法規名稱：建立證券商資通安全檢查機制
公布日期：民國 113 年 02 月 05 日

1、風險評鑑與管理（CC–11000，適用網際網路下單證券商，不適用語音下單及傳統下單之證券商，年度查核）
（1）應鑑別公司適用資訊安全風險範圍內之所有資訊資產以及其擁有者。
（2）應確定公司各作業可接受之資訊安全風險等級。
（3）公司應至少每年進行一次資訊安全風險評鑑，並留存相關紀錄，營運相關的重大風險與控管措施議題（包括新產品、新興技術和資訊系統的風險）應納入風險評估範圍，以確保公司政策、程序和控管措施之有效性。
（4）應評估核心系統可容忍中斷時間、復原時間目標（ RTO）、資料復原點目標（ RPO），並依經紀業務規模市占率暨自然人客戶數比率分級，訂定核心系統可容忍中斷時間。

2、資訊安全政策（CC–12000，年度查核）
（1）公司應依據相關法令規定及公司業務需求，訂定資訊安全政策、資訊作業之安全水準。
（2）制訂資訊安全政策，應包括下列事項：
a.資訊安全之定義、資訊安全之目標及資訊安全之範圍等。
b.資訊安全政策之解釋及說明，資訊安全之原則、標準以及員工應遵守之相關規定。
c.推行資訊安全工作之組織、權責及分工。
d.發生資訊安全事件之緊急通報程序、處理流程、相關規定及說明。
（3）公司所訂定之資訊安全政策，應經管理階層核准，並應正式發布要求所有員工共同遵守，並轉知與公司連線作業之公私機關（構）、提供資訊服務之廠商共同遵行。
（4）公司訂定之資訊安全政策，應至少每年評估一次，以反映法令規章、技術及業務等最新發展現況，確保資訊安全實務作業之有效性，前開之評估工作應留存相關紀錄。
（5）資訊安全政策之評估，應以獨立及客觀之方式進行，並由內部或委託外部專業機構辦理。
（6）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。

（7）公司應參考「建立證券商資通安全檢查機制–分級防護應辦事項附表」辦理資訊安全分級防護應辦事項。

（8）公司應依其所屬資安分級辦理核心系統導入資訊安全管理系統，並通過公正第三方之驗證，且持續維持驗證有效性。

3、安全組織（CC–13000，年度查核）

（1）公司應依規定配置適當人力資源及設備負責資訊安全制度之規劃、監控及執行資訊安全管理作業，且相關人員之工作職掌與兼辦業務情形應符合規定。

（2）公司應指定副總經理或高層主管人員，綜理資訊安全政策推動及資源調度事務，並得視需要，成立跨部門之「資訊安全推行小組」；如公司符合主管機關所訂一定條件者，應指定副總經理以上或職責相當之人兼任資訊安全長辦理上開業務。

（3）公司應視資訊安全管理需要及所屬資安分級，指定專人或專責單位負責規劃與執行資訊安全工作，且資訊安全人員及主管每年應定期參加十五小時以上資訊安全專業課程訓練或職能訓練並通過評量。其他使用資訊系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程。

（4）公司資訊安全人力、能力及經驗，如有不足之處，得委請外界的學者專家或民間專業組織及團體，提供資訊安全顧問諮詢服務。

（5）資訊處理部門與業務單位之權責，應明確劃分。

（6）公司應依其所屬資安分級要求資訊安全人員取得並維持相當資通安全專業證照。

4、資產分類與控制（CC–14000，半年查核）

（1）資訊資產應列有清冊，清冊並應加以維護。

（2）應訂有資訊分級並作標示處理之相關規範。（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商）

（3）公司應對自行或委外開發之資訊系統完成資訊系統分級，資訊系統等級應至少區分核心與非核心系統，每年應至少檢視一次資訊系統分級妥適性。（111 年 1 月底生效）

（4）公司應對資訊資產之資料與文件的保存期限進行規範，並於保存期限到期後進行刪除與銷毀。

5、人員安全（CC–15000，半年查核）

（1）員工應依相關法令課予機密維護責任，並應填具保密切結書，以

明責任。

（2）員工離職時應取消其識別碼，並收繳其通行證、卡及相關證件。

（3）應定期（每年至少一次）對全公司員工辦理資訊安全宣導講習（例如：資訊安全政策、資訊安全法令規定、資訊安全作業程序以及如何正確使用資訊科技設施等），並留存紀錄。

