目 錄

一、依據目的

1.日進證券股份有限公司（以下簡稱本公司）為強化資訊安全管理，確保資料、系統、設備及網路安全，以期整體資訊業務順利進行，並保護企業資產完整，減少可能發生之損害，維護良好的企業形象，特依據臺灣證券交易所股份有限公司94年3月4日函頒之「建立證券商資通安全檢查機制」、「電腦處理個人資料保護法」，訂定本政策。

2.本政策適用對象為本公司全體員工，並依業務區分，由各業務主管分別考核資訊安全管理或辦法之實施。

二、資訊安全政策制定及評估

（一）資訊安全政策制定

1.資訊安全定義

為了確保本公司資訊資產的可用性、完整性、機密性及業務之持續性，依政府資訊安全管理政策、法令、資訊技術、公司業務發展需要及資訊資產可能面臨之風險，特制定本政策，作為本公司資訊作業之準則，以形成公司由上到下對資訊安全要求的共識，將公司有限之資源用在最需要的地方，相關人員亦有所遵循以執行良好之資訊安全控管。

2.資訊安全目標

成立跨部門資訊安全委員會，負責公司整體資訊整合暨規劃未來資訊發展方向，提供管理與指導，積極推動資訊建設，利用資訊科技，增強公司競爭力，創造客戶價值，並加強資訊安全作業，以保護資訊資產安全、維持業務持續運作，企業永續經營之目標。

3.資訊安全範圍

本公司就下列事項，訂定資訊安全管理計畫實施，並定期評估實施成效：

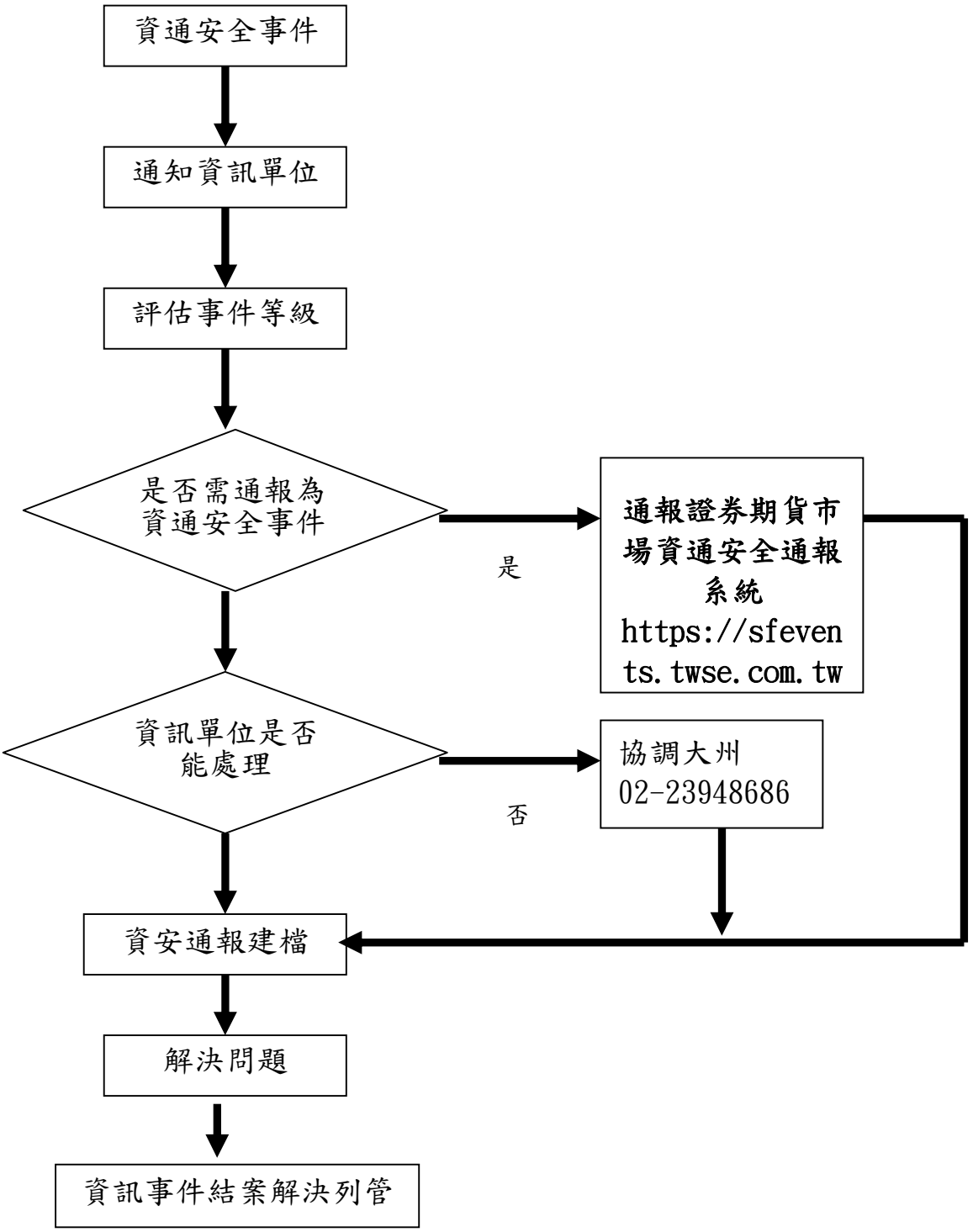
（1）資訊安全政策制定及評估
（2）資訊安全組織及權責
（3）人員安全管理及教育訓練
（4）資訊資產安全管理
（5）實體及環境安全管理
（6）系統存取控制
（7）電腦系統作業安全管理
（8）網路安全管理
（9）系統發展及維護之安全管理
（10）營運持續管理計畫管理

