臺灣證券交易所
TAIWAN STOCK EXCHANGE
流通證券・活絡經濟

竭誠為您服務

主機共置服務
查核缺失態樣暨未來查核方向

券商輔導部
109年12月31日

企業籌資更便捷 大眾投資更穩當 ・ 企業資訊更透明 交易機制更公正 金融商品更多元

主機共置服務管理辦法相關規定

- 主機共置服務管理辦法第11條第2項規定，證券商經紀業務使用本服務前，應自訂使用規則且納入企業內控及稽核制度，並依使用規則公平對待投資人；經投資人檢舉或主管機關發現有違反使用規則情事者，本公司得暫停服務；經本公司通知限期改善而未改善者，得終止契約。

- 主機共置管理辦法第14條規定，本服務使用者不得將機櫃空間分租、轉租、出借或以任何方式提供第三人使用。

- 主機共置管理辦法第19條規定，使用者放置於主機共置機房之軟體、硬體設備應具備完善之資訊安全防護措施，並應定期執行安全漏洞偵測及修補作業。

主機共置專案查核範圍

CA-11210受託買賣及成交作業『公司經營經紀業務且與證交所簽訂主機共置服務契約者，應依「主機共置服務管理辦法」規定辦理，使用該服務前，應自訂使用規則並於公司內部控制制度制定適當之控管機制及查核程序(請公司自訂)』

1.盤點證券商置放於主機共置機房之相關設備。
2.瞭解證券商主機共置服務使用情形是否公平對待投資人。
3.系統控管情形(僅提供給少數客戶使用之證券商)。

TAIWAN STOCK EXCHANGE

本次查核未盡妥適之處

- 未公平對待投資人。
- 主機共置機櫃存放客戶軟、硬體或提供第三人使用。
- 交易指令係由軟體自行運算產生，並將委託資料傳送至證交所主機，未留存接收客戶委託時間。
- 主機共置服務網路連接證交所之設備未裝置防火牆，或防火牆之進出紀錄及備份未完整保存。
- 最高權限帳號提供廠商使用。
- 系統使用密碼未依規定時間變更。
- 系統稽核日誌紀錄內容(包括使用者識別碼、登入日期時間等)未依規完整保存。
- 未依規定時間辦理弱點掃描作業，未針對所辨識出之潛在系統弱點，評估其相關風險及安裝修補程式，並留存紀錄。

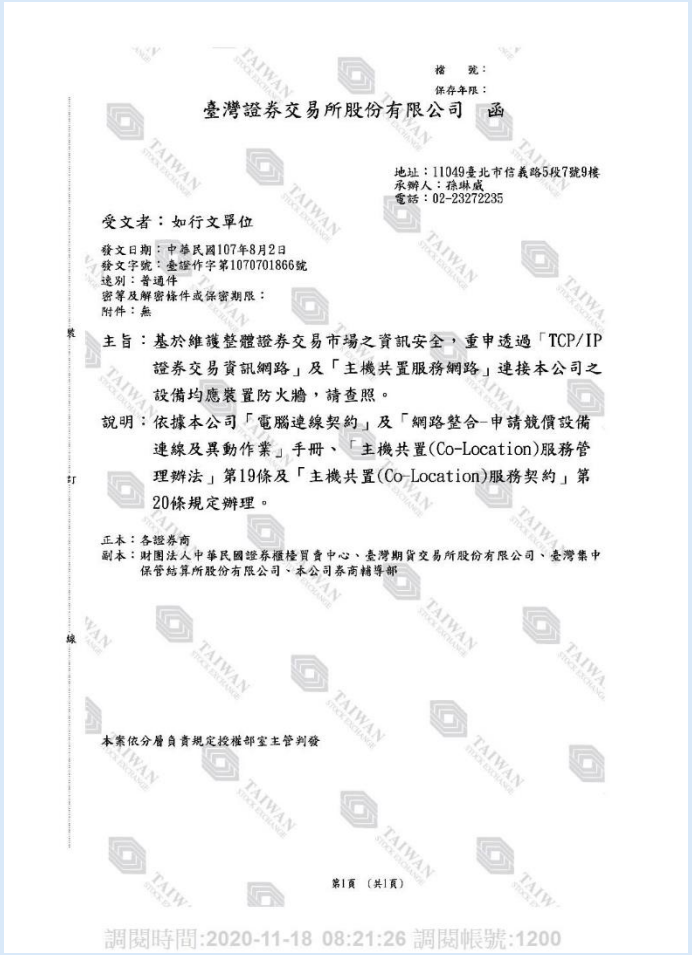
查核發現一

查核發現	現行規範
交易指令係由軟體自行運算產生後，將委託資料傳送至證交所主機，未留存接收客戶委託時間。	CA-11210 受託買賣及成交作業 (二十二)「對於以語音、網際網路、專線、封閉式專屬網路等電子式交易型態委託者，得免製作、代填委託書，惟應依時序別即時列印買賣委託紀錄，並由經辦人員及部門主管簽章，委託紀錄應含委託人姓名或帳號、委託時間……」

查核發現二

查核發現	現行規範
主機共置服務網路連接證交所之設備未裝置防火牆，或防火牆之進出紀錄及備份未完整保存。	CC-17010 網路安全管理 (二)防火牆之安全管理： ➢ 應建立防火牆。 ➢ 防火牆進出紀錄及其備份應至少保存三年。

