台中銀證券股份有限公司
資訊安全政策

103 年 2 月 11 日初版
103 年 12 月 15 日第一次修正
104 年 12 月 04 日第二次修正
105 年 12 月 30 日第 2 屆第 6 次董事會通過
106 年 12 月 5 日第 2 屆第 16 次董事會通過
107 年 12 月 10 日第 2 屆第 26 次董事會通過

第一條　政策依據參考

為強化本公司資訊安全管理，以期整體資訊業務順利進行，特依據台灣證券交易所「建立證券商資通安全檢查機制」，訂定本政策。

第二條　資訊安全之定義

資訊安全係將管理程序及安全防護技術應用於各項資訊作業，包含作業執行時所使用之各項資訊系統軟、硬體設備及存放各種資訊及資料之檔案媒體，以確保資訊蒐集、處理、傳送、儲存及流通之安全。

第三條　資訊安全之目標

確保電腦使用安全、維護資訊機密及加強作業管制，俾整體公司業務順利運作，永續營運，進而建立安全及可信賴之資訊環境。

第四條　資訊安全之範圍

一、　資訊安全政策訂定。
二、　資訊安全權責分工。
三、　人員管理及資訊安全教育訓練。
四、　電腦系統安全管理。
五、　網路安全管理。
六、　系統存取管制。
七、　系統發展及維護安全管理。
八、　資訊資產安全管理。
九、　實體及環境安全管理。
十、　業務永續運作計畫管理。
十一、資訊安全查核。

第五條　資訊安全組織

本公司設「資訊安全推行小組」，由督導資訊服務部之主管擔任召集人，資訊服務部之主管擔任副召集人，小組成員由各部室主管擔任委員，負責制定、定期評估本公司資訊

安全政策，並統籌資訊安全計畫、資源調度等事項之協調、研議。

第六條　資訊安全分工原則

一、資訊安全政策、計畫、措施、技術規範之研議、建置及評估等相關事項，由資訊服務部負責辦理。資訊服務部主管所指派資訊安全人員除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。

二、資料及資訊系統之安全需求研議、使用管理及保護等事保護等事項，由各業務單位負責辦理。

三、資訊機密之維護及資訊安全使用管理之查核，由稽核室會同有關單位辦理。

四、人員進用之安全評估由人力資源處負責辦理；資訊安全教育訓練，由資訊服務部負責辦理。

五、有關跨單位安全事項權責分工之協調、應採用之資訊安全技術、方法及程序之協調研議、整體資訊安全措施之協調研議、資訊安全計畫之協調研議及其它重要資訊安全事項之協調研議、資訊查核工作計畫及報告之審議由本公司「資訊安全推行小組」負責辦理。

第七條　資訊作業安全規定

一、人員管理及資訊安全教育訓練應考量事項如下：

（一）　員工皆應填具保密切結書；離職時應取消其識別碼，並收繳其通行證、卡及相關證件。

（二）　應定期(每年至少一次)對全公司員工辦理資訊安全宣導講習(例如：資訊安全政策、資訊安全法令規定、資訊安全作業程序以及如何正確使用資訊科技設施等)，並留存紀錄。

（三）　負責資訊安全之主管及人員，每年應至少接受十五小時以上資訊安全專業課程訓練或職能訓練。其他使用資訊系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程。

二、資訊提供管理應考量事項如下：

（一）　各種重要法令規章及通知應立即張貼於公佈欄。

（二）　營業廳內應裝置「公開資訊觀測站」，供客戶自行操作使用。

（三）　資訊閱覽室不得裝設專用競價用終端機。

（四） 不得於資訊閱覽室從事與客戶簽定開戶契約、接受買賣有價證券之委託交割及其他類似證券商業務行為。

（五） 應依「個人資料保護法」，妥善處理客戶及公司內部人個人資料。

（六） 於所設網站上提供股市即時交易資訊，應經由與證交所簽約之資訊公司提供。

（七） 應定期檢查網站內對外提供之資訊，對具機密性、敏感性之資訊內容，應立即移除；並應遵守證券商推介客戶買賣有價證券作業辦法規定，且不得以公司名義將屬於證券投資顧問事業範圍之資訊代為公開。

