新興科技應用

|  |  |
| --- | --- |
| 文件編號： | SC-01-012 |
| 文件版次： | V1.1 |
| 發行日期： | 2024/08/28 |

|  |
| --- |
| © 版　權　說　明 ©  本文件為公司所專有之財產，  未經許可，不得以任何形式使用、引用、複製或公開等。 |

文件修訂履歷

| 修訂版次 | 修訂日期 | 發行與變更說明 | 修訂人員 | 核准人員 | 備註 |
| --- | --- | --- | --- | --- | --- |
| V1.0 | 2023/11/01 | 新版發行。 | 丘建華副總經理 | 李文柱總經理 | 因應2022轉版，重新發行。 |
| V1.1 | 2024/08/08 | 因應內控調整「第一章目的」。 | 吳允文副總經理 | 李文柱總經理 |  |

目 錄

[第一章 目的 4](#_Toc147137032)

[第一節 證券商資通安全檢查機制 4](#_Toc147137033)

[第二章 範圍 6](#_Toc147137034)

[第一節 雲端運算服務範圍 6](#_Toc147137035)

[第二節 社群媒體範圍 6](#_Toc147137036)

[第三節 行動裝置範圍 6](#_Toc147137037)

[第四節 電子式交易範圍 6](#_Toc147137038)

[第三章 名詞定義 6](#_Toc147137039)

[第一節 雲端服務 6](#_Toc147137040)

[第二節 社群媒體 6](#_Toc147137041)

[第三節 行動裝置 7](#_Toc147137042)

[第四節 物聯網 7](#_Toc147137043)

[第五節 遠距辦公 8](#_Toc147137044)

[第六節 電子式交易 8](#_Toc147137045)

[第七節 深度偽造 8](#_Toc147137046)

[第四章 相關文件 8](#_Toc147137047)

[第五章 權責 8](#_Toc147137048)

[第一節 權責單位 8](#_Toc147137049)

[第二節 權責單位主管 8](#_Toc147137050)

[第三節 資安人員 8](#_Toc147137051)

[第六章 作業內容 8](#_Toc147137052)

[第一節 雲端服務 8](#_Toc147137053)

[第二節 社群媒體 10](#_Toc147137054)

[第三節 行動裝置 12](#_Toc147137055)

[第四節 物聯網 14](#_Toc147137056)

[第五節 遠距辦公 15](#_Toc147137057)

[第六節 電子式交易控管 16](#_Toc147137058)

[第七節 深度偽造 16](#_Toc147137059)

[第七章 輸出文件記錄 16](#_Toc147137060)

# 目的

為強化群益金鼎證券（以下簡稱本公司）管理及應用雲端服務、社群媒體、行動裝置、物聯網、遠距辦公，以及臺灣證券交易所發布「建立證券商資通安全檢查機制」、「中華民國證券商業同業公會雲端運算、社群媒體、行動裝置資通安全自律規範」及「證券期貨市場相關公會新興科技資通安全管控指引」相關規定有所遵循，特訂定本要點以維護公司之內容管理以達成以下目標：

## 證券商資通安全檢查機制

### 雲端服務：

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。

#### 本公司為雲端服務使用者時，已訂定雲端服務提供者之遴選機制、查核措施、備援機制、服務水準（含資訊安全防護）與復原時間及服務終止措施要求等，如有不符需求之處，需有其它補償性措施。使用具有合法版權之軟體。

#### 本公司為雲端服務提供者時，已訂定雲端運算服務安全控管措施，應包含法律遵循、權限控管、權責歸屬及資訊安全防護等項目。如涉及敏感性資料之傳遞，應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。

