6.5 資訊安全

6.5.1 資訊安全機制

國泰配合金管會推動之「金融資安行動方案」，持續強化資安防護能力，達成安全、便利、營運不中斷的金融服務。國泰金控與主要子公司皆設有資安人員，且依法規要求設立資安長或是成立獨立資安專責單位，負責規劃、監控及執行資訊安全管理作業，並每年於董事會提報前一年度資安執行情形。而國泰金控設有資訊安全委員會，掌理集團資訊安全政策之擬議及管理制度之推展。

2021 年國泰金融集團最新資安重點則是韌性（Resilience）。國泰金控設有跨公司之金控資訊安全聯繫會以及金控資安事件緊急應變小組，全力投入資安控管及提升品質。此外，為即時掌握資安風險並能提早進行因應，國泰金控於 2020 年建立 7X24 資安監控中心（Security Operation Center）服務機制，以監控集團資安狀態，掌握資安風險。國泰也藉由外部專業資安顧問及應變團隊，以其業界豐富之資安事件應變經驗，提供適切且專業的建議與緊急應變支援。

國泰金控暨各子公司皆有訂定「資訊安全政策」，核決層級為董事會，透過每年定期檢視，確保資訊資產的機密性、完整性、可用性及適法性。國泰金控主要子公司國泰人壽、國泰世華銀行及國泰產險皆通過「ISO 27001:2013 資訊安全管理系統」國際標準認證，至 2021 年底止，全集團資訊系統導入 ISO 27001:2013 之涵蓋率達 97.2%，國泰金控亦於 2021 年起推動國泰證券、國泰期貨、國泰投信、國泰投顧導入 ISO 27001:2013 框架，預計 2022 年完成驗證，藉此完善資安治理架構與資安管理體系，並強化資安事件的預警、通報與應變流程，提供客戶安全無虞的金融服務。

6.5.2 從業務角度思考資安如何設計

國泰在應用面策略則採取「設計預設資安（Security by Design）」原則，在數位轉型的過程中，從業務角度思考資安如何設計在新的轉型專案中，秉持「事前預防」勝於治療的理念，在所有服務或商業模式設計之初，就將安全考慮進去。

因應數位轉型，不只軟體或程式得在一開始就安全開發，更重要的是，企業導入許多新興科技發展創新的服務模式或商業模式，皆應基於安全來設計。國泰在每個專案開始，資安人員就加入討論服務模式與商業模式的創新，站在業務端立場進行安全設計，也會讓企劃人員理解資安人員關心的議題，進一步培養人員的資安意識與文化。

6.5.3 資訊安全教育訓練

國泰金控重視資訊安全，定期舉行教育訓練及多元的宣導管道，提升員工資訊安全意識，確實落實資安控管。國泰金控暨各子公司每年皆對全體員工實施「資訊安全教育訓練」達 3 小時，各公司 2021 年完訓率皆達 100%，另資訊安全專責單位人員每年至少接受 15 小時以上專業資訊安全訓練。

此外，國泰金控暨子公司設置「集團資訊與威脅情資共享機制」，包含每月不定期國泰金控彙整並產出資安新聞報，提供國泰金控及各子公司資安單位使用，提升同仁資安意識並強化資安事件發生時的敏感度。

6.5.4 資訊安全侵害管理

國泰金控暨子公司於發現網路攻擊及惡意程式入侵等資安事件時，將啟動「資安事件通報暨緊急應變機制」，各公司之緊急資安事件應變最高層級皆為總經理，依循「國泰金控暨子公司重大資訊安全事件通報暨緊急應變管理要點」辦理，並統一由國泰金控彙整各公司重大資安事件呈報資安委員會。

為強化資安防護能力，國泰人壽[註]及國泰世華銀行每年請廠商執行白帽駭客滲透測試，2021 年起，國泰產險及國泰證券亦參與測試，以各式駭客手法分析可能遭遇駭客攻擊的漏洞與情境，包含連線狀態管理、存取權限測試、權限提升與跳脫等，針對檢測結果中的高風險項目均會進行改善，透過強化措施持續提升資安防護品質。此外，2021 年國泰金控暨各子公司皆由外部專業廠商執行電腦系統資訊安全評估，包含資訊架構檢視、網路活動檢測、弱點掃描與滲透測試、安全設定檢視、合規檢視等，據此追蹤系統安全狀況並實行改善措施，並針對其中重大風險及高風險項目改善完成率均達 100%，以確保資安無虞。

註：國泰人壽因新系統上線，延至 2022 年 2 月執行。