

新光銀行資訊安全政策

2021.05.03 董事會核定實施
2022.02.23 第 09 屆第 083 次董事會核定實施
2025.02.12 第 10 屆第 083 次董事會核定實施
2025.08.27 第 10 屆第 111 次董事會核定實施

第一條 (目的)

臺灣新光銀行（以下簡稱本行）為提供客戶全方位的金融服務，確保資料、系統、設備及網路等各項資訊資產之機密性、完整性及可用性，強化資訊系統作業安全管理機制，避免受到任何形式的威脅，以期有效防範資訊安全事件的發生，使可能造成的有形及無形的損害降至最低，以確保公司的永續經營，並保障客戶權益，特訂定本政策，明確宣示本行高階主管支持資訊安全的決心，並使本行所有相關人員於執行資訊安全保護時有所依循。

第二條 (制定依據及授權)

本行依據「金融控股公司及銀行業內部控制及稽核制度實施辦法」、「金融機構資通安全防護基準」及母公司「資訊安全政策」等相關規範建立內部管理制度，以落實資安風險控管。

第三條 (適用範圍)

本行所有同仁、約聘僱人員及提供資通系統與服務之供應商均應共同遵行，並且適用所有相關的資訊組織、人員、實體與技術之安全管理作業。

第四條 (組織與權責)

本行設置資訊安全委員會統籌本行資訊安全相關事務，並指派副總經理以上或職責相當之人擔任資訊安全長，綜理資訊安全政策推動及資源調度事務。

本行設置具職權行使獨立性之資訊安全部為本行資訊安全專責單位，除配置適當人力資源及設備外，並指派協理以上或職責相當之人擔任資訊安全專責單位主管，負責規劃、監控及執行資訊安全管理作業。資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務。

第五條 (資訊安全目標)

為確保本行資料、系統、設備及網路等各項資訊資產之機密性、完整性及可用性，強化資訊系統作業安全管理機制，以保障客戶之權益，本行資訊安全目標，建構獨立資安職能、提升自我資安風險抵禦能力，並建立資安管理基準及自主風險評估機制。

第六條 (資訊安全管理)

本行資訊安全專責單位為落實資訊安全管理，應辦理以下事項：

- 一、依國際標準化組織(ISO)及國際電工委員會(IEC)制定之資訊安全管理要求(ISO/IEC 27001)及主管機關相關法令之規定，自資訊之組織、人員、實體與技術等面向建立安全管理制度，以落實資安風險控管。
- 二、每年將前一年度資訊安全整體執行情形向資訊安全委員會報告，並納入本行內部控制制度聲明書。

第七條 (資訊安全傳達)

本行應經由政策宣導、教育訓練或電子媒體等方式，將資訊安全政策傳達至所有同仁與配合本行業務之資通系統與服務供應商。

第八條 (定期檢討與授權)

本政策應每年至少檢討一次，以確保其合宜性、適切性及有效性；本行資訊安全之內部管理制度，由資訊安全專責單位依分層負責之授權另行訂定。

第九條 (附則)

本政策如有未盡事宜，悉依主管機關法令與本行相關規定辦理。

第十條 (修正程序)

本政策經資訊安全委員會審議，並提請董事會核定後公布實施，修正時亦同。