# 國泰金融控股股份有限公司資訊安全管理辦法

110年3月22日訂定

權責單位：資訊安全部

**主旨**

第一條　為強化國泰金融控股股份有限公司(以下簡稱本公司)之資訊安全管理，建立安全及可信賴之資訊作業環境，確保資訊財產之機密性、完整性及可用性，並提升同仁對資訊安全之認知，以保障員工、客戶、合作夥伴與本公司之權益，依據「國泰金融控股股份有限公司資訊安全政策」訂定資訊安全管理辦法(以下簡稱本辦法)。

**適用對象及範圍**

第二條　本辦法適用對象為本公司所有員工(含各級主管、實習生及工讀生，以下同)及其他得接觸本公司資訊及資訊財產之合作夥伴、委託廠商(含顧問) (以下合稱「受委託者」)等。

本辦法適用範圍如下，以下合稱資訊財產(Information Assets)：

一、 本公司所有或持有之資料與文件。

二、 本公司使用之主機、伺服器、個人電腦(含可攜式電腦，以下同)、行動裝置、終端設備、通訊線路、儲存設備(含可讀寫CD裝置、外接硬碟、USB儲存媒體、記憶卡等，以下同)，以及與前述相關或是與本公司資訊系統相連之硬體資訊財產。

三、 本公司使用於存放資訊財產之實體環境。

四、 本公司使用之資訊系統，以及與前述資訊系統相關或相連之軟體資訊財產。

五、 其他本公司所有或有權使用之資訊財產。

**用詞定義**

第三條　本辦法相關用詞定義如下：

資訊安全：目的在確保資訊的機密性、完整性、可用性、私密性及合法性，使資訊能安全地、正確地、適切地及可靠地被運用在達成本公司經營目標之規劃、執行、管理及相關作為上。

**資訊財產安全管理作業**

第四條　本公司資訊財產安全管理作業之權責職掌應適當劃分，並視需要建立代理人制度。

本公司資訊財產相關業務於委託「受委託者」辦理前，應與其簽署合約並納入本辦法中「受委託者」應遵循之相關事項。

第五條　本公司員工之資訊安全教育訓練，應依下列規定辦理：

一、各級主管須負責督導所屬員工之資訊作業安全，防範不法及不當行為。

二、所有員工須依公司安排之課程參與資訊安全教育訓練，以瞭解維護資訊安全為每位員工之義務，且於執行各項作業時，應確保所執行作業之資訊安全，對執行業務過程中所得知之資訊，應嚴格保密，其保密義務不因調離職而免除。

三、資訊安全部得視實際需要辦理或責成相關單位執行資訊安全教育訓練及宣導，以建立員工資訊安全認知，並提升公司整體資訊安全水準。

第六條　資訊財產管理，應依下列規定辦理：

一、本公司資訊財產之使用，應遵循本公司及受本公司委託管理維運公司之相關規範。

二、本公司嚴禁使用來源不明之儲存媒體及非法軟體程式或未經公司許可之軟體，所有員工及受委託者，均有責任及義務保護其所取得或使用之本公司資訊財產，並防止未經授權之存取、擅改、破壞或不當揭露，以確保資訊財產之機密性、完整性及可用性。

三、本公司資訊財產應由資訊處或受委託者安裝管控軟體及防毒

軟體並開啟即時掃瞄功能，惟若符合《辦公室資訊作業管理要點》規範之例外狀況，得依該要點辦理。

四、 本公司資訊財產應由資訊處或受委託者啟動存取軌跡，惟若有將資訊複製或移動至外部儲存裝置之需求者，應遵循《辦公室資訊作業管理要點》進行申請並取得核准，資訊處或受委託者並須將複製或移動之資訊留存紀錄。

五、 本公司硬體資訊財產，如經評估不堪使用或不再使用時，應依《辦公室資訊作業管理要點》進行報廢程序後，方可進行處分或報廢。

第七條　就本公司資訊財產實體與資訊安全管制區域之安全，資訊處、數位數據暨科技發展中心(以下簡稱數數發中心)或受委託者應依下列規定辦理：

一、 本公司就單獨使用非屬資訊共用之主機或伺服器，應配置符合該等設備需求之獨立機房，並應強化機房實體環境的安全保護與維運，包含但不限於門禁控管、監視設備、空調、不斷電設備、溫度控管、溼度控管、消防設施等，以避免資訊財產遭未經授權存取、損害或意外災害，影響營運活動正常運作。