三、應用系統管理應考量事項如下：

（一） 應使用具有合法版權之軟體。

（二） 委外作業應簽訂契約。

（三） 委外人員電腦通行使用權利應經適當控管；委外期間結束後，應立即收回該項權利。

（四） 已完成之程式因故需維護時，應依據經過正式核准之程序辦理。

（五） 各項文件與手冊應經適當維護與控制。

（六） 應用系統之維護應指派專人負責。

（七） 對於進駐於公司內之委外作業人員應納入公司安全管理，如欲使用內部網路資源時，應有安全管制措施(如透過轉接方式或另建網路者，宜與內部網路作實體隔離)。

四、電腦系統安全管理應考量事項如下：

（一） 為確定電腦設備維護內容，應與廠商訂有書面維護契約，做完維護時應留存維護紀錄並由資訊單位派人會同廠商維護人員共同檢查。

（二） 因經營業務需要而為個人資料之蒐集、處理或國際傳遞及利用，應訂定「與軟硬體廠商機密維護及損害賠償等雙方權責劃分」。

（三） 電腦作業系統環境設定及使用權限設定應經有關主管核示，並由系統管理人員執行。

（四） 電腦系統檔案異動前後皆有完善之備份處理措施。

（五） 對於程式的存取使用，應有詳細的書面管制說明。

（六） 使用者第一次使用系統時，應更新初始密碼後方可繼續作業。

（七） 密碼應以亂碼方式儲存。

（八） 人員異動時應及時更新其使用權限。

（九） 對於程式及檔案之存取使用，應按權限區分。

（十） 對於使用者忘記密碼之處理,應有嚴格的身分確認程序,方可再次使用系統。

（十一）宜使用優質密碼設定(長度超過六個字元，且具有文數字及符號)，並加強宣導定期更新使用者密碼以不超過三個月為宜。

（十二）檢查公司現有之網站、伺服器、網路芳鄰、路由器、交換器、作業系統及資料庫等軟硬體設備應設定使用密碼,且避免使用預設（如 administrator、root 、sa)或簡易(如 1234)之帳號密碼及未設管理者存取權限。

（十三）正式作業與測試作業之程式、資料、工作控制指令等檔案應分開存放。

（十四）程式經修改其相關文件應及時更新。

（十五）應配備經營業務所需、且有適足容量之電腦系統。

（十六）電腦系統應訂定定期(每年至少一次)由內部或委託外部專業機構評估電腦系統容量及安全措施之機制與程序，定期對系統容量進行壓力測試，並留存紀錄。

（十七）應定期（至少每半年乙次）辦理資訊系統弱點掃描作業，針對所辨識出之潛在系統弱點，宜評估其相關風險或安裝修補程式，並留存紀錄。

（十八）設備報廢前應就機密性、敏感性資料及授權軟體予以移除或實施安全性覆寫或以人為方式破壞其儲存設備，確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄。

五、網路安全管理應考量事項如下：

（一） 應定期評估自身網路系統安全(例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等)，並留存相關紀錄。

（二） 定期或適時修補網路運作環境之安全漏洞（含伺服器、攜帶型、個人端及營業處所內供投資人共用之電腦等)，並留存相關文件。

（三） 有關電腦網路安全(如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等)之事項應隨時對內部公告。

