# 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」

中華民國 105 年 12 月 16 日中華民國期貨業商業同業公會
第 5 屆理監事第 3 次聯席會決議通過
中華民國 105 年 12 月 29 日金融監督管理委員會
金管證資字第 1050053221 號函同意備查
中華民國 107 年 8 月 24 日中華民國期貨業商業同業公會
第 5 屆理監事第 13 次聯席會決議通過
中華民國 107 年 9 月 17 日金融監督管理委員會證券期貨局
證期（期）字第 1070333577 號函同意備查
中華民國 107 年 12 月 21 日中華民國期貨業商業同業公會
第 5 屆理監事第 15 次聯席會決議通過
中華民國 108 年 1 月 18 日金融監督管理委員會
金管證期字第 1070348280 號函同意備查
中華民國 109 年 4 月 17 日中華民國期貨業商業同業公會
第 6 屆理監事第 5 次聯席會決議通過
中華民國 109 年 11 月 25 日金融監督管理委員會
金管證期字第 1090136261 號函同意備查
中華民國 111 年 8 月 19 日中華民國期貨業商業同業公會
第 7 屆理監事第 1 次聯席會決議通過
中華民國 111 年 9 月 28 日金融監督管理委員會
金管證期字第 1110355610 號函同意備查

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。

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。

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、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。

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。

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。

# 附錄：檢測實驗室 APP 檢測報告自我檢核表參考範例

依據：依行動應用資安聯盟 111 年 1 月行動應用 App 基本資安檢測基準 V3.2

L1 檢測項：23 項，L2 檢測項：29 項，L3 檢測項：35 項，F 檢測項：6 項。

F 類檢測為加測項目，視送檢單位之需求自行選擇是否加測。

| 檢測項目 | 編號 | 資訊安全技術要求事項 | 技術要求 | 各類型行動應用程式必要符合檢測項目 | | | |
|---|---|---|---|---|---|---|---|
| | | | | L1 | L2 | L3 | F |
| 4.1.1 行動應用程式發布安全 | 1 | 4.1.1.1.行動應用程式發布 | 4.1.1.1.2.行動應用程式應於發布時說明欲存取之安全敏感性資料、行動裝置資源及宣告之權限用途。 | ★ | ★ | ★ | — |
| 4.1.1 行動應用程式發布安全 | 2 | 4.1.1.1.行動應用程式發布 | 4.1.1.1.3 行動應用程式應於顯著位置(如官網、應用程式下載頁面等)提示使用者於行動應用裝置上安裝防護軟體。 | — | — | — | ★ |
| 4.1.1 行動應用程式發布安全 | 3 | 4.1.1.3.行動應用程式安全性問題回報 | 4.1.1.3.1.行動應用程式開發者應提供回報安全性問題之管道。 | — | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 4 | 4.1.2.1.敏感性資料蒐集 | 4.1.2.1.1.行動應用程式應於蒐集敏感性資料前，取得使用者同意。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 5 | 4.1.2.1.敏感性資料蒐集 | 4.1.2.1.2.行動應用程式應提供使用者拒絕蒐集敏感性資料之權利。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 6 | 4.1.2.2 敏感性資料利用 | 4.1.2.2.3.行動應用程式如採用通行碼認證，應主動提醒使用者設定較複雜之通行碼。 | — | — | — | ★ |
| 4.1.2. 敏感性資料保護 | 7 | 4.1.2.2 敏感性資料利用 | 4.1.2.2.4.行動應用程式應提醒使用者定期變更通行碼。 | — | — | — | ★ |

