資訊安全

資訊安全治理制度

安泰銀行為維護作業環境之資訊安全及服務客戶之理念，除基本必要之資訊安全控管措施，並且定期依照主管機關所修訂相關資安法規進行內部規章修訂，更落實推動資訊安全管理作業，以提昇本行之服務品質。另設立下列資安專責單位及組織，執行資訊安全相關管理作業：

- 設置「資訊安全專責單位」辦理本行資訊安全管理工作之規章研擬、管理方法設計、管理工作執行，執行結果監督、弱點改善與遵循資訊安全法規要求執行合規檢視。
- 資訊安全管理工作之規章研擬、管理方法設計、管理工作執行。
- 設立「資訊安全小組」每季定期評估資訊安全作業。
- 每半年定期召開「全行資安會議」，由資訊服務部最高督導主管主持，並邀請相關部門主管列席討論，審議有關電腦安全對策提案，並針對全行資訊安全執行情形進行研討。

「資訊安全專責單位」於會計年度終了後三個月內，將前一年度資訊安全整體執行情形，提報董事會通過，由董事長、總經理、總稽核及資訊安全專責主管聯名出具「資訊安全整體執行情形聲明書」，並依主管機關之規定揭露該聲明書內容。

資訊安全管理機制

本行資訊安全管理機制是以科技運用部署防護機制，以法令遵循持續檢視內部作業流程及規範

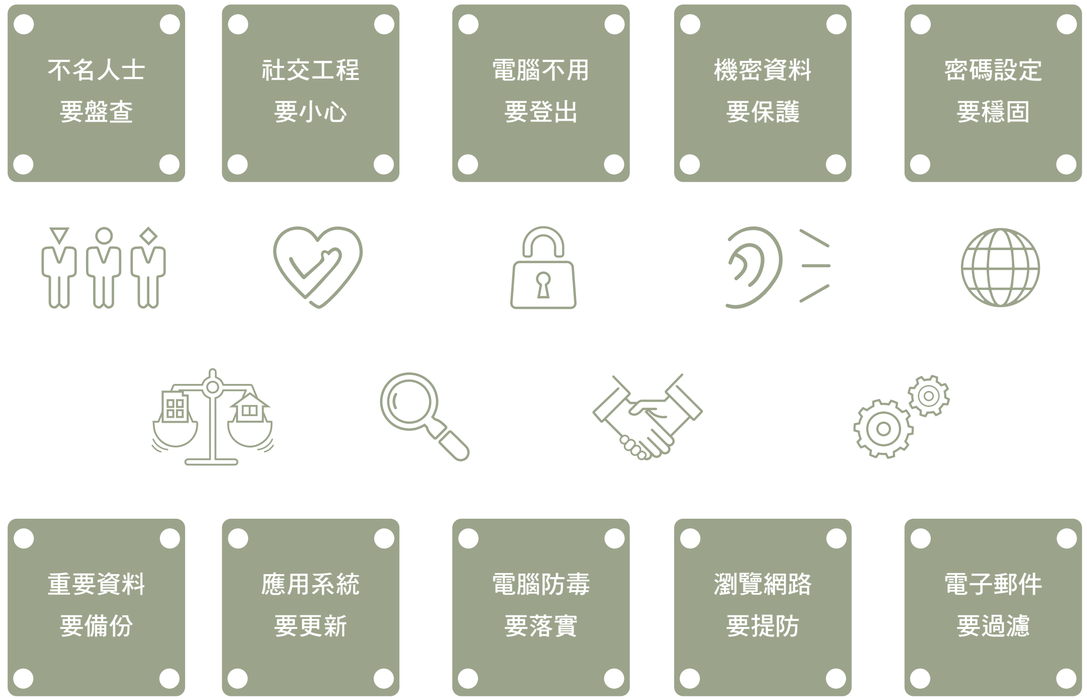
- 在Internet，DMZ及Intranet三大構面建置嚴謹的網路架構及各類防禦機制，包括防火牆、網路入侵防禦、網路防毒系統、網路應用程式防火牆、垃圾郵件防禦系統、對外電子郵件審核系統、微軟目錄服務系統及個人資料掃瞄工具等，以避免遭受資安威脅保障本行資訊安全。
- 為了強化人員之資安應變能力，對不同的資安情境進行各種程序演練 (如DDos，SWIFT，ATM)，並定期舉行備援演練、災變復原演練及社交工程演練。
- 定期實施行動裝置應用程式App安全檢測作業，並且取得行動應用App基本資安檢測合格，以維護所提供行動應用App使用安全。
- 因應資安威脅種類日益增加，本行於2018年加入F-ISAC金融資安情資中心，運用彼此資安情資分享與通報，對於立即性威脅及攻擊能夠及時掌握，並阻擋防禦以防止資安危害。
- 定期對全行同仁進行社交工程演練及實施資訊安全教育訓練，提高同仁資訊安全威脅意識，將資訊安全文化深植於日常工作。
- 為強化資安事故通報與應變處理，訂立資訊安全事故通報與處理作業程序以確保同仁面臨資訊安全事故發生時得以判別風險等級及因應有所依循，及時通報與處理得以降低對關鍵與重要資訊資產及作業的危害與損失。
- 為維護本行資訊設備及電腦系統安全，每年定期辦理電腦系統資訊安全評估專案，以利及時發現資安威脅與弱點，藉以實施技術面與管理面相關控制措施，以改善並提升網路與資訊系統安全防護能力。

教育訓練與宣導

安泰銀行「資訊安全行為要點」規範同仁正確資訊系統使用行為，以避免不必要資訊安全威脅及減少管理成本。資安人員每年須接受15小時以上資安專業課程或資安職能訓練，同仁每年須參加3小時資訊安全教育訓練，了解最新資訊安全威脅與建立良好資訊安全觀念。

另不定期透過內部公佈欄進行資安宣導，將近期發生之重大資安事件提供同仁了解參考，以及本行配合主管機關推行最新資安措施同步修正本行相關資安法規宣導，作為同仁資安防範及遵守依據。

個人資安防護良好習慣



數位資料保護

安泰銀行致力於保障客戶權益，針對客戶數位資料保護，採行相關防護措施，以期於意外發生時能確實保護數位資料安全，並降低可能之損害。

- 硬體管制措施：本行於內湖資訊機房設置門禁、防火設備及警衛等安全防護措施，用以防範天然災害及人為之強力蓄意破壞。
- 災變復原程序：於本行「資訊中心災變復原管理作業細則」訂立相關災變復原程序，於遭遇重大災變時，以保護員工優先，並於最短時間內恢復營運以保障客戶權益，確保企業持續經營。
- 異地備援機制：本行異地備援中心位於宏碁龍潭渴望園區。中心內建置專屬備援主機及Hot site即時備援方式，並每年定期舉辦一次災害備援演練，以確保異地備援系統之可用性。
- 個資掃描作業及採行相關防護措施：本行實施全行電腦資料定期個資掃描，確保所有個資均已加密保護。另針對本行內部傳送個資資料至外部採行系統嚴格監查機制，以確保個資資料安全。