4.資訊安全事件之緊急通報程序：

(1)同仁發現資安事件必須立即回報資訊人員處理。

(2)資訊人員處理必須立刻依循資訊安全事件處理流程來處理，並迅速做出適當的回應。

# 資訊安全事件之緊急通報程序



（二）資訊安全政策之評估

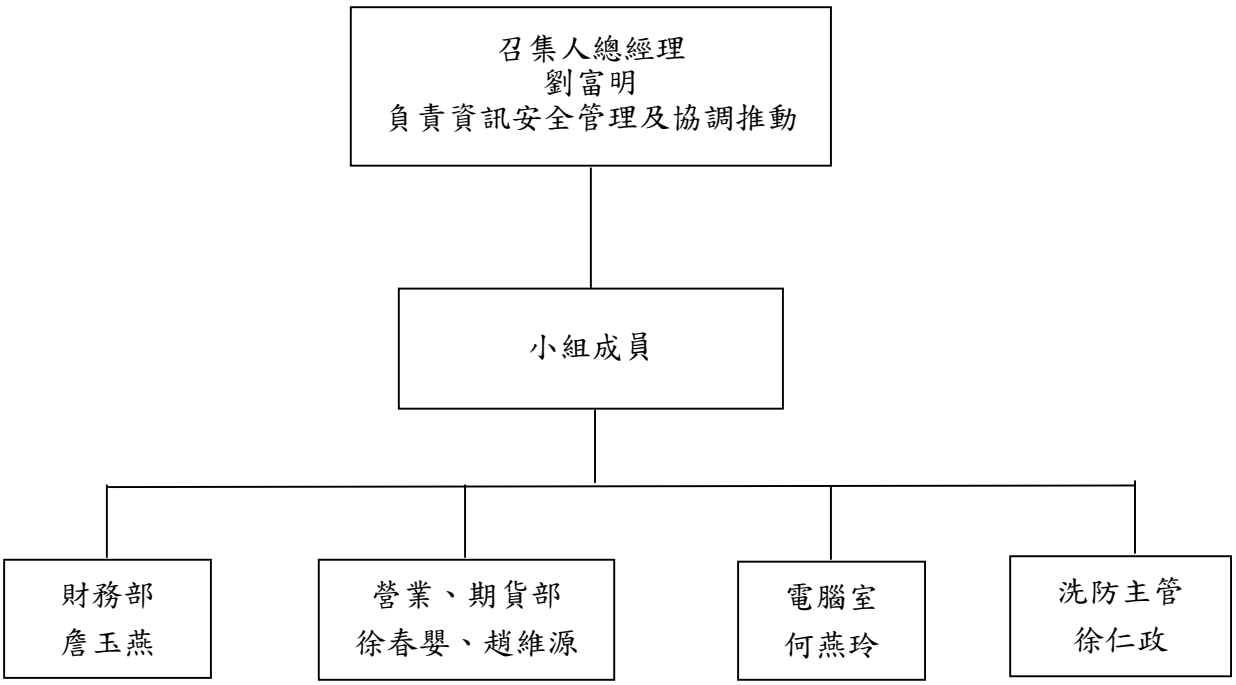
1. 應每年定期稽查資訊安全事項辦理情形，如有未符合本管理規範之規定者，應依公司之相關紀律處理。
2. 本政策範圍內管理要點、細則，資訊部每年應定期評估，視當時法令及環境之需要修訂，以確保資訊安全實務作業之順-利執行。
3. 本政策範圍內管理辦法、細則等，皆以書面、電子郵件（E-MAIL）或其他方式通知員工及與本公司連線之機關（公司）、提供資訊服務之廠商共同遵行。
4. 本資訊安全政策，應至少每年評估一次，以反映法令規章、技術及業務等最新發展現況，確保資訊安全實務作業之有效性，前開之評估工作應留存相關紀錄。
5. 資訊安全政策之評估，應以獨立及客觀之方式進行，並由內部或委託外部專業機構辦理。
6. 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。
7. **公司應參考「建立證券商資通安全檢查機制-分級防護應辦事項附表」辦理資訊安全分級防護應辦事項。**