（4）員工應依職務層級進行適當的資訊安全教育訓練，每年並達內部所定之訓練時數。

（5）證券商應設置電腦稽核人員。（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商）

6、實體與環境安全（CC–16000，半年查核）

（1）電腦機房應有門禁管制（例如：刷卡）。

（2）機房應有防火設施，並應定期檢驗。

（3）另應將地震、水災等天然災害因素列入考量。

（4）電腦設備之電源供應系統應含不斷電設備及發電機。

（5）應訂定設備報廢作業程序，報廢前應將機密性、敏感性資料及授權軟體予以移除、實施安全性覆寫或實體破壞，應確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄。

（6）公司應定期審查資訊機房門禁管制權限。

7、通訊與作業管理（CC–17000）

（1）網路安全管理（ CC–17010，適用網際網路下單證券商，另 a、b、f 項並適用於所有證券商，每月查核）

a.網路系統安全評估：

(a)應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。

(b)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。

(c)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）之事項應隨時對內部公告。

(d)各電腦主機、重要軟硬體設備應有專人負責。

(e)公司網路應依用途區分為 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）。

(f)個人資料及機敏資料應存放於安全的網路區域，不得存放於網際網路等區域。

(g)系統應僅開啟必要之服務及程式，未使用之服務功能應關閉

。

(h)公司應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身分認證，並留存相關維護紀錄並由權責主管定期覆核。

(i)公司應防止未經授權設備使用內部網路。

(j)應避免使用生命週期終止（End of Service, EOS／ End of Life, EOL）之網路設備，並針對 EOS／EOL 之網路設備擬定汰除相關計畫。

b.網路設備之安全管理：

(a)應建立防火牆。

(b)防火牆應有專人管理。

(c)防火牆進出紀錄及其備份應至少保存三年。

(d)重要網站及伺服器系統（如網路下單系統等）應以防火牆與外部網際網路隔離。

(e)防火牆系統之設定應經權責主管之核准。

(f)公司應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，並留存相關檢視紀錄。

(g)公司交易相關網路直接連線之設備應避免使用危害國家資通安全產品。

(h)公司建立網路設備規則應以最小授權及正面表列為原則。

(i)公司應至少每年檢視一次對外網路設備規則，並留存相關紀錄。

c.網路傳輸及連線安全管理：

(a)網路下單畫面應採加密方式（例如：SSL）處理。

(b)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。

(c)公司提供網路下單服務，應於網路下單登入時採多因子認證方式（例如：固定密碼、圖形鎖、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。

d.多因子驗證：

公司使用多因子驗證應具下列三項之任兩項技術：

(a)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）。

(b)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。

(c)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。

e.身分認證與憑證管理

(a)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。

(b)網路下單證券商應全面使用認證機制。

(c)公司應於伺服器端驗證客戶交易身分及使用者帳號。

(d)公司對電子交易身分之申請、交付、使用、更新與驗證應訂定相關規範。

f.電腦病毒及惡意軟體之防範：

(a)應安裝防毒軟體，並及時更新程式及病毒碼。

(b)應定期對電腦系統及資料儲存媒體進行病毒掃瞄（含電子郵件）。

(c)防毒應涵蓋個人端（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。

(d)勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤應特別小心開啟。

(e)為防範電腦病毒擴散，影響電腦安全，公司應訂定電子郵件使用安全相關規定及建立郵件過濾機制。

(f)公司應建立上網管制措施，以避免下載惡意程式。

(g)公司應偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。

(h)公司宜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。

g.網路系統功能檢查：

(a)應定期檢查網路下單系統提供之功能，並留存紀錄。

(b)應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。

h.公司提供 API 服務規範：公司提供客戶使用應用程式介面（API）服務之申請流程、核可標準及相關控管配套措施相關作業，應依「證券商受理客戶使用應用程式介面（ API）服務作業規範」辦理。

i.網際網路下單服務品質相關標準：

公司提供網際網路下單業務時，兼顧客戶服務品質，應訂定網際網路下單服務品質相關標準，並應包含下列重點如：交易之安全性、交易之穩定及系統可用性、提供客戶服務。

j.網路攻擊防護機制導入及安全性檢測

(a)公司應依其所屬資安分級定期對提供網際網路服務之核心系統辦理滲透測試，並依測試結果進行改善。（111 年 1 月底生效）

(b)公司應依其所屬資安分級定期辦理資通安全健診（應含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視）。（112 年 1 月底生效）

