# 證券商內部控制制度標準規範—內部控制制度修正對照表

| 編號 | 作業項目 | 修正後內容 | 修正前內容 | 修正說明 |
|---|---|---|---|---|
| CC-18000 | 存取控制 | 作業程序及控制重點：<br>(一)公司應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。<br>(二)權限管理：<br>1.申請使用系統資源之人員以書面提出申請：<br>(1)申請內容應註明使用目的及權限。<br>(2)使用人為應用系統使用者則需經應用系統負責人簽註意見。<br>(3)每一使用者限用唯一代碼。<br>2.申請內容應經使用單位主管及資訊單位主管核可後辦理。<br>3.本項結果由系統管理人員依核定結果執行。<br>4.使用者因業務需要或職務變動等因素而需增加、刪除或變更使用權限時亦應提出更動需求。<br>5.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。<br>6.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 | 作業程序及控制重點：<br>(一)公司應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。<br>(二)權限管理：<br>1.申請使用系統資源之人員以書面提出申請：<br>(1)申請內容應註明使用目的及權限。<br>(2)使用人為應用系統使用者則需經應用系統負責人簽註意見。<br>(3)每一使用者限用唯一代碼。<br>2.申請內容應經使用單位主管及資訊單位主管核可後辦理。<br>3.本項結果由系統管理人員依核定結果執行。<br>4.使用者因業務需要或職務變動等因素而需增加、刪除或變更使用權限時亦應提出更動需求。<br>5.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。<br>6.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 | 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 |
| --- | --- | --- | --- | --- |
| | | 隔離)。<br>7.應定期(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)。<br>8.公司應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。<br>9.資通系統帳號應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。<br>(三)密碼管理：<br>1.使用者申請使用代碼時應於接到使用許可後立即更新密碼。<br>2.初始密碼應隨機產生,並與使用者身分無關。<br>(本項不適用採自行訂定交付電子式交易密碼條之方式)<br>3.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定時，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。<br>4.對因忘記密碼而無法登入系統之使用者或客戶申請核發原密碼時，應採取嚴格 | 隔離)。<br>7.應定期(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)。<br>8.公司應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。<br>9.資通系統帳號應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。<br>(三)密碼管理：<br>1.使用者申請使用代碼時應於接到使用許可後立即更新密碼。<br>2.初始密碼應隨機產生,並與使用者身分無關。<br>(本項不適用採自行訂定交付電子式交易密碼條之方式)<br>3.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定時，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。<br>4.對因忘記密碼而無法登入系統之使用者或客戶申請核發原密碼時，應採取嚴格 | |

| 編號 | 作業項目 | 修正後內容 | 修正前內容 | 修正說明 |
| --- | --- | --- | --- | --- |
| | | 確認其身分及核發程序後(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，方可開放其使用系統。<br>5.除語音按鍵下單外，公司應使用優質密碼設定（長度六個字元（含）以上，且具有文數字或符號）並進行管控，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。公司使用者之密碼**除提供系統使用之帳號應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，**應至少每三個月變更一次。<br>6.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。<br>7.為防止密碼洩漏，應採取不顯示、不印錄等措施。<br>8.客戶申請採電子式交易型態者，公司得以一般電子方式交付或自訂交付電子密碼條，並依下列說明辦理：<br>(1)(2)、(3)適用於一般電子方式，(4)、(5)、(6)、(7)適用於自訂交付方式。<br>(1)客戶應於聲明書中聲明同意以電子方 | 確認其身分及核發程序後(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，方可開放其使用系統。<br>5.除語音按鍵下單外，公司應使用優質密碼設定（長度六個字元（含）以上，且具有文數字或符號）並進行管控，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。<br>6.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。<br>7.為防止密碼洩漏，應採取不顯示、不印錄等措施。<br>8.客戶申請採電子式交易型態者，公司得以一般電子方式交付或自訂交付電子密碼條，並依下列說明辦理：<br>(1)(2)、(3)適用於一般電子方式，(4)、(5)、(6)、(7)適用於自訂交付方式。<br>(1)客戶應於聲明書中聲明同意以電子方 | |

