證券商內部控制制度標準規範—內部控制制度修訂對照表（111年）

編號	作業項目	修訂後內容	修訂前內容	修訂說明
CC-12000	資訊安全政策	作業程序及控制重點： (一)~(五)略。 (六)、公司每年應將前一年度資訊安全整體執行情形，由**資訊安全長或**負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具**「證券暨期貨市場各服務事業建立內部控制制度處理準則」第二十四條規定之內部控制制度聲明書，於會計年度終了後三個月內提報董事會通過，並將該聲明書內容揭露於主管機關指定之申報網站。** (以下略)	作業程序及控制重點： (一)~(五)略。 (六)、公司每年應將前一年度資訊安全整體執行情形，由負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具資訊安全整體執行情形聲明書，並提報董事會通過，於會計年度終了後三個月內將該聲明書內容揭露於公開資訊觀測站。 (以下略)	**依據主管機關110年9月30日金管證券字第11003637894、11003637895號令辦理。**

CC-17010(適用網際網路下單證券商，另(一)、(二)、(五)項並適用於所有證券商)	網路安全管理	(一)~(二)略 (三)、網路傳輸安全管理： 1、(略) 2、公司應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**嘗試**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)，應即時了解異常原因**，並留存相關紀錄。 3. (略) (四)、CA 認證與憑證管理： 1、網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。**客戶申請或更新憑證下載，必須採用多因子(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。** 2、(略)	(一)~(二)略 (三)、網際網路下單服務品質相關標準: 1、(略) 2、公司應每日針對核心系統之帳號登入失敗紀錄、非客戶帳號登入嘗試紀錄等進行監控及分析，並留存相關紀錄。 3. (略) (四)、CA 認證與憑證管理： 1、網路下單應訂定憑證交付程序，避免非本人取得憑證。	**依據證交所110年11月30日臺證輔字第1100503618函辦理。鑑於駭客攻擊資通安全事件頻傳，為維護證券市場交易秩序及保障投資人權益，爰增修證券商強化網際網路下單之資通安全控管機制，並修訂證券商內部控制制度標準規範。**

		(五)~(九)、(略)	2、(略) (五)~(九)、(略)	
		(十)、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應即通知客戶，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。 (112 年 2 月 28 日生效)	(十)、(新增)	鑑於 110 年 11 月間證券市場發生多起駭客攻擊資通安全事件，為維護證券市場交易秩序及保障投資人權益，爰增修(十)及(十一)等二款之證券商強化網際網路下單之資通安全控管機制，並修訂證券商內部控制制度標準規範。
		(十一)、異常 IP 登入之監控與預警： 公司應依其所屬資安分級對異常及不明來源 IP 連線進行監控分析及留存紀錄，如有發現下列情形，應設有警示機制，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。	(十一)、(新增)	

		3. 發現異常來源 (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。 (111 年 9 月 30 日生效) (以下略) 作業程序及控制重點： (一)~(二)略。	(以下略)	

CC-18000	存取控制	(三)、密碼管理： 1~2 略 3.密碼輸入錯誤次數達三次者，應予中斷連線且鎖定該帳號，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。(111 年 11 月 30 日生效) 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。 5.除語音按鍵下單外，~~輸入介面僅可輸入數字外（例如：語音按鍵下單），~~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	作業程序及控制重點： (一)~(二)略。 (三)、密碼管理： 1~2 略 3.密碼輸入錯誤次數達三次者，應予中斷連線。 4、對因忘記密碼而無法登入系統之使用者申請核發原密碼時，應採取嚴格確認其身分及核發程序後，方可開放其使用系統。 5、除輸入介面僅可輸入數字外(例如：語音按鍵下單)，公司應使用優質密碼設定(長度六個字元(含)	依據主管機關 111 年 3 月 23 日金管證券字第 111033046 號函指示研議強化證券商對客戶帳號之密碼加強規範及管理，爰修訂(三)、(五)等相關項次，並修訂證券商內部控制制度標準規範。

		期更新~~使用者~~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。**(111 年 11 月 30 日生效)** 6.~8.(略) (四)略 (五)資料輸入管理： 1.~4.略 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。(111 年 11 月 30 日生效)** (以下略) (一)~(十四)略。 (十五)、程式原始碼安全規範：	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使用者密碼以不超過三個月為宜。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。 6.~8.(略) (四)略 (五)資料輸入管理： 1.~4.略 5.對隱密性高之重要資料，如通行碼之存放，應予亂碼後存放。 (以下略)	

CC-19000	系統開發及維護	1~4 略 5.委外開發之行動應用程式如涉及機敏性資料傳送(如：客戶帳號密碼或交易資料等)應自行或委外檢視驗證傳遞對象是否適當並留存相關紀錄。 6. 公司應依上開安全事項檢驗程式原始碼並符合安全事項之要求;無法取得程式原始碼時,應要求程式提供者符合上開前五項安全事項之佐證。 (以下略)	(一)~(十四)略。 (十五)、程式原始碼安全規範： 1~4 略 5.(新增) 6. 公司應依上開安全事項檢驗程式原始碼並符合安全事項之要求;無法取得程式原始碼時,應要求程式提供者符合上開前四項安全事項之佐證。 (以下略)	依據主管機關指示研議檢討110年11月間證券商複委託遭駭客攻擊之原因並據以修訂相關資安規範，爰規範證券商須檢視及驗證行動應用程式機敏性資料傳輸對象之妥適性，並修訂證券商內部控制制度標準規範。