### 社群媒體：

#### 公司訂定社群媒體相關資訊安全規範與運用社群媒體管理辦法，應包含以下內容：

##### 界定可於公務用社群媒體上分享之業務相關資料。

##### 私人與公務用社群媒體之區別與應注意事項。

#### 針對開放員工使用社群媒體評估其風險程度，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。

#### 已訂定經營官方社群媒體資訊安全規範與管理辦法，並包含以下內容：

##### 事先了解所經營之社群媒體隱私政策，並定期（每年一次）檢視其隱私政策之異動及評估其風險。

##### 於官方網站提供連結供使用者連至公司外之社群媒體時，出現提示視窗告知使用者該連結非公司本身之網站。

##### 對經營之社群媒體應標示證券商名稱、聯絡方式、許可證字號、客戶申訴聯繫方式及處理窗口，以區別為官方經營之社群媒體。

##### 建立帳號權限管理機制，對發布內容進行控管與監視，並針對不適當言論及異常事件，進行通報或處置。

### 行動裝置：

#### 已訂定公務用行動裝置之資訊安全規範與管理辦法，包含以下項目：

##### 行動裝置設備管理辦法對於申請、使用、更新、繳回與審核訂有相關規範。

##### 人員異動時，行動裝置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。

##### 行動裝置避免安裝非官方發佈之行動應用程式，或僅安裝由公司列出通過檢測可安裝之行動應用程式。

##### 公務用行動裝置管理辦法內容應包含行動裝置儲存機密資料之限制與管理方式。

#### 已訂定員工自攜行動裝置之資訊安全規範與管理辦法，包含以下項目：

##### 本公司要求員工自攜行動裝置使用用途。

##### 本公司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。

##### 本公司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。各項文件與手冊建立適當維護與控制之機制。

##### 員工自攜行動裝置管理辦法內容應包含行動裝置儲存機密資料之限制與管理方式。

### 物聯網：

#### 應訂定物聯網相關資訊安全規範與管理辦法，須包含下列項目:

##### 建立物聯網設備管理清冊並至少每年更新一次，且變更前開設備之初始密碼。

##### 物聯網設備具備安全性更新機制且定期（每年一次）更新，如存在已知弱點無法更新時，需建立補償性管控機制。

##### 關閉物聯網設備不必要之網路連線及服務，避免使用對外公開的網際網路位置。

##### 如與物聯網設備供應商簽定採購合約時，其內容包含資訊安全相關協議，明確約定相關責任（如：服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案），確保設備不存在已知安全性漏洞。

##### 本公司採購物聯網設備時，優先採購取得資安標章之物聯網設備。

##### 本公司定期辦理物聯網設備使用及管理人員資安教育訓練。程式經修改其相關文件及時更新。

##### 應建立物聯網設備存取權限控管措施。

### 遠距辦公：

#### 本公司對使用遠距辦公之設備安裝資訊安全相關軟體，控管應用程式存取權限，以降低資訊外流風險。

#### 本公司依業務範圍及控管權限設定居家辦公員工之系統功能權限。

#### 本公司依員工執行業務內容訂定連線時段限制及相關規範。

#### 本公司留存遠距辦公員工使用者登入系統、電腦設備操作及交易紀錄軌跡。

#### 本公司採多因子驗證機制（員工帳號密碼、動態密碼、一次性帳密）及建立安全的遠距網路通道，降低相關帳號密碼遭假冒或竊用之風險。

#### 本公司阻擋惡意或未經授權之連線，並採用最小權限原則設定遠距帳號存取規則。

#### 本公司定時更新VPN連線和其他遠端連結系統之安控措施。

#### 本公司對客戶隱私、資料及紀錄之安全性建立保護措施。

#### 本公司加強宣導資訊安全，教育遠距辦公員工應對網路風險保持警覺等資訊安全機制。

### 深度偽造(Deepfake)

1. 使用影像視訊方式進行身分驗證時應強化驗證並搭配其他驗證因子（如上傳身分證件、手機簡訊OTP）。
2. 應定期辦理涵蓋深度偽造認知及防範議題之資訊安全教育訓練。

