

兆豐金控
兆豐期貨
資訊安全政策
(IT-A02-11)

兆豐期貨股份有限公司－資訊部
中華民國 108 年 12 月 17 日



第一條 目的

兆豐期貨股份有限公司（以下簡稱本公司）為強化資訊安全管理，保護本公司資訊資產，免於遭受內外蓄意或意外之破壞，特制定本資訊安全政策，以作為實施各項資訊安全措施之標準。

第二條 制定範圍

本政策係依據主管機關等有關法令，考量本公司業務需求訂定，並以書面、電子或其他方式告知所屬員工及提供資訊服務之廠商共同遵行。

本政策之範圍如下，有關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效，以反映相關法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性：

- 一、安全教育訓練。
- 二、電腦系統安全管理。
- 三、網路安全管理。
- 四、系統存取控制。
- 五、應用系統開發及維護安全管理。
- 六、資訊資產安全管理。
- 七、實體及環境安全管理。
- 八、業務永續運作計畫之規劃與管理。

第三條 組織及權責

各部門應依下列分工原則，配賦有關單位及人員之權責：

- 一、資訊安全政策、計畫及技術規範之研議、建置及評估等事項，由資訊單位負責辦理。
- 二、資料及資訊系統之安全需求研議、使用管理及保護等事項，由業務單位負責辦理。
- 三、資訊機密維護及稽核使用管理事項，由稽核單位會同相關單位負責辦理。

第四條 範圍說明

人員管理及資訊安全教育訓練

- 一、應針對各單位管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導並通過評量，以建立員工資訊安全認知，提升公司資訊安全水準。
- 二、應加強各單位資訊安全管理人力之培訓，提升資訊安全管理能力。
- 三、各單位資訊安全人力或經驗如有不足，得洽請外部專家或專業機關(構)提供顧問諮詢服務。
- 四、各單位負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，



- 分散權責，並視需要建立制衡機制，實施人員輪調，建立人力備援制度。
- 五、各單位最高主管及各級業務主管人員，應負責督導所屬員工之資訊作業安全，防範不法及不當行為。
- 六、電腦網路安全(如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等)之事項需對內部隨時公告。

電腦系統安全管理

- 一、辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並定期考核。
- 二、對重要系統變更作業，應建立控管制度，並建立紀錄，以備查考。
- 三、應依相關法規或契約規定，複製及使用軟體，並建立軟體使用管理制度。
- 四、應採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。
- 五、禁止以任何方式，進行任何會危害公司資訊安全之行為，例如洩漏或竊取公務所知悉之資訊，竄改公司資訊資料，損毀公司資訊資產之資料（例擅自格式化、使用還原程式或刻意破壞個人 PC 內部資料等）。
- 六、建置「資料外洩防護系統(Data Loss Prevention；DLP)」自動判別高風險個資及加密檔案，並保存相關個資傳送記錄。
- 七、本公司發生個人資料之竊取、竄改、毀損、滅失或洩漏等安全事故者，應即函報期交所及副知主管機關。

網路安全管理

- 一、利用公眾網路傳送資訊或進行交易處理，應評估可能之安全風險，確定資料傳輸具完整性、機密性、身分鑑別及不可否認性等安全需求，並針對資料傳輸、撥接線路、網路線路與設備、接外連接介面及路由器等事項，研擬妥適的安全控管措施。
- 二、應定期評估自身網路安全。
- 三、開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。
- 四、與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與機關內部網路之資料傳輸與資源存取。
- 五、開放外界連線作業之資訊系統，必要時應以內、外部網站區隔等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料。
- 六、利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。公司網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭不當或不法之竊取使用。
- 七、應訂定電子郵件使用規定，機密性資料及文件，不得以電子郵件或其他電



子方式傳送。機密性資料以外之敏感性資料及文件，如有電子傳送之需要，應視需要以適當的加密或電子簽章等安全技術處理。業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。

