陽信證券股份有限公司

資通安全檢查編

103 年 7 月 11 日第六屆第 27 次董事會修正通過
107 年 12 月 19 日第八屆第 7 次董事會修正通過
109 年 2 月 25 日第八屆第 21 次董事會修正通過
110 年 1 月 22 日第八屆第 32 次董事會修正通過
110 年 8 月 20 日第九屆第 3 次董事會修正通過
111 年 9 月 21 日第九屆第 17 次董事會修正通過
111 年 10 月 20 日第九屆第 18 次董事會修正通過
112 年 1 月 12 日第九屆第 21 次董事會修正通過
112 年 6 月 20 日第九屆第 26 次董事會修正通過
112 年 8 月 11 日第九屆第 28 次董事會修正通過
112 年 9 月 13 日第九屆第 29 次董事會修正通過
113 年 5 月 23 日第九屆第 37 次董事會修正通過
114 年 4 月 24 日第十屆第 12 次董事會修正通過
114 年 7 月 17 日第十屆第 15 次董事會修正通過

第一章 資訊安全政策

壹、依據

台灣證券交易所最新版本「證券商資通安全檢查機制」及本公司業務需求訂定之。

貳、資訊安全定義

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，以確保資訊在蒐集、處理、傳送、儲存、使用及銷毀過程中之機密性、完整性及可用性，範圍包含作業相關之報表文件、電腦檔案、軟硬體設備、儲存媒體及人員之安全管理。

參、資訊安全目標

一、 確保交易資料之機密性，防止非法使用。

二、 確保資通系統之可用性及安全性。

三、 確保資訊業務運作之有效性及持續性。

肆、資訊安全範圍

一、 資訊安全權責分工。

二、 人員管理及資訊安全教育訓練。

三、 電腦系統安全管理。

四、 網路安全管理。

五、 系統存取管制。

六、 系統發展及維護安全管理。

七、 資訊資產安全管理。

八、 實體及環境安全管理。

九、 業務永續運作計畫管理。

十、 資訊安全稽核。

伍、資訊安全組織 (CC-13000，年度查核)

一、 本公司設「資訊安全推行小組」，由總經理擔任召集人，小組成員由稽核處、經紀業務處、行政管理處、資訊單位等部主管擔任委員，負責制定、應每年定期召開一次會議，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。

二、 應視資訊安全管理需要，指定專人或專責單位負責規劃與執行資訊安全工作，並應定期參加資訊安全教育訓練及通過評量。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。資訊處理部門與業務單位之權責，應明確劃分。

三、 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。

四、 公司應視資訊安全管理需要，指定專人或專責單位負責規劃與執行資訊安全工作，且資訊安全人員及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。其他使用資通系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程。

五、 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，本公司歸屬第 4 級(D 級)券商，如附表四「建立證券商資通安全檢查機制-分級防護應辦事項附表」(111.12.28)。

六、 公司應依其所屬資安分級辦理核心系統導入資訊安全管理系統，並通過公正第三方之驗證，且持續維持驗證有效性。本公司依分級規定暫不用辦理。

七、 公司應依其所屬資安分級要求資訊安全人員取得並維持相當資通安全專業證照。初次受核定或等級變更後之一年內，資通安全專責人員總計應持有一張以上，並持續維持證照之有效性。(113 年 12 月底)

陸、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，由資訊單位負責辦理。

二、 資訊技術類安全教育訓練，由資訊單位負責辦理。業務類資訊安全教育訓練，由稽核處會同相關業務單位辦理。

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

四、 資訊機密之維護及資訊安全使用管理之稽核，由稽核處會同有關單位辦理。

五、 人員進用之安全評估由人事單位負責辦理。

柒、公司所訂定之資訊安全政策，應經管理階層核准，並應正式發布要求所有員工共同遵守，並轉知與公司合作之公私機關（構）、提供資訊服務之廠商共同遵行。

捌、資訊安全作業規範

執行各項資訊作業時，應遵守「智慧財產權保護法」、「個人資料保護法」、「台灣證券交易所證券商內部控制制度標準規範」，並依照本公司各項資訊作業規定辦理。

玖、資訊安全事件之處理

一、 發現重大資訊安全事件，資訊單位即應通報「資訊安全推行小組」，應即評估設備、人力等，訂定應採行之應變措施，並將處理情形記錄備查。

二、 電腦設備經評估若無法正常運作，應即啟動備援作業；惟備援作業亦無法支援作業時，得連絡相關資訊廠商協助處理。

三、 緊急事件發生後應檢討並針對缺失研擬改進措施簽報上級，以防止類似事件發生。

拾、資訊安全之問責

本公司資訊安全依本政策各項目計畫、執行、檢查與行動，日常業務執行並受本公司設置之永續經營管理委員會督導，各級層業務於執行過程或結果導致公司經營上之重大疏失者，或嚴重影響公司正常運作者，專案提報董事會追究相關權責之討論。