| 編號 | 作業項目 | 修正後內容 | 修正前內容 | 修正說明 |
| --- | --- | --- | --- | --- |
| | | 式交付電子密碼條。<br>(2)公司業務人員應確實辨認客戶身分，並確認其手機號碼及電子信箱為本人使用。<br>(3)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，客戶需以 OTP 密碼解密方能取得密碼，此流程相關系統紀錄應留存。<br>(4)應訂定交付電子式交易密碼之作業程序。<br>(5)應確實辨認電子式交易密碼交付對象為本人並留存相關紀錄。<br>(6)應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。<br>(7)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），並加強宣導客戶定期更新使用者密碼以不超過三個月為宜。<br>(四)電腦稽核紀錄管理：<br>1.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。<br>2.對上開重要系統之電腦稽核紀錄，應有專人定期檢視。 | 式交付電子密碼條。<br>(2)公司業務人員應確實辨認客戶身分，並確認其手機號碼及電子信箱為本人使用。<br>(3)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，客戶需以 OTP 密碼解密方能取得密碼，此流程相關系統紀錄應留存。<br>(4)應訂定交付電子式交易密碼之作業程序。<br>(5)應確實辨認電子式交易密碼交付對象為本人並留存相關紀錄。<br>(6)應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。<br>(7)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），並加強宣導客戶定期更新使用者密碼以不超過三個月為宜。<br>(四)電腦稽核紀錄管理：<br>1.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。<br>2.對上開重要系統之電腦稽核紀錄，應有專人定期檢視。 | |

| 編號 | 作業項目 | 修正後內容 | 修正前內容 | 修正說明 |
| --- | --- | --- | --- | --- |
| | | 3.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。<br>4.核心系統電腦稽核紀錄(日誌)應建立監控機制，處理失效時，應採取適當之行動。<br>(五)資料輸入管理：<br>1.上線應用系統之資料輸入與修改，由業務單位人員依之畫面為之。其執行人員之姓名、職稱應有詳細紀錄，並由專人管理。<br>2.輸入或修改重要或特殊資料，應由權責主管人員核可後始得執行，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。<br>3.所輸入或修改之資料應留存紀錄，並核對資料之正確性；其使用前揭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」），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。<br>4.對重要及機密性檔案，應使用密碼或存取 | 3.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。<br>4.核心系統電腦稽核紀錄(日誌)應建立監控機制，處理失效時，應採取適當之行動。<br>(五)資料輸入管理：<br>1.上線應用系統之資料輸入與修改，由業務單位人員依之畫面為之。其執行人員之姓名、職稱應有詳細紀錄，並由專人管理。<br>2.輸入或修改重要或特殊資料，應由權責主管人員核可後始得執行，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。<br>3.所輸入或修改之資料應留存紀錄，並核對資料之正確性；其使用前揭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」），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。<br>4.對重要及機密性檔案，應使用密碼或存取 | |

| 編號 | 作業項目 | 修正後內容 | 修正前內容 | 修正說明 |
| --- | --- | --- | --- | --- |
| | | 控制軟體限制其使用或設定等級，按等級使用。<br>5.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。<br>6.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。<br>7.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。<br>8.公司應依「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。<br>9.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。<br>10.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」。<br>11.應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。 | 控制軟體限制其使用或設定等級，按等級使用。<br>5.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。<br>6.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。<br>7.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。<br>8.公司應依「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。<br>9.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。<br>10.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」。<br>11.應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。 | |

| 編號 | 作業項目 | 修正後內容 | 修正前內容 | 修正說明 |
| --- | --- | --- | --- | --- |
| | | (六)資料輸出管理：<br>1.報表之列印應由經授權之人員執行，產生之報表分送各使用單位。<br>2.輸出資料使用後若無保存需要，應經適當銷毀處理。<br>3.輸出資料若以磁性媒體保存，應定期檢查以確定必要時能以報表方式印出。<br>4.機密性、敏感性之報表列印或瀏覽應有適當之管制程序。<br>5.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：TLS)，以確保投資人於網站查詢資料之保密性。<br>6.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以去識別化為原則，並依「機敏資訊類型及隱匿之具體作法原則」辦理。 | (六)資料輸出管理：<br>1.報表之列印應由經授權之人員執行，產生之報表分送各使用單位。<br>2.輸出資料使用後若無保存需要，應經適當銷毀處理。<br>3.輸出資料若以磁性媒體保存，應定期檢查以確定必要時能以報表方式印出。<br>4.機密性、敏感性之報表列印或瀏覽應有適當之管制程序。<br>5.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)，以確保投資人於網站查詢資料之保密性。<br>6.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以去識別化為原則，並依「機敏資訊類型及隱匿之具體作法原則」辦理。 | |