三、資訊安全組織及權責

1. 由本公司總經理擔任召集人，負責資訊安全管理事項之協調及推動，並成立「資訊安全委員會」，統籌資訊安全政策、計畫、資源調度等事項之協調、研議，。
2. 資訊安全推行委員會成員就其權責，定期召開會議，以檢討策進資訊建設、安全政策、責任分配，並協助稽核單位稽核資訊安全作為。
3. 公司應視資訊安全管理需要**及所屬資安分級**，指定專人或專責單位負責規劃與執行資訊安全工作，且**資訊安全專責人員及專責主管**每年應定期參加十五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，每年應至少接受三小時以上資訊安全宣導課程。
4. 公司資訊安全人力、能力及經驗，如有不足之處，得委請外界的學者專家或民間專業組織及團體，提供資訊安全顧問諮詢服務。
5. 資訊處理部門與業務單位之權責，應明確劃分。

# 日進證券股份有限公司

## 資訊安全委員會架構圖




四、人員安全管理及教育訓練

1. 員工應依相關法令課予機密維護責任，並應填具保密切結書，以明責任。
2. 員工離職時應取消其識別碼，並收繳其通行證、卡及相關證件。
3. 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。
4. 員工應依職務層級進行適當的資訊安全教育訓練，每年並達內部所定之訓練時數。
5. 電腦稽核人員由稽核擔任之。

五、資訊資產安全管理

（一）資訊資產分類原則

1. 本公司資訊資產分為軟體類資產、硬體類資產、電子類資產、文件類資產、及人員類資產等五類。
2. 界定資訊安全等級之責任，應由資料的原始產生者，或是由指定的系統所有者負責。
3. 已列入安全等級分類的資訊及系統之輸出資料，應有相關管制措施以利使用者遵循。
4. 資訊資產分類清冊完成後，若有異動應依規定執行作業程序。

（二）資訊資產控制管理

1. 應該建立一份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。
2. 資料資產（ 資料庫、系統文件、使用手冊、操作手冊等)、軟體資產(作業系統軟體、應用系統、開發工具語言等)、硬體資產(電腦設備、通訊設施、資料儲存設備、週邊設備等)，均需依照資訊安全政策管理。
3. 依照公司訂立之資訊資產的項目、擁有者及安全等級等實施管理。

（三）資訊安全等級分類

1. 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。
2. 資訊安全分類標準應考量資料的機密性、資料正確性及可用性，以減少未經授權的系統存取或系統損害對公司業務造成衝擊。
3. 公司之資訊安全可區分機密性、敏感性（如屬個人資料）及一般性等三類。
4. 公司須執行或參考其他公司訂定之資訊安全等級分類時，應特別注意其與本公司的資訊安全等級，在定義及標準，應取得一致。
5. **公司應對自行或委外開發之資訊系統完成資訊系統分級，資訊系統等級應至少區分核心與非核心系統，每年應至少檢視一次資訊系統分級妥適性。**

