 A.12.4.4、A.12.6.1。
二十八、	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		
二十九、	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。 二、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(包含但不限於車牌、原廠車輛唯一識別碼)。
加密及金鑰管理		
三十、	公約聯盟成員應建立金鑰管理程序，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。	一、參酌 ISACA Blockchain Framework and Guidance KM-1、KM-1.01、KM-1.02、KM-1.03、KM-2.01、KM-

	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、公約聯盟成員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。	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
事件與營運持續管理		
三十一、	公約聯盟成員應確保區塊容量大小(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。	參酌 ISACA Blockchain Framework and Guidance G-4.02、I-1.06、I-1.07；ISO 27001 ISO 27001 A.12.6.1、A.17.1.1。
三十二、	一、公約聯盟成員應針對區塊鏈生態圈制定網路安全事件處置計畫，包含： 1. 補償性措施； 2. 溝通計劃； 3. 權責單位及人員； 4. 針對新興網路安全事件之情資蒐集與紀錄(包含但不限於受影響的物件、數位證據等)； 5. 網路安全事件處置進度追蹤措施； 6. 網路安全事件結案標準及後續行動方案。 二、公約聯盟成員應於電動車軟、硬體功能更新或重大變更時，更新前述網路安全事件處置計畫。	參酌 ISO 27001 A.12.4；ISO 21434 RQ-13-01、RQ-13-02、RQ-13-03 及 WP-13-01。
脆弱性管理		

三十三、	一、公約聯盟成員應針對區塊鏈生態圈識別資訊資產、對應之網路安全屬性及威脅情境進行以下措施： 1. 蒐集網路安全威脅情資(包含但不限於網路安全事件)。 2. 進行風險評估，以識別區塊鏈生態圈相關威脅情境。 3. 對於潛在損害影響進行分級。 4. 風險處置措施(對應每個威脅情境)。 二、公約聯盟成員應建立威脅情境清單。	一、參酌 ISACA Blockchain Framework and Guidance I-1.02；ISO 27001 A.14.2；ISO 21434 RQ-08-01、RQ-08-02、RQ-08-03、RQ-08-04、RQ-08-05、RQ-08-06、WP-08-01、WP-08-02、WP-08-03、WP-08-04、WP-08-05。 二、公約聯盟成員可參酌以下要求，進行風險評估： 1. 透過網路協定傳輸的目的及用途。 2. 網路協定是否合乎法規或主管機關的要求。 3. 傳輸的方式(實體或非實體)。 4. 傳輸標的之機密性。 三、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。 四、網路安全威脅情資可為公約聯盟成員內部或外部來源。內部來源可包含(1)已執行之弱點分析(e.g. 弱點掃描報告)(2)使用者使用資訊；外部來源可包括(1)網路安全研究組織(2)公約聯盟成員相關業界資訊(3)政府來源。 五、威脅情境係指如資料損毀、資料遺失、未經授權存取硬體設備等。
三十四、	公約聯盟成員應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	參酌 ISACA Blockchain Framework and Guidance G-5.02、I-3.01、I-3.02、I-

	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。	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。
三十五、	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		
三十六、	一、如區塊鏈生態圈及相關關鍵資訊系統涉及第三方單位(包含但不限於委外供應商)，公約聯盟成員應視委外項目及範圍，與其簽署諒解備忘錄(MOU)及網路安全介面協議(Cybersecurity interface agreement)，並針對第三方單位進行遴選評估(包含但不限於技術、財務等)，以確保公約聯盟成員與第三方單位間之互動層級、依賴性及責任歸屬。 二、諒解備忘錄應包含以下： 1. 應要求第三方單位遵守本基準及其他適當資訊安全國際標準要求，確保資料安全。 2. 應與第三方單位就服務品質、水準、效能等方面訂定服務要求。 3. 應對第三方單位進行適當監督。 4. 爭議解決條款。 5. 公約聯盟成員與第三方單位雙方權責義務。 三、網路安全介面協議應包含以下： 1. 第三方單位應承擔網路安全責任。 2. 公約聯盟成員與第三方單位協議之網路安全要求與標準。	參酌 ISO 27001 A.15；ISO 21434 RQ-07-01、RQ-07-02、RQ-07-03、RQ-07-04、RQ-07-07、RQ-07-08、WP-07-01。

	3. 網路安全活動定義，包含以下： (1)電動車網路安全活動(包含但不限於網路安全監控)。 (2)電動車資料共享範圍。 4. 爭議解決條款。 5. 公約聯盟成員與第三方單位雙方權責義務。	