中華民國證券商業同業公會新興科技資通安全自律規範修正條文對照表

修正後條文	原條文	說明
自律規範名稱 中華民國證券商業同業公會新興科技資通安全自律規範	**自律規範名稱** 中華民國證券商業同業公會新興科技資訊安全自律規範	一、變更自律規範名稱。 二、依證交所 111 年 5 月 11 日公告「證券期貨市場相關公會新興科技資通安全管控指引」(下稱管控指引)修正。
第一條(規範目的) 為強化證券商管理及應用新興科技，特訂定本自律規範。	**第一條(規範目的)** 為強化證券商運用雲端運算服務、社群媒體及行動裝置之資訊安全，特訂定本自律規範。	依管控指引第一條(目的) 修正規範目的。
第二條(用詞定義) **一、雲端運算服務：**透過網路技術達成共享運算資源之前提下，提供使用者具備彈性、可擴展及可自助之服務(如：IaaS(基礎架構即服務)、PaaS(平台即服務)、SaaS(軟體即服務))。惟本自律規範定義之雲端運算服務不包含建置組織內部且僅對內提供服務之私有雲。 **三、行動裝置：**一種具有資料運算處理、儲存與網路連線功能之可攜式設備，包括但不限於智慧型手機、筆記型電腦、平板電腦與 PDA 等裝置，惟本自律規範定義之行動裝置僅限可用於處理組織內部定義之敏感性事務且可直接連接組織網路設備、服務之行動裝置。 六、電子式交易驗證：指以組織同意之電子式委託買賣前對使用者身分驗證資訊進行確認。惟本自律規	**第二條(用詞定義)** **一、雲端運算服務：**透過網路技術達成共享運算資源之前提下，提供使用者具備彈性、可擴展及可自助之服務，惟本自律規範定義之雲端運算服務不包含建置組織內部且僅對內提供服務之私有雲。 **三、行動裝置：**一種具有資料運算處理、儲存與網路連線功能之可攜式設備，包括智慧型手機、筆記型電腦、平板電腦與 PDA 等裝置，惟本自律規範定義之行動裝置僅限可用於處理組織內部定義之敏感性事務且可直接連接組織網路設備、服務之行動裝置。	一、 修正本條「一、雲端運算服務」、「三、行動裝置」，新增「六、電子式交易驗證」、「七、深度偽造(Deepfake)」。 二、 依管控指引第二條(雲端運算服務定義)、第十五條(行動裝置定義)、第三十二條(電子式交易身分驗證定義)、第三十四條(電子式交易身分驗證指引適用範圍)、第三十九條(深度偽造定義)增修訂。

修正後條文	原條文	說明
範定義之電子式交易驗證僅適用透過網際網路交易之系統，不包含電話語音、電子式專屬線路下單(DirectMarketAccess，簡稱DMA)、主機共置(Co–Location)等服務型態。 七、深度偽造(Deepfake)：指使用電腦合成或其他科技方法製作或散布涉及真實人物實際未發生的行為舉止影像紀錄、動態圖像、錄音、電子圖像、照片及任何言語或行為等技術表現形式。		
第三條(資通安全法令遵循) 證券商管理及應用新興科技除應遵循主管機關金融監督管理委員會「指定非公務機關個人資料檔案安全維護辦法」、臺灣證券交易所「建立證券商資通安全檢查機制」等相關規範外，並應依本自律規範辦理。 外資集團在台子公司或分公司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(資訊安全法令遵循)** 證券商運用雲端運算服務、社群媒體及行動裝置之資訊安全除應遵循主管機關金融監督管理委員會「指定非公務機關個人資料檔案安全維護辦法」、臺灣證券交易所「建立證券商資通安全檢查機制」等相關規範外，並應依本自律規範辦理。	一、 依管控指引第一條(目的)，本條修正為資通安全法令遵循，並修正第一項。 二、 本條新增第二項「外資集團在台子公司或分公司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(雲端運算服務運作安全) 證券商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	**第四條(雲端運算服務運作安全)** 證券商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	一、 本條新增第三項「就雲端服務中斷及終止應訂立管理措施」。 二、 依管控指引第九條(雲端服務中斷及終止管理)增訂。

修正後條文	原條文	說明
全規範，其內容包含下列項目： 一、證券商為使用者時應訂定雲端運算服務提供者之遴選機制及查核措施。 二、證券商為提供者時應訂定雲端運算服務安全控管措施。 三、就雲端服務中斷及終止應訂立管理措施。	務相關運作安全規範，其內容包含下列項目： 一、證券商為使用者時應訂定雲端運算服務提供者之遴選機制及查核措施。 二、證券商為提供者時應訂定雲端運算服務安全控管措施。	
第九條（電子式交易相關控管） 證券商提供電子式交易登入時，其安全設計應具有下列三項之任兩項以上技術： 一、證券商所約定之資訊，且無第三人知悉（如固定密碼、圖形鎖或手勢等）。 二、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），證券商應確認該設備為客戶與證券商所約定持有之設備。 三、客戶提供給證券商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），證券商應直接或間接驗證該生物特徵。間接驗證係指由客戶端設備（如行動裝置）		一、新增條文。 二、依管控指引第三十七條(電子式交易身分驗證控管)及第三十八條(電子式交易稽核軌跡)及金融監督管理委員會 111 年 9 月 15 日金管證券字第 1110355166 號函增訂。

修正後條文	原條文	說明
驗證或委由第三方驗證，證券商僅讀取驗證結果，必要時應驗證來源辨識；採用間接驗證者，應事先評估客戶身分驗證機制之有效性。 證券商對於電子式交易身分的申請、交付、使用、更新與驗證應訂有相關控管措施。 證券商應就帳號登入失敗、非客戶帳號登入嘗試紀錄留存相關監控及分析紀錄。 證券商對電子式交易身分的驗證資訊於網際網路傳輸時應全程加密。 證券商對電子式交易身分的驗證資訊應進行雜湊或加密儲存。 證券商應於伺服器端驗證客戶電子式交易身分。 證券商應使用優質密碼設定並進行管控，確實執行密碼輸入錯誤次數達 3 次者應予帳號鎖定。 證券商應提供客戶定期更新密碼之機制並使用優質密碼。 證券商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。		

修正後條文	原條文	說明
第十條 (深度偽造之防範) 證券商使用影像視訊方式進行身分驗證應強化驗證。 證券商宜定期辦理涵蓋深度偽造認知及防範議題資訊安全教育訓練。		一、新增條文。 二、依管控指引第四十一條(影像視訊身分驗證控管)及第四十二條(深度偽造防範控管) 增訂。
第十一條 (違規處理程序) 證券商違反本自律規範，依本公會會員自律公約及其他有關之規定辦理。	**第九條(違規處理程序)** 證券商違反本自律規範，依本公會會員自律公約及其他有關之規定辦理。	調整條次。
第十二條 (本法施行程序) 本自律規範經本公會理事會會議通過，並報奉主管機關核備後實施，修正時亦同。	**第十條(本法施行程序)** 本自律規範經本公會理事會會議通過，並報奉主管機關核備後實施，修正時亦同。	調整條次。