永豐金融控股股份有限公司

資訊安全管理準則

■非因應外規訂定

□因應外規訂定

制定單位：資訊安全處　　核定層級：總經理

第 一 條　目的

為強化本公司及各子公司整體資訊業務與資訊安全管理之順利運作，並符合資訊安全相關規定，建立安全及可信賴之資訊安全管理系統，特訂定本準則。

第 二 條　適用範圍

一、本準則所稱之子公司，應依金融控股公司法第四條規定認定。

二、本準則適用於本公司及各子公司之所有員工、約聘雇人員、協力廠商及其相關人員等之管理。

第 三 條　為確保資訊安全管理制度之落實，依「資訊安全政策辦法」針對下列事項，訂定資訊安全計畫：

一、資訊安全權責分工

(一)負責資訊安全事務之部門應規劃、監控及執行資訊安全管理作業。

(二)應視資訊安全管理需要，設置資訊安全單位或配置適當人力資源及設備。

(三)資訊安全權責分工應符合金融監督管理委員會及相關法令規定要求。

二、資訊安全教育訓練

(一)為作業需要或提升同仁之工作能力，資訊安全教育訓練應考量以人員角色及職能為基礎，針對不同工作類別之同仁，進行相關的資訊安全教育訓練。

(二)資訊安全教育訓練內容應考量資訊安全相關之議題，如資訊安全管理制度實施規範、資訊安全法令規定、資訊作業程序、資訊安全事件或案例、資訊安全技術與其他相關知識。

(三)本公司及各子公司負責資訊安全事務之部門應定期舉辦資訊安全教育訓練，並符合「金融控股公司及銀行業內部控制及稽核制度實施辦法」及相關法令規定要求。

三、資訊系統安全管理

(一)各種作業系統環境配置、資料庫管理、資訊資源控管、換版作業管理、及系統結構變更管理等，並依系統特性建立相關之控管流程。

(二)為確保資訊系統或設備正常運作，應建立電腦病毒、挖礦等其他惡意程式預防及控制措施。

(三)應取得資訊系統或設備供應商已公布之技術脆弱性資訊，或定期執行伺服器弱點掃瞄，評估是否應採取適當的管控措施，以處理所面臨之風險。

(四)辦理各項資訊業務作業，應事先將資訊安全納入評估並對廠商進行審慎評估，明訂廠商之資訊安全責任及保密規定，並列入合約要求廠商遵守。

(五)應考量確保稽核軌跡資料的可用性、完整性、機密性、來源辨識性、不可重複性及不可否認性，並進行檢核且留下相關紀錄。

(六)使用雲端服務時，應符合相關法令或作業規定，如「金融機構運用新興科技作業規範」。

四、網路安全管理

(一)網路規劃或調整時，應對網路架構是否滿足營運需求及資訊安全進行考量。

(二)因業務或營運需要新增之設備，須遵照各網段使用之用途設計，未經授權不可任意交叉混用或串接。重要網段應施予適當防護及監控機制，例如：安裝防火牆或入侵偵測系統，定期檢視稽核紀錄等，且稽核紀錄不得被新增、刪除、修改。

(三)應明訂電子郵件使用規定，如需透過電子郵件或其他電子方式對外傳送含有客戶基本資料或涉及業務機密資料之文件，需經加密或電子簽章等安全技術處理後方可寄發。

(四)對外網站服務之資訊系統管理

1. 應視資料及系統之重要性，進行適當且有效之加密技術運用，以確保資料機密性、認證與資料完整性。
2. 防止資料及系統被入侵、破壞、竄改、刪除及未經授權之存取。
3. 對外網站公布資訊之新增、異動、刪除須經過正式授權，以確保公布資訊之機密性與完整性。
4. 網站存有個人資料及檔案，應加強安全保護措施，防止個人資料遭不當或不法之竊取或使用。