| 檢測項目 | 編號 | 資訊安全技術要求事項 | 技術要求 | 各類型行動應用程式必要符合檢測項目 | | | |
|---|---|---|---|---|---|---|---|
| | | | | L1 | L2 | L3 | F |
| 4.1.2. 敏感性資料保護 | 8 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.1.行動應用程式應於儲存敏感性資料前，取得使用者同意。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 9 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.2.行動應用程式應提供使用者拒絕儲存敏感性資料之權利。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 10 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.4.行動應用程式應避免在關閉及登出後將敏感性資料儲存於冗餘檔案或日誌檔案中。 | ★ | ★ | — | — |
| 4.1.2. 敏感性資料保護 | 11 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.5.行動應用程式應避免將敏感性資料儲存於冗餘檔案或日誌檔案中。 | — | — | ★ | — |
| 4.1.2. 敏感性資料保護 | 12 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.6.敏感性資料應採用適當且有效之金鑰長度與加密演算法，進行加密處理再儲存。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 13 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.7.敏感性資料應儲存於受作業系統保護之區域，以防止其他應用程式未經授權之存取。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 14 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.8.敏感性資料應避免出現於行動應用程式之程式碼。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 15 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.9.行動應用程式於非使用者主動進行的畫面擷取時應主動警示使用者。 | — | — | ★ | — |
| 4.1.2. 敏感性資 | 16 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.10.行動應用程式應將個人可識別資 | ★ | ★ | ★ | — |

| 檢測項目 | 編號 | 資訊安全技術要求事項 | 技術要求 | 各類型行動應用程式必要符合檢測項目 | | | |
|---|---|---|---|---|---|---|---|
| | | | | L1 | L2 | L3 | F |
| 料保護 | | | 訊、使用者憑證及加密金鑰等敏感性資料儲存於系統憑證儲存設施。 | | | | |
| 4.1.2. 敏感性資料保護 | 17 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.11.行動應用程式應於使用者輸入敏感性資料時將鍵盤的快取機制關閉。 | — | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 18 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.12.行動應用程式應避免在 IPC 機制中洩漏敏感性資料。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 19 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.13.行動應用程式中的使用者介面應避免洩漏敏感性資料。 | — | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 20 | 4.1.2.3.敏感性資料儲存 | 4.1.2.3.14.行動作業系統的備份資料中不應存有行動應用程式的敏感性資料。 | — | — | ★ | — |
| 4.1.2. 敏感性資料保護 | 21 | 4.1.2.4.敏感性資料傳輸 | 4.1.2.4.1.行動應用程式透過網路傳輸敏感性資料，應使用適當且有效之金鑰長度與加密演算法進行安全加密。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 22 | 4.1.2.5.敏感性資料分享 | 4.1.2.5.1.行動裝置內之不同行動應用程式間，應於分享敏感性資料前，取得使用者同意。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 23 | 4.1.2.5.敏感性資料分享 | 4.1.2.5.2.行動應用程式應提供使用者拒絕分享敏感性資料之權利。 | ★ | ★ | ★ | — |
| 4.1.2. 敏感性資料保護 | 24 | 4.1.2.5.敏感性資料分享 | 4.1.2.5.3. 行動應用程式分享敏感性資料時，應避免未授權之行動應用程式存取。 | ★ | ★ | ★ | — |

| 檢測項目 | 編號 | 資訊安全技術要求事項 | 技術要求 | 各類型行動應用程式必要符合檢測項目 | | | |
|---|---|---|---|---|---|---|---|
| | | | | L1 | L2 | L3 | F |
| 4.1.3.交易資源控管安全 | 25 | 4.1.3.1.交易資源使用 | 4.1.3.1.1.行動應用程式應於使用交易資源時主動通知使用者。 | — | — | ★ | — |
| 4.1.3.交易資源控管安全 | 26 | 4.1.3.1.交易資源使用 | 4.1.3.1.2.行動應用程式應提供使用者拒絕使用交易資源之權利。 | — | — | ★ | — |
| 4.1.3.交易資源控管安全 | 27 | 4.1.3.2.交易資源控管 | 4.1.3.2.1.行動應用程式應於使用交易資源時進行使用者身分鑑別。 | — | — | ★ | — |
| 4.1.3.交易資源控管安全 | 28 | 4.1.3.2.交易資源控管 | 4.1.3.2.2.行動應用程式應記錄使用之交易資源與時間。 | — | — | ★ | — |
| 4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全 | 29 | 4.1.4.1.使用者身分鑑別與授權 | 4.1.4.1.1.行動應用程式應有適當之身分鑑別機制，確認使用者身分。 | — | ★ | ★ | — |
| 4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全 | 30 | 4.1.4.1.使用者身分鑑別與授權 | 4.1.4.1.2.行動應用程式應依使用者身分授權。 | — | ★ | ★ | — |
| 4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全 | 31 | 4.1.4.2.連線管理機制 | 4.1.4.2.1.行動應用程式應避免使用具有規則性之交談識別碼。 | — | ★ | ★ | — |

