四、資訊安全

管理方針

衝擊說明 實際／正面／經濟 & 人權

Fintech 浪潮下，健全的資訊安全防護與顧客資料保護，為金融服務的基本配備。國泰投信遵循金管會「金融資安行動方案 2.0」，並發揮發揮資安聯防綜效，為客戶打造最完善、最具韌性的資訊安全交易環境。

行動

- 維持核心營運系統 BCM
- 提升資安團隊核心能力與人才培育
- 強化全體同仁資安意識與演練
- 完成企業網路資訊安全保險投保作業

政策與承諾

- 資訊安全政策

為維護各利害關係人的數位交易的安全，並強化國泰投信之資訊安全管理，建立安全及可信賴之資訊作業環境，以保障員工、客戶與本公司之權益。

目標

資訊外洩事件、個資相關資訊外洩事件、因資訊外洩事件而受影響的客戶數為 0。

評估機制

- 資訊安全相關課程及宣導完成率
- 資安事件通報演練達成率，並連結於全體同仁績效考核中

面對近年 Fintech 浪潮，國泰投信作為最大的資產管理公司，以「零碳運營・數位轉型」為願景，承襲集團 ESG 價值理念，投入許多資源優化資訊安全交易基礎建設，為兩百萬投資人提供便捷安全、友善環境的投資服務。

資訊安全政策與組織

為強化客戶數位交易安全與整體資訊安全防護，本公司持續建構安全、穩定且值得信賴的資訊作業環境。2021 年制定《資訊安全政策》，設置資訊安全長及「資訊安全管理小組」由資訊安全長擔任召集人，負責推動各項資訊安全管理作業、執行資訊安全管理小組之決策及日常資訊安全管理事務工作。

每年定期召開資訊安全管理審查會議，檢視制度之適切性與有效性，並持續精進改善。自 2022 年取得 ISO ／ IEC 27001 國際認證後，每年持續通過第三方驗證，確保資訊安全管理制度符合國際標準並穩健運作。

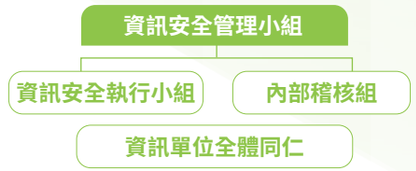
在資安預算上，國泰投信在主管機關強化金融韌性及金融資安行動方案的指導方針下，2025 年的資安預算為 3,566 萬，佔資訊類總預 36.42%。

國際認證


Certificate of Registration

Certificate of Registration

國泰投信資訊安全管理組織



國泰投信三大資訊安全政策（目標）

資安預算及資訊費用比例

年度	2023	2024	2025
資安預算金額（單位新台幣萬元）	5,288	5,242	3,566
資安佔資訊總預算比例	42.00%	37.04%	36.42%

2025 年資安預算投入資源佔整體資訊預算

36.42%

資安經費 (包括軟硬體授權費用、人員訓練費用) 占全部資訊預算費用之比率
2025 年資安預算：$35,666,664 元
2025 年整體資訊費用：$97,921,316 元

維持核心營運系統 BCM

國泰投信於 2022 年導入營運持續管理系統（BCM），並引用 ISO 22301 營運持續性管理系統標準，遵循國泰金控資安聯防、雙中心機房運作及全體同仁落實關鍵業務演練，實施管理系統以減少破壞性事件的影響，並建置從中斷恢復的回應機制，且因金管會「金融資安行動方案 2.0」，為於區域性災損時可維持核心業務運作，異地備援演練時，納入實際業務運作驗證，成功於 2022 年取得「ISO 27001:2013 資訊安全管理系統」及「ISO 22301:2019 營運持續管理系統」雙國際認證，也因此榮獲英國標準協會（British Standards Institution，BSI）舉辦之 2023 BSI 國際資安標準管理年會之「資訊韌性應變力獎」，為首家獲頒該項大獎的投信公司。