第二章　員工申請登錄密碼或補發程序

本公司電腦系統員工若有新申請登錄密碼者，或忘記、變更、重新申請而需補發密碼者、須依下列步驟辦理：

壹、 向各部門主管報備。

貳、 填寫資通系統密碼申請表（附表一），並經部門主管簽章同意。

參、 由資訊人員建置密碼檔，確認為員工本人無誤後，補發新密碼。

肆、 提醒申請人注意，必須於補發使用後至少 3 個月定期更改密碼，再行使用。

第三章 資訊、電力故障復原處理程序

壹、 前檯故障復原處理：

一、 查看中華電信、遠傳電信 4M 專線是否正常。

二、 查看網路下單是否連線正常。

三、 查看即時報價資料是否正常。

四、 報請中華電信或遠傳電信查修。

壹、 後檯故障復原處理：

一、 進入備援交易系統（石牌與民生互相備援：主機位於石牌分公司、民生分公司，二台主機備援方式詳如附表二）。

二、 檢查交易所 PVC 連線是否正常。

三、 檢查分公司連線是否正常。。

四、 委託回報補列印。

五、 成交回報補送要求（交易所）、轉檔。

六、 報請中華電信或遠傳電信查修。

貳、 電力故障復原斷電：

一、 檢查ＵＰＳ是否正常運作。

二、 檢查發電機是否啟動。

三、 關閉非必要使用電腦。

四、 向電力公司查詢停電原因、及復原時間。

第四章　營運持續計劃政策

壹、依據

證券商資通安全檢查機制標準規範CC-20000 及本公司業務需求訂定之。

貳、實施條件

本公司啟動營運持續計劃程序條件大致分三類，自然災害、人為災害、設備事故。

第一類發生自然災害，台灣常見的颱風和地震等，自然現象造成的災害。

第二類發生人為災害，例如，縱火和偷竊等，人為造成的災害。

第三類發生設備事故，例如電力設備老舊引發的火災，或是網路設備異常，造成網路中斷，這些因設備不正常引發的問題就稱為設備事故。

參、目標

為建立本公司重大災害危機管理及緊急事故應變措施方式暨加強員工對災害緊急應變之認識，提高預防措施且員工能隨機應變，降低災害損害，儘速恢復公司正常運作。

肆、緊急應變小組：

本公司緊急應變小組由總經理擔任召集人，小組成員由稽核處、經紀業務處、行政管理處、資訊單位等部主管為主要成員，各單位若發生災害緊急事故，各單位主管應迅速聯絡「緊急應變小組」總召集人，並應迅即召開緊急應變小組會議，辦理相關應變事宜。

伍、緊急應變對策：

一、　平時預防措施：

（1）舉辦教育訓練與演練

各單位每年一次教育講習、訓練及實際演練，應留存相關記錄。

（2）加強設施安全維護檢查

本公司應加強各項防護設施，如消防、防震、防爆等科技設備及急救藥品、 器材等。對於水、電、瓦斯及各類防護設備均應定期檢修保養，危險、易燃物應加以隔絕保管，以避免危險及影響使用時堪用性。

（3）確保資訊設備在蒐集、處理、傳送、儲存、使用及銷毀過程中之機密性、完整性及可用性，範圍包含作業相關之報表文件、電腦檔案、軟硬體設備、儲存媒體及人員之安全管理。

二、　發生災害及緊急事故時作為：

（1）緊急應變小組應即至總管理處報告，統籌召開會議辦理各相關單位應變措施處理事宜。屬於天然災害侵襲時，須依「台灣證券交易所股份有限公司天然災害侵襲處理措施」配合辦理相關事項。屬於資訊設備故障致無法下單作業可至主管機關（交易所）申請借用交易所雲端備用之終端機設備。若營業處所無法正常營運時，須向主管機關(交易所)填寫「發生不可抗力事故繼續營業申請書」

准予得另覓臨時營業處所繼續營業。

各單位連絡通報人（主管）應即主動通報單位受災情況，俾以提供緊急應變小組為必要決策之考量。

（2） 各單位人員應相互勉勵，保持沉著、冷靜，確實執行本公司防護措施，緊急連絡通報人應立即回報防護措施之執行狀況。

三、 發生災害及緊急事故穩定後作為：

(1) 各單位連絡通報人(主管)應於災情穩定後，查看各營業單位，並將實情儘速通報緊急應變小組，並立即向上級主管暨相關單位聯絡通報，且依上級指示辦理相關復原事宜。

(2) 各單位主管、行政人員應立即主動關懷所屬人員，往來客戶之安全狀況。如有傷患，應立即救助與送醫，並向總管理處報告屬員安全狀況，俾利業務復原人力調配之參考。

(3) 擬訂對客戶宣告事項

各受災單位應即就災害狀況、停業期限、恢復正常營業時機或停業期間替代方案等事項，擬定對客戶宣告事項，並予公告，以避免引發客戶恐慌，影響客戶權益。

陸、業務復原措施：

緊急事故及災害發生後，本公司除應立即採行各項緊急應變對策外，尚需依據主管機關對各證券商受災時，其股務業務、交割事宜復原之相關規定措施辦理各項業務復原，以解決客戶金融需求。

柒、故障復原程序：

一、 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、 每半年舉行系統回復測試，測試後召開檢討會議，針對測試缺失謀求改進，並留存紀錄。

三、 主要之交易主機應有備援措施，每半年舉行備援演練，並留存紀錄。

四、 應訂定資訊安全訊息通報機制（例如：正式之通報程序及資安事件通報聯絡人），宜針對與資通系統有關之資訊安全事故，採取適當矯正程序，並留存紀錄。

五、 發生個人資料之竊取、竄改、毀損、滅失、或洩漏等資安事故者，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、 應明確訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序。

捌、其他附則：

一、 重大災害發生時之緊急應變、搶救復原措施，各單位主管應於平時利用各種機會向員工講解，使每人確實明瞭任務，熟練執行任務之方法與應變措施，使損害減至最低程度。

二、 為確保災害發生時，各項業務得以營運持續，各單位應衡量其營業規模、周遭環境、業務維護能力、員工應變能力等因素，指派緊急業務處理人

員，俾便善後工作及早進行。

玖、營運持續管理（CC-20000，半年查核）

（1） 應明確訂定（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）故障復原程序，並落實執行且留存紀錄。

（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） 證券經紀商之交易主機應有備援措施，並依所屬資安分級建置異地備援機房。

（4） 公司應執行營運衝擊分析，評估核心系統可容忍中斷時間、復原時間目標（RTO ）、資料復原點目標（RPO ），並擬訂營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及其必要之維護，依其所屬資安分級定期辦理業務持續運作演練，且視演練範圍是否涉及第三方，邀請相關廠商參與演練。網路下單證券商應依經紀業務規模市占率暨自然人客戶數比率分級，訂定核心系統可容忍中斷時間。

（5） 公司應訂定資訊安全訊息通報機制（例如：正式之通報程序及資安事件通報聯絡人），針對與資通系統有關之資訊安全或服務異常事件應依「證券期貨市場資通安全事件通報應變作業注意事項」及「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」辦理，並採取適當矯正程序，留存紀錄。

（6） 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，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。

（7） 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。

（8） 公司應辦理下列資安防護事宜：

1. 指定人員及部門統籌並協調聯繫各有關部門。
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。
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。