# 範圍

## 雲端運算服務範圍

### 本要點定義之雲端服務，但不包含建置本公司內部且僅對內部提供服務之私有雲。

## 社群媒體範圍

### 要點定義之社群媒體，但不包含組織內部溝通使用之社群媒體或平台。

## 行動裝置範圍

### 要點定義之行動裝置，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。

## 電子式交易範圍

### 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（DirectMarket Access，簡稱DMA）、主機共置（Co–Location）等服務型態。

# 名詞定義

## 雲端服務

### 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))。

#### 雲端服務提供者

### 透過網路提供雲端運算服務之外部業者。

#### 雲端服務使用者

### 權責單位因業務需求與發展之目的，得選擇使用雲端服務者。

## 社群媒體

### 社群媒體平台(Social Media Platform)

### 可於網際網路上供使用者即時發佈訊息或活動，利用推播至所有社群或預設社群可得接收的位置，以達到用戶參與、公眾互動及共用之社交功能，如：LINE、Facebook、Youtube。

### 社群媒體平台用戶

### 社群媒體平台用戶是指任何可於社群媒體平台評論、張貼發文及視頻等活動，非由公司內部人員擔任。

### 服務準則

### 於社群媒體平台上所制定之服務準則，以利於社群媒體平台用戶了解如何以適當方式使用此服務。

### 官方社群

### 於社群媒體平台上，以本公司官方名義所成立與經營之社群。

### 官方帳號

### 於社群媒體平台上，以本公司官方名義所設立之帳號，供社群媒體平台內容管理維護人員以官方名義公告資訊、回覆留言等使用。

### 社群媒體異常事件

### 因社群媒體之異常危害公司信譽、社群經營或用戶權益的事件，包含：

#### 官方社群於單日內連續出現不利於公司商譽之惡意留言時。

#### 官方社群資料遭竊取，冒用本公司名義設立偽冒社群進行詐騙，可能致公眾無法辨識官方社群時。

#### 其他資通訊安全或個資外洩事件，例如：

##### 官方帳號遭冒用

##### 用戶資料外洩

##### 駭客攻擊

### 上述類型為協助本公司權責單位據以判斷異常事件之類型參考。惟權責單位仍須自行研擬判斷異常事件之具體標準，以作為判定是否須向上通報之異常事件依據。

## 行動裝置

### 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。

### 員工自攜行動裝置(BYOD)

### 指非屬公司資訊資產用於處理公司事務、直接連接公司內部網路設備或服務，並具備資料運算處理、儲存與網路連線功能之電子設備或裝置。

### 行動應用程式(App)

### 設計在行動裝置上所運行的應用程式。

## 物聯網

本要點所稱物聯網設備係指具網路連線功能並連線於Internet或Intranet之崁入式系統（具有小型作業系統）設備（以下簡稱設備），包含自動化辦公設備（如數位錄影機、電話交換機、傳真機、錄音設備、影印機等）及不具備遠端操控介面功能之感測器。

## 遠距辦公

因特殊情況(如：COVID-19)，而透過遠端技術的模式在辦公室以外的場合辦公。

## 電子式交易

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。惟本要點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(DirectMarket Access，簡稱DMA)、主機共置(Co–Location)等服務型態。