2025 年本公司於維持核心營運系統及設備營運所需之資源約 $6,439 萬，佔整體資訊預算 66%[註]。

註 : $64,387,915 ／ $97,921,316 元（2025 年整體資訊費用）=65.75%

持續營運管理資訊安全相關議題指標
重點資訊設施與實體管理

指標	措施／方案
網路安全控管	•對內網段依業務運作，達到管制不必要之連接埠開啟，降低風險 •對外防制駭客攻擊，採購各式防火牆與採購流量清洗服務 •加強管控減少資安漏洞，如防火牆及 WAF 申請開通、異動等作業均需進行申請、審核並每季定期檢視異動紀錄及使用狀況
資訊資產管理	•導入資訊安全管理系統（ISMS）及 ISO 27001 取得認證，落實資訊資產清查與管理 •藉由資訊資產清冊確實掌握資訊設備生命週期終止（End of Service, EOS ／ End of Life, EOL），提升資訊資產效率 設備維運檢查： •內部一設置固定拋送健康檢查（Health check）訊息以確認系統及設備維運正常 •外部一透過資通安全威脅偵測管理服務（Security Operation Center, SOC），確認監控設備是否異常 •資安監控廠商如 SOC、透過企業外部資安風險與安全績效管理評級系統等，提供定期新版產品教育訓練及案例分享
存取控制安全	•2021 年導入特權帳號管理暨代登系統，納管帳號、密碼降低密碼外洩之風險 •針對高權限之帳號進行所有使用狀態之監控，並納入集團「資訊安全監控中心」（Security Operation Center, SOC）監控 •針對新型態資安攻擊，透過企業外部資安風險與安全績效管理評級系統，由外部第三方單位偵測組織暴露在外弱點，即時進行修補 •由集團導入「外部偽冒偵測關閉及情資服務」（RSA FraudAction Service）、「暗網威脅情資服務」以達到防微杜漸之效
實體及環境安全	•委外廠商進行弱點掃描，以爭取時間提早進行弱點修補與評估補償性措施 •採購白帽駭客演練服務，預計於下半年進行紅隊攻防演練，以駭客角度瞭解組織需加強之資安面向 •因應公司「零碳運營．數位轉型」願景，將進行機房搬遷集團新建之機房，將藉由 DWDM 高速網路架構達到雙資訊機房，將成為投信業界首先導入之公司

資訊安全風險管理

國泰投信為強化整體資訊安全監控能力，遵循母公司金控資訊安全委員會決策，於 2020 年導入「資訊安全監控中心（SecurityOperation Center,SOC）服務」，彙整各種資安訊息，提供事前威脅的預警情報、事中威脅的即時告警以及事後威脅的分析建議，有效管理各種資安警訊，共同防堵資安威脅，讓公司可以即時瞭解內外部資安威脅，在第一時間內對資安事件做應變處理，將損害降至最低。

為確保資訊環境運作順暢及了解各項資訊資產可能產生的營運風險，國泰投信訂定「資訊資產安全管理暨風險評估作業管理辦法」，用以執行資訊資產安全管理及風險評估。定期及不定期依據各資訊資產的機密性、完整性與可用性依量化標準分級給予資訊資產價值高中低級別評分，同時以威脅發生機率以及威脅發生對營運造成之衝擊分別給定威脅權值和影響程度之評分。針對情資作業管理制定追蹤管理與處理流程，除 FISAC 金融資安資訊分享與分析中心外，廠商自主通報弱點與外部情資來源接收，並加入 HITCON ZeroDay 漏洞通報平台，主動識別與資訊資產相關之風險，及時應對漏洞與威脅。綜合上述各因子評分後給定各資訊資產風險評估值，並就風險評估值達一定程度之高風險項目進行風險轉移、減少弱點、降低威脅以及其它足以降低風險等措施或處置，以確保本公司資訊環境運作之安全順暢。

2025 年為持續精進資訊安全管理，全面檢視公司所有資訊暨資安相關規範，增修「網路通訊資料傳輸安全管理辦法」、「雲端服務運用作業細則」、「雲端 SaaS 服務運用作業細則」等規範。

2025 年資訊外洩事件數量 **0** 件

提升資安團隊核心能力與人才培育

國泰投信為提升資安團隊核心能力，投入大量的人力與資源強化資安人員之專業職能，持續提升資訊安全高度相關的資訊系統人員。此外持續增進營運持續管理能量，鼓勵資訊人員精進資安技能，投入大量資源鼓勵同仁獲取相關職安證照，國泰投信截至 2025 年底資訊維運與資安人員擁有金融資安行動方案中認可的證照達到 47 張，年年持續增長，其中 15 張為主導稽核員認證，也為導入資訊安全管理系統、營運持續管理系統奠下基石。

