中華民國期貨業商業同業公會
「新興科技資通安全自律規範」
修正條文對照表

修正後內容	修正前內容	說明
自律規範名稱： 中華民國期貨業商業同業公會「新興科技資通安全自律規範」	自律規範名稱： 中華民國期貨業商業同業公會「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(目的) 為強化期貨業管理及應用新興科技，特訂定本自律規範。	**第一條（目的）** 為強化期貨業運用雲端運算服務、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(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。 二、社群媒體：一種結合科技、社交互動與內容創造之網路應用，允許創造或交換使用者產出內容；且透過此高度互動的平台，個人及群體可以分享、共創、討論並修改使用者產出內容，惟本自律規範定義之社群媒體不含組織內部溝通使用之社群媒體或平台。 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	**第二條（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。 二、社群媒體：一種結合科技、社交互動與內容創造之網路應用，允許創造或交換使用者產出內容；且透過此高度互動的平台，個人及群體可以分享、共創、討論並修改使用者產出內容，惟本自律規範定義之社群媒體不包含組織內部溝通使用之社群媒體或平台。 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	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。

修正後內容	修正前內容	說明
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。 四、員工自攜行動裝置(BYOD)：非屬組織行動裝置用於處理組織事務、直接連接組織網路設備或服務。 五、物聯網設備：指具網路連線功能之嵌入式系統設備及其周邊連網之裝置(如：感測器)。 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。惟本自律規範定義之電子式交易驗證僅適用於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(Direct Market Access，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。	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。 四、員工自攜行動裝置(BYOD)：非屬組織行動裝置用於處理組織事務、直接連接組織網路設備或服務。 五、物聯網設備：指具網路連線功能之嵌入式系統設備及其周邊連網之裝置(如：感測器)。	
第三條(資通安全法令遵循) 期貨業管理及應用新興科技除應遵循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」、臺灣期貨交易所「建立期貨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)** 期貨業運用雲端運算服務、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」、臺灣期貨交易所「建立期貨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」。

修正後內容	修正前內容	說明
第四條(雲端運算服務運作安全) 期貨業應事先評估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，其內容包含下列項目： 一、期貨業為使用者時，應訂定對雲端運算服務提供者之遴選機制及查核措施。 二、期貨業為提供者時，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。	**第四條（雲端運算服務運作安全）** 期貨業應事先評估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，其內容包含下列項目： 一、期貨業為使用者時，應訂定對雲端運算服務提供者之遴選機制及查核措施。 二、期貨業為提供者時，應訂定雲端運算服務安全控管措施。	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。
第五條（社群媒體安全控管） 期貨業應訂定社群媒體相關資訊安全規範，其內容包含下列項目： 一、擬定社群媒體使用政策，以規範員工使用社群媒體之行為。 二、就開放員工使用之社群媒體類型評估其風險程度（包含資料外洩、社交工程、惡意程式攻擊等），並就高風險部分採適當的安全控管措施。 三、經營官方社群媒體之資訊安全控管： （一）檢視所經營之社群媒體隱私政策及評估其風險。 （二）標示期貨業名稱、地址、電話及許可證字號。 （三）建立帳號權限管理機制，並對發布內容進行控管。 四、制定異常通報及申訴處理機制： （一）經營官方社群媒體之管理單位，宜不定時監看該社群媒體之討論內容，並針對不適當言論	**第五條（社群媒體安全控管）** 期貨業應訂定社群媒體相關資訊安全規範，其內容包含下列項目： 一、擬定社群媒體使用政策，以規範員工使用社群媒體之行為。 二、就開放員工使用之社群媒體類型評估其風險程度（包含資料外洩、社交工程、惡意程式攻擊等），並就高風險部分採適當的安全控管措施。 三、經營官方社群媒體之資訊安全控管： （一）檢視所經營之社群媒體隱私政策及評估其風險。 （二）標示期貨業名稱、地址、電話及許可證字號。 （三）建立帳號權限管理機制，並對發布內容進行控管。 四、制定異常通報及申訴處理機制： （一）經營官方社群媒體之管理單位，宜不定時監看該社群媒體之討論內容，並針對不適當言論	本條文內容未修訂。