## 深度偽造

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。

# 相關文件

### 無

# 權責

## 權責單位

### 本公司各單位因業務需求需使用雲端運算、社群媒體、行動裝置、物聯網設備，則皆屬於權責單位。

### 物聯網設備權責單位定期接受資安教育訓練。

## 權責單位主管

### 各部處主管為權責單位主管，應瞭解並遵循此份資訊安全控管作業要點，並監督所屬人員遵循作業要點內之規範。如需以官方名義成立或移除官方社群時，需經過總經理核可後辦理。

### 應每季協助權責單位檢視社群媒體平台內容監控檢查之正確性。

## 資安人員

#### 應定期辦理物聯網設備權責單位人員教育訓練。

# 作業內容

## 雲端服務

### 為確保本公司使用雲端運算服務之安全與關鍵業務之機密性與可用性，本公司權責單位應事先評估使用雲端服務之風險，及檢視是否存在潛在遵法性議題，如：隱私保護、國際傳輸議題，以符合相關法令法規之規定。

### 權責單位應確認雲端服務提供者是否能滿足本資訊安全控管作業要點之規範。若雲端服務涉及關鍵性系統、資料或服務者，應避免採用雲端運算服務或需符合本要點建議。

### 雲端服務提供者之選擇應符合下列要求：

#### 應事先評估雲端服務提供者之服務水準(含資訊安全防護控制措施)、供應鏈關係、合約內容項目權責歸屬等，若有不符合需求之處，應考量其他補償性措施。

#### 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。

#### 應確認雲端服務提供者所提供之服務可用性等級與資訊安全等級服務和本公司規範之要求。

#### 應落實定期對雲端服務提供者之雲端服務委外作業查核。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。

### 雲端服務提供者之互通性和可移植性應符合下列要求：

#### 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。

#### 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。

#### 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。

#### 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。

### 雲端服務提供者之雲端供應鏈管理應符合下列要求：

#### 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。

#### 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。

#### 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。

### 雲端服務提供者之雲端基礎設施與虛擬化安全應符合下列要求：

#### 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。

#### 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。

#### 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。

#### 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。

#### 終止提供IaaS服務(基礎設施即服務)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。

## 社群媒體

### 社群媒體管理者應了解使用之社群媒體之隱私政策，確認隱私資料的取得與保護機制。管理者應定期檢視其隱私政策是否有異動，並針對相關維護人員進行教育訓練，並填寫《SC-01-012-F03\_社群媒體使用條款閱讀確認單》留存紀錄。

### 社群媒體維護人員由權責單位主管指派社群媒體平台內容管理維護人員與代理人。其應依照本公司「廣告、業務招攬及營業促銷活動之宣傳資料製作、散發公布管理辦法」辦理，才可進行發佈。如轉載金融相關新聞等則可不需核可。

### 社群媒體平台內容由權責單位指派監控人員每月針對社群媒體平台進行內容檢查，並填寫《SC-01-012-F02\_社群媒體平台內容監控檢查表》留存相關紀錄。

### 社群媒體平台使用政策

### 本公司內部網路禁用社群網站(例如：FB、微博)、外部個人郵件(例如：GMAIL、HOTMAIL)與外部儲存空間(例如：SKYDRIVE、GDRIVE)；若有直接之業務需要，需填寫資訊需求申請單(系統類別：社群網站、外部WEB MAIL、外部儲存空間)，經總經理核准後開放。使用社群網站應遵循下列使用原則：