（四） 各電腦主機、重要軟硬體設備應有專人負責。

（五） 應建立防火牆且應有專人管理。

（六） 防火牆進出紀錄及其備份應至少保存三年。

（七） 重要網站及伺服器系統(如網路下單系統等)應以防火牆與外部網際網路隔離。

（八） 防火牆系統之設定應經權責主管之核准。

（九） 網路使用者帳號初始密碼應隨機產生，並與使用者身分無關。

（十） 網路使用者帳號密碼輸入錯誤次數達三次者，應予中斷連線。

（十一）網路下單畫面應採加密方式(例如：SSL)處理。

（十二）網路下單應訂定憑證交付程序，避免非本人取得憑證。

（十三）網路下單應全面使用認證機制。

（十四）電腦應安裝防毒軟體，並及時更新程式及病毒碼。

（十五）應定期對電腦系統及資料儲存媒體進行病毒掃瞄(含電子郵件)。

（十六）防毒應涵蓋個人端（含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦。

（十七）勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤應特別小心開啟。

（十八）公司應訂定網際網路下單服務品質相關標準，並應包含交易之安全性、交易之穩定及友善、提供客戶服務。

（十九）網路下單系統功能檢查：

1. 應定期檢查網路下單系統提供之功能，並留存記錄。

2. 應就網路下單系統偵測網頁與程式異動、記錄並通知相關人員處理。

六、系統資料存取控制應考量事項如下：

（一） 系統存取政策及各級人員之存取權限應予明確規定，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） 離（休）職人員，應立即取消各項資訊資源之所有權限，並列入機關人員離（休）職之必要手續。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。

（三） 為加強作業系統之安全管理，應使用者註冊管理制度，並落實使用者通行密碼管理，使用者通行密碼之更新周期，最長以不超過三個月為原則。

（四） 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。

（五） 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，並設簿登記課其相關安全保密責任。

（六） 安全性或重要性較高之資料，應由權責主管人員核可後始得執行輸入或修改。

（七） 所輸入或修改之資料及其執行人員姓名、使用者帳號皆應留存紀錄。

（八） 對隱密性高之重要資料(例如：密碼檔)應以亂碼後之資料形式存放。

（九） 電子式及非電子式交易型態以電子郵件執行成交回報之傳輸，公司對姓名、帳號及信用帳號等機敏資訊，應依「機敏資訊類型及隱匿之具體作法原則」辦理。

（十） 使用電子憑證ＩＣ卡或其他類型憑證晶片卡或其他憑證載具等代表公司簽署之作業（例如：「公開資訊觀測站」、「證券商申報單一窗口」、「公文電子交換系統」等），該等憑證載具應由專人負責保管並設簿登記，且應訂定相關帳號、密碼保管及使用程序，並據以執行。

（十一）使用代表公司憑證載具簽署之作業系統端若屬證券商應用系統者（例如：「電子對帳單系統」），應留存電腦稽核紀錄（log），其保存年限比照各作業資料應保存年限。

（十二）公司應定期或不定期稽核依「個人資料保護法」定義之個人資料檔案管理情形。

（十三）前揭個人資料檔案之資料，其更新、更正或註銷均應報經備查，並將更新、更正、註銷內容、作業人員及時間詳實紀錄。

（十四）機密性、敏感性之報表列印或瀏覽應有適當之管制程序。

（十五）重要系統之稽核日誌紀錄內容(應包括使用者識別碼、登入日期時間、電腦的識別資料或其網址等事項)須定期檢視，相關紀錄須至少留存三年。

（十六）重要軟體及其文件、清冊應抄錄備份存於另一安全處所。

（十七）重要之備份檔案及軟體若儲存於與電腦中心同一建築物內，應鎖存於防火之房間或防火且防震之防火櫃中。

（十八）存放備份資料之儲存媒體，應於其標籤上註明存放資料之名稱及保存期限。

（十九）電腦媒體之安全管理應建立回存測試機制，以驗證備份之完整性及儲存環境之適當性。

（二十）操作日誌應詳實記載並逐日經主管核驗，操作人員不可與主管為同一人。

（二十一）系統主控台所留存之紀錄，應經專人檢查訊息內容且定期送主管核驗。

（二十二）為維護資訊安全，應建立資訊安全查核制度，定期或不定期進行資訊安全查核作業。

七、系統發展及維護安全管理應考量事項如下：

（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。如基於實際作業需要，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，應在本公司相關人員監督及陪同下始得為之。

