4.4 資訊安全

4.4.1 資訊安全管理

為統籌資訊發展與資訊安全管理事項、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」、「資訊安全政策－系統存取控制」等相關辦法，並於 2023 年持續導入並取得國際資安認證 ISO27001 資訊安全管理系統，同年並取得 ISO 22301 驗證，經由資安治理、法令遵循、風險控管與稽核審查等機制運作，配合科技運用，全面提升資安防護能力。此外，並訂有「資訊安全通報應變作業規範」，對資訊安全事件分級管理（分一至四級），以掌握資通訊系統遭受各項因素破壞或不當使用等緊急事故發生時，能迅速作必要之通報及應變處置，以降低可能之損害發生機率，確保公司各資訊通訊系統之正常運作。

兆豐證券股份有限公司
資訊安全政策

資訊安全小組

一、 兆豐證券設有資訊安全小組（以下簡稱資安小組）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，每半年召開一次資安會議。

二、 資安小組成員與權責劃分如下：

1. 資安小組負責人：為資訊本部本部主管，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。
2. 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。
3. 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。

◆ 管理架構圖

資訊安全小組組織架構

- 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

資安事件通報流程與資安事件

若資訊安全事件屬兆豐證券重大偶發事件作業辦法第二條第一項第六款定義之資通安全事件或符合本規範第三條第三項重大資訊安全事件態樣，即應列為重大資訊安全事件，並執行下列作業：

1. 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。
2. 填寫「重大偶發事件通報單」，並於事實發生日之次一工作日 17 時前完成通報兆豐金控作業。
3. 應依「證券期貨市場資通安全事件通報應變作業注意事項」於證券期貨市場資通安全通報系統（https://sfevents.twse.com.tw/）進行資安事件通報作業；或經判斷符合本規範第三條第三項之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」，執行下列作業：
   (1) 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」。
   (2) 通報重大資訊安全事件後，應於七個營業日內向證交所或櫃買中心函報詳細資料，並填具「證券商重大資安事件通報單 - 結案通報作業」，包括事件發生時間、事件發生原因、事件分類、對證券商及投資人造成之影響、有無敏感資料外洩、處理措施、恢復情形、事件後續處理進度、投資人糾紛處理、改善情形及相關預防措施等。
   (3) 若因不可抗力之情事致無法於七個營業日內函報者，經通報證交所或櫃買中心核備後，得以延後函報期限。

兆豐證券 2023 年度未發生資料（含個人資料）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	2021 年	2022 年	2023 年
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

資訊安全精進措施

1. 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，編制資訊安全主管 1 名及資訊安全人員 3 名，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。
2. 核心系統導入資訊安全管理系統，並通過公正第三方 (SGS) 之 ISO 27001 驗證，且持續維持驗證有效性 (效期至 2025 年 10 月 31 日)。
3. 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。
4. 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。
5. 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)。

6. 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。
7. 定期對公司全體同仁執行社交工程演練作業，以提升同仁資訊安全意識。
8. 定期執行系統、網頁弱點掃描與入侵滲透測試，以強化公司資訊系統安全。
9. 定期執行異地備援市場實況模擬測試，以確保備援系統有效性。
10. 每年針對兆豐證券行動應用程式 (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。
11. 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。
12. 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。
13. 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。
14. 建置網站應用程式防火牆 (Web Application Firewall, WAF)，提升兆豐證券資訊安全。
15. 建置 IDS/IPS- 入侵偵測及防禦機制系統，以強化公司資訊安全。
16. 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。
17. 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。
18. 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，瞭解兆豐證券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。
19. 主要資安設備導入資訊安全監控中心 (SOC)，以強化公司資訊安全監控及防禦。
20. 核心系統導入營運持續管理制度，並通過公正第三方 (BSI) 之 ISO 22301 驗證，且持續維持驗證有效性 (效期至 2026 年 12 月 27 日)。
21. 為維持系統穩定，已完成升級交易系統中台作業系統及資料庫 (APGW)。
22. 完成建置記錄伺服器，將 Log 集中管控。

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，每年不定期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。2023 年度實際資安支出 (包括軟硬體及授權相關費用) 占 2023 年度資訊預算比例為 5%，其中兆豐證券持續核心營運系統及設備營運 2023 年實際支出占 2023 年核心營運系統及設備營運預算 82.63%。