（9） 公司應辨識風險情境，就各項風險情境當災害發生造成資訊作業異常或中斷時，擬定各系統之應變、減災或復原措施相關作業流程。

（10）核心系統原服務中斷時，應於可容忍時間內，由備援設備或其他方式取代並提供服務。

（11）證券商資訊委外作業如涉及核心資通系統與資通服務，資訊服務供應商應定期提供資通系統與資通服務之回復計畫，回復計畫可以災難復原計畫、備援演練、營運持續計畫等形式呈現。

第五章　機密性及敏感性資料媒體處理程序

壹、 對可存取機密性、敏感性資訊或系統者及配賦系統存取特別權限之人員，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。

貳、 資訊委外服務契約註明涉及機密性、敏感性或關鍵性的應用系統之機密等級。

參、 機密性及敏感性資料之處理：

一、 機密性、敏感性的資料，防範洩漏或不法及不當的使用。

二、 敏感性資料之安全處理作業，加強下列事項：

(1) 輸出及輸入資料之處理程序及標示。

(2) 收受機密性、敏感性資料，除依一般規定辦理外，並有正式收文紀錄。

(3) 分發對象應以必要的人員為限；收受過程應避免不必要之經手。

(4) 為提醒使用者注意安全保密，應在儲存媒體上明確標示資料機密等級。

(5) 定期檢討機密性、敏感性資料的等級及分發對象。

肆、 內含機密性或敏感性資料的媒體報廢時，由專人以安全的方式處理，例如：燒毀、以碎紙機處理，或將資料從媒體中完全清除。

伍、 利用公眾網路傳送敏感性資訊，採取資料加密之保護措施。

陸、 存放機密性及敏感性資料之大型主機或伺服器主機，除作業系統既有的安全設定外，視需要使用安全等級較高之密碼辨識系統，以強化身份辨識之安全機制。

柒、 機密性及敏感性的資料或文件，不得存放在對外開放的資通系統中。

捌、 密等以上的公文及資料，不得以電子郵件傳送；敏感性資訊如有電子郵件傳送之必要，須經加密處理後傳送。

玖、 對機密及敏感性資料的處理，由業務單位自行於獨立的或是專屬的電腦作業環境中執行。

壹拾、 應視各業務單位之要求，對高敏感性的資料，在傳輸或儲存過程中以加密方法保護。

壹拾壹、 已列入安全等級分類的資訊及系統之輸出資料，應以文字及顏色標示適當的安全等級以利使用者遵循，例如：機密性為紅底黑字、敏感性為黃底黑字。

壹拾貳、 含有儲存媒體的設備，應在處理前詳加檢查，以確保機密性、敏感性之資料及有版權之軟體已被移除。

壹拾參、 公文及儲存媒體長時間不使用及下班後，應妥為存放；機密性、敏感性資訊，應妥為收存。

第六章 資訊設備故障復原檢核測試程序表

資訊設備故障復原檢核測試程序表 ／ ／	
一、與交易所、資訊廠商連線是否正常（含備援撥接）	
交易所 TCP 專線	
是 □ 總公司	□ 否
是 □ 分公司	□ 否
是 □ 集保公司專線	□ 否
是 □ 精業行情專線	□ 否
是 □ 總分公司備援專線	□ 否
二、與總分公司切換連線下單作業是否正常	
是 □ 盤中交易連線下單切換	□ 否
是 □ 定盤交易連線下單切換	□ 否
是 □ 零股交易連線下單切換	□ 否
三、交易主機資料庫存資料是否正常	
是 □ 定期檢查硬碟容量是否正常	□ 否
是 □ 定期刪除舊有資料	□ 否
是 □ 每日備份交易資料	□ 否
是 □ 通知由維護廠商作定期保養	□ 否
四、資訊、通訊設備運作是否正常	
是 □ 中菲 AS400 主機群是否正常	□ 否
是 □ 中菲中台主機群是否正常	□ 否
是 □ 三竹手機電子主機群是否正常	□ 否
是 □ 精誠 AP 電子主機群是否正常	□ 否
是 □ 奇唯興櫃主機群是否正常	□ 否
是 □ 台網主機群(含 ssca、ssra、ssl)是否正常	□ 否
是 □ 網路設備（LOADBALANCE、FIREWALL、SWITCH）是否正常	□ 否
是 □ 印表機（含前、後檯所有印表機）是否正常	□ 否
是 □ 是否與資訊廠商簽訂維護合約(軟硬體)	□ 否
是 □ 電話交換總機是否正常	□ 否
是 □ 語音總機是否正常	□ 否
是 □ 電話交換總機是否定期維護保養	□ 否
五、UPS、發電機運作是否正常	
是 □ UPS 電壓是否正常	□ 否
是 □ UPS 放電是否正常	□ 否
是 □ 電源開關後，發電機、UPS 是否正常啟動	□ 否
是 □ 發電機油料是否足夠	□ 否

是 □ 發電機、UPS 維護廠商是否定期保養		□ 否
總經理：	資訊主管：	經　辦：

第七章 資訊廠商遠端遙控管理程序

壹、平時防火牆政策關閉，必要連線時開防火牆政策。

貳、詢問處理內容、預估使用時間、動用資料及程式，作成紀錄。

參、給予廠商一組專用帳號及密碼。

肆、利用現有程式或指令監看處理狀況。

伍、離線後關閉防火牆政策，查詢電腦留存紀錄，比對第二項之紀錄並留存。

陸、更改廠商使用之密碼並留存紀錄。

第八章檢測電腦系統容量及安全措施規劃程序

壹、應隨時注意及觀察分析系統的作業容量，以避免容量不足而導致電腦當機。

貳、應進行電腦系統作業容量之需求預測，以確保足夠的電腦處理及儲存容量。

參、應特別注意系統之作業容量，預留預算及採購行政作業的前置時間，俾利進行前瞻性的規劃，及時獲得必要的作業容量。

肆、系統管理人員，應隨時注意及觀察分析系統資源使用狀況，包括處理器、主儲存裝置、檔案儲存、印表機及其他輸出設備及通信系統之使用狀況；管理人員應隨時注意上述設備的使用趨勢，尤應注意系統在業務處理及資訊管理上的應用情形。