此外，國泰投信除資安專業人員的培育外，為遵循金管會「金融資安行動方案 2.0」，強化資安監理增進經營階層對資安的監督職能，本公司於 2025 年設立董事會資安諮詢小組，並聘請勤業眾信聯合會計師事務所擔任董事會資安諮詢小組成員，，提供董事會廣域專業諮詢，以增進對資安情勢掌握並實質將資安議題納入經營決策考量因子，帶動機構重視資安的組織文化。且於 2025 年提供董監事參加自辦「金融業零信任架構解析與因應」、「數位信任與永續發展」、「韌性即服務：金融機構如何利用雲端技術提升韌性」資安講座，並且確認所有董事皆完成資安訓練，以強化決策層級對於資安議題之即時掌握，裨益於資安政策推動協調與資源調度。並完成企業網路資訊安全保險投保作業包含事故應變、營運中斷、網路勒索、緊急事故應變及數據系統回復等，以預防並減緩降低業務中斷、客戶或第三人因受到損害而衍生之賠償風險。

國泰投信資安專職人員相關證照

證照（張）	2023 年	2024 年	2025 年
資安相關管理系統證照（ISO 27001、ISO 27701、ISO 22301）	10	11	19
ISC2 國際資訊系統安全認證協會	1	2	2
EC-Council	5	10	15
Information Systems Audit and Control Association（ISACA）	3	4	6
The Computing Technology Industry Association（CompTIA）	4	4	5
總計	23	31	47

1. 此表揭露 ISO 22301 證照僅包含資訊、資安專職人員所持有之證照數量
2. 員工取得資安防護證照之張數除以總資產之比率 47 ／ 73=64.38%
3. 2025 年經會計師查核後之合併資產總額為 7,381,265 千元 =73.81 億元

員工取得資安防護證照之張數之比率

64.38%

導入資安威脅情資蒐集及管理 (ISAC) 及反詐戰警專案

本公司自 2024 年導入資安威脅情資蒐集及管理（ISAC）及反詐戰警專案，與專業資安廠商團隊，透過偵測外部偽冒事件範圍包含釣魚詐騙（網站／網頁／郵件）、偽冒行動應用程式、社群媒體偽冒（含 Facebook,Instagram, LinkedIn, Twitter）及外部木馬事件，並且與全球 ISP／託管業者、各大入口網站及資安業者形成聯合防護網，萬一發現釣魚網站，RSA 可以立即協調聯防合作夥伴進行阻擋，避免客戶鏈接釣魚網站。並且運用大數據與 AI 反詐技術，快速聯防封鎖立即反應。

2025 年透過該機制，成功偵測 810 筆風險資訊（並成功下架 761 筆風險資訊），並即時回報相關主管機關。

強化全體同仁資安意識與演練

為深化員工資安意識，培養資安人員與全體員工的資安意識與應變能力，本公司依職務類型與職務層級，規劃由基礎教育至進階訓練的培訓機制，全面提升全體員工的資安意識與資安人員的專業技能：

對象	成效
一般同仁訓練	全體員工每年須完成至少 3 小時以上資安課程並通過測驗。2025 年，全公司資安課程完成率皆達 100%。
資安專責人員進修	平均每人每年受訓時數達 46 小時，遠高於法規要求之每年 15 小時標準。
董事會資安職能強化	為提升公司治理層對資安議題的理解與監督能力，亦針對董事設計資安專題訓練課程。2025 年董事資安訓練完訓率達 100%。

為將資安意識深化於日常工作中，本公司每月發送資安電子報，傳遞最新攻擊手法、防範技巧，期盼透過持續不間斷的宣導活動，厚植資安專業能量，也深化全員對資訊安全的重視。同時，本公司定期與外部機構合作實務演練，引入真實攻防情境與最新駭客手法，加強人員實務應對能力，培養團隊快速判斷與協作解決問題的能力。