應建立防火牆



檔　號：
保存年限：

臺灣證券交易所股份有限公司　函

地址：11049臺北市信義路5段7號9樓
承辦人：孫琳威
電話：02-23272235

受文者：如行文單位

發文日期：中華民國107年8月2日
發文字號：臺證作字第1070701866號
速別：普通件
密等及解密條件或保密期限：
附件：無

主旨：基於維護整體證券交易市場之資訊安全，重申透過「TCP/IP證券交易資訊網路」及「主機共置服務網路」連接本公司之設備均應裝置防火牆，請查照。

說明：依據本公司「電腦連線契約」及「網路整合-申請競價設備連線及異動作業」手冊、「主機共置(Co-Location)服務管理辦法」第19條及「主機共置(Co-Location)服務契約」第20條規定辦理。

正本：各證券商
副本：財團法人中華民國證券櫃檯買賣中心、臺灣期貨交易所股份有限公司、臺灣集中保管結算所股份有限公司、本公司券商輔導部

本案依分層負責規定授權部室主管判發

第1頁 (共1頁)

調閱時間:2020-11-18 08:21:26 調閱帳號:1200

- 本公司電腦作業部於107年8月2日發函各證券商，重申透過「TCP/IP證券交易資訊網路」及「主機共置服務網路」連接本公司之設備均應裝置防火牆。

查核發現三

查核發現	現行規範
最高權限帳號提供廠商使用。	CC-18000 存取控制 (二)權限管理： ➢ 查核委外人員所使用之電腦紀錄，確認未授予委外人員過高之電腦通行使用權利或不當使用權，且於委外期間結束後，立即收回該項權利，以免被盜用、竄改資料。

查核發現四

查核發現	現行規範
系統使用密碼未依規定時間變更。	CC-18000 存取控制 (三)密碼管理： ➢ …，公司其他使用者之密碼應至少每三個月變更一次。

查核發現五

查核發現	現行規範
系統稽核日誌紀錄內容(包括使用者識別碼、登入日期時間等)未依規完整保存。	CC-18000 存取控制 (四)電腦稽核紀錄管理： ➢對重要系統（如主機連線系統、網路下單系統等）之稽核日誌紀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。 ➢對上開重要系統之電腦稽核紀錄，應有專人定期檢視。 ➢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。

查核發現六

查核發現	現行規範
未依規定時間辦理弱點掃描作業，未針對所辨識出之潛在系統弱點，評估其相關風險及安裝修補程式，並留存紀錄。	CC-19000 系統開發及維護 (十四)資訊系統弱點掃描： ➢ 各資訊系統應定期(至少每半年一次)進行弱點掃描。

查核發現七

查核發現	現行規範
未公平對待投資人。	主機共置服務管理辦法 第十一條 ➢ 證券經紀商業務使用本服務前，應自訂使用規則且納入企業內控及稽核制度，並依使用規則公平對待投資人.....。

查核發現八

查核發現	現行規範
主機共置機櫃存放客戶軟、硬體或提供第三人使用。	主機共置服務管理辦法 第十四條 本服務使用者不得有下列情形 ➢ 七、除符合第十五條共同使用同一機櫃情形者外，將機櫃空間分租、轉租、出借或以任何方式提供第三人使用。

TAIWAN
STOCK EXCHANGE

未來查核方向

- 網路安全管理CC-17010。
- 電腦系統及作業安全管理CC-17020。
- 存取控制CC-18000。
- 系統開發及維護CC-19000。

網路安全管理CC-17010

網路系統安全評估

- 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，留存相關維護紀錄並由權責主管定期覆核。

防火牆之安全管理

- 應建立防火牆。
- 防火牆進出紀錄及其備份應至少保存三年。
- 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。
- 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。

電腦作業系統環境設定及使用權限設定

- 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。

存取控制CC-18000

權限管理

- 申請使用系統資源之人員以書面提出申請：申請內容應註明使用目的及權限、每一使用者限用唯一代碼。
- 申請內容應經使用單位主管及資訊單位主管核可後辦理。
- 查核委外人員所使用之電腦紀錄，確認未授予委外人員過高之電腦通行使用權利或不當使用權，且於委外期間結束後，立即收回該項權利，以免被盜用、竄改資料。
- 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)」。

存取控制CC-18000

密碼管理

- 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），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。
- 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。

存取控制CC-18000

電腦稽核紀錄管理

- 對重要系統（如主機連線系統、網路下單系統等）之稽核日誌紀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。
- 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。

系統引進

- 如應用系統委託專業機構辦理者，應注意下列重點：
  1. 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。
  2. 委外作業之開發、設計、程式撰寫、測試、驗收等各段依合約規定程序進行，並備妥各階段之相關文件程式於引用之函式庫有更新時，應備妥對應之更新版本。

系統維護

- 應用系統之程式、作業方式或其他內容需更動時由提出需求人員填具書面申請資料，交應用系統維護人員表示意見。
- 呈相關權責主管核定後由應用系統維護人員負責辦理。
- 需求經修改測試正常後，依上線應用系統異動管理程序修訂上線應用系統之內容。

應用系統異動管理

- 上線系統之執行程序或資料等之新增、修改、刪除等處理除經由正式程式為之外，只能由系統負責人依核定後結果執行之。

資訊系統弱點掃描

- 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，應評估其相關風險或安裝修補程式，並留存紀錄（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)。

配合修正內控內稽制度

現行內控規定：

CA-11210受託買賣及成交作業

- 公司經營經紀業務且與證交所簽訂主機共置服務契約者，應依「主機共置服務管理辦法」規定辦理，使用該服務前，應自訂使用規則並於公司內部控制制度制定適當之控管機制及查核程序(註：請公司自訂) 。

※將配合「主機共置服務管理辦法」修正第四章使用者公平待客原則之內容，調整證券商內控內稽制度。