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」

第六條修正條文對照表

| 修正後內容 | 修正前內容 | 說明 |
| --- | --- | --- |
| 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、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、行動應用程式之發佈及安全事項：  (一)行動應用程式發佈前，應確認程式碼或程序庫符合以下安全事項：  1.通過內容安全或驗證程序，如：程式原始碼檢測或掃描，確認未含惡意程式碼。  2.程式碼未含有敏感性資料。  3.行動應用程式宜完整定義特殊符號篩選機制。  (二)無法取得行動應用程式原始碼時，應要求行動應用程式提供者符合前項安全事項。 | 配合臺灣期貨交易所股份有限公司修正「建立期貨商資通安全檢查機制」及「期貨商內部控制制度標準規範」，將原「三、行動應用程式之發佈及安全事項」調整為「三、行動應用程式安全事項」，並調整相關規範事項。 |