六、實體及環境安全管理

（一）設備安全管理

1. 各項資訊設備應置放於安全區內。
2. 電腦設備及電子媒體放置之安全區應有有效之防竊盜設備，如門禁系統，放置設備應有財產編號及記錄。
3. 電腦設備及電子媒體放置之安全區應有有效之防火設備，如偵煙警示設備、氣體滅火設備等，亦應有有效之空調設備、不斷電設備及自動發電機設備。
4. 電源線纜與通訊電纜應儘可能相互隔離，避免干擾。
5. 含有儲存媒體的設備項目(如硬碟)如需送修或報廢，應在處理前詳加檢查，以確保任何機密性、敏感性的資料不會遺失。
6. 為了防止資訊設施被誤用，提供的資訊設施，如有業務目的以外的使用，或是超出授權目的以外的使用需求，應經權責主管的核准，並課予相關人員的責任，若有不當使用情形應作適當的紀律處理。
7. 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、實施安全性覆寫或實體破壞，應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。

（二）周邊安全管理

1. 周圍環境之安全

（1）實體環境的安全保護，應以事先劃定的各項周邊設施為基礎，並設置必要的障礙（門禁系統)，以達安全控管的目的。

（2）實體環境的安全保護程度，應視資訊資產及系統價值的安全風險而決定。

2. 人員進出管制：

（1）管制區內應有適當的門禁系統，並記錄來訪人員進出時間和目的，以確保只有被授權的人員始得進入（如：電腦機房、媒體檔案庫房等)。

（2）電腦廠商的資訊人員或維護服務人員，只有在被要求或是被授權的情形下，才能進入管制區域，並視需要限制（例如限制存取敏感性的資料）及監督其活動。

3.電腦機房安全管理：

（1）電腦機房應設立良好的實體安全措施；地點的選定，應考量水災、火災、地震等自然及人為災害的可能性，並考量鄰近空間的可能安全威脅。

（2）電腦設備及電子媒體放置之安全區應有有效之防火設備，如偵煙警示設備、氣體滅火設備等，亦應有有效之空調設備、不斷電設備及自動發電機設備。

（3）凡進入電腦機房之人員，除應配掛專用識別證外，應於機房門口設置門禁系統或監錄等保護措施。

**(4)公司應定期審查資訊機房門禁管制權限。**

4.辦公桌面之安全管理：

（1）員工於公司內，應隨時注意清理桌面之文件等資訊，如離開座位，應清除電腦畫面之資訊、將終端機登出，或以密碼保護。

（2）個人電腦應依需要以開機密碼保護。

（3）具敏感性之資訊，如紙張與媒體，應置於加鎖之空間內。

5.財產移轉的安全管理：

電腦設備、資料或軟體，未經主管許可，不得帶離辦公室。

七、系統存取控制

各應用系統根據業務需求、安全需求、資訊傳播及授權等規定，明訂資訊存取之控制政策及規則，**並以書面、電子或其他方式告知員工遵守**。並對資訊存取及業務流程加以控制，以防止資訊之非法存取。

（一）用戶身份識別及驗證

1.所有用戶皆應有個人專用的代號(ID)，以便追溯具體責任人。

2.應有適當方法對用戶進行身份驗證，如密碼，憑證等。

**3.權限管理：**

**(1) 對於程式的存取使用，應有詳細的書面管制說明。**

**(2) 人員異動時應及時更新其使用權限。**

**(3) 對於程式及檔案之存取使用，應按權限區分。**

**(4) 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。**

**(5) 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）。**

**(6) 應定期（至少每半年一次）審查並檢討久未使用之使用者權限（使用者為客戶者除外）。**

（二）資料輸入管理

1.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。

2.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。

3.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。

4. 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。
5. 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。
6. 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。
7. 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。
8. 前揭個人資料檔案之資料，其更新、更正或註銷均應報主管核准，並將更新、更正、註銷內容、作業人員及時間詳實記錄。
9. 因經營業務需要而為個人資料之蒐集、處理或國際傳輸及利用，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）密碼管理

1. 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。
2. 密碼應以亂碼方式儲存。
3. 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。
4. 初始密碼應隨機產生，並與使用者身分無關。
5. 密碼輸入錯誤次數達三次者，應予中斷連線。
6. 除輸入介面僅可輸入數字外(例如：語音按鍵下單)，公司應使用優質密碼設定(長度6個字元（含）以上，且具有文數字或符號)，並加強宣導客戶定期更新使用者密碼以不超過三個月為宜。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。。
7. 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。