#### 使用社群媒體平台時，應遵循本公司規範之資訊安全政策、個人資料保護政策、隱私權聲明；並遵守智慧財產權相關法令規範。

#### 於社群媒體平台上所披露與提供的資訊，應經過授權，且遵守本公司內部相關規定(包括但不限於廣告、業務招攬及營業促銷活動之宣傳製作散發公佈管理辦法)及相關法令法規之要求，未經本公司授權與公司相關資訊禁止於社群媒體平台上公布。

#### 應依據業務推展與宣導目標，選擇合適、安全且可信賴之社群媒體平台，並於使用前應詳讀該平台之使用條款與使用風險，以採行適當之安全控管機制。

#### 使用社群媒體平台應事先評估社群媒體平台用戶的特性，確認是否為業務推展與宣導的目標客群。

#### 本公司各權責單位如需以官方名義成立官方社群時，應先確認該社群媒體平台是否已有其他權責單位已開立同質性之官方社群，且經過權責主管核可後方得成立。

#### 使用社群媒體平台應事先了解該社群媒體之隱私政策，確認社群媒體平台對於隱私資料的取得與保護機制，並應定期檢視其隱私政策是否有異動以評估使用風險。

#### 授權擔任社群媒體平台內容管理維護人員之員工，應接受相關教育訓練，充分瞭解本公司社群媒體平台使用政策，以及該社群媒體之隱私政策、平台使用風險與資料保護控管機制。

#### 使用之社群媒體平台若涉及個人資料蒐集時，應符合個資蒐集之最小化原則，並應針對該社群媒體平台對於個人資料保護的安全性進行評估。

#### 若透過官方網站連結至社群媒體平台網站時，應出現提示視窗告知使用者該連結非本公司之網站。

#### 以官方名義經營之社群媒體，應於所使用之社群媒體平台網站標註本公司正式名稱、許可證字號、地址、電話、企業識別標誌(logo)、申訴聯絡方式及處理窗口，以區別此為官方名義使用之社群媒體。

#### 如遇有社群媒體異常事件，應遵循本公司相關程序辦理。

### 社群媒體平台管理

#### 官方社群維護

##### 社群媒體平台之管理、更新與維護，應由權責單位負責。

##### 為確保社群媒體平台的安全或可用性，對於可能會影響權責單位的業務推展或政令宣導之資訊與內容，社群媒體平台內容管理維護人員應定期維護與保留相關資訊。

##### 權責單位透過社群媒體平台進行服務或行銷活動時，應揭露公司名稱、客戶申訴聯繫方式及處理窗口，以使社群媒體平台用戶了解如何以適當方式使用社群媒體平台。

##### 權責單位透過社群媒體平台進行行銷活動時，所收集之個資，應由權責單位負管理責任，皆應遵循本公司之個人資料保護政策、個資蒐集之最小化原則等要求。

#### 官方社群移除

##### 如權責單位之官方社群無需繼續使用時，為避免突然移除而造成對公司商譽影響，應確認是否符合以下任一因素，並經權責主管核准、正式公告後方得移除：

###### 已完成既定業務推展

###### 不符合預先目標

###### 未有足夠人力維護、管理及監控

###### 社群媒體平台停止提供服務

###### 社群媒體平台隱私政策或權利義務改變，造成與本公司政策不一致時

##### 官方社群如有移除之情形，原社群平台之資料，應由權責單位依據相關資料保存期限保管及刪除。

#### 官方帳號管理

##### 社群媒體平台內容管理維護人員於官方社群上，應使用官方帳號進行內容管理與維護作業。

##### 官方帳號之申請與移除，應填寫《SC-01-012-F01\_社群媒體帳號暨官方社群申請單》，由權責單位主管核准後辦理，並交由社群媒體平台內容管理維護人員負保管責任。

##### 官方帳號之使用，應比照本公司資訊安全要求，並嚴禁將官方帳號密碼借予他人使用。

##### 官方帳號限公務用途使用，禁止挪為私用，或以官方帳號發表個人言論。

##### 官方帳號和密碼皆屬於公司財產，相關人員離調職時，須歸還相關帳號及密碼，接任者須立即進行密碼變更。

### 官方社群媒體平台內容維護

#### 社群媒體平台內容管理維護人員

##### 權責單位之社群媒體平台內容維護，應由權責單位主管指派社群媒體平台內容管理維護人員與代理人，負責該平台單位內容維護（含新增、修改、刪除及回覆）之作業，包含文章、動態訊息、照片、視頻、活動、廣告及應用程式等。

##### 相關指派人員應接受適當教育訓練，以期了解其角色及責任，以有效執行單位業務活動。

##### 非受指派社群媒體平台內容管理維護人員或其代理人，禁止以官方名義發言。

#### 權責單位張貼於社群媒體平台之內容經權責單位主管核定，檢視之原則如下：

##### 張貼內容事項核准(新增、修改、刪除)及拒絕。

##### 張貼內容資料正確性、完整性及可用性。

##### 張貼內容如涉及個人資料部分，應遵循本公司個人資料保護政策。

##### 張貼內容包含公司品牌與政策相關事項，應與相關負責單位協商。

##### 張貼內容如有社群媒體平台用戶意見，應確保回應內容適當性，並確認其意見得到解決。

##### 張貼內容如被社群媒體平台用戶回文，其內容影響企業商譽或不堪字語，有權阻止或刪除社群媒體使用者回文。

##### 張貼內容如含有轉貼文章，應確認智慧財產權相關法令。

##### 張貼內容勿談論與公務無關之議題，如：政治、宗教等議題。

### 社群媒體平台內容監控

#### 權責單位應指派社群媒體平台內容監控人員，並定期針對所負責之社群進行社群媒體平台內容檢查，將檢查結果記錄於《SC-01-012-F02\_社群媒體平台內容監控檢查表》中，監控項目應包含抽查檢視該單位負責之社群媒體平台動態內容之妥適性、正確性，如有錯誤或不恰當之內容，應立即執行更正，並留存相關紀錄。