- 八、應建置電腦使用者 IP 配置表，包含控管外來電腦所使用的 IP，以便即時隔離中毒電腦，阻絕繼續擴散。

系統存取控制

- 一、應訂定系統存取政策及授權規定，並以書面、電子或其他方式告知員工及使用者之相關權限及責任。
- 二、應依資訊安全政策，賦予各級人員必要的系統存取權限；公司員工之系統存取權限，應以執行業務所必要者為限。對被賦予系統管理最高權限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權評估。
- 三、離（休）職人員，應立即取消使用公司內各項資訊資源之所有權限，並列入公司人員離（休）職之必要手續。公司人員職務調整及調動，應依系統存取授權規定，限期調整其權限。
- 四、應建立系統使用者註冊管理制度，加強使用者通行密碼管理，並要求使用者定期更新。
- 五、開放外界連線作業，應事前簽訂契約或協定，明定其應遵守之資訊安全規定、標準、程序及應負之責任。
- 六、對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。
- 七、重要資料委外建檔，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。
- 八、應確立系統稽核項目，建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業；系統中之稽核紀錄檔案，應禁止任意刪除及修改。
- 九、應訂定設備報廢作業程序，報廢前應將機密性、敏感性資料及授權軟體予以移除或實施安全性覆寫，若委託第三者銷毀時，應簽訂保密合約。

應用系統開發及維護安全管理

- 一、自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。
- 二、對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用。但使用完畢後應立即取消其使用權限。
- 三、委託廠商建置及維護重要之軟硬體設施，應在公司相關人員監督及陪同下始得為之。

資訊資產安全管理



- 一、建立與資訊系統有關的資訊資產目錄，訂定資訊資產的項目、擁有者及安全等級分類等，且應指派專人管理資訊資產目錄並隨時更新。
- 二、依據相關法規，建立資訊安全等級之分類標準，以及相對應的保護措施。
- 三、已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

實體及環境安全管理

就設備安置、周邊環境及人員進出管制等，訂定妥善之實體及環境安全管理措施。

業務永續運作計畫之規劃與管理

- 一、訂定業務永續運作計畫，評估各種人為及天然災害對機關正常業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。
- 二、建立資訊安全事件緊急處理機制，在發生資訊安全事件時，依規定之處理程序，立即向權責主管單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。
- 三、應依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及充足之資訊安全措施。

電子郵件社交工程防護

- 一、為提升人員電子郵件社交工程防護觀念，證券母公司資訊本部將會定期執行下列作業：
 - (一) 每月宣導如何防範惡意電子郵件。
 - (二) 每半年進行一次電子郵件警覺性測試作業，並針對測試統計結果進行下列作業：
 1. 對於連續兩次以上都被誘騙成功之人員，通知本人及其單位主管。
 2. 連續三次都被誘騙成功之人員，另通知其單位主管建議將其列入該員年考核之評分參考。
- 二、如人員不慎點選惡意電子郵件，導致電腦/通訊/資料檔案發生異常，應立即拔除網路線或關機，並通知資訊部協助處理後續作業。

第五條 其他

本政策應至少每年評估一次，以反映相關法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

第六條 核准層級

本政策經 董事會核定後實施，修正時亦同。

第七條 修訂履歷

本政策制定 97 年 3 月 3 日。



本政策第一次增訂 98 年 2 月 17 日。
本政策第二次沒有增訂 99 年 12 月 31 日。
本政策第三次增訂 100 年 3 月 02 日。
本政策第四次沒有增訂 101 年 12 月 31 日。
本政策第五次增訂 102 年 11 月 11 日。
本政策第六次增訂 103 年 11 月 27 日。
本政策第七次增訂 104 年 12 月 16 日。
本政策第八次增訂 105 年 12 月 12 日。
本政策第九次增訂 106 年 08 月 01 日。
本政策第十次增訂 108 年 01 月 22 日。
本政策第十一次增訂 108 年 12 月 17 日。