8. 客戶申請採電子式交易型態者，**公司得以一般或自訂電子方式交付電子密碼條，應依下列說明辦理：**

**(1)採一般電子方式交付電子密碼條，應傳送 OTP（One Time Password）密碼至客戶開戶留存之手機號碼，及將加密後之電子密碼條以電子方式傳送至客戶留存之電子信箱，此流程相關系統紀錄應留存。**

**(2)採自訂交付電子密碼條方式，應訂定交付電子式交易密碼之作業程序及安全控管機制，並辦認電子式交易密碼交付對象為本人及留存相關紀錄。**

（四）電腦稽核紀錄管理：

1.對重要系統（如主機連線系統、網路下單系統等）之稽核日誌記錄內容應包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項。

2.對上開重要系統之電腦稽核紀錄，應有專人定期檢視。

3.相關留存紀錄應確保數位證據之收集、保護與適當管理程序，至少留存三年。

（五）資料輸出管理

1. 報表是否按時產生並分送各使用單位。

2. 機密性、敏感性之報表列印或瀏覽應有適當之管制程序。

3. 投資人於公司網站查詢個人資料應具有加密傳輸機制(例如：SSL)。

4. 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。

（六）電腦媒體之安全管理：

1. 重要軟體及其文件、清冊應抄錄備份存於另一安全處所。

2. 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。

3. 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。

4. 應建立機密性及敏感性資料媒體之相關處理程序，防止資料洩露或不當使用。

5. 應建立回存測試機制，以驗證備份之完整性及儲存環境的當性。

（七）電腦操作管理

1. 操作人員應確實依規定操作程序執行。

2. 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。

3. 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。

（八）經紀商應配備業務所需、且適足容量之電腦系統

(九)證券經紀商之電腦系統應訂定定期(每年至少一次)由系統管理員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。

八、電腦系統作業安全管理

（一）設備管理

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」。

（二）電腦作業系統環境設定及使用權限設定

1. 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。

2. 電腦系統檔案異動前後皆有完善之備份處理措施。

**3. 公司應建立系統最高權限帳號管理辦法(含作業系統及應用系統)，如需使用最高權限帳號時須取得權責主管同意，並留存相關紀錄。**

**4. 公司應建立並落實個人電腦、伺服器及網路通訊設備之安全性組態基準(如密碼長度、更新期限等)。**

**5. 公司透過網際網路使用管理帳號登入重要系統時，應採用多因子認證機制。**

（三）系統使用者管理

1. 對於程式的存取使用，應有詳細的書面管制說明。
2. 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。
3. 密碼應以亂碼方式儲存。
4. 人員異動時應及時更新其使用權限。
5. 對於程式及檔案之存取使用，應按權限區分。
6. 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。
7. 軟硬體設備應設定使用密碼，且避免使用預設（如 administrator、root）或簡易（如 1234）之帳號密碼及未設管理者存取權限。
8. **操作人員應確實依規定操作程序執行。**
9. **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。**
10. **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。**

（四）應用系統異動管理

1. 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。
2. 程式經修改其相關文件應及時更新。

（五）資訊提供作業

1. 各種重要法令規章及通知應立即張貼於公佈欄。
2. 上市公司之營運資料、公開說明書應陳列於證券投資資料櫃供客戶閱覽。
3. 營業廳內應裝置「公開資訊觀測站」，供客戶自行操作使用。
4. 資訊閱覽室應未限定對象並且無收費行為。
5. 資訊閱覽室不得裝設專用競價用終端機。
6. 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。
7. 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。
8. 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。

**(六)電腦媒體之安全管理：**

1. **重要軟體及其文件、清冊應抄錄備份存於另一安全處所。**
2. **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。**
3. **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。**
4. **應建立機密性及敏感性資料媒體之相關處理程序，防止資料洩露或不當使用。**
3. **應建立回存測試機制，以驗證備份之完整性及儲存環境的適當性。**

**(七).公司應配備經營業務所需、且有適足容量之電腦系統。**

**(八).證券經紀商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，並留存紀錄。**

九、網路安全管理

（一）網路系統安全評估

1. 應定期評估自身網路系統安全（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），並留存記錄。
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. **公司網路應依用途區分為 DMZ、營運環境、測試環境及其他環境，並有適當區隔機制（如防火牆、虛擬區域網路、實體隔離等）。**
6. **個人資料及機敏資料應存放於安全的網路區域，不得存放於網際網路等區域。**
7. **系統應僅開啟必要之服務及程式，未使用之服務功能應關閉。**
8. **公司應建立遠端連線管理辦法，對使用外部網路遠端連線至公司內部作業進行控，留存相關維護紀錄並由權責主管定期覆核。**
9. **公司應防止未經授權設備使用內部網路。**

