兆豐國際商業銀行資訊安全政策

99 年 11 月 24 日第 13 屆第 16 次董事會核定
108 年 10 月 18 日第 16 屆第 15 次董事會修訂
111 年 6 月 10 日第 17 屆第 7 次董事會修訂
114 年 10 月 17 日第 18 屆第 8 次董事會修訂

第 一 條(目的及依據)

本行為強化資訊暨網路安全管理，建立安全及可信賴之作業環境，確保資料、系統、設備及網路安全，保障客戶權益，特依「資通安全管理法」、「金融控股公司及銀行業內部控制及稽核制度實施辦法」及「兆豐金控資訊安全政策」訂定本政策，以作為實施各項資訊安全措施之依據。

第 二 條(權責單位)

本政策之權責單位為資訊安全處。

第 三 條(資訊安全定義)

本政策所稱資訊安全，係指防止資訊系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

第 四 條(適用範圍)

本政策適用於本行所有員工(含勤務員及約聘雇人員)、顧問、協力廠商及委外廠商人員等。

第 五 條(組織及職掌)

本行應指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務。另設置資訊安全處為專責單位，負責規劃、監控及執行資訊安全管理作業。

第五條之一(資訊安全管理運作機制)

本行為統籌資訊安全管理事項，應定期召開資訊安全管理會議，由資訊安全長擔任召集人，並由資訊安全處負責執行與協調會議相關之決議。

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。

資訊安全處應於每年第一季結束前，將前一年度資訊安全整體執行情形提報董事會，另依「金融控股公司及銀行業內部控制及稽核制度實施辦法」第二十七條第一項規定，由資訊安全長聯名出具內部控制制度聲明書。

第 六 條(資訊暨網路安全管理範圍)

資訊暨網路安全管理範圍應至少涵蓋下列事項：

一、資訊安全政策之訂定與維護。

二、資訊安全組織與權責。

三、人員管理及資訊安全教育訓練。

四、資訊系統作業安全管理。

五、網路安全規劃及風險評估管理。

六、系統存取控制管理。

七、系統(應用系統)發展及維護安全管理。

八、資訊資產安全管理。

九、實體及環境安全管理。

十、業務永續運作計畫管理。

十一、資訊作業供應鏈安全管理。

十二、其他資訊安全管理事項。

第 七 條(資訊安全原則)

本行將依下列各項原則致力於各項作業安全,以達成降低資安風險衝擊本行營運、避免內部疏失傷害本行信譽及形象、堅持高品質的資安防護要求及維持客戶的信賴與保障客戶權益之目標：

一、進行各項作業時,應遵循主管機關頒布之各項法令及本行相關之規定辦理。

二、工作分派應考量職能分工,職務責任範圍應予區分,以避免資訊或服務遭未授權修改或誤用。

三、依本行員工招募方式進用相關人員,應視業務性質需要執行適當之背景調查。為規範員工對其所保管及使用資訊保密之目的,應要求所有員工簽訂保密合約。

四、應審查資訊作業相關協力廠商、委外廠商及顧問之資格,確認其所提供之技術、產品或服務滿足合約服務水準,及遵循本行資訊安全與保密要求,於業務性質有必要時,本行得要求其簽訂保密合約。

五、所有員工有義務保護本行機密敏感資料及客戶資料,禁止未授權的情況下接觸、使用或是將該資訊揭露、告知予與業務無關之同仁、廠商、顧問及其它客戶。

六、所有員工對於異常事件及有違反安全政策與程序之虞者,應隨時保持警戒,並依程序進行通報。

七、對資訊安全事件應建立緊急應變及通報機制,在發生資訊安全事件時,應依應變處理程序辦理,並立即向主管機關通報。

八、應定期執行網路安全風險評估、滲透測試和脆弱性評估,以監控資訊作業環境存在之弱點狀況。

九、應視業務需求訂定業務持續運作計畫,並定期測試演練,維持其適用

性。

十、本行各單位重大資訊配備（含軟、硬體）異動，應經資訊處協助技術及規格之評估，如經評估涉及資訊安全風險，應邀集資訊安全處共同參與。

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、應對所有員工施以資訊安全教育訓練及宣導，建立員工資訊安全認知，提升本行資訊安全水準及資訊安全管理能力。

十三、所有員工應參照相關作業程序並經授權方可存取運用各項資訊資產(含資料文件)，除應妥善保護且負保管責任，確保重要資訊資產之機密性、完整性及可用性，防止未經授權存取、擅改、破壞、不當揭露或損失，以符合本行營運利益並遵循相關法令要求。

十四、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。

第 八 條(作業規範)

資訊安全處及資訊處應依據本政策另訂相關資訊安全作業規範，供各單位遵循。各單位應秉持維護本行作業環境之資訊安全遵照辦理，以持續提昇各項作業服務之機密性、完整性與可用性。

第 九 條(政策評估)

本政策應至少每年評估一次，或於組織發生重大變動時重新評估，以反映政府法令、技術及業務等最新發展現況。

第 十 條(未盡事宜)

本政策未盡事宜，悉依相關法令及本行其他相關規定辦理。

第 十一 條(核定層級)

本政策經董事會通過後施行，修正或廢止時亦同。