伍、應隨時掌握及利用電腦及網路系統容量使用狀況的資訊，分析及找出可能危及系統安全的瓶頸，預作補救措施之規劃。

第九章 資通系統存取控制政策

壹、資通系統使用者存取管理

一、 使用者註冊管理

(1) 資通系統負責人應對所負責之系統使用人員予以管理。

(2) 資通系統負責人於受理業務使用人員註冊申請時，須考慮下列事項：

A. 是否重複申請使用該資通系統之正式授權。

B. 被授權的程度是否與業務目的相稱，是否符合資訊安全政策及規定。
C. 在系統使用者尚未完成正式授權程序前，資訊服務提供者不得對其提供系統存取服務。
D. 應建立及維持系統使用者註冊資料紀錄，以備日後查考。
E. 使用者調整職務及離（休）職時，應儘速註銷其系統存取權利。
F. 閒置不用的識別碼，不應重新配賦給其他的使用者。

二、 系統存取特別權限管理

(1) 資通系統負責人應針對使用者業務性質，賦予不同存取權限，並分開管理。
(2) 資通系統負責人如有必要賦予使用者系統存取特別權限，應依下列的授權程序管理：
A. 應確認系統存取特別權限事項，例如作業系統、資料庫管理系統、以及須賦予系統存取特別權限的人員名單。
B. 應依執行業務需求，視個案逐項考量賦予使用者系統存取特別權限；系統存取特別權限配賦，應以執行業務及職務所必要者為限。
C. 應建立申請系統存取特別權限授權程序，並只能在完成正式授權程序後，才能配賦給使用者；另外，應將系統存取特別權限之申請及授權資料建檔，以明責任及備日後查考。

貳、系統存取之責任

一、 使用者通行碼管理

(1) 使用者帳號，原則上採單一帳號，亦即每一員工在不同的資通系統，須使用相同的使用者帳號。
(2) 使用者通行碼之配賦、管理要點如下：
A. 個人應負責保護通行碼，維持通行碼的機密性。
B. 應避免將通行碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。
C. 當有跡象足以顯示系統及使用者密碼可能遭破解時，應立即更改密碼。
D. 應儘量避免以下列事項作為通行密碼：
甲、 年、月、日等時間資訊。
乙、 個人姓名、出生日、身分證字號或汽機車牌照號碼。
丙、 機關、單位名稱、識別代碼或是其他相關事項。
丁、 電話號碼。
戊、 連續數字。

二、 暫時不使用或無人看管設備之安全管理

(1) 當作業結束時，應關閉有效的通信管道。
(2) 當通信結束時，應完全登出電腦系統，不宜只關閉電腦系統或是端末機。
(3) 當個人電腦或終端機不使用時，應使用鍵盤鎖或其他控管措施保護個人電腦及端末機的安全。

參、電腦系統之存取控制

一、 登入程序

登入本公司任何電腦系統，均須作身分鑑別，其查驗考量程序如下：

(1) 在登入成功之前，不應顯示系統及應用系統識別碼。

(2) 系統不應在登入程序中，提供未經授權的使用者有關登入系統的說明或協助性的訊息。

(3) 只有在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正確性；如果登入發生錯誤，系統不應顯示那一部分資料是正確的，那一部分資料是錯誤的。

(4) 應限制系統登入不成功時可以再嘗試的次數，原則上以三次為原則。

(5) 在系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。

(6) 應限制系統登入程序的最長及最短時間，如果超出時間限制，系統應自動中斷登入。

二、 使用者密碼管理

(1) 登入本公司電腦系統的使用者，一律須使用密碼。

(2) 本公司對於使用者密碼的規定如下：

A. 使用者得申請更改密碼；系統應具備資料輸入錯誤之更正功能。

B. 使用者至少三個月須更改密碼一次。

C. 更改密碼應避免再次使用已用過的密碼。

D. 使用者密碼應與應用系統資料分開存放。

E. 使用者密碼的選定，應符合下列條件：

甲、 不得使用與日期有關的年、月、日。

乙、 不得使用公司名稱、識別碼或是其他參考性資訊作為通行碼。

丙、 不得以使用者識別碼團體識別碼或其他系統識別碼作為使用者通行碼。

肆、外部人員存取資訊之安全管理

一、 第三者存取本公司資訊設施，應於實際存取作業前，簽訂正式的契約或協定，俟契約或約定生效後始能提供存取服務。

二、 契約或協定內容應規定第三者須遵守之資訊安全規定、標準及必要的連線條件。

伍、存取控制（CC-18000，每月查核）

(1)訂定資通系統存取控制相關規定，並以書面、電子或其他方式告知員工遵守。

(2)權限管理：

a. 對於程式的存取使用，應有詳細的書面管制說明。

b. 人員異動時應及時更新其使用權限。

c. 對於程式及檔案之存取使用，應按權限區分。

d. 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。

e. 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）。

f. 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）。

(3)密碼管理：

a. 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。

b. 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。

c. 對於使用者及客戶忘記密碼之處理，公司應有嚴格的身分確認程序(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，方可再使用系統。

d. 初始密碼應隨機產生，並與使用者及客戶身分無關。(本項不適用採自行訂定交付電子式交易密碼條之方式)

e. 密碼輸入錯誤次數達五次者，應予中斷連線及鎖定該帳號至少十五分鐘不允許該帳號繼續嘗試登入，並留存紀錄。公司於接獲客戶聯繫申請解除鎖時，應確實辨認身分（如聯繫客服驗證基本資料、 OTP、臨櫃辦理等方式），並留存相關紀錄後，始得辦理之。

f. 除語音按鍵下單外，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）並進行管控，及加強宣導客戶定期更新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。

g. 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。

h. 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：

(a)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。

(b)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。

(4)電腦稽核紀錄管理：

a. 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。

b. 對上開重要系統之電腦稽核紀錄，應有專人定期檢視。

c. 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。

(5)資料輸入管理：

a. 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。

b. 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。

c. 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。

d. 公司如屬公開發行公司者，應於內部控制制度納入「公開發行公司網路申報公開資訊應注意事項」，並據以辦理相關申報事宜。

e. 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。

f. 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。

g. 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。

h. 公司應定期或不定期稽核依「個人資料保護法」定義之個人資料管理情形。

i. 前揭個人資料，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記錄。

j. 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」。

(6)資料輸出管理：

a. 報表是否按時產生並分送各使用單位。

b. 機密性、敏感性之報表列印或瀏覽是否有適當之管制程序。

c. 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）。

d. 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。

第十章　資訊安全事件通報暨作業處理程序

法條：「台灣證券交易所股份有限公司天然災害侵襲處理措施」(附表三)