（二）防火牆之安全管理

1. 應建立防火牆。
2. 防火牆應有專人管理。
3. 防火牆進出紀錄及其備份應至少保存三年。
4. 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。
5. 防火牆系統之設定應提出申請經權責主管之核准。
6. **公司應每年定期檢視並維護防火牆存取控管設定，並留存相關檢視紀錄。**
7. **公司交易相關網路直接連線之設備應避免使用危害國家資通安全產品。**

（三）網路使用者帳號管理

1. 初始密碼應隨機產生，並與使用者身分無關。
2. 密碼設定六位元以上且符合複雜原則，並定期更新。
3. 密碼輸入錯誤次數達三次者，應予中斷連線。

（四）網路傳輸安全管理

網路下單畫面應採加密方式（SSL）處理。

（五）CA 認證與憑證管理

1. 網路下單應訂定憑證交付程序，避免非本人取得憑證。
2. 網路下單應全面使用認證機制。

（六）電腦病毒及惡意軟體之防範

1. 電腦應安裝防毒軟體，並及時自動更新程式及病毒碼。
2. 應定期對電腦系統及儲存媒體進行病毒掃瞄（含電子郵件）。
3. 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。
4. 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。

5. 為防範電腦病毒擴散，影響電腦安全，應訂定電子郵件使用安全相關規定。

**6. 為防範電腦病毒擴散，影響電腦安全，公司應訂定電子郵件使用安全相關規定及建立郵件過濾機制。**

**7. 公司應建立上網管制措施，以避免下載惡意程式。**

**8. 公司應偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。**

**9. 公司宜每年定期辦理社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。**

（七）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，並留存檢查紀錄。
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。

(八)公司提供 API 服務規範：公司提供客戶使用應用程式介面（API）服務之申請流程、核可標準及相關控管配套措施相關作業，應依「證券商受理客戶使用應用程式介面(API)服務作業規範」辦理。

(九)網際網路下單服務品質相關標準：

公司提供網際網路下單業務時，兼顧客戶服務品質，應訂定網際網路下單服務品質相關標準，並應包含下列重點如：交易之安全性、交易之穩定及友善、提供客戶服務。

十、系統發展及維護之安全管理

在新系統開發或舊系統維護前，應先分析安全需求，並於規劃期間即內建安全控制措施於資訊系統內。在評估套裝軟體時，亦應做同樣考量。資訊系統在設計階段引入控制機制，其代價遠小於在開發階段中或開發完成後引入之控制措施。

（一）系統安全需求規劃

1. 系統安全需求分析及規格

新發展的資訊系統，或是現有系統功能之強化，應在系統規劃之需求階段，即將安全需求納入系統功能。

2. 除由系統自動執行的安控措施之外，亦可考量由人工執行安控措施；在採購套裝軟體時，亦應進行相同的安全需求分析。
3. 系統的安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，對機關可能帶來的傷害程度。
4. 凡屬有關安全控管程式非經權責主管授權，不得擅自更改

（二）應用系統之安全

1. 輸進應用系統的資料，應在事前查驗（例如是否有超出設定範圍的數值等），以確保資料的真確性。
2. 系統內部的作業，應建立驗證資料正確性的作業程序，避免正確輸入資料到應用系統中，卻因系統處理錯誤或是人為因素而遭受破壞。
3. 對高敏感性的資料，應在傳輸或儲存過程中以加密方法保護。
4. 偵測資料內容是否遭受未經授權的竄改，或驗證傳送之訊息內容是否遭受破壞。

（三）應用系統軟體之安全

1. 在作業系統上執行應用軟體，應建立控制程序並嚴格執行，為減少可能危害作業系統的風險，作業用的應用程式館更新作業，應限定只能由授權的管理人員才可執行，且應建立應用程式館的更新稽核紀錄。
2. 作業用的應用程式館均應以目的程式為原則；除非核准，不得以原始程式作業。
3. 應保護及控制測試資料，避免以含有個人資料的真實資料庫進行測試。
4. 測試完畢後，真實資料應立即從測試系統中刪除。
5. 真實資料的複製情形予以記錄，以備稽核運用。

