德信綜合證券公司

資訊安全政策

107.12.21 訂定
113.01.19 更新

一、政策依據參考

（一）交易所「建立證券商資通安全檢查機制」。

（二）「財政部暨所屬機關(構)資訊安全管理準則」。

二、資訊安全之定義

所謂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。

三、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。

四、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）資訊安全稽核。

五、資訊安全組織

本公司應配置至少一名資訊安全人員，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。

本公司設「資訊安全推行小組」，由總經理擔任召集人，小組成員由經紀部、自營部、承銷部、債券部、資訊服務部、稽核室、法令遵循室、風險管理室、總管理部、財會部主管擔任委員，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。

六、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。

（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稽核，由稽核室會同有關單位辦理。

（四）人員進用之安全評估由人事室負責辦理；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、資訊稽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。

七、資訊作業安全規定

(一) 人員管理及資訊安全教育訓練。

人員管理及資訊安全教育訓練應考量事項如下：

(1) 資訊作業人員皆應填具保密切結書；離職時應取消其相關帳號。

(2) 應指定專人或專責單位負責規劃與執行資訊安全工作且每年應定期參加 15 小時以上資訊安全專業課程訓練或職能訓練並通過評量。其他使用資訊系統之從業人員，每年應至少接受 3 小時以上資訊安全宣導課程（例如：防毒、資料備份、使用合法軟體及電子郵件使用規定等），並留存紀錄。

(二) 資訊提供管理

資訊提供管理應考量事項如下：

(1) 各種重要法令規章及通知應立即張貼於公佈欄。

(2) 營業廳內應裝置「公開資訊觀測站」，供客戶自行操作使用。

(3) 資訊閱覽室不得裝設專用競價用終端機。

(4) 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。

(5) 應依「電腦處理個人資料保護法」，妥善處理客戶資料。

(6) 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。

(7) 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) 應用系統管理維護

應用系統管理應考量事項如下：

(1) 應使用具有合法版權之軟體。

(2) 委外作業應簽訂契約。

(3) 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。

(4) 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。

(5) 各項文件與手冊應經適當維護與控制。

(6) 應用系統之維護應指派專人負責。

(7) 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

電腦系統安全管理應考量事項如下：

(1) 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。

(2) 因經營業務需要而為個人資料之蒐集、電腦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」。

(3) 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。

(4) 電腦系統檔案異動前後皆有完善之備份處理措施。

(5) 對於程式的存取使用，應有詳細的書面管制說明。

(6) 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。

(7) 密碼不得使用簡易密碼，應使用公開安全且未遭破解之演算法(例如：雜湊演算法等不可逆運算式)產生亂碼並加密儲存，為防止密碼洩漏，應採取不顯示、不印錄等措施。

(8) 人員異動時應及時更新其使用權限。

(9) 對於程式及檔案之存取使用，應按權限區分。

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

(11)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，如客戶密碼超過一年未變更或變更密碼與前一代相同，公司應做妥善處理。除客戶外，公司其他使用者之密碼應至少每三個月變更一次。

(12)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。

(13)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。

(14)程式經修改其相關文件應及時更新。

(15)公司應配備經營業務所需、且有適足容量之電腦系統。

(16)公司之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，應用系統有重大調整或變更時，將系統壓力測試納入測試範圍，並於系統上線時進行系統壓力測試作業，並留存紀錄。

(五) 網路安全管理。

網路安全管理應考量事項如下：

(1) 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。

(2) 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。

(3) 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)之事項應隨時公告。

(4) 各電腦主機、重要軟硬體設備應有專人負責。

(5) 應建立防火牆。

(6) 防火牆應有專人管理。

(7) 防火牆進出紀錄及其備份應至少保存三年。

(8) 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。

(9) 防火牆系統之設定應經權責主管之核准。

(10)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。

(11)網路使用者帳號密碼輸入錯誤次數達三次者，應予鎖定帳號。公司於接獲客戶申請解除鎖定時，應確實辨認身分，始得辦理之。

(12)網路下單畫面應採加密方式(例如：SSL)處理。

(13)公司應訂定憑證交付程序，避免非本人取得憑證。

(14)公司應全面使用認證機制。

(15)電腦應安裝防毒軟體，並及時更新程式及病毒碼。

(16)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)。

(17)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。

(18)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。

(六) 系統資料存取控制。

系統資料存取控制應考量事項如下：

(1) 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。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

