

證券股份有限公司

電腦作業與資訊提供：通訊與作業管理

網路安全管理查核明細表

作業週期：(每月至少查核乙次)

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
(FC-17010-M) 網路安全管理	<p>適用網際網路下單證券商，另一、二、六、十三項並適用於所有證券商</p> <p>一、網路系統安全評估：</p> <p>(一)是否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。</p> <p>(二)是否定期或適時修補網路運作環境及作業系統之安全漏洞(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。</p> <p>(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)之事項是否隨時對內部公告。</p> <p>(四)各電腦主機、重要軟硬體設備是否有專人負責。</p> <p>(五)公司網路是否依用途區分為 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)。</p> <p>(六)個人資料及機敏資料是否存放於安全的網路區域。</p> <p>(七)系統是否僅開啟必要之服務及程式，未使用之服務功能應關閉。</p> <p>(八)公司是否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份認證，留存相關維護紀錄並由權責主管定期覆核。</p> <p>(九)是否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。</p> <p>二、網路設備之安全管理：</p> <p>(一)是否建立防火牆。</p> <p>(二)防火牆是否有專人管理。</p> <p>(三)防火牆進出紀錄及其備份是否至少保存三年。</p> <p>(四)重要網站及伺服器系統(如網際網路下單系統等) 是否以防火牆與外部網際網路隔</p>				

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
	<p>離。</p> <p>(五)防火牆系統之設定是否經權責主管之核准。</p> <p>(六)是否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，是否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是否調整或停用該 規則，並留存相關紀錄。</p> <p>(七)建立網路設備規則是否以最小授權及正面表列為原則。</p> <p>(八)是否至少每年檢視一次對外網路設備規則，並留存相關紀錄。</p> <p>三、網路傳輸安全管理：</p> <p>(一)網際網路下單畫面是否採加密方式(例如：<u>TLSSL</u>)處理。</p> <p>(二)公司是否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)，是否即時了解異常原因，並留存相關紀錄。</p> <p>(三)網際網路下單登入時是否採多因子認證方式(例如：字元或圖形密碼、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。</p> <p>四、公司使用多因子驗證是否具下列三項之任兩項技術：</p> <p>(一)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）。</p> <p>(二)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。</p> <p>(三)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。</p> <p>五、身份認證與憑證管理：</p> <p>(一)網際網路下單是否訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，是否採用多因子(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。</p> <p>(二)網際網路下單是否全面使用認證機制。</p>				

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
	<p>(三)是否於伺服器端驗證客戶交易身分及使用者帳號。</p> <p>(四)電子交易身分之申請、交付、使用、更新與驗證是否訂定相關規範。</p> <p>六、電腦病毒及惡意軟體之防範：</p> <p>(一)是否安裝防毒軟體，並及時更新程式及病毒碼。</p> <p>(二)是否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)。</p> <p>(三)防毒是否涵蓋個人端（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。</p> <p>(四)是否對於電子郵件中帶電腦病毒之附件或網頁連結，進行掃毒作業或阻擋。</p> <p>(五)為防範電腦病毒擴散，影響電腦安全，公司是否訂定電子郵件使用安全相關規定及建立郵件過濾機制。</p> <p>(六)公司是否建立軟體白名單及上網控管機制。</p> <p>(七)公司是否偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。</p> <p>(八)公司是否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。</p> <p><u>(九)公司是否就所接收資安情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。</u></p> <p>七、網路系統功能檢查：</p> <p>(一)是否定期檢查網際網路下單系統提供之功能，並留存紀錄。</p> <p>(二)是否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。</p> <p>八、公司提供 API 服務規範：</p> <p>公司提供客戶使用應用程式介面(API)服務，是否於首次下單前就相關傳輸設定進行連線測試，並留存相關測試紀錄。</p> <p>九、網際網路下單服務品質相關標準：</p> <p>公司提供網際網路下單業務時，兼顧客戶服務品質，是否訂定網際網路下單服務品質相關標準，並包含下列重點如：交易之安全性、交易之穩定及系統可用性、提供客戶服務。</p> <p>十〇、網路攻擊防護機制導入及安全性檢測：</p>				

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
	<p>(一)核心系統身分驗證機制是否防範自動化程式之登入或密碼更換嘗試。</p> <p>(二)公司是否依其所屬資安分級及「證券商辦理資通系統資通安全評估作業程序」定期辦理資通安全健診。</p> <p>十一、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是否即通知客戶，並留存紀錄，避免非客戶本人登入情事：(1)密碼輸入錯誤或帳戶被鎖定；(2)申請或更新憑證；(3)變更基本資料；(4)異常來源或行為嘗試登入等；(5)密碼申請異動或補發時。</p> <p>十二、異常 IP 登入之監控與預警： 公司對於嘗試登入帳號之異常及不明來源 IP，如發現下列情形，是否有警示機制，進行監控分析及留存紀錄，並定期檢視以確認機制有效運作：(1)同一來源 IP 登入不同帳號達一定次數以上；(2)同一帳號在一定時間內由不同國家登入；(3)發現異常 IP(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。</p> <p>十三、無線網路管理： (一)公司設置無線網路是否採用現行公開資訊已認可且無弱點之安全協定。 (二)公司提供內部無線網路使用是否限內部人員公務用或資訊服務供應商是否於申請核准後使用。</p>				
備 註：使用主機共置服務者，稽核人員應另就屬主機共置服務業務之查核程序再進行查核，並同時作成查核報告。					

稽核人員 _____ 日期 _____