中華民國證券商業同業公會網路安全防護自律規範

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

為強化證券商網路安全，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、存取：係指存取資訊資產的各種方式，包含取得、使用、保管、查詢、修改、調整、銷毀等。

三、網路設備：係指傳輸資料、應用程式、服務和多媒體所需的網路通訊元件，如防火牆、路由器、交換器…等，亦為組織的網路架構圖包含的項目。

四、資通安全事件：係指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

五、資訊資產：係指與資訊處理相關之資產，包括硬體、軟體、資料、文件及人員等(如：伺服器主機及使用者電腦之作業系統及應用程式等軟體資訊)。

六、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。

七、第二類證券商：係指非屬第一類證券商之證券商。

八、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 網路架構與網路安全管理

一、網路架構圖

應呈現證券商維持業務運作之必要網路環境設備(如：防火牆、

路由器、交換器、系統設備、線路配置、伺服器與服務、無線網路)，另針對網段、路由規劃、主機 IP 位址、備援線路應有相關檔案紀錄。

二、網路區域劃分

(一)為確保網路架構安全，應獨立劃分各工作區域並落實網段隔離。

(二)網段應以維持業務運作劃分區域：如隔離區(非軍事區，Demilitarized Zone, DMZ)、營運區(Production, Prod.)、測試區(Unit Test, UT 或 User Acceptance Test, UAT)及其他等網段。

(三)證券商應定義外部網路與內部網路，外部網路連接網際網路，內部網路區域為組織人員與內部服務的伺服器配置區域。由外部網路到內部網路的流量需要經過存取控制，避免非允許的服務進入。

(四)證券商之內部網段區域劃分方式可依據組織內部單位、部門、業務性質等，並規範不同網段(VLAN)間的存取。

(五)證券商應使用適當方式隔離限制存取與特定服務，且應視區隔方式，定期檢視防火牆規則或存取控制清單(Access Control List, ACL)。

三、內部網路管理

(一)證券商如有提供無線網路供內/外部人員使用，無線網路存取保護應採用現行公開資訊已認可且無弱點之安全協定。

(二)證券商應建立無線網路密碼原則，以降低密碼破解之風險。

(三)證券商如允許內/外部人員使用外部設備存取內部網路，應提出申請並檢視設備安全性與相關授權，並限制存取範圍。

第四條 網路設備安全管理

一、網路設備管理

(一)證券商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。

(二)證券商應定期檢視官方發布之軟體、韌體、弱點修補程式之更新，將網路設備更新至最新版本或廠商建議版本。

(三)證券商經由網際網路連線至內部網路進行遠距之系統維護，應落實身份認證機制。

(四)網路設備管理人員之管理帳號應僅限管理人員使用且不得共用帳號，管理帳號之密碼設定原則應遵循證券商之身份驗證管理規範。

(五)證券商應限制網路設備管理使用之人員、設備、 IP、網段，或採用一次性密碼(One-time password, OTP)、短暫性存取(Temporary Privileged Access)等措施，並留存使用人員操作紀錄。

(六)證券商所有網路設備之防護基準應依「本公會資通系統安全防護基準自律規範」。

二、網路設備規則管理

(一)網路存取規則、防火牆規則等新增、異動、刪除應審核使用者需求，經評估資通安全風險程度後進行規則變更，並保留相關紀錄備查。

(二)網路設備規則設立應以使用者角色最小授權及正面表列為原則。

(三)證券商應至少每年檢視一次網路設備規則。

三、網路設備日誌

證券商應留存網路設備存取日誌並至少保留三年，供留存備查。另應防止未經授權存取，並定期檢視以確保可用性。

四、網路設備委外

證券商所有網路設備若委由外部廠商維運或管理應依「本公會供應鏈風險管理自律規範」。

第五條 網路連線安全

一、網路連線安全憑證

(一)證券商應確保 SSL/TLS 憑證之有效性及合法性，以維持網路

連線之安全性。

(二)證券商如提供網路下單服務，應訂定憑證交付程序，避免非本人取得憑證，並搭配與登入雙因子之不同因子驗證機制交付憑證，及全面使用認證機制。

(三)證券商如使用網路專線與合作第三方機構網路連線，應架設防火牆，關閉非約定之埠號以確保內部網域安全。

二、網路傳輸安全

如有國際傳輸客戶個人資料時，證券商應建立加密傳輸機制，當涉及客戶資訊，傳輸前應告知當事人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、遠端連線管理

(一)證券商應訂定遠端連線管理辦法，建立使用限制、組態需求、連線需求的遠距連線機制，亦應包含採多因子身分驗證機制、加密連線、採最小授權原則、留存完整使用者操作稽核軌跡、監控與警示異常操作行為、執行安全性漏洞更新等安控措施，並留存相關紀錄由權責主管定期覆核。

(二)證券商須透過安全的連線機制來阻擋惡意或未經授權之連線，並以最小權限原則設定規則及關閉非必要之埠號，並應監控網路流量及異常警告及中斷連線機制。

第六條 網路攻擊防護機制

一、具網路下單服務或設有官方網站之證券商應建立分散式阻斷服務之防護機制。

二、具有對外服務之資通系統者，應建置應用程式防火牆。

三、安全性檢測

(一)證券商應定期評估自身網路環境安全，例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等。

(二)證券商應定期修補網路環境之安全漏洞，並留存相關文件。

(三)第一類證券商資通系統應定期辦理系統滲透測試。

（四）第一類證券商應定期辦理資通安全健診，包含網路架構檢視、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及目錄伺服器設定及防火牆連線設定檢視。

第七條 資通安全事件通報與應變

一、證券商應訂定資通安全事件內部通報機制，包含正式之通報程序及資通安全事件通報聯絡人。

二、於發生影響客戶權益或正常營運之資訊服務異常事件或資通安全事件應依「證券期貨市場資通安全事件通報應變作業注意事項」辦理，並採取適當應變程序及留存紀錄。

三、證券商遇有重大個人資料安全事故者，應立即通報主管機關。所稱重大個人資料安全事故，係指個人資料遭竊取、竄改、毀損、滅失或洩漏，將危及組織正常營運或大量當事人權益之情形。

第八條 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。