證券商內部控制制度標準規範—內部稽核實施細則修正對照表

編號	作業項目	修正後內容	修正前內容	修正說明
AC-18000	存取控制之稽核目的：確定上述作業是否符合規定辦理	不定期（每月至少查核乙次） (一)對於程式的存取使用，是否有詳細的書面管制說明。 (二)人員異動時是否及時更新其使用權限。 (三)對於程式及檔案之存取使用，是否按權限區分。 (四)委外人員電腦通行使用權利是否經適當控管；委外期間結束後，是否立即收回該項權利。 (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)。 (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)。 (七)公司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。 (八)資通系統帳號是否定義人員角色及責任，授權是否採最小權限原則，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。 (九)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。	不定期（每月至少查核乙次） (一)對於程式的存取使用，是否有詳細的書面管制說明。 (二)人員異動時是否及時更新其使用權限。 (三)對於程式及檔案之存取使用，是否按權限區分。 (四)委外人員電腦通行使用權利是否經適當控管；委外期間結束後，是否立即收回該項權利。 (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)。 (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)。 (七)公司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。 (八)資通系統帳號是否定義人員角色及責任，授權是否採最小權限原則，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。 (九)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。	1.增訂系統使用帳號密碼之例外管理規定；2.調整用字一致性；3.調整範例，避免使用安全性不足之協議。

編號	作業項目	修正後內容	修正前內容	修正說明
		(十)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。；初始密碼是否隨機產生，並與使用者或客戶身分無關。(本項不適用採自行訂定交付電子式交易密碼條之方式)。 (十一)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，並留存紀錄。公司於接獲客戶聯繫申請解除鎖定時，是否確實辨認身分（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。 (十二)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)，方可再次使用系統。 (十三)除語音按鍵下單，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。 (十四)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。公司使用者之密碼**，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，**是否至少每三個月變更一次。 (十五)檢查公司現有之網站、伺服器、網路芳	(十)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。；初始密碼是否隨機產生，並與使用者或客戶身分無關。(本項不適用採自行訂定交付電子式交易密碼條之方式)。 (十一)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，並留存紀錄。公司於接獲客戶聯繫申請解除鎖定時，是否確實辨認身分（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。 (十二)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)，方可再次使用系統。 (十三)除語音按鍵下單，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。 (十四)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**使用者之密碼是否至少每三個月變更一次。 (十五)檢查公司現有之網站、伺服器、網路芳	

編號	作業項目	修正後內容	修正前內容	修正說明
		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。 (十六)為防止密碼洩漏，是否採取不顯示、不印錄等措施。 (十七)客戶申請採電子式交易型態者，公司以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，此流程相關系統紀錄是否留存。 (十八)公司是否對客戶申請電子式交易型態者採自訂交付電子密碼條訂有電子交易密碼之作業程序。 (十九)公司是否對客戶申請電子式交易型態者採自訂交付電子密碼條訂定電子式交易密碼交付流程與安全控管機制相關內部控制制度。 (二十)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。 (二十一)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，是否採取適	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。 (十六)為防止密碼洩漏，是否採取不顯示、不印錄等措施。 (十七)客戶申請採電子式交易型態者，公司以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，此流程相關系統紀錄是否留存。 (十八)公司是否對客戶申請電子式交易型態者採自訂交付電子密碼條訂有電子交易密碼之作業程序。 (十九)公司是否對客戶申請電子式交易型態者採自訂交付電子密碼條訂定電子式交易密碼交付流程與安全控管機制相關內部控制制度。 (二十)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。 (二十一)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，是否採取適	

編號	作業項目	修正後內容	修正前內容	修正說明
		當之行動。 (二十二)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。 (二十三)所輸入或修改之資料及其執行人員姓名、職稱皆是否留存紀錄。 (二十四)對重要及機密性檔案其存取使用是否依規定之作業程序辦理。 (二十五)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。 (二十六)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。 (二十七)公司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。 (二十八)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），該等憑證載具是否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。 (二十九)使用前揭代表公司憑證載具簽署之作	當之行動。 (二十二)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。 (二十三)所輸入或修改之資料及其執行人員姓名、職稱皆是否留存紀錄。 (二十四)對重要及機密性檔案其存取使用是否依規定之作業程序辦理。 (二十五)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。 (二十六)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。 (二十七)公司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。 (二十八)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），該等憑證載具是否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。 (二十九)使用前揭代表公司憑證載具簽署之作	

編號	作業項目	修正後內容	修正前內容	修正說明
		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），其保存年限比照各作業資料應保存年限。 (三十)是否依「個人資料保護法」，妥善處理客戶及公司內部人個人資料。 (三十一)公司是否依「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。 (三十二)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 (三十三)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「與軟硬體廠商機密維護及損害賠償等雙方權責劃分」。 (三十四)報表是否按時產生並分送各使用單位。 (三十五)機密性或敏感性報表列印或瀏覽是否有適當管制程序。 (三十六)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：TLS)。 (三十七)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	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），其保存年限比照各作業資料應保存年限。 (三十)是否依「個人資料保護法」，妥善處理客戶及公司內部人個人資料。 (三十一)公司是否依「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。 (三十二)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 (三十三)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「與軟硬體廠商機密維護及損害賠償等雙方權責劃分」。 (三十四)報表是否按時產生並分送各使用單位。 (三十五)機密性或敏感性報表列印或瀏覽是否有適當管制程序。 (三十六)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：SSL)。 (三十七)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	

編號	作業項目	修正後內容	修正前內容	修正說明
		理。 (三十八)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。 (三十九)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。	理。 (三十八)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。 (三十九)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。	