5.3 資訊安全

5.3.1 資訊安全管理

資訊安全政策

為管理資訊安全以降低資安風險，兆豐證券訂有經董事會通過之「資訊安全政策」及其相關辦法，並自 2023 年起導入並取得 ISO 27001 資訊安全管理系統認證及 ISO 22301 營運持續管理驗證並持續維持有效性。透過資安治理、法令遵循、風險控管與稽核審查等機制，結合科技應用提升資安防護能力，以符合國際標準。另訂有「資訊安全通報應變作業規範」，依事件分級（一至四級），進行通報與應變，以確保資通訊系統於遭受破壞或不當使用等緊急事故發生時，能迅速作出處置，以降低損害並維持資通訊系統正常運作。2025 年資訊相關費用為 368,312 仟元，其中資安經費為 43,650 仟元（包括軟硬體及相關授權共 43,504 仟元、資安相關教育訓練 146 仟元），資安經費占資訊費用比例由 2024 年 9.21% 提升至 11.85%。

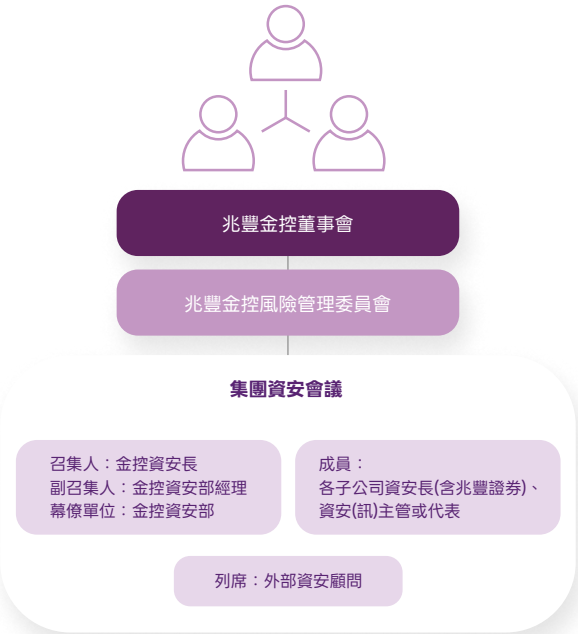
資訊安全政策

兆豐集團資安管理架構

兆豐金控為建立集團資安穩健基礎，每季召開集團資安會議，由金控資安長擔任召集人，並由子公司資安長、資安（訊）主管或指派代表參與會議，以統籌集團資訊安全管理事項，督導子公司完備資安相關規範、強化系統防護，建立金融資安聯防體系，以確實降低資安風險，如有重大議題或決議，則陳報至金控董事會及風險管理委員會（兆豐證券董事長亦為金控董事）。2025 年度共召開 4 次集團資安會議。

兆豐證券每年定期將前一年度資訊安全整體執行情形報告提交金控陳報其董事會；兆豐金控亦每年開辦集團董事、監察人資安專設課程，兆豐金控及子公司並共同委任集團資安諮詢顧問提供董事會資訊安全管理諮詢及參與集團資安會議討論，持續增納外部專業人員參與集團資安議題諮詢與建議。透過制度化會議、專業顧問導入及教育訓練，持續完善資安防護機制，並帶動集團重視資安的組織文化，確保永續經營。

此外，為進一步強化資安管理，除了使用集團資安顧問資源外，兆豐證券亦自行委任資安顧問，列席董事會針對兆豐證券年度資安計畫與執行情形提供建議以及分享金融資安認知，並協助審閱外部資安報告。



兆豐證券資訊安全小組

兆豐證券「資訊安全通報應變作業規範」明訂設置資訊安全小組(以下簡稱資安小組)並由各部門人員組成，進行資訊安全政策、計畫、資源調度等事項之協調、研議及資安事件之通報應變作業。資訊安全小組每半年召開一次資安會議，2025 年共召開 2 次會議。子公司兆豐期貨亦訂有「資訊安全政策」，每年定期召開資安會議，由總經理主持。

資安小組成員與權責劃分

資安小組成員	權責
資安小組負責人	為資訊本部主管，負責資訊安全管理事項之推動及資源調度，並於分級屬三、四級之資訊安全事件發生時，通報總經理。
資安小組召集人	由資安小組負責人指派資訊本部人員擔任，協助資安小組負責人，執行資訊安全管理事項。
各部門資安小組成員	由各部門主管指派 1 人為小組成員(如為事業群單位，則由事業群主管指派)，負責所屬部門內部應配合執行之各項事宜。