(c)公司應依其所屬資安分級建立資通安全威脅偵測管理機制（應含括事件收集、異常分析、偵測攻擊並判斷攻擊行為）

(d)公司應依其所屬資安分級建立入侵偵測及防禦機制。

(e)公司應依其所屬資安分級設置應用程式防火牆。

(f)公司應依其所屬資安分級辦理進階持續性威脅攻擊防禦措施。（112 年 1 月底生效）

(g)核心系統身分驗證機制應防範自動化程式之登入或密碼更換嘗試，非核心系統宜防範自動化程式之登入或密碼更換嘗試。

k.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：

(a)密碼輸入錯誤或帳戶被鎖定。

(b)申請或更新憑證。

(c)變更基本資料。

(d)異常來源或行為嘗試登入等

(e)密碼申請異動或補發時。

l.異常 IP 登入之監控與預警：

公司應對異常及不明來源 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：

(a)同一來源 IP 登入不同帳號達一定次數以上。

(b)同一帳號在一定時間內由不同國家登入。

(c)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。

（2）電腦系統及作業安全管理（CC–17020，半年查核）

a.電腦設備之管理：

為確定電腦設備維護內容，應與廠商訂有書面維護契約，做完維護時應留存維護紀錄並由資訊單位派人會同廠商維護人員共同檢查。

b.電腦作業系統環境設定及使用權限設定：

(a)電腦作業系統環境設定及使用權限設定應經有關主管核示，並由系統管理人員執行。

(b)電腦系統檔案異動前後皆有完善之備份處理措施。

(c)公司應建立系統最高權限帳號管理辦法（含作業系統及應用系統），如需使用最高權限帳號時須取得權責主管同意，並留存相關紀錄。

(d)公司應建立並落實個人電腦、伺服器及網路通訊設備之安全性組態基準（如密碼長度、更新期限等）。

(e)公司透過網際網路使用帳號登入系統時，應採用多因子認證機制。

(f)資通系統內部時鐘應定期與基準時間源進行同步。

(g)公司應依其所屬資安分級對核心系統重要組態設定檔案及其他具保護需求之資訊進行加密或以其他適當方式儲存。

(h)公司應依其所屬資安分級訂定對核心系統之閒置時間或可使用期限與核心系統之使用情況及條件（如：帳號類型與功能限制、操作時段限制、來源位址限制、連線數量及可存取資源等）。

c.電腦媒體之安全管理：

(a)重要軟體及其文件、清冊應抄錄備份存於另一安全處所。

(b)重要之備份檔案及軟體若儲存於與電腦中心同一建築物內，應鎖存於防火之房間或防火且防震之防火櫃中。

(c)存放備份資料之儲存媒體，應於其標籤上註明存放資料之名稱及保存期限。

(d)應建立機密性及敏感性資料媒體之相關處理程序，防止資料洩露或不當使用。

(e)應建立回存測試機制，以驗證備份之完整性及儲存環境的適當性。

(f)公司應依據系統特性與資料復原點目標（ RPO），考量備份頻率、儲存媒體類型（光碟、外接硬碟、磁帶）、資料類型（虛擬機映像檔、系統源碼、資料庫與組態設定檔等）、備份類型（完整備份、增量備份與差異備份）、備份方式（網路同步寫入、網路非同步寫入與離線備份）等，制定適當之資料備份機制，如採離線備份應依備份類型建立適當的備份基準（baseline），以確保資料可正確回存。