八、資訊資產安全管理應考量事項如下：

（一） 資訊資產應建立目錄，訂定資訊資產的項目、擁有者及安全等級分類法。

（二） 依據個人資料保護法及政府資訊公開等相關法規，建立資訊安全等級之分類標準，以及相對應的保護措施。

九、實體及環境安全管理應考量事項如下：

（一） 就資訊相關設備安置、周邊環境及人員進出管制等，應訂定實體及環境安全管理措施。

（二） 電腦機房應有門禁管制(例如：刷卡或密碼鎖)；機房應有防火設施，並應定期檢驗。另應將地震、水災等天然災害因素列入考量。

（三） 電腦設備應有獨立之電源供應系統，其電源供應系統應含不斷電設備及發電機。

十、業務永續運作計畫之規劃與管理應考量事項如下：

（一） 故障復原程序(例如：電腦設備、通訊設備、電力系統、資料庫、電腦作業系

統等備援及回復計畫)應明確訂定，並製成文件。

（二） 故障復原程序應週期性測試，測試後應召開檢討會議，針對測試缺失謀求改進，並留存紀錄。

（三） 證券交易主機應有備援措施。

（四） 為維持業務正常運作，對資訊安全事件應建立緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施。

（五） 公司發生個人資料之竊取、竄改、毀損、滅失、或洩漏等資安事故者，將危及公司正常營運或大量當事人權益之情形時,應立即函報證交所(或櫃檯買賣中心、券商公會)轉陳主管機關。

（六） 公司應明確訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序。

十一、資通安全事件管理應考量事項如下：

（一） 通報程序:公司員工如發現或懷疑有資訊安全事件時(包括系統有安全漏洞、受威脅、系統弱點及功能不正常事件等)，應迅速向資訊人員通報，要求立即處理。

（二） 處理流程：發現資訊安全事件時，應迅速通知資訊人員處理，資訊人員應通知系統管理人員或維護廠商協助處理，系統管理人員處理後，應向直屬主管回報處理結果，並作成紀錄。

（三） 應變規定說明：

1. 內部危安事件：發現(或疑似)遭人為惡意破壞毀損、作業不慎等危安事件時，應迅速查明事件影響狀況、受損程度等，啟用備份資料、程式或啟動備援計畫相關措施，期儘速回復正常運作。

2. 病毒感染事件：病毒入侵後，隨時掌握電腦病毒感染最新動態，隔離病毒避免疫情擴散，同時儘速取得所需病毒清除程式，並按病毒修護程序，完成病毒清除及修護復原工作。

3. 駭客攻擊事件：發現被入侵時，立即隔離受入侵系統及拒絕入侵者任何存取動作，如切斷入侵者之實體連線或調整防火牆設定等，以阻絕駭客進一步入侵，並迅速啟動備援系統或程序，全面檢討網路安全措施、修補安全漏洞或修正防火牆之設定等具體改善補救措施，以防止類似入侵或攻擊情

事再度發生，正式紀錄入侵情形、被駭統計分析及損失評估等資料，以供防護與預警之參考。

（四） 天然災害事件：如遇颱風、水災、地震等天然災害或火災、爆炸、重大建築災害等重大意外事件，應迅速攜帶重要資料及程式等離開現場，或儲存於防火保險櫃等設施內，以利爾後系統重置復原。

（五） 主幹頻寬中斷事件：如遇通訊網路系統骨幹(主幹頻寬)中斷事件，應立即查明障礙點、影響區間及範圍，啟動應變機制，緊急調撥備援系統或替代路由，實施流量控管，執行搶修作業。

第八條　本政策應至少每年評估一次，以反映法令規章、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，並留存相關紀錄。

第九條　本政策應以書面、電子或其他方式通知員工共同遵守，並轉知與本公司連線作業之資訊服務廠商共同遵行。

第十條　本政策經董事會通過後實施，修正時亦同。