二、 本公司之資訊安全管制區域，應落實門禁管控及物品攜出入規定，並應嚴格管制電腦機房人員進出，留存進出紀錄。

第八條　本公司伺服器資訊系統作業之安全管理，資訊處、數數發中心或受委託者應依下列規定辦理：

一、 正式環境作業系統安裝時應進行強化措施，如設定相關系統強化參數、檢核系統稽核原則之符合性、移除或停用不必要預設及測試帳號、關閉非必要服務及功能等，並遵照最小安裝原則執行安裝。

二、 適時取得有關使用中資訊系統技術弱點的資訊，以及評估本公司對此弱點之曝險情形，並採取適當的措施來因應相對應之風險，如日常系統強化作業應考量透過定期檢核系統安全設定、執行弱點掃描、版本更新或安裝修補程式等方式加以維持，並適時

評估補強需求，修補已知之系統漏洞。

三、 特殊權限帳號，如具有作業系統管理權限、特殊資料存取權限、其它系統資源控制權限或存取稽核軌跡之帳號，其使用應僅限於被授權核准之事項，並留存適當之稽核軌跡。

四、 正式環境作業系統設定檔或參數因業務或作業上實際需要變更時，應先進行相關之評估或測試，始得進行變更。

五、 正式環境作業系統應使用自動化時間同步工具。無法自動化時間同步之硬體資訊財產，應由系統管理者至少每月對時乙次，並留存相關紀錄。

六、 在效能與監控平衡考量之下，就各資訊系統特性，應保留設定操作軌跡以供日後稽核。

七、 資訊系統稽核紀錄應定期檢視、分析，並針對異常紀錄予以標示並追蹤。

八、 資訊系統得因所提供之服務重要性或因其為正式/測試環境之不同，設定不同等級之管理標準。

第九條　本公司網路暨通訊管理之相關作業，資訊處或受委託者應依下列規定辦理：

一、 在網路規劃時，應協同資訊安全單位，對網路架構的規劃是否滿足營運需求及資訊安全相關規範進行評估。

二、 針對防火牆應制定相關管理作業程序，並遵循相關系統安全要求建置之。

三、 公司與外部網路連接的網點，應加裝防火牆，以控管外界與公司內部網路間之資料傳輸與資源存取；內部網路資源之存取，應訂定適當的網路區隔。

四、 於規劃與建置網路時，重要設備如連結網路骨幹之中心交換器(Core Switch)、防火牆、路由器等，應配置備援(Redundant)機制，以滿足高可用性要求。

五、 網路線路之設置須經本公司防火牆；若因業務需要須設置免經防火牆之網路連線，應提出申請由資訊處及資訊安全部進行評估。

六、 應設置必要之安全設施(如：入侵偵測防禦系統、網路APT等)以保護內外部網路。

七、 針對惡意軟體、電腦病毒、惡意網站、垃圾郵件及非法網站等應採取偵測及預防控制措施。

八、 針對本公司重要網路設備及電腦系統應進行弱點掃描。

九、 針對遠端登入行為，應制定相關之管理作業程序，以便對遠端登入活動進行控管，其中應明確定義可開放連線情況、連線系統、連線最長閒置時間、與最大連線時間，並應留存連線紀錄且定期檢視。

十、 伺服器憑證建置、撤銷、備份憑證重新匯入等作業應依系統管理單位之管理規範提出申請，其中須載明伺服器憑證名稱、伺服器憑證生效日期、伺服器憑證到期日、申請說明，經覆核程序後，方可進行。

