中華民國證券投資信託暨顧問商業同業公會
雲端運算、社群媒體、行動裝置資訊安全自律規範

107年8月31日金管證投字第1070326433號函准予備案

第一條（規範目的）

為強化投信投顧事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。

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。

第三條（資訊安全法令遵循）

公司運用雲端運算服務、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」、本公會「投信投顧事業資訊安全內部控制制度範本」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）

公司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、公司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、公司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）

公司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、訂定公司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)標示公司名稱、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）

公司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。

第七條（違規處理程序）

公司違反本自律規範，依本公會會員自律公約及其他有關之規定辦理。

第八條（本法施行程序）

本自律規範經本公會法遵稽核及基金事務委員會會議通過，並報奉主管機關核備後實施，修正時亦同。