壹、依據本公司內部控制制度 CC-2000 營運持續管理業務需求，為有效掌握資訊及網路系統遭受破壞、不當使用等危安或重大災害事件時，能迅速通報及緊急應變處置，並在最短時間內回復，以確保正常運作，特訂定資訊安全事件通報暨作業處理程序。

貳、資訊安全事件範圍：

內部危安事件—發現(或疑似)遭人為惡意破壞毀損、資料遭竊等。

外部攻擊事件─病毒感染事件、駭客攻擊(或非法入侵)事件。

天然災害事件─颱風、水災、地震。

重大突發事件─火災、爆炸等。

參、資安事件等級概分為四級：

『A』級：影響公共安全、社會秩序、人民生命財產。

『B』級：系統停頓、業務無法運作。

『C』級：業務中斷，影響系統效率。

『D』級：業務短暫停頓，可立即修復。

肆、資安事件危機通報作業：

一、 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），應迅速通報權責主管及相關人員立即處理。

二、 員工及與機關簽訂資訊安全協定的外部人員，需明確告知各種資訊安全事件的反應，使其瞭解相關的應變處理程序。

三、 各單位資訊或通信系統發生危安事故時，應立即向本公司「資訊安全推行小組」反應事實或請求支援，完成內部通報流程。

四、 各單位如遇資安事件，危及人員生命或設備遭到破壞等涉及民、刑事案件時，應即時通報檢警單位請求處理。

伍、資安事件分類應變步驟如下：

一、 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，啟用備分資料、程式或啟動備援計畫相關措施，期儘速回復正常運作。

二、 外力入侵事件：

(1) 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。

(2) 駭客攻擊（或非法入侵）事件：發現（或）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。

(3) 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。正式紀錄入侵情形及損失評估等資料，以供防護與預警之參考，並向檢警單位反映。

陸、資訊安全弱點之反映：

一、 員工隨時注意資通系統或資訊設備內部之安全弱點、可能面臨的威脅，並迅速告知直屬業務主管或是系統服務廠商。

二、 系統安全上的弱點，由專業人員陪同處理，不任由系統使用者自行修改並且備份。

柒、軟體功能不正常之反映

一、 使用者發現軟體功能有異常時，迅速告知資訊支援單位或是服務廠商處理。

二、 建立軟體功能不正常之反映及處理程序：

(1) 注意螢幕上出現的徵兆或訊息。
(2) 立即停止使用電腦，迅速通知資訊支援單位。
(3) 檢視軟體功能不正常的設備，再次啟動前，以離線方式處理。
(4) 在任何狀況下，使用者不自行移除功能不正常的軟體；系統回復作業應由受過適當訓練及有被授權的人員，才可執行系統及資料回復作業。

捌、復原追蹤及改善措施：

一、 發生資訊危安單位執行災後復原工作，首先檢驗資通安全環境及硬體設備是否可以正常運作，並執行環境重建、系統復原及掃描作業，其步驟包含軟硬體設備重新取得建置、重置作業系統及應用系統，以及運轉測試等；並俟運作正常後即進行安全備份檔案下載、資料回復、資料重置等相事宜。

二、 當危機解除後，發生單位應將災害應變處置復原過程相關完整紀錄，如事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料，予以建檔管制，以利加強資訊安全管理。

第十一章　通訊與作業管理（CC-17000）

(1) 網路安全管理（CC-17010，每月查核）

a.網路系統安全評估：

(a)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。

(b)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。

(c)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。

(d)各電腦主機、重要軟硬體設備應有專人負責。

(e)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)。

(f)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。

(g)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。

(h)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管及多因子身分認證，並留存相關維護紀錄並由權責主管定期覆核。

(i)公司應防止未經授權設備使用內部網路。

(j)應避免使用生命週期終止（End of Service,EOS／End of Life,EOL）之軟體及網路設備，且於到期前擬定汰除計畫，並視情況建立補償性措施。

b.防火牆之安全管理：

(a)應建立防火牆。

(b)防火牆應有專人管理。

(c)防火牆進出紀錄及其備份應至少保存三年。

(d)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。

(e)防火牆系統之設定應經權責主管之核准。

(f)公司應每年定期檢視並維護防火牆存取控管設定，每半年檢視 DMZ 區之防火牆規則，包含評估高風險設定及六個月內無流量之防火牆之必要性，及針對已下線資通系統於六個月內調整或停用該規則，並留存相關檢視紀錄。

(g)公司建立網路設備規則應以最小授權及正面表列為原則。

(h)公司應至少每年檢視一次對外網路設備規則，並留存相關紀錄。

c.網路傳輸安全管理：

(a)網路下單畫面應採加密方式（例如：SSL）處理。

(b)公司應每日針對核心系統之帳號登入失敗紀錄、非客戶帳號嘗試登入紀錄等進行監控及分析，發現有帳號登入異常情事(如密碼輸入錯誤達三次、一定時間內大量帳號登入失敗、帳戶申請或更新憑證下載異常)，應即時了解異常原因，並留存相關紀錄。

(c)公司提供網路下單服務，應於網路下單登入時採多因子認證方式(例如：下單憑證、綁定裝置、OTP、生物辨識等機制)，以確保為客戶本人登入。

(d)公司加密機制應優先考慮使用公開、國際機構驗證且未遭破解之演算法。

d.多因子驗證：

公司使用多因子驗證應具下列三項之任兩項技術：

（a）公司所約定之資訊，且無第三人知悉（如固定密碼、圖形鎖或手勢等）。

（b）客戶所持有之實體設備（如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等），公司應確認該設備為客戶與公司所約定持有之設備。

（c）客戶提供給公司其所擁有之生物特徵（如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），公司應直接或間接驗證該生物特徵。

e.身分認證與憑證管理

（a）網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，必須採用多因子（如：下單憑證、綁定裝置、OTP 、生物辨識及 SIM 認證等）驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀錄。

