資通安全管理

項　　目	內　　容
1. 資通安全風險管理組織與架構	本行風險管理組織架構係以董事會為最高管理階層，設置風險管理委員會統籌全行風險管理，並於總經理下設置資訊安全委員會(每季召開，113年共開 4 次會議)負責全行資訊安全之風險管理，設置資訊安全處負責建立全行性資訊安全風險管理機制，行使全行資安治理之風險辨識、評估與管理。此外，總經理下另設置副總經理層級之資訊安全長，綜理資通安全政策之推動及資源之調度。
2. 資通安全政策	本行配合政府政策，提供社會大眾金融服務。為確保資訊資產之機密性、完整性、可用性及適法性，避免遭受內、外部蓄意或意外之威脅，爰導入國際資訊安全管理系統(ISO 27001)並參酌相關法令，根據本行之業務需求訂定資訊安全政策。
3. 資通安全風險管理系統	本行資通安全係以風險為本持續優化，建立資通安全風險管理系統，依據資訊資產之機密性，落實存取公司資訊之安全性，確保資訊作業處理方法之完整性、資料修改之正確性及資訊資產之可用性，以維持本行資訊系統之持續運作，資訊作業安全之措施均符合相關法令規定要求，資通安全環境符合國際金融資通安全評級。

項　　目	內　　容
4. 資通安全與網路之風險評估	本行每半年實施資安與網路之風險評估，並針對風險評估結果修訂適當資訊安全防護機制及緊急應變計畫，針對以下之資訊安全控制領域，實作各項安全防護機制及內部控制措施以確保資訊安全。 ■ 資訊安全組織。 ■ 人力資源安全。 ■ 資產安全。 ■ 存取控制。 ■ 密碼管理。 ■ 實體與環境安全。 ■ 作業管理。 ■ 通訊管理。 ■ 系統獲取、開發及維護。 ■ 供應商管理。 ■ 資訊安全事故處理。 ■ 營運持續管理。 ■ 遵循性。
5. 具體資通安全管理方案及投入資通安全之資源	本行以防禦縱深概念建立全面之網路與電腦相關資安防護措施，包括建置 DMZ 以區隔內/外部網段及防火牆(F/W) 、入侵防護(IPS)及程式防火牆(WAF)等防護設備，並因應主管機關之規範，已建立 SIEM 及委外 24 小時全天候 SOC 監控，期於最短時間內發現惡意攻擊，採取適當防護措施。此外，本行亦依主管機關之規定，每年辦理電腦系統資訊安全評估，進行弱點掃描、滲透測試、DDoS 攻擊演練等，以及資通安全事件演練，以強化資通安全防護之韌性。

項　　目	內　　容
6. 資安管理系統(ISMS)驗證	為顯示本行對資訊安全之重視及努力，已導入資安管理系統，於 2007 年通過認證，獲英國標準協會(BSI)頒發 ISO 27001:2005 資訊安全管理制度證書；嗣後並持續接受 ISO 27001 每半年複審及三年重審。2016 年通過英國標準協會(BSI)頒發 ISO 27001:2013 新版本資訊安全管理制度之認證。並於 2022 年三月間通過三年重審，效期為 2022 年 6 月 1 日至 2025 年 5 月 31 日。另為因應 ISO 頒佈 ISO27001:2022，本行業已完成相關作業調整，於 2024 年 11 月通過 ISO27001:2022 版認證。
7. 營運持續管理系統(BCMS)驗證	為顯示本行對服務客之重視及努力，確保本行於事故或災害發生時，能維持並快速回復至一定水準進行運作。將災害發生時所帶來的衝擊和中斷時間降至最低，並在危機期間能維持服務客戶。於 2022 年成立 BCMS 建置專案，於 2024 年 7 月通過認證，獲英國標準協會(BSI)頒發 ISO 22301:2019 營運持續管理系統(BCMS)證書，嗣後並持續接受 ISO 22301 每年複審及三年重審。
8. 資通安全保險之安排	本行將持續關注符合本行需求之資安保險產品。
9. 已發生重大資通安全事件之影響及因應措施	本年度無重大資安事件發生。