資訊安全管理措施	2023 年兆豐證券資訊安全管理措施及執行情形
資訊安全監控中心 (SOC)	已建置 SOC(資訊安全監控中心),進行資防護機制、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。
弱點掃描	每年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。
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,對於釣魚郵件有更高的警覺性。
持續營運測試	每年辦理業務持續運作演練作業,確保重要系統及備援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 27001:2013 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,維持證書之有效性。(證書請見附錄 8.3 外部獨立驗證聲明)

資訊安全教育訓練

近年資訊安全已成為金融業 ESG 重點,對客戶的資安防護是兆豐證券核心項目,為確保員工具備資訊安全知識與提升意識,每半年辦理資訊安全相關教育訓練,並透過線上授課讓員工每年提升資安知識以因應多變的資安議題。2023 年教育訓練執行 2 場,共 3,033 人次完訓,教育訓練總時數達 9,099 小時,平均每人受訓 3 小時。

2023 年度其他資安管理亮點案例	
案例內容	兆豐證券已完成國際資安認證: 1. 經紀業務核心系統 ISO22301(營運持續管理制度) 驗證 (有效期間 2023.12.28 至 2026.12.27) 2. ISO/IEC 27001:2013 持續驗證 (有效期間 2023.7.12 至 2025.10.31)
重點績效成果	1. 2023 年 12 月 28 日通過經紀業務核心系統 ISO22301(營運持續管理制度) 驗證。 2. ISO 27001:2013 持續驗證 (資訊安全相關之管理活動,包括機房管理、網路管理以及證券交易中台系統、後台系統、前台系統、行動 VIP 、E 網通、全球理財通、 HTS(Home Trading System) 、兆豐贏家、兆豐 API 、嘉實 API 、 Multi Chart 、 E 雷達及財富管理系統之開發、維護與管理。) (有效期間 2023.7.12 至 2025.10.31)
新聞稿 / 照片 / 相關資訊公開連結	詳 ISO22301 及 ISO 27001 驗證證書,證書請見附錄 8.3 外部獨立驗證聲明。

4.4.2 客戶隱私與個資保護

兆豐證券對個人資料及客戶隱私資料善盡客戶資料保密之職責，訂定「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」，敘明依「個人資料保護法」、「個人資料保護法施行細則」、「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」等相關規定，蒐集、處理及利用客戶資料，訂定客戶資料安全管理措施，並且透過客戶個資保護納入內控系統、辦理員工教育訓練，以及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，確保落實客戶隱私與個資保護。

此外，為了成為客戶最信賴的夥伴，兆豐證券「公司員工行為準則」、「公司員工獎懲辦法」及「兆豐金融控股公司及其子公司客戶資料保密措施」規範員工對於公司資訊及客戶隱私資料應負保密義務，非依法令或經核准不得洩漏，離職後亦同。若員工有違反本準則與保密措施之規定者，將立即終止違法員工使用公司資訊之權限，並按情節輕重，依公司懲處相關規定提報議處並追究其法律責任，以示兆豐證券對個資保護與客戶隱私權之重視。

兆豐證券僅於合法情況下允許政府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，或是發生侵犯客戶隱私權或遺失客戶資料之事件。

客戶資料被二次行銷使用情形	2021 年	2022 年	2023 年
客戶資料被二次行銷使用之客戶數（可為帳戶數）	0	0	0
總客戶數（可為帳戶數）	384,996	408,600	434,115
客戶資料被二次行銷使用之客戶數百分比 (%)	0	0	0

資訊安全事件	2021 年	2022 年	2023 年
資訊安全事件總數	0	0	0
因資訊安全事件導致顧客資料遺失數	0	0	0
因資訊安全事件受影響的顧客數	0	0	0

2023 年度「個人資料保護教育訓練課程」之執行情形

相關教育訓練課程主題內容	課程次數（場次）	受訓人次	課程總時數（= 受訓人次 x 每次課程時數）
1. 2023 年企業誠信經營守則、個資法、檢舉制度及性騷擾防治辦法線上課程 2. 2023 年度法遵講座 _ 檢舉案件處理及個資保護 3. 2023 年個資強力監管時代來臨 4. 以去識別化達到個資最大的利用價值	4	1,671	3,479