（b）網路下單證券商應全面使用認證機制。

（c）公司應於伺服器端驗證客戶交易身分及使用者帳號。

（d）公司對電子交易身分之申請、交付、使用、更新與驗證應訂定相關規範。

f. 電腦病毒及惡意軟體之防範：

（a）應安裝防毒軟體，並及時更新程式及病毒碼。

（b）應定期對資通系統及資料儲存媒體進行病毒掃描（含電子郵件）。

（c）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。

（d）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。

（e）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。

（f）公司應建立軟體白名單控管機制。

（g）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。

（h）公司應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。　f. 網路系統功能檢查：

（a）應定期檢查網路下單系統提供之功能，並留存紀錄。

（b）應就網路提供外部連線使用系統偵測網頁與程式異動、記錄並通知相關人員處理。

g. 網路系統功能檢查：

（a）應定期檢查網路下單系統提供之功能，並留存紀錄。

（b）應就提供外部連線使用網路系統偵測網頁與程式異動、記錄並通知相關人員處理。

h. 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。

i. 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、交易之穩定及系統可用性、提供客戶服務。

j. 網路攻擊防護機制導入及安全性檢測

（a）公司應依其所屬資安分級定期對提供網際網路服務之核心系統辦理滲透測試，並依測試結果進行改善。

（b）公司應依「證券商辦理資通系統資訊安全評估作業程序」並就其所屬資安分級定期辦理資通安全健診作業。

（c）公司應依其所屬資安分級建立資通安全威脅偵測管理機制（應

含括事件收集、異常分析、偵測攻擊並判斷攻擊行為）

（d）公司應依其所屬資安分級建立入侵偵測及防禦機制。

（e）公司應依其所屬資安分級設置應用程式防火牆。

（f）公司應依其所屬資安分級辦理進階持續性威脅攻擊防禦措施。

（g）核心系統身分驗證機制應防範自動化程式之登入或密碼更換嘗試，非核心系統宜防範自動化程式之登入或密碼更換嘗試。

k.帳號登入或異常態樣通知：

公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣應即通知客戶，並留存紀錄，避免非客戶本人登入情事：

（a）密碼輸入錯誤或帳戶被鎖定。

（b）申請或更新憑證。

（c）變更基本資料。

（d）異常來源或行為嘗試登入等

（e）密碼申請異動或補發時。

l.異常 IP 登入之監控與預警：

公司應對異常及不明來源 IP 連線進行監控分析及留存紀錄，如有發現下列情形，應設有警示機制，並定期檢視以確認機制有效運作：

（a）同一來源 IP 登入不同帳號達一定次數以上。

（b）同一帳號在一定時間內由不同國家登入。

（c）發現異常來源（如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單或國外 IP ）嘗試登入。

m.無線網路管理：

（a）公司設置無線網路應採用現行公開資訊已認可且無弱點之安全協定。

（b）公司提供內部無線網路使用應限內部人員公務用或資訊服務供應商申請核准後使用。

(2) 電腦系統及作業安全管理（CC-17020，半年查核）

a.電腦設備之管理：

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。

b.電腦作業系統環境設定及使用權限設定：

(a)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。

(b)電腦系統檔案異動前後皆有完善之備份處理措施。

(c)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。

(d)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）。

(e)公司透過網際網路使用帳號登入系統時，應採用多因子認證機制。

c. 電腦媒體之安全管理：

(a)重要軟體及其文件、清冊應抄錄備份存於另一安全處所。

(b)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。

(c)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。

(d)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。

(e)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。

d. 電腦操作管理：

(a)操作人員應確實依規定操作程序執行。

(b)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。

(c)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。

e. 證券經紀商應配備經營業務所需、且有適足容量之電腦系統。

f. 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。

第十二章 系統開發及維護（CC-19000，半年查核）

(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)委外廠商管理：

a. 公司與委外資訊服務供應商提供服務應訂定合約，合約所含內容應包含以下內容：合約期限、服務範圍、服務交付日期、服務水準要求、服務變更規範、服務驗收之標準、資通安全事件通報及應變處理作業程序、對資訊服務供應商之稽核權條款、合約轉讓或同意分包之規範、保密義務條款、罰則與損害賠償條款、爭議處理程序、違約處理條款、合約終止規範、合約終止後之處理、保固、權利及責任。

b. 證券商應針對資訊委外業務項目之資通安全風險與委外作業可行

性，及資訊服務供應商作業能力及集中度，由相關資訊單位共同執行風險評估，評估結果應提報適當管理層級並取得同意。

c. 資訊服務供應商應提供安全性檢測證明（如行動應用程式資安檢測、源碼檢測、弱點掃描等），並應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過源碼掃描或黑箱測試。

d. 公司應訂定相關規範管控，與資訊服務供應商資訊委外關係於終止、解除或結束後之相關作業。

e. 委外資訊服務供應商應揭露第三方程式元件之來源與授權證明。

f. 公司應管控資訊服務供應商存取權限，對於電腦通行使用權利進行適當控管。

g. 公司應對資訊服務供應商服務內容變更進行風險評估。

h. 公司對於委外資訊服務供應商於委外關係所涉及公司資訊資產，應於委外關係終止、解除或結束時完整歸還、確保銷毀或轉交予其他資訊服務供應商，並要求資訊服務供應商持續遵守保密承諾。

i. 委外資訊服務供應商如自行發現程式漏洞、版本老舊，或於使用相同服務之其他證券商應用系統發生故障或異常時，應儘速瞭解原因，並主動轉知及提供因應措施。

j. 委外資通系統之服務規格書應包括硬體規格、軟體版本、作業環境變動、作業系統底層架構及系統程式相容性等，並包含維持委外廠商服務水準之要求與橫向溝通機制。

k. 公司應載明資訊服務供應商配合進行壓力測試及調整服務負載量之義務，並於市場交易量、業務變化及客戶屬性等發生顯著異動時發動辦理，俾憑評估系統資源調配或擴增。

l. 公司於資訊服務委外期間應定期對資訊服務供應商進行稽核，並應要求資訊服務供應商定期提交服務水準報告，相關結果應提報適當管理層級審查。

(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：

a. 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。

b. 程式經修改其相關文件應及時更新。

c. 系統變更完成後須檢核與申請內容是否相符，並進行必要驗證以確認變更作業之正確性。

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

(10)程式原碼安全規範：

a.程式應避免含有惡意程式等資訊安全漏洞。

b.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。

c.程式於引用之函式庫有更新時，應備妥對應之更新版本。

d.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。

e.委外開發之行動應用程式如涉及機敏性資料傳送(如：客戶帳號密碼或交易資料等)應自行或委外檢視驗證傳遞對象是否適當並留存相關紀錄。

f.無法取得程式原碼時，應要求程式提供者符合上開前四項(a、b、c、d、e)安全事項。

(11)行動應用程式安全管理：

a.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」。

b.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。

c.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。

第十三章　新興科技應用(CC-21100，年度查核)

