中華民國證券商業同業公會 新興科技資訊安全自律規範

（雲端運算、社群媒體、行動裝置資訊安全自律規範）

金融監督管理委員會 105 年 12 月 9 日金管證資字第 1050049273 號函准予備查

中華民國證券商業同業公會 105 年 12 月 13 日中證商電字第 1050007641 號函公告實施

金融監督管理委員會 107 年 8 月 8 日金管證券字第 1070324830 號函准予備查

中華民國證券商業同業公會 107 年 8 月 13 日中證商電字第 1070004336 號函公告實施

（新興科技資訊安全自律規範）

金融監督管理委員會 108 年 1 月 4 日金管證資字第 1070348059 號函准予備查

中華民國證券商業同業公會 108 年 1 月 11 日中證商電字第 1080000124 號函公告實施

金融監督管理委員會 109 年 6 月 10 日金管證券字第 1090335756 號函准予備查

中華民國證券商業同業公會 109 年 6 月 16 日中證商業一字第 1090002617 號函公告實施

金融監督管理委員會 108 年 1 月 4 日金管證資字第 1070348059 號函准予備查

中華民國證券商業同業公會 108 年 1 月 11 日中證商電字第 1080000124 號函公告實施

金融監督管理委員會 109 年 6 月 10 日金管證券字第 1090335756 號函准予備查

中華民國證券商業同業公會 109 年 6 月 16 日中證商業一字第 1090002617 號函公告實施

金融監督管理委員會 110 年 4 月 27 日金管證券字第 1100336750 號函准予備查

中華民國證券商業同業公會 110 年 5 月 3 日中證商業一字第 1100002080 號函公告實施

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。

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。

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)。

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。

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。

第五條 （社群媒體安全控管）

證券商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、訂定證券商運用社群媒體管理辦法，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（例如資料外洩、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辦法：

(一)檢視所經營之社群媒體隱私政策及標明其風險。

(二)標示證券商名稱、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繫方式及處理窗口。

第六條 （行動裝置安全控管）

證券商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、公務用行動裝置設備管理辦法。

二、員工自攜行動裝置管理辦法。

三、行動應用程式安全管理：

(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、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 TOP 10 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）

證券商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。

證券商採購物聯網設備時，宜優先採購取得資安標章之物聯網設備。

證券商應定期辦理物聯網設備使用及管理人員資安教育訓練。

第八條 （網路釣魚之防範）

證券商應偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。

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。

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。

中華民國證券商業同業公會

新興科技資訊安全自律規範修正條文對照表

修正後條文	原條文	說 明
第七條(物聯網設備安全控管) 證券商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。 證券商採購物聯網設備時，宜優先採購取得資安標章之物聯網設備。 證券商應定期辦理物聯網設備使用及管理人員資安教育訓練。	第七條(物聯網設備安全控管) 證券商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。	・本條文新增第3、4項規定文字係參考金管會證期局109年7月17日證期(券)字第1090345141號函、證交所109年12月7日臺證輔字第1090023040號修正「建立證券商資通安全檢查機制」有關「新興科技應用(CC-21100)(4)物聯網 e.公司採購物聯網設備時，宜優先採購取得資安標章之物聯網設備。f.公司應定期辦理物聯網設備使用及管理人員資安教育訓練」。
第八條 (網路釣魚之防範) 證券商應偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。	第八條 (網路釣魚之防範) 證券商應偵測釣魚網站，提醒客戶防範網路釣魚。	・本條文修正文字係參考證交所109年12月7日臺證輔字第1090023040號修正「建立證券商資通安全檢查機制」有關「通訊與作業管理(CC-17000)(1)網路

修正後條文	原條文	說 明
		安全管理 e.電腦病毒及惡意軟體之防範(g)公司應偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚」。