（四）系統維護管理

1. 應用系統在規劃分析時應將資訊安全需求納入分析及規格。
2. 輸入資料是否有作檢查，以確認其正確性。
3. 應使用具有合法版權之軟體。
4. 委外作業應簽訂契約，委外作業契約內容應包含資訊安全協定與對委外廠商資安稽核權等條款。
5. 已完成之程式因故需維護時，應經過主管核准之程序辦理。
6. 各項文件與手冊應經適當維護與控制。
7. 應用系統之維護應指派專人負責。
8. 應用系統異動管理：
   (1)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。
   (2)程式經修改其相關文件應及時更新。
9. 公司應定期（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。
10. 程式原始碼安全規範：
    (1)程式應避免含有惡意程式等資訊安全漏洞。
    (2)程式應使用適當且有效之完整性驗證機制，以確保其完整性。
    (3)程式於引用之函式庫有更新時，應備妥對應之更新版本。
    (4)程式應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。
    (5)無法取得程式原始碼時，應要求程式提供者符合上開前四項(1、2、3、4)安全事項。
11. 行動應用程式安全管理：
    (1)行動應用程式發布：
       a. 行動應用程式應於可信任來源之行動應用程式商店或網站發布，且應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。
       b. 應於官網上提供行動應用程式之名稱、版本與下載位置。
       c. 應建立偽冒行動應用程式偵測機制，以維護客戶權益。
       d. 應於發布前檢視行動應用程式所需權限應與提供服務相當，首次發布或權限變動應經資安、法遵單位同意，並留有紀錄，以利綜合評估是否符合個人資料保護法之告知義務」。
    (2)敏感性資料保護：
       a. 行動應用程式傳送及儲存敏感性資料時應透過憑證、雜湊（Hash）或

加密等機制以確保資料傳送及儲存安全，並於使用時應進行適當去識別化，相關存取日誌應予以保護以防止未經授權存取。

b.啟動行動應用程式時，如偵測行動裝置疑似遭破解（如 root、jailbreak、USB debugging 等），應提示使用者注意風險。

(3)行動應用程式檢測：

a.涉及投資人使用之行動應用程式於初次上架前及每年應委由經財團法人全國認證基金會(TAF)認證合格之第三方檢測實驗室進行並完成通過資安檢測，檢測範圍以經濟部工業局委託執行單位「行動應用資安聯盟」公布之行動應用程式基本資安檢測基準項目進行檢測。如通過實驗室檢測後一年內有更新上架之需要，應於每次上架前就重大更新項目進行委外或自行檢測；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。檢測範圍以 OWASP MOBILE TOP 10 之標準為依據，並留存相關檢測紀錄。

b.公司對第三方檢測實驗室所提交之檢測報告，應建立覆核機制，以確保檢測項目及內容一致，並留存覆核紀錄。

十一、營運持續管理

為防止業務中斷，保護重要業務流程不受重大事故及災難之影響，應擬訂應變計劃，將災難及事故造成之影響降至最低。

（一）營運持續管理之規劃

1.資訊部應建立相關資訊營運持續管理計劃程序，並指定權責人員研訂及維護業務持續運作之計畫。

2.營運持續管理的規劃作業，應研析並降低人為或是意外因素對重要業務運作可能導致的威脅，使重要業務在資訊作業系統、資料檔案及人員發生事故、設施失敗或是受損害時，仍可持續運作。

3.營運持續管理計畫應考量，評估各種災害對業務作業可能的衝擊、人員責任界定以及緊急應變措施之安排、建立作業程序及流程、進行員工教育及訓練、測試緊急應變計畫、定期更新緊急應變計畫。