壹、行動裝置：

a. 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：

(a). 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。

(b). 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。

(c). 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。

(d). 公務用行動裝置管理辦法內容應包含行動裝置儲存機密資料之限制與管理方式。

b. 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：

(a). 公司應要求員工自攜行動裝置使用用途。

(b). 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。

(c). 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。

(d). 員工自攜行動裝置管理辦法內容應包含行動裝置儲存機密資料之限制與管理方式。

貳. 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：

a. 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。

b. 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。

c. 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。

d. 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。

e. 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。

f. 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。

參. 遠距辦公：

a. 公司應對使用遠距辦公之設備安裝資訊安全相關軟體，控管應用程式存取權限，以降低資訊外流風險。

b. 公司應依業務範圍及控管權限設定遠距辦公員工之系統功能權限，且妥善設定遠距辦公軟體(如禁止連接至本機印表機、跨端剪貼資料等)。

c. 公司應依員工執行業務內容訂定連線時段限制及相關規範，並設定閒置時間螢幕鎖定或中斷連線機制。

d. 公司應留存遠距辦公員工使用者登入系統、電腦設備操作及交易紀錄軌跡。

e. 公司應採多因子驗證機制（員工帳號密碼、動態密碼、一次性帳密）及建立安全的遠距網路通道，降低相關帳號密碼遭假冒或竊用之風險。

f. 公司應阻擋惡意或未經授權之連線，並採用最小權限原則設定遠距帳號存取規則。

g. 公司應定時更新 VPN 連線和其他遠端連結系統之安控措施。

h. 公司應對客戶隱私、資料及紀錄之安全性建立保護措施。

i. 公司應加強宣導資訊安全，教育遠距辦公員工應對網路風險保持警覺等資訊安全機制。

肆、 深度偽造（Deepfake）

a. 使用影像視訊方式進行身分驗證時應強化驗證並搭配其他驗證因子（如上傳身分證件、手機簡訊 OTP）。

b. 應定期辦理涵蓋深度偽造認知及防範議題之資訊安全教育訓練。

伍、 人工智慧（AI）：

a. 使用人工智慧技術應列有清冊並加以維護，且應遵循資通安全、個人資料保護、智慧財產權等金融法規及其他法律規範與相關資訊使用規定。

b. 使用人工智慧技術與客戶直接互動時，應告知該互動或服務係利用人工智慧技術自動完成，或揭露其適用人群、場景或用途。

第十四章　其他（CC-22000，半年查核）

資訊提供作業（CC-22010）

a. 各種重要法令規章及通知應立即張貼於公佈欄。

b. 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。

c. 營業廳內應裝置「公開資訊觀測站」，供客戶自行操作使用。

d. 資訊閱覽室應未限定對象並且無收費行為。

e. 資訊閱覽室不得裝設專用競價用終端機。

f. 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。

g. 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。

h. 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。

i. 證券商若於網站平台上進行推介，應設有密碼以控管得閱覽個股研究報告之客戶；且客戶應與證券商簽訂推介契約（國內機構投資人及外國機構投資人得免簽）。

第十五章　安全控管

壹、 風險評鑑與管理（CC-11000，年度查核）

(1)應鑑別公司適用資訊安全風險範圍內之所有資訊資產以及其擁有者。

(2)應確定公司各作業可接受之資訊安全風險等級。

(3) 公司應至少每年進行一次資訊安全風險評鑑，並留存相關紀錄，營運相關的重大風險與控管措施議題（包括新產品、新興技術和資訊系統的風險）應納入風險評估範圍，以確保公司政策、程序和控管措施之有效性。

貳、資產分類與控制（CC-14000，半年查核）

(1)資訊資產且包含軟體、硬體、場地及資料等類別，應列有清冊，並應加以維護。

(2)應訂有資訊分級並作標示處理之相關規範。（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商）

(3)公司應對自行或委外開發之資通系統完成資通系統分級，資通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通系統分級妥適性。

(4)公司應對資訊資產之資料與文件的保存期限進行規範，並於保存期限到期後進行刪除與銷毀。

(5)公司應避免使用危害國家資通安全產品。

叁、人員安全（CC-15000，半年查核）

(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，每年並達內部所定訓練時數。

(5)證券商應設置電腦稽核人員。（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商。

肆、實體與環境安全（CC-16000，半年查核）

(1)電腦機房應有門禁管制（例如：刷卡）。

(2)機房應有防火設施，並應定期檢驗。

(3)另應將地震、水災等天然災害因素列入考量。

(4)電腦設備之電源供應系統應含不斷電設備及發電機。

(5)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。

(6)公司應定期審查電腦機房門禁管制權限。

第十六章　附則

壹、本資訊安全政策經 董事會核定後實施，修正時亦同。

（附表一）

本表係依據本公司資通系統存取控制政策辦理　　機密等級:□一般□敏感□機密

紀錄編號:

陽信證券資通系統需求申請單

所屬單位				申請日期	年　月　日
員工姓名	申請人親簽	營業員編號		分機號碼	
有效期間	□永久 □　年　月　日至　年　月　日			希望完成日期	年　月　日
資通系統類別申請	**□新增　□異動　□刪除**				
申請系統	**□後台帳務系統 、前台系統　□營業員自打系統　□交易暨帳務管理系統** **□營業員查詢系統　□其他(　　)**				
申請項目	**□功能增修　□系統安裝　□帳密申請　□資料下載**				
申請原因	(請務必填寫)				
附　件	**□無附件　□有附件(　　)**				