(五)應建立防火牆及其他必要安全設施加強網路安全管理，以確保網路傳輸資料與資源存取之安全性。

(六)所有人員不得私自串接外部網路與內部網路，並應設置必要之安全設施以保護內外部網路。

(七)利用公眾網路傳送機密等級資訊，應將資料加密保護，以保護資料在公眾網路傳輸的完整性及機密性，並保護連線作業系統之安全性，以避免其被未經授權之存取。

(八)使用者或廠商以遠端登入方式進入內部網路，應加強控管，採取特別的安全控管機制，如使用帳號密碼或其它認證機制。

五、應用系統存取管理

(一)應依其職務提出申請做為授權之依據，僅提供予使用者存取其已被特定授權使用之網路、系統及服務之存取，並防止未經授權之存取。

(二)對被賦予系統管理最高權限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

(三)特殊權限帳號，如具有資訊設備管理權限、特殊資料存取權限、其他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，並留存適當之稽核軌跡。

(四)使用者離/調職時，應確認取消或變更其各項作業權限。

(五)為加強使用者之控管，除受限於系統特性外，任何使用者帳號均需輸入密碼，以進行使用者身分識別與鑑別之作業。

(六)應建立通行密碼管理，如密碼原則及變更週期。

(七)爲確保對存取資料和資訊服務進行有效控制，應定期進行授權帳號權限之審視作業。

六、應用系統開發及維護管理

(一)自行或委外開發之系統，應於規劃分析階段，將資訊安全因素納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、後門、電腦病毒及惡意程式等危害系統安全。

(二)在程式撰寫階段，應將 OWASP 等常見的弱點納入開發安全參考，避免產生類似弱點，並執行程式碼安全檢測，以減少程式的安全漏洞。

(三)應用程式原始碼應進行適當管理。

(四)對廠商應規範及限制可接觸之系統與資料範圍。

(五)開發或維護應用系統、新購應用軟體於正式上線前，須經妥善之測試。系統開發及測試不可使用真實資料，如果測試作業必須使用真實資料，應評估控制措施來保護資料的機密性

(六)提供對外服務之資訊系統開發使用金鑰做為安全防護機制時，應考量金鑰的管理與保護方式。

(七)電子商務服務應依主管機關規定，應用系統開發人員應考量交易之特性及需求後，採取相關防護措施。

(八)提供客戶使用行動裝置程式之相關應用程式開發應符合金融監督管理委員會或公會公佈之作業基準，如「金融機構提供行動裝置應用程式作業規範」等。

(九)應用系統開發及維護管理應符合相關法令或作業規定。

七、電腦資產管理

(一)各項設備應設置適當之防護，以避免遭受損壞以致影響業務之持續運作。

(二)應採用行動裝置安全措施，以管理使用行動裝置所導致之風險。

(三)定期執行必要的資料、軟體備份及備援作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

(四)個人資料檔案應定期檢視是否需要存在，並定期進行刪除。資訊設備移交或汰換時應確認已刪除非關業務需要之個人資料檔案、機密性資料及授權軟體。

(五)委外處理的電腦設備、媒體蒐集及委外處理資料，應慎選具有足夠安全管理能力及經驗的機構作為委辦對象。

(六)應定期清查電腦安裝之軟體，以確保遵循智慧財產權之規定。

八、系統環境安全管理

(一)系統伺服主機、網路設備等應置於具有門禁管理、空調、電源供應穩定、防火、耐震與抗洪之管制區域內，以避免非法存取或破壞行為。

(二)無人看管之資訊設備，應考量以錄影監視或其他遠端監控設備控管。

九、資訊系統災害復原管理

(一)應訂定資訊系統災害復原計畫，評估各種人為及天然災害對正常業務運作之影響，並定期演練及調整更新計畫。

(二)應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應立即依「緊急事件因應要點」辦理及依內、外部規定相關程序進行通報。

十、其他資訊安全管理事項

(一)應確保所有委託他人處理內部資訊作業符合資訊安全要求。

(二)遵循內外部相關法令規定，建立對應之管控程序。

第 四 條　本準則如有未盡事宜，悉依主管機關相關法令與本公司相關規定辦理。

第 五 條　本準則經總經理核定後公布施行，修正時亦同。

中華民國一〇七年十二月十七日總經理核定

中華民國一〇九年七月二十三日修正(依金控內部規章制定及公告規則第三條及中華民國一〇九年六月十九日第七屆董事會一〇九年第三次會議修正通過)