**證券期貨市場相關公會**

**雲端運算、社群媒體、行動裝置資訊安全管控指引**

1. **總則**

# （目的）

## 為強化證券期貨市場資訊安全，依據金管會有關強化金融市場資訊安全議題之討論決議，針對雲端運算服務運作安全、行動裝置及社群媒體之風險議題，擬定資訊安全控管指引。

1. **雲端運算服務運作安全**

# （雲端運算服務定義）

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。

# （雲端運算服務指引適用範圍）

### 為確保組織使用雲端運算服務之安全，組織應事先評估使用雲端服務之風險，若雲端服務涉及關鍵性系統、資料或服務者，應符合本指引控管建議。

### 本指引定義之雲端服務，不包含建置組織內部且僅對內提供服務之私有雲。

# （雲端服務提供者選擇）

### 雲端服務使用者應事先評估雲端服務提供者之服務水準(含資訊安全防護)等，若有不符合需求之處，應考量其他補償性措施。

### 雲端服務使用者應評估雲端服務提供者是否已建立雲端服務備援機制，並建議於合約中明文規定雲端服務復原時間之相關要求。

### 雲端服務使用者就雲端服務委外作業，應落實定期對雲端服務提供者之查核。如雲端服務提供者已取得雲端安全國際認證(CSA-Star)銅牌以上者，則可視實際情況要求提供驗證報告或進行實地查核。

# （雲端互通性和可移植性）

### 雲端服務提供者應滿足雲端使用者對於應用程式及資訊處理之互通性與可移植性需求，並提出相關說明文件供使用者參考。

### 雲端服務提供者宜使用業界常見之虛擬化平台、虛擬機檔案格式、資料檔案格式，以確保互通性。

### 雲端服務提供者應依雲端服務使用者需求，使用標準化的網路協定。如涉及敏感性資料之傳遞，宜使用超文字傳輸安全協定(HTTPS)、安全檔案傳輸協定(SFTP)等加密之網路協定。

### 雲端服務提供者提供之雲端服務若涉及應用程式介面存取服務，宜使用開放或已公開之應用程式介面(API)，以確保應用程式元件可以較容易地轉移。

# （雲端供應鏈管理）

### 雲端服務提供者應根據與雲端服務使用者之服務水準協議，維持其服務水準，且應定期提供協議中各項服務水準指標之報告。

### 雲端服務提供者應負責檢視雲端服務供應鏈中其他合作夥伴可能影響服務品質的風險與錯誤。

### 雲端服務提供者應於雲端服務運作發生資訊安全事件時，及時通知受影響的客戶與供應鏈中的合作夥伴，並定期更新事件處理的相關訊息。

# （雲端基礎設施與虛擬化安全）

### 雲端服務提供者應確保虛擬機映像檔之完整性，有關映像檔的重要異動，如：調整虛擬機記憶體大小、調整虛擬機硬碟容量等，都應該被記錄，並提供客戶檢視相關變更紀錄之機制。

### 雲端服務提供者應依據雲端服務使用者需求，提供虛擬機隔離性(isolation)說明，隔離性失效時應立即通知雲端服務使用者。

### 雲端服務提供者應就雲端作業系統，包含虛擬層 (hypervisor)與虛擬機的作業系統(guest operating systems)，輔以適當的安全控管措施，如：僅開放必要連接埠(Port)、通訊協定(Protocols)與服務(Service)、病毒防護、安全漏洞評估機制、檔案完整性監控等。