| 檢測項目 | 編號 | 資訊安全技術要求事項 | 技術要求 | 各類型行動應用程式必要符合檢測項目 | | | |
|---|---|---|---|---|---|---|---|
| | | | | L1 | L2 | L3 | F |
| 4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全 | 32 | 4.1.4.2.連線管理機制 | 4.1.4.2.2.行動應用程式應確認伺服器憑證之有效性。 | ★ | ★ | ★ | – |
| 4.1.4.行動應用程式使用者身分鑑別、授權與連線管理安全 | 33 | 4.1.4.2.連線管理機制 | 4.1.4.2.3.行動應用程式應確認伺服器憑證為可信任之憑證機構所簽發。 | ★ | ★ | ★ | – |
| 4.1.5.行動應用程式碼安全 | 34 | 4.1.5.1.防範惡意程式碼與避免資訊安全漏洞 | 4.1.5.1.1.行動應用程式應避免含有惡意程式碼。 | ★ | ★ | ★ | – |
| 4.1.5.行動應用程式碼安全 | 35 | 4.1.5.1.防範惡意程式碼與避免資訊安全漏洞 | 4.1.5.1.2.行動應用程式應避免資訊安全漏洞。 | ★ | ★ | ★ | – |
| 4.1.5.行動應用程式碼安全 | 36 | 4.1.5.3.函式庫引用安全 | 4.1.5.3.1.行動應用程式於引用之函式庫有更新時，應備妥對應之更版本，更新方式請參酌 4.1.1.行動應用程式發布安全。 | ★ | ★ | ★ | – |
| 4.1.5.行動應用程式碼安全 | 37 | 4.1.5.4.使用者輸入驗證 | 4.1.5.4.1.行動應用程式應針對使用者於輸入階段之字串，進行安全檢查。 | ★ | ★ | ★ | – |
| 4.1.5.行動應用程式碼安全 | 38 | 4.1.5.4.使用者輸入驗證 | 4.1.5.4.2.行動應用程式應提供相關注入攻擊防護機制。 | ★ | ★ | ★ | – |
| 4.1.5.行動應用程式碼安全 | 39 | 4.1.5.5.防止動態分析及竄改 | 4.1.5.5.1.行動應用程式須偵測行動作業系統保護層是否有被破解(如：Root、Jailbreak)或 | – | – | – | ★ |

| 檢測項目 | 編號 | 資訊安全技術要求事項 | 技術要求 | 各類型行動應用程式必要符合檢測項目 | | | |
|---|---|---|---|---|---|---|---|
| | | | | L1 | L2 | L3 | F |
| | | | 保護不當之情形，如有，應主動通知使用者或關閉應用程式。 | | | | |
| 4.1.5.行動應用程式碼安全 | 40 | 4.1.5.5.防止動態分析及竄改 | 4.1.5.5.5.屬於該行動應用程式的可執行檔案以及函式庫都應在檔案層級中加密或者在可執行檔案中重要的程式碼區段以及資料區段都應加密或加殼，使得一般的靜態分析不易取出重要的程式碼或資料。 | ー | ー | ー | ★ |
| 4.1.5.行動應用程式碼安全 | 41 | 4.1.5.5.防止動態分析及竄改 | 4.1.5.5.6.行動應用程式應有程式碼混淆機制。 | ー | ー | ー | ★ |
| 4.2.2 伺服器端安全檢測 | 42 | 4.2.2.1.Webview 安全檢測 | 4.2.2.1.2.行動應用程式於 Webview 呈現功能時，所連線之網域應為安全網域。 | ★ | ★ | ★ | ー |

填寫人：_____ 單位主管：_____