(g)公司制定資料備份機制時，宜考量「 3–2–1 備份原則」，至少製作三份備份；將備份分別存放在兩套獨立不同儲存設備；至少一份放在異地保存。

d.電腦操作管理：

(a)操作人員應確實依規定操作程序執行。

(b)操作日誌應詳實記載並逐日經主管核驗，操作人員不可與主管為同一人。

(c)系統主控台所留存之紀錄，應經專人檢查訊息內容且定期送主管核驗。

e.證券經紀商應配備經營業務所需、且有適足容量之電腦系統。

f.證券經紀商之電腦系統應訂定定期（每年至少一次）由內部或委託外部專業機構評估電腦系統容量及安全措施之機制與程序，定期對系統容量進行壓力測試，並留存紀錄。

8、存取控制（CC–18000，每月查核）

（1）公司應訂定資訊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。

（2）權限管理

a.對於程式的存取使用，應有詳細的書面管制說明。

b.人員異動時應及時更新其使用權限。

c.對於程式及檔案之存取使用，應按權限區分。

d.委外人員電腦通行使用權利應經適當控管；委外期間結束後，應立即收回該項權利。

e.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隔離）。

f.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）。

g.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。

h.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。

（3）密碼管理：

a.使用者第一次使用系統時，應更新初始密碼後方可繼續作業。

b.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。

c.對於使用者及客戶忘記密碼之處理，公司應有嚴格的身分確認

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。

d.初始密碼應隨機產生，並與使用者及客戶身分無關。（本項不適用採自行訂定交付電子式交易密碼條之方式）

e.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。

f.除語音按鍵下單外，公司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。（ 111 年 11 月 30 日生效）

g.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。

h.客戶申請採電子式交易型態者，公司得以一般或自訂電子方式交付電子密碼條，應依下列說明辦理：

(a)採一般電子方式交付電子密碼條，應傳送 OTP（OneTimePassword）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應留存。

(b)採自訂交付電子密碼條方式，應訂定交付電子式交易密碼之作業程序及安全控管機制，並辦認電子式交易密碼交付對象為本人及留存相關紀錄。

（4）電腦稽核紀錄管理：

a.對重要系統（如主機連線系統、網路下單系統等）之稽核日誌記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。

b.對上開重要系統之電腦稽核紀錄，應有專人定期檢視。

c.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。

d.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。

（5）資料輸入管理：

a.安全性或重要性較高之資料，應由權責主管人員核可後始得執行輸入或修改。

b.所輸入或修改之資料及其執行人員姓名、職稱皆應留存紀錄。

c.對隱密性高之重要資料（例如：密碼檔）應以亂碼後之資料形式存放。

d.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。

e.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。

f.使用代表公司憑證載具簽署之作業系統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。

g.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。

h.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。

i.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。

j.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」。

k.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。

（6）資料輸出管理：

a.報表是否按時產生並分送各使用單位。

b.機密性、敏感性之報表列印或瀏覽是否有適當之管制程序。

c.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）。

d.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，應依「機敏資訊類型及隱匿之具體作法原則」辦理。

9、系統開發及維護（CC–19000，半年查核）

（1）應用系統在規劃分析時應將資訊安全需求納入分析及規格。

（2）輸入資料是否有作檢查，以確認其正確性。

（3）應使用具有合法版權之軟體。

（4）委外廠商管理：

a.公司與委外資訊服務供應商提供服務應訂定合約，合約所含內容應包含以下內容：合約期限、服務範圍、服務交付日期、服務水準要求、服務變更規範、服務驗收之標準、資通安全事件通報及應變處理作業程序、對資訊服務供應商之稽核權條款、合約轉讓或同意分包之規範、保密義務條款、罰則與損害賠償條款、爭議處理程序、違約處理條款、合約終止規範、合約終止後之處理、保固、權利及責任。

b.證券商應評估資訊服務供應商之集中度，包括評估資訊服務供應商作業能力，採取適當風險管控措施，確保作業委外處理之品質，並注意作業委託資訊服務供應商之適度分散以控管作業風險。

c.資訊服務供應商應提供安全性檢測證明（如行動應用程式資安檢測、源碼檢測、弱點掃描等），並應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過程式碼掃描或黑箱測試。

d.公司應訂定相關規範管控，與資訊服務供應商資訊委外關係於終止、解除或結束後之相關作業。

e.委外資訊服務供應商應揭露第三方程式元件之來源與授權證明。

f.公司應管控資訊服務供應商存取權限，對於電腦通行使用權利進行適當控管。

g.公司應對資訊服務供應商服務內容變更進行風險評估。

h.公司對於委外資訊服務供應商於委外關係所涉及公司資訊資產，應於委外關係終止、解除或結束時完整歸還、確保銷毀或轉交予其他資訊服務供應商，並要求資訊服務供應商持續遵守保密承諾。