(6) 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。

(7) 所輸入或修改之資料及其執行人員姓名、職稱皆應留存紀錄。

(8) 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。

(9) 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。

(10)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。

(11)公司應定期或不定期稽核依電腦處理個人資料保護法定義之個人資料檔案管理情形。

(12)前揭個人資料檔案之資料，其更新、更正或註銷均應報經核准，並將更新、更正、註銷內容、作業人員及時間詳實記錄。

(13)機密性、敏感性之報表列印或瀏覽應有適當之管制程序。

(14)重要軟體及其文件、清冊應抄錄備份存於另一安全處所。

(15)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。

(16)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。

(17)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。

(18)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。

(19)為維護資訊安全，應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。

(20)公司對於客戶之帳號登入失敗紀錄、非客戶帳號嘗試登入嘗試紀錄等進行監控，發現有客戶帳號登入異常情事，應通知客戶了解異常原因，並留存相關紀錄，避免非客戶本人登入情事。

(21)公司針對異常及不明來源 IP 連線進行監控及留存紀錄，如有發現異常之情事，應進行了解與確認。

（七）系統發展及維護安全管理。

系統發展及維護安全管理應考量事項如下：

(1) 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。

(2) 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，得核發長期性之系統辨識及通行密碼供廠商使用，但每次使用其權限前需知會本公司相關人員，告知其使用之原由及目的。

(3) 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。

(4) 廠商應於每次重大更新項目程式交付時，需同時檢付軟體證明書

(Code review 及掃描驗證)，行動應用程式應增加檢付原碼檢測報告(需涵蓋 OWASP MOBILE TOP 10 之標準)。

所謂重大更新項目為與「下單交易」、「帳務查詢」、「身份辨識」及「客戶權益有重大相關項目」有關之功能異動。

(八)資訊資產安全管理。

資訊資產安全管理應考量事項如下：

(1) 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。

(2) 依據電腦處理個人資料保護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。

實體及環境安全管理應考量事項如下：

(1) 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。

(2) 應建立防火牆電腦機房應有門禁管制(例如：刷卡)；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。

(3) 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。

業務永續運作計畫之規劃與管理應考量事項如下：

(1) 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。

(2) 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。

(3) 公司之交易主機應有備援措施。

(4) 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。

(5) 資安防護應辦理下列事宜：

(5.1)指定人員及部門統籌並協調聯繫各有關部門。

(5.2)定期評估核心營運系統及設備，對評估結果採取適當措施，並提報董事會，以確保營運持續及作業韌性之能力。

(5.3)於永續報告書、年報、財務報告或公司網站，揭露年度內公司持續核心營運系統及設備營運所需之資源及落實於年度預算或教育訓練計畫等項目。

(十一)資通安全事件管理。

資通安全事件管理應考量事項如下：

(1) 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。

(2) 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。

(3) 應變規定說明：

(3.1) 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。

(3.2) 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。

(3.3) 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。

(3.4) 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。

(3.5) 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。

八、本政策應至少每年評估一次，以反映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。

九、本政策自發布日施行。並以書面、電子或其他方式通知員工與本公司連線作業之有關機構、廠商。

十、公司每年應將前一年度資訊安全整體執行情形，由負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具資訊安全整體執行情形聲明書，並提報董事會通過，於會計年度終了後三個月內將該聲明書內容揭露於公開資訊觀測站。

十一、本作業依董事長核可後實施，修正亦同。

附則：

1. 本辦法於民國一〇七年十二月二十一日訂定。

2. 本辦法於民國一〇八年十月九日修訂

3. 本辦法於民國一〇九年九月十日修訂

4. 本辦法於民國一一〇年九月十六日修訂

5. 本辦法於民國一一〇年十一月十五日修訂

6. 本辦法於民國一一一年十一月三十日修訂

7. 本辦法於民國一一二年十二月十三日修訂

8. 本辦法於民國一一三年一月十九日修訂