中華民國證券商業同業公會資通系統安全防護基準自律規範

金融監督管理委員會 111 年 12 月 22 日金管證券字第 1110365208 號函准予備查
中華民國證券商業同業公會 111 年 12 月 23 日中證商業一字第 1110008167 號函公告實施

第一條 目的

為使證券商強化資通系統安全防護，特訂定本自律規範。

第二條 名詞定義

一、資通系統：係指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、核心系統：係指直接提供客戶交易或支持交易業務持續運作之必要系統(如交易系統、報價系統、中台風控、盤後結算系統、帳務系統等維持交易業務之必要系統)，其餘皆為非核心系統。

三、非客戶帳號：係指非客戶所使用之資通系統帳號(如：提供內部人員、管理者及廠商等所使用之資通系統帳號)。

四、資訊資產：係指與資訊處理相關之資產，包括硬體、軟體、資料及文件等。

五、第一類證券商：係指依「證券暨期貨市場各服務事業建立內部控制制度處理準則」第三十六條之二條文指派資訊安全長之證券商或「建立證券商資通安全檢查機制-分級防護應辦事項附表」所列第一級、第二級、第三級證券商。

六、第二類證券商：係指非屬第一類證券商之證券商。

七、外國證券商：係指外資集團在台子公司或分公司。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。

第三條 資通系統存取控制

一、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。

二、如有核准臨時或緊急使用之資通系統帳號，於作業結束後，應即時刪除或禁用該等資通系統帳號。

三、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。

四、第一類證券商應定義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)。

五、第一類證券商應依公司規定之情況及條件使用核心系統，逾越所定之許可閒置時間或可使用期限時，系統宜自動將使用者帳號登出。

六、提供網際網路下單服務之證券商，應每日針對核心系統帳號、非客戶帳號登入嘗試紀錄等進行監控及分析，如發現帳號違常使用時回報管理者並進行後續處理。

七、不得使用客戶之顯性資料(如統一編號、身分證號、手機號碼、電子郵件帳號、信用卡號、存款帳號等)作為唯一之識別，否則應另行增設使用者代號以資識別。

八、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。

九、應訂定遠端連線管理辦法，建立使用限制、組態需求、連線需求及文件化，對於任一允許之遠端存取類型，均應先取得授權，並留存相關紀錄。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。

十、應於伺服器端完成資通系統帳號權限登入驗證作業。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。

十一、組織應監控使用外部網路遠端連線存取組織內部網段之連線。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。

十二、資通系統之遠端存取應採用連線加密機制。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。

十三、資通系統遠端存取之來源應為公司已核准之存取控制點。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。

第四條 電腦稽核紀錄(日誌)與可歸責性

一、應訂定核心系統電腦稽核紀錄(日誌)之記錄時間週期及保存政

策，並至少保存三年。

二、核心系統電腦稽核紀錄(日誌)應確有記錄特定事件之功能，並決定應記錄之特定資通系統事件。

三、核心系統電腦稽核紀錄(日誌)應記錄管理者帳號所執行之各項功能，並逐日覆核使用結果。

四、應定期審查核心系統產生之電腦稽核紀錄(日誌)。

五、核心系統之電腦稽核紀錄(日誌)應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並應依組織所訂之資通安全政策及相關法令要求及組織業務需求納入其他相關資訊。

六、核心系統應依據電腦稽核紀錄(日誌)儲存需求，配置所需之儲存容量。

七、於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。

八、資通系統應使用系統內部時鐘產生電腦稽核紀錄(日誌)所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。

九、資通系統內部時鐘應定期與基準時間源進行同步。

十、對電腦稽核紀錄(日誌)之存取管理，僅限於有權限之使用者。

十一、核心系統應運用適當方式確保電腦稽核紀錄(日誌)機制之完整性。

第五條 營運持續管理

一、應訂定核心系統可容忍資料損失之時間要求。

二、證券商應執行核心系統程式原始碼與資料備份。

三、應定期測試核心系統備份資訊，以驗證備份媒體之可靠性及資訊之完整性。

四、第一類證券商應將核心系統之備份還原，作為營運持續計畫測試之一部分。

五、第一類證券商核心系統之軟體及備份檔案，應儲存在與運作系統不同地點之獨立設施或防火櫃中。

六、應訂定核心系統從中斷後至重新恢復服務之可容忍時間要求。

七、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。

八、應建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其合理範圍內。

第六條 身分驗證管理

一、資通系統應具備唯一識別及鑑別公司內部、外部使用者(或代表公司使用者行為之程序)之功能，禁止使用共用帳號。

二、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。

三、使用者使用預設密碼登入資通系統時，應於登入後要求立即變更預設密碼後方可繼續作業。

四、資通系統不以明文傳輸身分驗證相關資訊。

五、資通系統具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。

六、屬電子式交易資通系統，使用者密碼輸入錯誤次數達三次者，應記錄登入失敗事件、鎖定該登入帳號並中斷連線；受理解除鎖定之申請時，應確實辨認身分，並留存相關紀錄後，始得解除鎖定。

