

證券股份有限公司

電腦作業與資訊提供：存取控制

作業週期：(每月至少查核乙次)

查核明細表

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
(FC-18000-M) 存取控制	<p>一、公司是否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。</p> <p>二、權限管理：</p> <p>(一)對於程式的存取使用，是否有詳細的書面管制說明。</p> <p>(二)人員異動時是否及時更新其使用權限。</p> <p>(三)對於程式及檔案之存取使用，是否按權限區分。</p> <p>(四)委外人員之電腦通行使用權，是否設有適當之控管程序，委外期間結束後，是否立即收回該項權利。</p> <p>(五)對於進駐於公司內之委外作業人員是否納入公司安全管理，如欲使用內部網路資源時，是否有安全管制措施(如透過轉接方式或另建網路者，宜與內部網路作實體隔離)。</p> <p>(六)是否定期(至少每半年一次)審查資通系統帳號及權限之適切性，並視審查結果停用資通系統閒置帳號。(客戶帳號除外)。</p> <p>(七)是否建立資通系統帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。</p> <p>(八)資通系統帳號是否定義人員角色及責任，授權應採最小權限原則，僅允許使用者(或代表使用者行為之程序)依公司部門權責及業務功能，完成作業所需之授權存取。</p> <p>三、密碼管理：</p> <p>(一)使用者第一次使用系統時，是否更新初始密碼後方可繼續作業。</p> <p>(二)密碼是否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。</p> <p>(三)對於使用者及客戶忘記密碼之處理，公司是否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)，並留存相關紀錄，方可再次使用系統。</p> <p>(四)初始密碼是否隨機產生，並與使用者及客戶身分無關。(本項不適用採自行訂定交付</p>				

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
	<p>電子式交易密碼條之方式)</p> <p>(五)密碼輸入錯誤次數達五次者，是否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，並留存相關紀錄。公司於接獲客戶聯繫時，是否確認客戶身分後（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，始得恢復使用。</p> <p>(六)除語音按鍵下單外，公司是否使用優質密碼設定(長度六個字元(含)以上，且具有文數字或符號)並進行管控。</p> <p>(七)客戶密碼超過一年未變更或變更密碼與前一代相同，公司是否做妥善處理。除客戶外，公司其他使用者之密碼，<u>除提供系統使用之帳號採定期變更或適當安全控管措施（如限制人工登入、監控告警等）外</u>，是否至少每三個月變更一次。</p> <p>(八)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是否設定使用密碼，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。</p> <p>(九)客戶申請採電子式交易型態者，如以一般電子方式交付電子密碼條時，是否傳送 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；如採自訂交付電子密碼條方式，是否訂定交付電子式交易密碼</p> <p>四、電腦稽核紀錄管理：</p> <p>(一)對重要系統（如主機連線系統、網際網路下單系統等）之稽核日誌紀錄內容是否包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項，並由專人定期檢視。</p> <p>(二)相關留存紀錄是否確保數位證據之收集、保護與適當管理程序，且是否至少留存三年。</p> <p>(三)核心系統電腦稽核紀錄(日誌)是否建立監控機制，處理失效時，應採取適當之行動。</p> <p>五、資料輸入管理：</p> <p>(一)安全性或重要性較高之資料，是否由權責主管人員核可後始得執行輸入或修改。</p>				

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
	<p>(二)所輸入或修改之資料及其執行人員姓名、職稱是否皆留存記錄。</p> <p>(三)對隱密性高之重要資料（例如：密碼檔）是否以亂碼後之資料形式存放。</p> <p>(四)公司如屬公開發行公司者，是否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。</p> <p>(五)使用電子憑證 I C 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，該等憑證載具是否由專人負責保管並設簿登記，且是否訂定相關帳號、密碼保管及使用程序，並據以執行。</p> <p>(六)使用代表公司憑證載具簽署之作業系統端(server 端)若屬證券商應用系統者(例如：「電子對帳單系統」)，是否留存電腦稽核紀錄(log)，其保存年限是否比照各作業資料應保存年限。</p> <p>(七)是否依「個人資料保護法」，妥善處理公司保有之個人資料，並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。</p> <p>(八)前揭個人資料，其更新、更正或註銷均是否報經備查，並將更新、更正、註銷內容、作業人員及時間詳實記錄。</p> <p>(九)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，是否訂定「與軟體廠商機密維護及損害賠償等雙方權責劃分」。</p> <p>(十)是否留存個人資料使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況。</p> <p>六、資料輸出管理：</p> <p>(一)報表是否按時產生並分送各使用單位。</p> <p>(二)機密性、敏感性之報表列印或瀏覽是否有適當之管制程序。</p> <p>(三)投資人於公司網站查詢個人資料是否具有加密傳輸機制(例如：STLSL)。</p> <p>(四)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，是否依「機敏資訊類型及隱匿之具體作法原則」辦理。</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 _____