i.委外資訊服務供應商如自行發現程式漏洞、版本老舊，或於使用相同服務之其他證券商應用系統發生故障或異常時，應儘速瞭解原因，並主動轉知及提供因應措施。

j.委外資訊系統之服務規格書應包括硬體規格、軟體版本、作業環境變動、作業系統底層架構及系統程式相容性等，並包含維持委外廠商服務水準之要求與橫向溝通機制。

（5）已完成之程式因故需維護時，應依據經過正式核准之程序辦理。

（6）各項文件與手冊應經適當維護與控制。
（7）應用系統之維護應指派專人負責。
（8）應用系統異動管理：
a.正式作業與測試作業之程式、資料、工作控制指令等檔案應分開存放。
b.程式經修改其相關文件應及時更新。
（9）公司應定期（至少每半年乙次）辦理資訊系統弱點掃描作業，針對所辨識出之潛在系統弱點，應評估其相關風險或安裝修補程式，並留存紀錄（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商）。
（10）程式原始碼安全規範（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商）：
a.程式應避免含有惡意程式等資訊安全漏洞。
b.程式應使用適當且有效之完整性驗證機制，以確保其完整性。
c.程式於引用之函式庫有更新時，應備妥對應之更新版本。
d.程式應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。
e.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。
f.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（a、b、c、d、e）之佐證。
（11）行動應用程式安全管理（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商）：
a.行動應用程式發布：
(a)行動應用程式應於可信任來源之行動應用程式商店或網站發布，且應於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。
(b)應於官網上提供行動應用程式之名稱、版本與下載位置。
(c)應建立偽冒行動應用程式偵測機制，以維護客戶權益。
(d)應於發布前檢視行動應用程式所需權限應與提供服務相當，首次發布或權限變動應經資安、法遵單位同意，並留有紀錄，以利綜合評估是否符合個人資料保護法之告知義務」。
b.敏感性資料保護：
(a)行動應用程式傳送及儲存敏感性資料時應透過憑證、雜湊（Hash）或加密等機制以確保資料傳送及儲存安全，並於使用時應進行適當去識別化，相關存取日誌應予以保護以防止未

經授權存取。

(b)啟動行動應用程式時，如偵測行動裝置疑似遭破解（如 root、jailbreak、USB debugging 等），應提示使用者注意風險。

c.行動應用程式檢測：

(a)涉及投資人使用之行動應用程式於初次上架前及每年應委由經財團法人全國認證基金會（TAF）認證合格之第三方檢測實驗室進行並完成通過資安檢測，檢測範圍以目的事業主管機關委託執行單位「行動應用資安聯盟」公布之行動應用程式基本資安檢測基準項目進行檢測。如通過實驗室檢測後一年內有更新上架之需要，應於每次上架前就重大更新項目進行委外或自行檢測；所謂重大更新項目為與「下單交易」、「帳務查詢」、「身份辨識」及「客戶權益有重大相關項目」有關之功能異動。檢測範圍以 OWASP MOBILE TOP 10 之標準為依據，並留存相關檢測紀錄。

(b)公司對第三方檢測實驗室所提交之檢測報告，應建立覆核機制，以確保檢測項目及內容一致，並留存覆核紀錄。

（12）核心系統應針對風險評估使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。

（13）提供網際網路下單服務之核心系統上架前及系統更新時應執行「源碼掃描」安全檢測。

10、營運持續管理（CC–20000，半年查核）

（1）應明確訂定（例如：電腦設備、通訊設備、電力系統、資料庫、電腦作業系統等備援及回復計畫）故障復原程序，並落實執行且留存紀錄。

（2）故障復原程序應週期性測試，測試後應召開檢討會議，針對測試缺失謀求改進，並留存紀錄。

（3）證券經紀商之交易主機應有備援措施，並依所屬資安分級建置異地備援機房。

（4）公司應擬訂營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及其必要之維護，並擬訂關鍵性業務及其衝擊影響分析，評估核心系統中斷造成之衝擊程度，並依核心系統之復原時間目標（RTO）、資料復原點目標（RPO），作為恢復核心系統、備份備援規劃及執行復原作業之依據，再依其所屬資安分級定期辦理業務持續運作演練。公司應視