資訊安全小組織架構

資訊安全政策核准 ｜董事會

資訊小組負責人 ｜資訊本部主管

資訊小組召集人 ｜資訊本部人員

資訊小組成員 ｜各部門主管指派

資安事件暨通報流程

若資訊安全事件屬「兆豐證券重大偶發事件作業辦法」定義之資通安全事件或符合「資訊安全通報應變作業規範」重大資訊安全事件態樣，即應列為重大資訊安全事件，並執行金控及證交所或櫃買中心通報作業。2025 年度未發生資訊安全及網路安全之重大事件，亦未有相關裁罰金額。

- 應於通報重大偶發事件後，同步以電話或其他方式通知集團資安事件應變小組(簡稱 CSIRT 小組)執行秘書。
- 於次日起，三個營業日內再依兆豐金控「集團資安事件應變小組 CSIRT 組織設置要點」填列「集團資安事件應變通報單」傳送至 CSIRT 小組執行秘書。

應依「證券期貨市場資通安全事件通報應變作業注意事項」於金管會證券期貨市場資通安全通報系統進行資安事件通報作業；或經判斷符合重大資訊安全事件態樣者，須依據證交所「證券商通報重大資安事件之範圍申報程序及其他應遵循事項」，於 30 分鐘內填具「證券商重大資安事件通報單 - 初步(正式)通報作業」，並於通報重大資訊安全事件後，七個營業日內向證交所或櫃買中心函報詳細資料，填具「證券商重大資安事件通報單 - 結案通報作業」。

資訊安全管理機制與措施

對於科技發展所帶來的網路威脅與風險變化，兆豐證券持續檢視相關規範與措施之妥適性，建立完整的網路及電腦安全防護系統，每年進行系統弱點掃描及修補、執行滲透測試、社交工程演練、資通安全教育訓練等，並透過導入 ISO 27001 資訊安全管理系統驗證及建置 SOC(資訊安全監控中心)，確保資安與網路風險控管的適當性及有效性。與政府資安聯防方面，兆豐證券於 2025 年連續二年獲金融資安資訊分享與分析中心年度「F-ISAC 會員情資分享」評鑑優等。

資訊安全管理措施	2025 年兆豐證券資訊安全管理措施及執行情形
資訊安全管理作業	» 設有資訊安全長，綜理資訊安全政策推動及資源調度事務，並於資訊本部下成立資訊安全部，定期每半年召開資訊安全會議，以進行資訊安全制度之規劃、監控及執行資訊安全管理作業。 » 對兆豐證券各對外交易系統每日自動做程式版本比對，如有異常，即通知相關負責人員處理。 » 專人定期查詢是否有外部網站非法偽造兆豐證券官網之釣魚網站或偽冒兆豐證券 APP。如有發現，提醒投資人注意及通報金融資安資訊分享與分析中心 (F-ISAC)。 » 採購原始碼安全檢測工具與第三方元件檢測工具，用以檢測公司所開發維護之應用程式，可提早發現可能之潛在風險並及時修補，以強化公司資訊安全。 » 加入金控集團偽冒網站偵測機制，並與內政部警政署簽署「金融阻駭反詐暨資安聯防」合作意向書 (MOU)，有效下架偽冒網站及臉書帳號。 » 弱點掃描：每年不定期進行弱點掃描作業，並針對弱點進行改善與持續追蹤，以提早發現潛在資通安全威脅與弱點，強化資通系統安全防護能力；每兩年委請資訊廠商進行資通安全健檢服務，藉由健診結果，瞭解隱藏之資訊安全弱點，以做為未來規劃加強資訊安全管控時之參考依據。 » 滲透測試：每年定期委由第三方機構完成所有對外服務之滲透測試，經過檢測後未發現任何重大風險。 » 社交工程演練：每年定期執行電子郵件社交工程演練，並進行員工資安教育訓練及資安相關議題宣導，提升員工資安意識強化。 » 持續營運管理：每年定期辦理業務持續運作演練作業 (包含證交所連線下單測試，每半年執行異地備援市場實況模擬測試)，確保重要系統可持續提供關鍵服務，驗測結果以執行備援機制可使系統服務正常持續運作。
資訊安全管理系統	» 為將資安制度標準化與國際化，兆豐證券已完成 ISO 27001 資訊安全管理系統之導入及第三方驗證，並持續辦理第三方複查，及核心系統已導入營運持續管理制度並通過公正第三方 (BSI) 之 ISO 22301 驗證，維持證書之有效性。(證書請見附錄 9.3 外部獨立驗證聲明) » 建置資料外洩防護系統 (Data Loss Prevention；DLP)，針對個資進行監控及阻擋，以降低個資外洩風險。 » 每年針對行動應用程式 (兆豐行動 VIP) 進行第三方實驗室資安檢測作業，以加強此 APP 資訊安全。 » 建置電子郵件過濾系統 (Softnext SPAM SQR)，以強化公司電子郵件資訊安全。 » 建置端點設備自動化管理系統 (Security Intelligence Portal; SIP)，以防止未經授權設備使用內部網路。 » 建置個人電腦最高權限管理系統，集中管理全公司 Client 端之個人電腦最高權限，以強化公司資訊安全。 » 建置網站應用程式防火牆 (Web Application Firewall, WAF)，提升資訊安全。 » 建置 IDS/IPS- 入侵偵測及防禦機制系統，以強化公司資訊安全。 » 建置主機特權帳號管理系統，集中管理各系統特權帳號，以提升公司資訊安全。 » 導入阻斷服務攻擊 (DDoS) 防禦機制，防堵 DDoS 攻擊。 » 資訊安全監控中心 (SOC)：已建置 SOC(資訊安全監控中心)，進行資訊防護機制、儲存媒體管控機制及 IDS 資安防護，以強化資訊安全監控及防禦。
資訊安全意識培養	» 定期對公司全體同仁進行資訊安全宣導及教育訓練，以加強同仁資訊安全意識，內容包括深度偽造認知及防範議題。兆豐證券暨子公司 2025 年共辦理 6 場教育訓練，共 3,270 人次完訓，教育訓練總時數達 9,810 小時，平均每人受訓 3 小時。 » 積極投入資源培育資安人才，設有資安證照補助制度，鼓勵員工主動精進資安技術能力，維持自身專業性。