需求說明：1.資料下載與相關報表增修需求**應檢附檔案或報表格式文件**，以供程式設計參考。

需求說明：2.帳密申請：請填寫預設定之**帳號：**＿＿＿＿＿＿＿＿**密碼：**＿＿＿＿＿＿

注 意 事 項 ：功能增修：請於「申請系統」欄勾選欲增修之系統，並於「需求說明」欄詳述功能名稱、增修內容及使用時機，跨單位需求交會辦單位加註意見再送資訊部門。

簽核流程	總經理	會簽單位	單位主管

收件日期		預計完成日期	
處理項目			
	□需求明確　□需求不明確　□實施並列入進度　□暫緩實施		
處理說明：			

申請人/測試日期	申請人/驗收日期	承辦人員	資訊單位主管

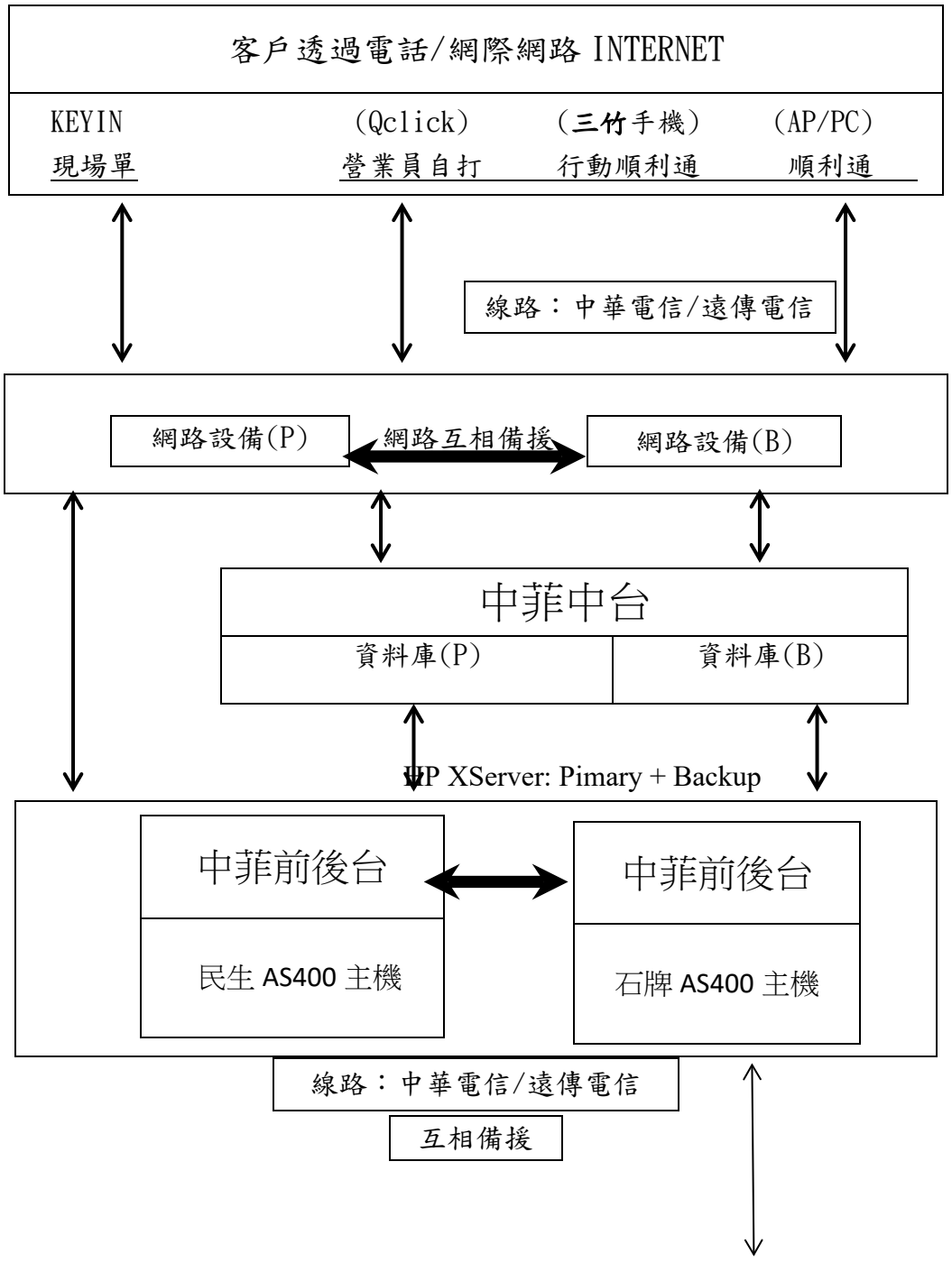
備註：1.請用優質密碼，長度須超過六個字元且具有文數字，三個月定期更新。

2.申請更新密碼時，請同時註銷舊密碼。

3.本申請表由資訊單位留存正本備查。

（附表二）

陽信證券主機備援架構圖



（附表三）

依據「臺灣證券交易所股份有限公司天然災害侵襲處理措施」規定，投資人對證券商之應屆交割款項依下列原則處理：

一、天然災害侵襲時本公司集中交易市場全日休市：

台北市市長宣布當日或當日上午台北市全體公教機關停止上班時，本公司集中交易市場全日休市，全體證券商當日停止營業，投資人對證券商之應屆交割款券順延辦理。

二、天然災害侵襲時本公司集中交易市場全日不休市：

1. 天然災害侵襲時，總分公司均在受災區域外之證券商正常營業，投資人對證券商之應屆交割款券正常辦理。
2. 天然災害侵襲致當地縣市政府首長宣布當日全體或局部區域公教機關停止上班時，於受災區域內之證券商得自行決定是否照常營業，不論營業否，投資人對證券商之應屆交割款順延辦理，應屆交割有價證券，其帳簿劃撥交割部分正常辦理。
3. 台北市市長宣布當日下午台北市全體公教機關停止上班時，本公司集中交易市場不休市，投資人對證券商之應屆交割款券正常辦理，惟收盤後其他交易均予停止。當日成交之鉅額買賣屬成交日交割者，其款券交割均順延辦理。

三、天然災害侵襲，證券商所在地正常上班，而投資人所在地卻停止上班，導致投資人無法如期履行交割時，可由證券商先行彙整因為天然災害侵襲致無法交割之投資人資料，向本公司申報備查並代辦交割手續。（97 年 8 月 1 日臺證交字第 0970204056 號）。

（附表四）

建立證券商資通安全檢查機制-分級防護應辦事項附表（114.07.03）