演練範圍是否涉及第三方，邀請相關廠商參與演練。

（5）公司應訂定資訊安全訊息通報機制（例如：正式之通報程序及資安事件通報聯絡人），針對與資訊系統有關之資訊安全或服務異常事件應依「證券期貨市場資通安全事件通報應變作業注意事項」及「證券商通報重大資安事件之範圍申報程序及其他應遵循事項」辦理，並採取適當矯正程序，留存紀錄。

（6）公司發生個人資料之竊取、竄改、毀損、滅失、或洩漏等資安事故者，應立即函報證交所（或櫃檯買賣中心、券商公會）轉陳主管機關。

（7）公司應明確訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序。

（8）公司應辦理下列資安防護事宜：

1.指定人員及部門統籌並協調聯繫各有關部門。

2.定期評估核心營運系統及設備，對評估結果採取適當措施，並提報董事會，以確保營運持續及作業韌性之能力。

3.於永續報告書、年報、財務報告或公司網站，揭露年度內公司持續核心營運系統及設備營運所需之資源及落實於年度預算或教育訓練計畫等項目。

（9）公司應辨識風險情境，就各項風險情境當災害發生造成資訊作業異常或中斷時，擬定各系統之應變、減災或復原措施相關作業流程。

（10）核心系統原服務中斷時，應於可容忍時間內，由備援設備或其他方式取代並提供服務。

（11）證券商資訊委外作業如涉及核心資通系統與資通服務，資訊服務供應商應定期提供資通系統與資通服務之回復計畫，回復計畫可以災難復原計畫、備援演練、營運持續計畫等形式呈現。

11、符合性（CC–21000，半年度查核）

（1）應定期（每年至少一次）辦理資訊安全查核作業（內部辦理或委託外部專業機構），並應留存查核紀錄。

（2）公司是否針對前開之資訊安全查核報告辦理追蹤改善情形（包括查核摘要、查核範圍、缺失說明及改進建議等）。

12、新興科技應用（CC–21100，年度查核）

（1）雲端服務：

應事先評估使用雲端運算服務之風險，若雲端運算服務涉及關鍵性系統、資料或服務者，應訂定雲端運算服務相關運作安全規範。

a.公司為雲端服務使用者時，應訂定雲端服務提供者之遴選機制、查核措施、備援機制、服務水準（含資訊安全防護）、復原時間及服務終止措施要求等，如有不符需求之處，需有其它補償性措施。

b.公司為雲端服務提供者時，應訂定雲端運算服務安全控管措施，應包含法律遵循、權限控管、權責歸屬及資訊安全防護等項目。如涉及敏感性資料之傳遞，應使用超文字傳輸安全協定（ HTTPS）、安全檔案傳輸協定（SFTP）等加密之網路協定。

