兆豐金融控股股份有限公司資訊安全政策

108.03.26 第七屆董事會第 10 次會議訂定
114.6.24 第九屆董事會第 15 次會議第一次修正

第一條（定義及目的）

為強化資訊安全管理，建立安全及可信賴之資訊作業，確保資料、系統、設備及網路之機密性、完整性及可用性並保障客戶權益，特訂定本政策，以作為本公司及子公司實施各項資訊安全措施之依據。

第二條（適用範圍）

本政策闡明本公司及子公司員工應遵循之資訊安全政策，以及在資訊安全工作規劃、實踐與持續改進過程中所應扮演之角色與權責。

範圍包括：

一、組織與人員：所有員工、約聘雇人員、協力商及顧問等。

二、資料文件：所有資料、文件、公文與報告等。

三、軟體資訊資產：所有應用系統、工具程式、套裝軟體、資料庫、作業系統等。

四、硬體資訊資產：所有伺服器，個人電腦，儲存媒體，終端設備、通訊線路等。

第三條（管理範圍）

資訊安全管理之範圍應至少涵蓋下列事項：

一、資訊安全管理組織及權責。

二、人員安全管理及教育訓練。

三、資訊系統安全管理。

四、網路安全管理。

五、系統存取控制。

六、系統開發及維護之安全管理。

七、資訊資產之安全管理。

八、實體環境及環境安全管理。

九、營運持續管理。

十、資訊作業供應鏈之安全管理。

十一、其他資訊安全管理事項。

第四條（資訊安全管理運作機制）

本公司為統籌集團資訊安全管理事項，應定期召開集團資安會議，並由資安長擔任召集人及指派幕僚單位，負責執行與協調資訊安全會議相關之決議。

管理階層應支持並提供資訊安全管理必要之資源，以持續提升資訊安全管理量能。

第五條（遵循項目）

資訊安全應遵循之項目：

一、應考量業務發展現況及網路環境威脅，持續投入必要之資訊安全管理資源。

二、擁有之資訊資產應妥善保護，且在公司內部資訊系統、設備及網路資源上所處理、儲存或傳輸交換之資訊均歸屬公司財產，公司具有觀看、複製或取用之權利。

三、凡使用公司資訊以提供資訊服務或執行專案工作等，均有責任及義務保護其所取得或使用之資訊資產(含資料文件)，以防止遭未經授權存取、擅改、破壞或不當揭露。

四、應審查資訊作業相關協力廠商及顧問之資格，確認其所提供之技術、產品或服務滿足合約服務水準，及遵循本公司資訊安全與保密要求。

五、所有員工對所負責業務而持有之資訊資產(含資料文件)應負保管責任，確保重要資訊資產之機密性、完整性及可用性，防止其遭受意外或蓄意破壞、擅改、不當揭露或損失(包含實體或電子方式竊取)，以符合公司之營運利益並遵循相關法律及法規之要求。

六、維護保障資訊安全為每位人員之義務，當認知有違資訊安全之情事，應予即時防制並進行通報。

七、各項管理、行政及技術作業之發展、制訂及變更，應考量資訊安全之需求。

八、各項作業中獲知之資訊，其資訊保護及保密責任不因工作變更而滅失。

九、各項資訊資產之存取運用，包括電腦、網路設施及資訊系統等軟硬體之安裝、建置、發展、使用及維護，應參照相關的作業程序並獲得授權後方可執行。

十、應針對管理、業務及資訊等不同工作類別之需求，定期辦理資

訊安全教育訓練及宣導，建立員工資訊安全認知，提升公司資訊安全水準及資訊安全管理能力。

十一、應持續關注威脅情資資訊，並建立防病毒及防駭機制，保護資訊作業及相關資產，防止人為意圖不當或不法使用，遏止駭客、病毒等入侵及破壞之行為。

十二、為維護網路安全，防範電腦病毒之侵襲，應購買合法防毒軟體或關閉不必要之網路連線及服務，並定時更新相關病毒碼及掃毒引擎。

十三、對資訊安全事件應建立緊急通報機制，在發生資訊安全事件時，應依處理程序，立即向主管機關通報，並視業務需求訂定業務持續運作計畫，定期測試演練。

十四、所訂定之資訊安全措施，應符合適用之法律規範與本政策要求。

第六條（政策評估）

本政策每年至少評估一次，或於發生重大變動時重新評估，以符合相關法令、技術及組織、營運之最新發展現況。

第七條（未盡事宜規定）

本政策未盡事宜，依主管機關法令及本公司相關規定辦理。

第八條（實施及修正）

本政策經董事會通過後實施，修正時亦同。