2025 年資訊安全相關課程及宣導

課程及宣導	時數	參與人數	達成率
資訊安全訓練專職人員	323	7	100% 法規要求每人每年資安訓練時數 15 小時
資訊安全訓練一般員工 【資訊安全基礎認知】包含： 物聯網安全、密碼安全、網頁與郵件安全、語音網路釣魚、電腦病毒的認知與防範、辦公室作業環境安全防護、保護敏感性的資訊、遠距工作安全、深度偽冒（Deepfake）認知等相關主題	1,344	448	100% 法規要求每人每年資安訓練時數 3 小時

資安演練結果連結全體同仁績效
100 %

擁有金融資安行動方案中認可的證照
47 張

2025 年資安預算投入資源
36.42 %

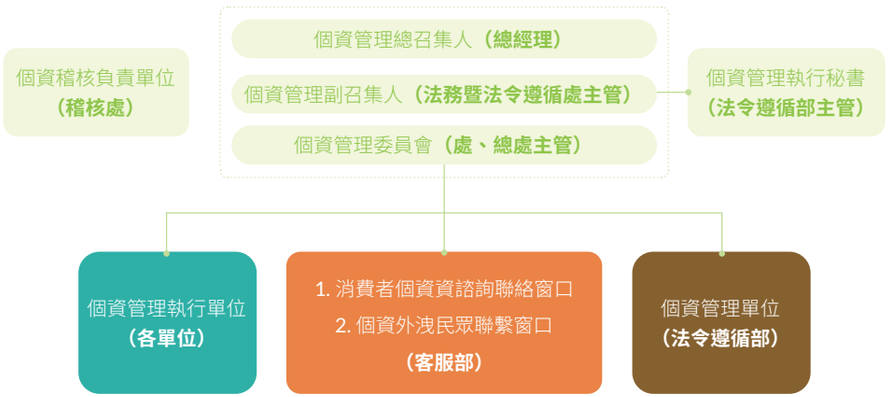
2025 年並未有資訊外洩事件發生
0 件

每月資安新聞報宣導

資訊安全演練成果		
演練專案	**說明**	**演練成果**
社交工程演練	造成業務營運遲緩全年度進行 4 次演練	提升人員資安意識
DDoS 演練	1 次實兵演練，請外部顧問進行實際攻擊包含 • 資源消耗型 DNS • 資源消耗型 HTTP 混合攻擊 • 頻寬消耗型 HTTP 攻擊	DNS 與網站服務皆可正常運作，確認防護機制有效
資安事件通報演練	公會主辦演練 2 次、投信主辦 2 次、金控主辦 2 次	增加人員熟練度及事故應變成熟度

個人資料保護

個人資料管理委員會組織架構



國泰投信為落實本公司保護客戶個人資料及交易資訊之職責，除履行《個人資料保護法》，於 2012 年成立個人資料管理委員會，負責協調、督導、檢討及改進本公司個人資料管理制度之運行，由總經理擔任總召集人，法務暨法令遵循處主管擔任副召集人，及法令遵循部主管擔任執行秘書，每年召開一次個人資料管理審查會議，不定期邀請個資專家於會議中指導，如 2022 年邀請安永會計事務所於會議中進行個資衝擊分析報告，且報備金控母集團會議結果。2023 年更優化個人資料保護作為，導入《桌面個資盤點系統》，讓公司精準掌握個資散布情況，進而落實管理、達到個資不外洩的目標，達成對客戶個資隱私權保障的承諾。

為防範未知之風險，國泰投信也於 2013 年訂立《國泰投信個人資料侵害事件緊急應變管理辦法》，因應若遭遇個人資料遭受侵害，相關之通報及應變程序，以俾降低侵害所造成之損害。2025 年度國泰投信資訊外洩事件數量、與個資相關資訊外洩事件占資訊外洩事件數量之比例、因資訊外洩事件而受影響的客戶數皆為 0。

2025 年個資保護相關專案作為		
專案	**執行頻率**	**完成率**
個資宣導	每月以電子郵件方式向全公司同仁宣導一次	100%
個資盤點	每年一次	
個資侵害事件緊急應變演練	二次	
個資電腦桌面個資掃描專案	每年一次	
個人資料管理審查會議	每年一次	
現行個資政策評估	每年一次	
DLP 系統檢視會議	每季一次	
NDLP 阻擋規則檢視	每年一次	