5.3.2 客戶隱私與個資保護

兆豐證券為善盡個人資料及客戶隱私資料保密之職責，已依「個人資料保護法」等法規訂定「個人資料保護管理政策」、「個人資料檔案安全維護計畫及業務終止後個人資料處理方法」等內部規範蒐集、處理及利用客戶資料，並透過納入內控系統、辦理員工教育訓練、定期執行個人資料現況盤點、風險評估、安全維護自我評估作業，每年亦委由第三方機構進行個人資料保護管理系統之持續審查及驗證，以確保落實客戶隱私與個資保護。2025 年兆豐證券通過 BS 10012 個人資料保護管理系統第三方持續審查及驗證。

兆豐證券暨子公司之「員工行為準則」、「員工獎懲辦法」及「兆豐金融控股公司及其子公司客戶資料保密措施」規範員工應對公司資訊及客戶隱私資料負保密義務，非依法令或經核准不得洩漏，離職後亦同，若有違反保密措施規定者，除立即終止使用公司資訊之權限，並依公司懲處相關規定提報議處及追究法律責任，以示公司對個資保護與客戶隱私權之重視。

兆豐證券暨子公司僅於合法情況下允許政府、主管機關或證券暨期貨週邊單位索取客戶隱私相關資料，並無其他不合法索取資料之情事，也無使用客戶資料進行二次行銷之行為，或發生侵犯客戶隱私權或遺失客戶資料之事件。

倘若發生個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故，兆豐證券將依據「個人資料檔案安全維護計畫及業務終止後個人資料處理方法」，啟動通報機制：發生重大個人資料事故時，應依「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第六條第二項規定，於 72 小時內按主管機關規定格式通報金融監督管理委員會。但於其他法令另有規定時，並應依各該法令之規定辦理。

2025 年度「個人資料保護教育訓練課程」執行情形

相關教育訓練課程主題內容
1. 2025 年個資保護宣導教育訓練
2. 個資保護內部稽查方法教育訓練
3. 業務流程及個資清冊說明教育訓練
4. 檢舉與個資保護法令與實務
5. 個資與人工智慧的雙刃劍

8
課程次數（場次）

3,326
受訓人次

5,007
課程總時數

兆豐證券暨子公司 2025 年度未發生資訊及個人資料外洩事件，且無因資訊外洩事件而受影響的客戶與員工，故無相關罰款支出。

資訊外洩事件	2023	2024	2025
來自外部各方並經由組織已證實的投訴	0	0	0
來自監管機關的投訴	0	0	0
資訊外洩事件數量	0	0	0
與個資相關的資訊外洩事件占比 (%)	0	0	0
因資訊外洩事件而受影響的顧客數	0	0	0

0
無資訊外洩事件

☆ 亮點案例｜兆豐證券總公司及忠孝分公司通過 BS 10012 國際個資保護認證

兆豐證券積極提升企業韌性與風險管理能力，再添國際認證肯定。繼通過 ISO 27001 資訊安全管理系統、ISO 22301 營運持續管理、營業部 BS 10012：2017 個人資訊管理系統等認證後，2025 年總公司及忠孝分公司再取得 SGS 台灣檢驗科技股份有限公司 BS 10012：2017 個人資訊管理系統 (Personal Information Management System PIMS) 認證。此次擴大範圍通過 BS 10012 認證，展現公司在個資保護及資安管理的努力以及已達到國際標準，不僅強化個資保護的制度及配套措施，也進一步確保未來個資處理的安全性，提升客戶對公司資料保護的信心。（證書請見附錄 9.3 外部獨立驗證聲明）