4.營運持續管理計畫應考量訂定緊急應變作業程序、回復作業程序、測試作業程序及相關人員之權責。

（二）營運持續管理計畫之測試

為使應變計畫維持有效性及相關人員確實瞭解計畫的最新狀態，每年應定期測試及演練，並留存記錄，測試以個別計畫的方式進行，減少測試完整計畫的需求及頻率。

（三）營運持續管理計畫之更新

1.營運持續管理計畫應配合業務、組織、人員及法令等事項之變動，更新計畫內容。

2.營運持續管理計畫之變更，由資訊部建立控管機制，並指定專人負責。

（四）資訊安全事件緊急處理機制及流程

應建立資訊安全事件之通報程序，員工如發現或懷疑有資訊安全事件時(如系統安全漏洞、病毒等)，應依程序迅速通知資訊單位系統管理人員及權責主管單位立即處理。

（五）證券經紀商之交易主機應有備援措施。

（六）應明確訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序。

十二、符合性

(一)　應定期（每年至少一次）辦理資訊安全查核作業（內部辦理或委託外部專業機構），並應留存查核紀錄。

(二)　針對前開之資訊安全查核報告辦理追蹤改善情形（包括查核摘要、查核範圍、缺失說明及改進建議等）。

十三、新興科技應用

(一)雲端服務：

1. 公司為雲端服務使用者時，應訂定雲端運算服務運作安全規範內含雲端提供者之遴選機制、查核措施、備援機制、服務水準（含資訊安全防護）與復原時間要求等，如有不符需求之處，需有其它補償性措施。
2. 公司為雲端服務提供者時，應訂定雲端運算服務安全控管措施，應包含法律遵循、權限控管、權責歸屬及資訊安全防護等項目。如涉及敏感性資料之傳遞，應使用超文字傳輸安全協定 （HTTPS）、安全檔案傳輸協定（SFTP）等加密之網路協定。

(二)社群媒體：

1. 公司應訂定社群媒體相關資訊安全規範與運用社群媒體管理辦法，應包含以下內容：
   (1). 界定可於公務用社群媒體上分享之業務相關資料。
   (2). 私人與公務用社群媒體之區別與應注意事項。
2. 應針對開放員工使用社群媒體評估其風險程度，包含：資料外洩、社交工程、惡意程式攻擊等，並採行適當的安全控管措施。
3. 公司應訂定經營官方社群媒體資訊安全規範與管理辦法，並包含以下內容：
   (1). 應事先了解所經營之社群媒體隱私政策，並定期（每年一次）檢視其隱私政策之異動及評估其風險。
   (2). 於官方網站提供連結供使用者連至公司外之社群媒體時，應出現提示視窗告知使用者該連結非公司本身之網站。
   (3). 對經營之社群媒體應標示證券商名稱、聯絡方式，以區別為官方經營之社群媒體。
   (4). 應建立帳號權限管理機制，對發布內容進行控管與監視，並針對不適當言論及異常事件，進行通報或處置。

(三)行動裝置：

1. 公司應訂定公務用行動裝置之資訊安全規範與管理辦法，須包含以下項目：
   (1). 行動裝置設備管理辦法應對於申請、使用、更新、繳回與審核應訂有相關規範。
   (2). 人員異動時，行動裝置應進行重新配置或清除配置程序，以確保行動裝置環境安全性。
   (3). 行動裝置應避免安裝非官方發佈之行動應用程式，或僅安裝由公司列出通過檢測可安裝之行動應用程式。
2. 公司應訂定員工自攜行動裝置之資訊安全規範與管理辦法，須包含以下項目：
   (1). 公司應要求員工自攜行動裝置使用用途。
   (2). 公司應與持有人簽署員工自攜行動裝置使用協議，含：使用限制及雙方責任等。
   (3). 公司應限制內部資訊設備透過員工自攜行動裝置私接存取網際網路（Internet）

之行為。

(四)物聯網：

應訂定物聯網相關資訊安全規範與管理辦法，須包含下列項目：

1. 應建立物聯網設備管理清冊並至少每年更新一次，且應變更前開設備之初始密碼。
2. 物聯網設備應具備安全性更新機制且定期（每年一次）更新，如存在已知弱點無法更新時，應建立補償性管控機制。
3. 應關閉物聯網設備不必要之網路連線及服務，避免使用對外公開的網際網路位置。
4. 如與物聯網設備供應商簽定採購合約時，其內容宜包含資訊安全相關協議，明確約定相關責任（如：服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案），確保設備不存在已知安全性漏洞。
5. **公司採購物聯網設備時，宜優先採購取得資安標章之物聯網設備。**
6. **公司應定期辦理物聯網設備使用及管理人員資安教育訓練。**

十四、施行

本管理政策經總經理核定後實施，修訂時亦同。

94 年 5 月 20 日訂定
108 年 6 月 25 日修訂
109 年 2 月 26 日修訂
109 年 12 月 21 日修訂