#### 社群媒體平台內容監控人員應定期搜尋是否有偽冒之官方名義所成立之社群媒體，若有發現應立即向相關單位進行舉發，並於官方社群媒體中進行澄清與聲明。

### 內部使用社群媒體管理原則

### 本公司基於內部溝通之目的，採用社群媒體進行訊息溝通與交流時，應遵守下列原則：

#### 限公務溝通使用，相關資訊未經公告不得對外部揭露。

#### 使用時應遵守本公司資訊安全與個人資料保護之要求。

#### 不得使用社群媒體討論與傳送客戶個人資料。

#### 不得使用社群媒體傳送公司機密性資訊。

## 行動裝置

### 行動裝置使用者須遵循本資訊安全控管作業要點之本公司配發行動裝置使用原則，僅在所獲得之授權內，使用、存取、安裝此行動裝置，並妥善保護所使用的行動裝置。

### 行動裝置收回處理者由總、分公司資訊人員擔任。如有人員異動，需將收回的筆記型電腦進行重新安裝。

### 行動裝置作業內容

### 本公司同仁於使用公司配發或自行攜帶之行動裝置，並且使用本公司內部網路與存取內部資源時，應經申請許可後方可使用，並遵循下列要求。

### 本公司配發行動裝置控管原則

#### 本公司應針對員工所持有之公司配發行動裝置進行安全防護措施，如：定時鎖定螢幕、開啟密碼驗證、安裝防毒軟體並定期掃描、更新或安裝資料保護軟體及確實更新修補程式。

#### 本公司應於員工異動時，針對其配發之行動裝置由總、分公司資訊人員進行系統重新配置或清除配置程序，以確保行動裝置環境安全性。

#### 本公司應控管存有機密資料或個人資料之行動裝置，如：安裝加密軟體予以防護、增設安全傳輸機制，並確認其使用目的與保管人員。

#### 為降低存有機密與個人資料之行動裝置遺失之風險，宜考量遠端抺除方式刪除該行動裝置相關資料。

#### 公司配發行動裝置，宜管控或限制行動裝置不需要之無線連線功能(如：NFC、wifi、紅外線或藍芽功能等)。

### 本公司配發行動裝置使用原則

### 行動裝置使用人員於使用本公司配發之行動裝置時，應遵循下列原則：

#### 公司配發行動裝置，宜管控或限制行動裝置不需要之無線連線功能(如：NFC、wifi、紅外線或藍芽功能等)。

#### 行動裝置之系統環境設定宜經由驗證後才可進行變更，避免私自異動設定，包含越獄(Jailbreaking)或提權(Rooting) 。

#### 行動裝置使用人員不可自行安裝非官方發佈之行動應用程式，或未經公司授權許可之行動應用程式。

#### 行動裝置使用人員應避免存放非業務所需之公司機密資料與客戶個人資料於行動裝置中；如需使用行動裝置傳輸資料，應使用受信任的網路連線。

#### 行動裝置使用者平時應關閉行動裝置不需要之無線連線功能(如：紅外線、NFC、wifi或藍芽功能等)，避免於無須使用時保持開啟狀態。

#### 行動裝置使用人員應避免讀取不明來源之訊息或使用資訊隱藏技術(如：QR code)製作之訊息連結。

#### 重要資料應定期執行備份，但公務資料不應儲存至外部雲端備份平台上(如iCloud與Dropbox)。

#### 當行動裝置有遺失、遭竊之情況時，行動裝置使用人員應即時通報單位主管與本公司相關管理單位。

### 本公司員工自行攜帶行動裝置管理原則(BYOD)

### 非本公司配發之行動裝置原則上不開放使用公司內部網路，如需使用公司內部網路，應遵循下列要求：

#### 非本公司配發之行動裝置，如欲使用公司內部網路時，應先取得權責主管及資訊單位核可後方可使用，並應限制其用途、使用期間及資料種類。

#### 經核准使用之員工攜帶自有行動裝置，須由持有人每年簽署本公司「自攜行動裝置隱私權責同意書」。

#### 營業員如因業務需求需使用行動通訊設備時，依據本公司「營業員使用行動通訊設備管理辦法」規定，須簽署「營業員使用行動通訊設備規範聲明書」，並填寫「行動通訊設備使用登記表」。

#### 行動裝置使用人員於內部網路環境中，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。

#### 行動裝置管理人員應定期對已申請核准之行動裝置進行盤點。

### 行動應用程式安全管理原則（Mobile App）

#### 本公司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。

#### 本公司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。

## 物聯網

### 物聯網設備保管者須遵循本要點，有關本公司配發物聯網設備使用原則，僅在所獲得之授權內，使用、存取、安裝此物聯網設備，並妥善保護所使用的物聯網設備。

### 相關指派人員應接受適當教育訓練，以期了解其角色及責任，以有效執行單位業務活動。

### 物聯網設備收回處理者由總、分公司受指派之人員擔任。

### 設備盤點評估

#### 本公司應建立物聯網設備管理清冊並至少每年更新一次，以識別設備用途、網路設定、存放位置與管理人員，評估適當之實體環境控管措施及存取權限管制。

#### 物聯網設備盤點及更新由總公司及分公司各權責單位管理人員負責，作法得參照《SO-23-001物聯網設備管理作業程序》。

### 設備軟體控管

### 本公司物聯網設備應具備安全性更新機制且定期更新，以維持設備之整體安全性。

### 設備權限控管

### 本公司物聯網設備應具備身份驗證機制或配對綁定機制，並應進行初始密碼變更，密碼採英數字混合使用且長度不應少於八位，且以最小權限原則針對不同的使用者身分進行授權，確保僅能由經授權之使用者進行資料存取、設備管理及安全性更新等操作。

### 設備連線控管

### 本公司應關閉物聯網設備不必要之網路連線及服務，並避免使用對外公開 的網際網路位置，如設備採用公開的網際網路位置，應於設備前端設置防 火牆予以防護，並採用白名單方式進行存取過濾。如設備以無線連接網路 者，應採用具加密協定之無線存取點連接網路，並以網路卡卡號白名單等 機制進行設備綁定。