### 雲端服務運作人員權限管理應採權限最小化原則，輔以適當安全控管措施，如：透過雙因子認證、稽核軌跡、IP地址過濾、防火牆，以及傳輸層安全性(TLS)封裝的通訊管理。

### 雲端服務提供者提供IaaS服務(基礎設施即服務)時，應依雲端服務使用者需求將含敏感資料之虛擬硬碟進行加密，限制快照或未授權存取。

### 雲端服務提供者提供IaaS服務(基礎設施即服務)終止後，應刪除虛擬機映像檔及相關備份檔，並出具資料完全刪除之證明。

1. **社群媒體安全控管**

# （社群媒體定義）

# 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。

# （社群媒體指引適用範圍）

# 本指引定義之社群媒體，不包含組織內部溝通使用之社群媒體或平台。

# （社群媒體使用政策）

### 組織應擬定社群媒體使用政策，以規範員工使用社群媒體行為，包含：

### 界定可於社群媒體上分享之業務相關資料。

### 界定私人與公務用社群媒體之區別與應注意事項。

### 組織應針對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，並採行適當的安全控管措施，如：教育訓練或宣導、內容過濾及監控、防範惡意程式等防護機制。

# （組織經營官方社群媒體）

### 組織應事先了解所經營之社群媒體隱私政策，並定期檢視其隱私政策之異動及評估其風險。

### 組織於官方網站提供連結供使用者連至組織外之社群媒體時，應出現提示視窗告知使用者該連結非組織本身之網站。

### 組織所經營之社群媒體應標示組織名稱及聯絡方式，以區別為官方經營之社群媒體。

### 組織經營社群媒體時，應建立帳號權限管理機制，並對發布內容進行控管。

1. **行動裝置安全控管**

# （行動裝置定義）

### 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。

### 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，並具備資料運算處理、儲存與網路連線功能之可攜式設備。

# （行動裝置指引適用範圍）

# 本指引定義之行動裝置，僅限於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。

# （公務用之行動裝置設備控管）

### 組織對於行動裝置的申請、使用、更新與繳回應訂有相關規範。

### 組織人員異動時，應進行重新配置或清除配置程序，以確保行動裝置環境安全性。

### 組織對行動裝置與行動裝置可存取的資源應進行風險評估作業，並依據風險評估結果採行適當的安全控管措施，如：螢幕鎖定、限制存取敏感資料、安裝防毒軟體、安裝行動裝置管理軟體等。

### 組織針對存有敏感性資料之行動裝置宜採行以下安全控管措施：

### 行動裝置宜建立身分識別機制。

### 行動裝置之作業系統環境設定宜由被授權者進行變更。

### 行動裝置之作業系統與防毒軟體宜定期檢查，避免持有者私自異動設定，如：越獄(Jailbreaking)或提權(Rooting)。

### 行動裝置宜考量遺失時資料清除方式，如：以遠端方式刪除資料或透過身分認證錯誤超過規定次數後自動刪除機制。

### 行動裝置宜限制或關閉不需要之無線連線功能，如：NFC、紅外線、Wifi或藍芽等。

### 行動裝置傳輸敏感性資料時，宜採加密或資料遮蔽方式進行保護。

### 行動裝置宜限制敏感性資料儲存於行動裝置上或將敏感性資料進行加密保護。

### 組織公務用之行動裝置應避免安裝非官方發佈之行動應用程式，或僅安裝由組織列出通過檢測可安裝之行動應用程式。

# （員工自攜行動裝置管理）（BYOD）

### 組織應定期審核並限制員工自攜行動裝置使用用途、使用期間及資料種類。

### 組織應與持有人簽署員工自攜行動裝置使用協議，含：使用限制及雙方責任等。

### 組織宜限制內部資訊設備透過員工自攜行動裝置私接存取網際網路(Internet)之行為。

# （行動應用程式安全控管）（Mobile App）

### 組織應針對交易或帳務等敏感性資料設計行動應用程式存取驗證機制，並僅供經授權之行動應用程式使用該敏感性資料。

### 組織透過行動應用程式發送簡訊或其他訊息通知方式告知使用者敏感性資料時，應進行適當去識別化。

### 組織透過行動應用程式傳送帳號、密碼及其他敏感性資料時，應以憑證驗證或加密機制確保傳送安全。

### 組織透過行動應用程式儲存密碼、憑證、交易或帳務等敏感性資料時，宜對儲存之資料進行雜湊(Hash)或加密控管保護。

### 組織透過行動應用程式處理交易或金流作業時，應留存存取日誌，且存取日誌應予以保護以防止未經授權存取。

# （行動應用程式發佈控管）

### 組織發佈行動應用程式前，應確認程式碼或程序庫符合安全要求：

### 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。

### 程式碼未含有敏感性資料。

### 行動應用程式宜完整定義特殊符號篩選機制。

### 組織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提出符合前項安全要求之佐證。