（2） 社群媒體：

a.公司應訂定社群媒體相關資訊安全規範與運用社群媒體管理辦法，應包含以下內容：

(a)界定可於公務用社群媒體上分享之業務相關資料。

(b)私人與公務用社群媒體之區別與應注意事項。

b.應針對開放員工使用社群媒體評估其風險程度，包含：資料外洩、社交工程、惡意程式攻擊等，並採行適當的安全控管措施。

c.公司應訂定經營官方社群媒體資訊安全規範與管理辦法，並包含以下內容：

(a)應事先了解所經營之社群媒體隱私政策，並定期（每年一次）檢視其隱私政策之異動及評估其風險。

(b)於官方網站提供連結供使用者連至公司外之社群媒體時，應出現提示視窗告知使用者該連結非公司本身之網站。

(c)對經營之社群媒體應標示證券商名稱、聯絡方式、許可證字號、客戶申訴聯繫方式及處理窗口，以區別為官方經營之社群媒體。

(d)應建立帳號權限管理機制，對發布內容進行控管與監視，並針對不適當言論及異常事件，進行通報或處置。

（3） 行動裝置：

a.公司應訂定公務用行動裝置之資訊安全規範與管理辦法，須包含以下項目：

(a)行動裝置設備管理辦法應對於申請、使用、更新、繳回與審核應訂有相關規範。

(b)人員異動時，行動裝置應進行重新配置或清除配置程序，以確保行動裝置環境安全性。

(c)行動裝置應避免安裝非官方發佈之行動應用程式，或僅安裝由公司列出通過檢測可安裝之行動應用程式。

(d)公務用行動裝置管理辦法內容應包含行動裝置儲存機密資料之

限制與管理方式。

b.公司應訂定員工自攜行動裝置之資訊安全規範與管理辦法，須包含以下項目：

(a)公司應要求員工自攜行動裝置使用用途。

(b)公司應與持有人簽署員工自攜行動裝置使用協議，含：使用限制及雙方責任等。

(c)公司應限制內部資訊設備透過員工自攜行動裝置私接存取網際網路（Internet）之行為。

(d)員工自攜行動裝置管理辦法內容應包含行動裝置儲存機密資料之限制與管理方式。

（4） 物聯網：

應訂定物聯網相關資訊安全規範與管理辦法，須包含下列項目：

a.應建立物聯網設備管理清冊並至少每年更新一次，且應變更前開設備之初始密碼。

b.物聯網設備應具備安全性更新機制且定期（每年一次）更新，如存在已知弱點無法更新時，應建立補償性管控機制。

c.應關閉物聯網設備不必要之網路連線及服務，避免使用對外公開的網際網路位置。

d.如與物聯網設備供應商簽定採購合約時，其內容宜包含資訊安全相關協議，明確約定相關責任（如：服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案），確保設備不存在已知安全性漏洞。

e.公司採購物聯網設備時，宜優先採購取得資安標章之物聯網設備。

f.公司應定期辦理物聯網設備使用及管理人員資安教育訓練。

g.應建立物聯網設備存取權限控管措施。

（5） 遠距辦公：

a.公司應對使用遠距辦公之設備安裝資訊安全相關軟體，控管應用程式存取權限，以降低資訊外流風險。

b. 公司應依業務範圍及控管權限設定居家辦公員工之系統功能權限。

c.公司應依員工執行業務內容訂定連線時段限制及相關規範。

d.公司應留存遠距辦公員工使用者登入系統、電腦設備操作及交易紀錄軌跡。

e.公司應採多因子驗證機制（員工帳號密碼、動態密碼、一次性帳密）及建立安全的遠距網路通道，降低相關帳號密碼遭假冒或竊用之風險。

f.公司應阻擋惡意或未經授權之連線，並採用最小權限原則設定遠距帳號存取規則。

g.公司應定時更新 VPN 連線和其他遠端連結系統之安控措施。

h.公司應對客戶隱私、資料及紀錄之安全性建立保護措施。

i.公司應加強宣導資訊安全，教育遠距辦公員工應對網路風險保持警覺等資訊安全機制。

（6）深度偽造（Deepfake）

a.使用影像視訊方式進行身分驗證時應強化驗證並搭配其他驗證因子（如上傳身分證件、手機簡訊 OTP）。

b.應定期辦理涵蓋深度偽造認知及防範議題之資訊安全教育訓練。

13、其他（CC–22000，半年查核）

資訊提供作業（CC–22010）

a.各種重要法令規章及通知應立即張貼於公佈欄。

b.上市公司之營運資料、公開說明書應陳列於證券投資資料櫃供客戶閱覽。

c.營業廳內應裝置「公開資訊觀測站」，供客戶自行操作使用。

d.資訊閱覽室應未限定對象並且無收費行為。

e.資訊閱覽室不得裝設專用競價用終端機。

f.不得於資訊閱覽室從事與客戶簽定開戶契約、接受買賣有價證券之委託交割及其他類似證券商業務行為。

g.於所設網站上提供股市即時交易資訊，應經由與證交所簽約之資訊公司提供。

h.應定期檢查網站內對外提供之資訊，對具機密性、敏感性之資訊內容，應立即移除；並應遵守證券商推介客戶買賣有價證券作業辦法規定，且不得以公司名義將屬於證券投資顧問事業範圍之資訊代為公開。

i.證券商若於網站平台上進行推介，應設有密碼以控管得閱覽個股研究報告之客戶；且客戶應與證券商簽訂推介契約（國內機構投資人及外國機構投資人得免簽）。

14、主機共置（Co_Location）服務管理（CC–23000，適用使用主機共置服務之證券商，月或半年查核）

（1）設備等資產進出主機共置機房，應於「主機共置用戶服務系統」進行申請，並配合清點及留存紀錄（半年查核）。

（2）配合定期盤點主機共置機房機櫃內主機與網路設備（半年查核）。

（3）公司放置於主機共置機房之軟體、硬體設備應依「建立證券商資通安全檢查機制」規定，具備完善之資訊安全防護措施並落實執行（月或半年查核）。