十一、 涉及重要系統以及資料分析平台的連線作業，僅能使用本公司提供具完整管控之個人電腦於內部網路環境中，透過本公司之授權進行連線(如VDI)。

十二、 所有電子郵件之收發均應留存紀錄，並於電子郵件伺服器建置防禦措施，以阻擋垃圾郵件、防止個資外洩、預防病毒入侵、以及進階持續性威脅等。

本公司網路暨通訊管理之相關作業，本公司所有員工應依下列規定辦理：

一、 利用網路傳送機密資訊時，應採取適當的安全保護措施，以保護資料傳輸之安全。

二、 嚴禁私自設定網路位址、架接集線器、交換器或無線路由器等網路連接設備。

三、 禁止執行有安全性或個資外洩疑慮之連線與服務(例如使用FTP、TELNET服務)，惟因業務需求有執行連線之必要時，應依《辦公室資訊作業管理要點》辦理。

四、 禁止由本公司內部網路連接使用包含且不限網頁式郵件在內的外部郵件(如yahoo mail、gmail、hotmail等Webmail)，例外狀況

應依《辦公室資訊作業管理要點》辦理。

五、 未經授權均不得於本公司內部網路使用外部即時通訊軟體，亦不得使用網頁或其他替代方式進行電腦即時通訊。

第十條　本公司資訊系統存取控制之相關作業，資訊處、數數發中心或受委託者應依下列規定辦理：

一、 資訊系統之管理帳號與使用帳號應有權責區分且制定規範原則，規範中需包含帳號申請、異動程序，並留存申請紀錄。

二、 非本公司員工之帳號及權限應於合約終止時予以調整、停用或刪除。

三、 伺服器特殊權限帳號，如具有作業系統管理權限、特殊資料存取權限、其它系統資源控制權限及存取稽核軌跡之帳號，其使用應僅限於被授權核准之事項，留存適當之稽核軌跡並定期進行檢視。

四、 每一經申請核准之使用者應有專屬且獨立的帳號及密碼，且每年應定期清查覆核。

五、 密碼之安全管理，應包含下列項目：

(一) 密碼長度、複雜性、密碼歷程之要求。

(二) 密碼定期變更及錯誤鎖定之要求。

本公司網路暨通訊管理之相關作業，應依下列規定辦理：

一、 帳號使用單位、資訊處、數數發中心或受委託者應定期審視分工區隔作業以及各帳號授權的妥適性，離職、調職、停職、留職停薪人員之權限應於生效日(含)前取消或停用。

二、 帳號使用者對所持有之帳號、密碼與權限應善盡保管責任並於授權範圍內妥善使用。

第十一條　本公司系統開發及維護之安全管理，資訊處、數數發中心或受委託者應依下列規定辦理：

一、 系統開發應於初始階段考量安控機制之布置，委託開發部分應

強化控管資訊安全並於合約載明相關義務，系統開發應注意時程之掌控，避免延誤脫序。

二、 系統開發之安全管理，應包含下列項目：

(一) 需求提出階段之安全管理。

(二) 系統分析階段之安全管理。

(三) 系統設計階段之安全管理。

(四) 系統測試階段之安全管理。

(五) 系統驗收及上線階段之安全管理。

三、 系統變更之安全管理，應包含下列項目：

(一) 原始碼之安全管理。

(二) 程式佈署之安全管理。

(三) 緊急變更之安全管理。

四、 測試環境與正式環境應分別獨立於不同電腦作業環境。

第十二條 資訊系統營運持續管理，應依下列規定辦理：

為避免因各種人為及天然災害造成資訊業務運作受影響，資訊處、數數發中心或受委託者應進行風險評估，判斷影響範圍、損害程度及復原所需時間，擬定應變策略與處理計畫，並落實執行。

第十三條 本公司資訊安全通報之相關作業，各單位應依下列規定辦理：

一、 應賦予相關人員必要的責任並要求提高警覺，以便迅速有效處理資訊安全事故，將安全事故所造成的損害降到最低。

二、 於發生資訊安全事故時，應依循本公司《重大事件處理辦法》、《作業風險事件通報辦法》、《重大資訊安全事件通報暨緊急應變管理要點》以及相關管理規範等要求，立即向各相關單位及資訊安全部進行通報。

第十四條 本公司資訊處、數數發中心或受委託者於進行相關資訊作業規劃或調整時，應協同資訊安全部識別適用之資訊安全法規、政策或第三方驗證標準，並遵從其要求。

本公司資訊安全之業務處理有涉及第三人之智慧財產權或其他權利時，應符合相關法律及授權規定。

資訊安全部得視需要委請外部獨立審查機構，就本公司資訊安全管理之執行成效進行專業評估。

**附則**

第十五條 本公司員工如有違反本辦法致影響公司權益，經查證屬實者，應由行政處行政管理部人資暨管理科依人事規章議處。

受委託者如有違反相關合約約定，致本公司受有損害者，應由權責單位會請法務室追究其法律責任。

**施行日期**

第十六條 本辦法之訂定、修正或廢止應經總經理同意。

本辦法經總經理核定後實施。