修正後內容	修正前內容	說明
或異常事件，進行必要之通報或處置。 （二）官方社群媒體應標示客戶申訴聯絡方式及處理窗口。	或異常事件，進行必要之通報或處置。 （二）官方社群媒體應標示客戶申訴聯絡方式及處理窗口。	
第六條（行動裝置安全控管） 期貨業應訂定行動裝置相關資訊安全規範，其內容包含下列項目： 一、公司提供之行動裝置設備之管理。 二、員工自攜行動裝置之管理。 三、行動應用程式安全事項： （一）行動應用程式發布： 1.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。 2.應於官網上提供行動應用程式之名稱、版本與下載位置。 3.應建立偽冒行動應用程式偵測機制，以維護客戶權益。 4.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單位或人員、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。 （二）敏感性資料保護： 1.行動應用程式傳送及儲存敏感性資料時應透過有效憑證、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。 2.啟動行動應用程式時，如偵測行動裝置疑似遭破解（如 root、	**第六條（行動裝置安全控管）** 期貨業應訂定行動裝置相關資訊安全規範，其內容包含下列項目： 一、公司提供之行動裝置設備之管理。 二、員工自攜行動裝置之管理。 三、行動應用程式安全事項： （一）行動應用程式發布： 1.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。 2.應於官網上提供行動應用程式之名稱、版本與下載位置。 3.應建立偽冒行動應用程式偵測機制，以維護客戶權益。 4.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單位或人員、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。 （二）敏感性資料保護： 1.行動應用程式傳送及儲存敏感性資料時應透過有效憑證、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。 2.啟動行動應用程式時，如偵測行動裝置疑似遭破解（如 root、	本條文內容未修訂。

修正後內容	修正前內容	說明
jailbreak、USB debugging 等)，應提示使用者注意風險。 （三）行動應用程式檢測： 1.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，檢測範圍以經濟部工業局委託執行單位「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。 2.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 TOP10 之標準為依據，並留存相關檢測紀錄。 3.公司對第三方檢測實驗室所提交之檢測報告，應依附錄所列檢測項目建立覆核機制，以確保檢測項目及內容一致，並留存覆核紀錄。	jailbreak、USB debugging 等)，應提示使用者注意風險。 （三）行動應用程式檢測： 1.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，檢測範圍以經濟部工業局委託執行單位「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。 2.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 TOP10 之標準為依據，並留存相關檢測紀錄。 3.公司對第三方檢測實驗室所提交之檢測報告，應依附錄所列檢測項目建立覆核機制，以確保檢測項目及內容一致，並留存覆核紀錄。	
第七條（物聯網設備安全控管） 期貨業就具備網路連線功能且有連接外部或內部網路之自動化辦公(OA)設備，應訂定物聯網設備資訊安全辦法，其內容包含下列項目： 一、設備盤點評估作業。 二、設備軟體控管措施。 三、設備權限控管措施。 四、設備連線控管措施。 五、供應商管理。	**第七條（物聯網設備安全控管）** 期貨業就具備網路連線功能且有連接外部或內部網路之自動化辦公(OA)設備，應訂定物聯網設備資訊安全辦法，其內容包含下列項目： 一、設備盤點評估作業。 二、設備軟體控管措施。 三、設備權限控管措施。 四、設備連線控管措施。 五、供應商管理。	本條文內容未修訂。

修正後內容	修正前內容	說明
六、例外控管措施：物聯網設備存在已知弱點且無法更新，或因設備功能限制無法落實本條第二、三、四款規範之例外控管措施。 七、不具備管理功能之感測器仍應依本條第一、四、五、六款辦理。 前項評估作業及控管措施應定期更新。	六、例外控管措施：物聯網設備存在已知弱點且無法更新，或因設備功能限制無法落實本條第二、三、四款規範之例外控管措施。 七、不具備管理功能之感測器仍應依本條第一、四、五、六款辦理。 前項評估作業及控管措施應定期更新。	
第八條（網路釣魚之防範） 期貨業應偵測釣魚網站，提醒客戶防範網路釣魚。	**第八條（網路釣魚之防範）** 期貨業應偵測釣魚網站，提醒客戶防範網路釣魚。	本條文內容未修訂。
第九條（電子式交易相關控管） 期貨業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、組織所約定之資訊，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），組織應確認該設備為客戶與組織所約定持有之設備。 三、客戶提供給組織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），組織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）驗證或委由第三方驗證，組織僅讀取驗證結果，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。 期貨業對於電子式交易身分的申請、交付、使用、更新與驗證		一、新增條文。 二、依管控指引第三十六條(電子式交易身分驗證機制管理)、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)增訂。

修正後內容	修正前內容	說明
應訂有相關控管措施。 期貨業應就帳號登入失敗、非客戶帳號登入嘗試紀錄留存相關監控及分析紀錄。 期貨業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。 期貨業對電子式交易身分的驗證資訊應進行雜湊或加密儲存。 期貨業應於伺服器端驗證客戶電子式交易身分。 期貨業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。 期貨業應提供客戶定期更新密碼之機制並使用優質密碼。 期貨業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。		
第十條（深度偽造之防範） 期貨業使用影像視訊方式進行身分驗證應強化驗證。 期貨業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（違規之處理） 期貨業違反本自律規範，依本公會會員自律公約及其他有關之規定辦理。	**第九條（違規之處理）** 期貨業違反本自律規範，依本公會會員自律公約及其他有關之規定辦理。	條文序號順修。
第十二條（附則） 本自律規範經本公會理事會通過，並報奉主管機關核備後實施，修正時亦同。	**第十條（附則）** 本自律規範經本公會理事會通過，並報奉主管機關核備後實施，修正時亦同。	條文序號順修。