七、資通系統如使用密碼進行驗證時，應採用優質密碼設定，設定密碼最長使用期限為三個月，檢核密碼最短使用期限及密碼歷程記錄為三代，如為客戶帳號者，除優質密碼設定外，其餘密碼設定可依公司自行規範辦理。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。

八、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。

九、提供對外服務之核心系統密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記(如：網站連結或一次性密碼One-time password(OTP)至使用者登記之電子信箱或手機)或其他驗證身分方式，非核心系統密碼重設後宜有驗證身分方式。

十、應遮蔽資通系統鑑別過程中之資訊。

十一、資通系統如以密碼進行資通系統鑑別時，該密碼應加密或經雜湊處理後儲存。

第七條 系統與服務獲得

一、資通系統於系統需求分析階段，應針對資通系統安全需求(含機密性、可用性、完整性)進行確認。

二、應根據核心系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。

三、應將核心系統風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。

四、資通系統應針對安全需求實作必要控制措施。

五、資通系統應注意避免軟體常見漏洞及實作必要控制措施。

六、核心系統應針對風險評估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。

七、提供網際網路下單服務之證券商核心系統上架前及系統更新時應執行「源碼掃描」安全檢測。

八、提供網際網路下單服務之證券商應定期（至少每半年乙次）辦理資通系統「弱點掃描」安全檢測。

九、提供網際網路下單服務之證券商，應定期對提供網際網路服務之核心系統辦理「滲透測試」安全檢測。

十、於部署環境中應針對資通系統相關安全威脅與漏洞，進行更新與修補，並關閉不必要服務及埠口。

十一、應檢視現有之核心系統，應設定使用優質密碼設定，且應避免使用預設密碼。

十二、資通系統發展生命週期之維運階段，應執行版本控制與變更管理。

十三、證券商如委外辦理核心系統開發應將系統發展生命週期各階段安全需求(含機密性、可用性、完整性)納入委外契約。

十四、資通系統正式作業環境應與開發、測試作業環境區隔。

十五、應儲存與管理資通系統發展生命週期之相關文件。

第八條 系統與通訊保護

一、核心系統透過網際網路及內部網路傳輸個人或機敏資料應採用加密傳輸機制，以防止未授權之資訊揭露或偵測資訊之變更(傳輸過程中如有替代之實體保護措施者,則無需採加密傳輸機制)。

二、如有國際傳輸客戶個人機敏資料時,證券商應建立加密傳輸機制,當涉及客戶資訊,傳輸前應告知取得當事人授權且不違反主管機關對國際傳輸之限制，並留存完整稽核紀錄。外國證券商如為同集團內之傳輸，其間傳輸方式已符合所在國當地的法令規定，得排除國際傳輸之規定。

三、加密機制應使用公開、國際機構驗證且未遭破解之演算法。

四、加密機制之金鑰或憑證應定期更換。

五、加密機制宜支援演算法最大長度金鑰。

六、加密機制於伺服器端之金鑰保管宜訂定管理規範及實施應有之安全防護措施。

七、第一類證券商核心系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。

八、加解密程式或具變更權限之公用程式(如資料庫工具程式)應列管並限制使用，防止未經授權存取並保留稽核軌跡。

第九條 系統與資訊完整性

一、 資通系統之漏洞修復針對不同風險研訂適當修補措施及完成時間。

二、 如發現資通系統有被入侵跡象時，應通報公司權責人員進行處理。

三、 應監控核心系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。

四、 核心系統宜採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。

第十條 個人資料保護

一、為維護所保有個人資料資通系統之安全，應採取下列資料安全管理措施：

(一)訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，應採取防範資料洩漏之適當措施。

(二)針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。

(三)作業過程有備份個人資料之需要時，對備份資料予以適當保護。

二、為維護保有個人資料資通系統安全，應依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員約定保密義務。

三、應針對資通系統所保有之個人資料進行風險評估及控管。

四、保有個人資料之資通系統應建置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。

五、保有個人資料之資通系統應建立個人資料外洩防護機制，管制個人資料檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁或網路檔案等方式傳輸，並應留存相關紀錄、軌跡及證據。

六、資通系統如刪除、停止處理或利用所保有之個人資料後，應留存下列紀錄：

(一)刪除、停止處理或利用之方法、時間。

(二)將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。

第十一條 施行程序

本自律規範經本公會理事會會議通過，並報奉主管機關備查後實施，修正時亦同。