### 供應商管理

#### 本公司如與物聯網設備供應商簽定採購合約時，其內容應包含資訊安全相關協議，明確約定相關責任(如：服務承諾、安全性更新機制、網路連線與服務安全性、主動通報設備已知資安漏洞並提出相關應變處置方案等)，確保設備不存在已知安全性漏洞。

#### 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。

### 例外控管

### 本公司知悉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 落實本安全控管第二至四項之規範，應中斷設備網路連線，僅於必要時連 接內部網路並擬定汰換計畫，汰換前應設置於獨立網段與內部網路進行區 隔。

### 不具備管理功能之感測器控管

### 本公司針對不具備管理功能之物聯網設備感測器，其功能雖較為單純且風 險較低，仍應遵循本安全控管第一、四、五、六項之要求辦理。

## 遠距辦公

### 同仁遠距辦公時應遵循本作業要點，應依各自業務範圍申請及開放相關系統功能權限，並做好資訊安全的控管。

### 對使用遠距辦公之設備安裝資訊安全相關軟體，控管應用程式存取權限，以降低資訊外流風險。

### 依業務範圍及控管權限設定居家辦公員工之系統功能權限，相關權限管理設定依據《SC-01-008 存取控制》。

### 應依員工執行業務內容訂定連線時段限制及相關規範，相關規定依據《SC-01-006實體環境與安全》。

### 公司應留存遠距辦公員工使用者登入系統、電腦設備操作及交易紀錄軌跡，相關軌跡留存辦法依據《SC-01-008存取控制》。

### 公司應採多因子驗證機制(員工帳號密碼、動態密碼、一次性帳密)及建立安全的遠距網路通道，降低相關帳號密碼遭假冒或竊用之風險，相關密碼原則設定依據《SC-01-008存取控制》。

### 公司應阻擋惡意或未經授權之連線，並採用最小權限原則設定遠距帳號存取規則，相關遠端連線管控依據《SC-01-007通訊與作業管理》。

### 公司應定時更新VPN連線和其他遠端連結系統之安控措施，相關遠端連線管控依據《SC-01-007通訊與作業管理》。

### 公司應對客戶隱私、資料及紀錄之安全性建立保護措施，相關隱私保護規定依據《SC-01-008存取控制》。

### 公司應加強宣導資訊安全，教育遠距辦公員工應對網路風險保持警覺等資訊安全機制，相關教育訓練規範依據《SC-01-005人員安全》。

## 電子式交易控管

### 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：

#### 證券商所約定之資訊，且無第三人知悉(如固定密碼、圖形鎖或手勢等)。

#### 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)，證券商應確認該設備為客戶與證券商所約定持有之設備。

#### 客戶提供給證券商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)，證券商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，證券商僅讀取驗證結果，必要時驗證來源辨識；採用間接驗證者，應事先評估客戶身分驗證機制之有效性。

### 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，相關規定依據《SC-01-006實體環境與安全》。

### 若帳號登入失敗、非客戶帳號登入嘗試紀錄留存相關監控及分析紀錄，相關。

### 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，相關加密機制依據《SC-01-006實體環境與安全》。

### 對電子式交易身分的驗證資訊應進行雜湊或加密儲存，相關規定依據《SC-01-008存取控制》。

### 應於伺服器端驗證客戶電子式交易身分，相關驗證規定依據《SC-01-007通訊與作業管理》。

### 使用優質密碼設定並進行控管，確實執行密碼輸入錯誤次數達3次者應予帳號鎖定，相關規定依據《SC-01-008存取控制》。

### 應提供客戶定期更新密碼之機制並使用優質密碼，相關客戶密碼原則設定依據《SC-01-008存取控制》。

### 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)來辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況，相關稽核軌跡留存規定依據《SC-01-008存取控制》。

## 深度偽造

### 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，相關教育訓練規範依據《SC-01-005人員安全》。

# 輸出文件記錄

1. SC-01-012-F01\_社群媒體帳號暨官方社群申請單。
2. SC-01-012-F02\_社群媒體平台內容監控檢查表。
3. SC-01-012-F03\_社群媒體使用條款閱讀確認單。