通訊與作業管理

|  |  |
| --- | --- |
| 文件編號： | SC-01-007 |
| 文件版次： | V 1.1 |
| 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 | 新版文件。 | 丘建華副總經理 | 李文柱總經理 | 因應2022轉版，重新發行。 |
| V1.1 | 2024/08/07 | 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](#_Toc149666809)

[第一節 證券商資通安全檢查機制 4](#_Toc149666810)

[第二節 相關控制管理要點 8](#_Toc149666811)

[第二章 範圍 8](#_Toc149666812)

[第三章 名詞定義 8](#_Toc149666813)

[第四章 相關文件 8](#_Toc149666814)

[第五章 權責 9](#_Toc149666840)

[第六章 作業內容 9](#_Toc149666969)

[第七章 輸出文件記錄 9](#_Toc149666982)

# 目的

為維繫本公司所有業務及日常作業之持續進行、強化本公司網路相關作業之管理、規範網路相關系統設施之使用、授權、監督管理、資安威脅情資以及遵循臺灣證券交易所發布「建立證券商資通安全檢查機制」等各項作業程序，特訂定本要點以確保本公司於必要時能及時提供作業復原之所需、交易處理與日常作業之資料傳輸及相關系統設備安全，並規範網路相關系統、設施之使用、授權、監督與管理等各項作業程序，以避免不當之使用遭致網路資源的浪費或可能的內外部資訊安全破壞或意外事故造成的損害，本公司以達成以下目標。

證券商資通安全檢查機制

### 網路安全管理包含以下：

#### 網路系統安全評估：

##### 訂定定期評估自身網路系統安全並留存相關紀錄之機制，如作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等。

##### 訂定修補網路運作環境及作業系統之安全漏洞之機制，包含伺服器、攜帶型、個人端及營業處所內供投資人共用之電腦等。

##### 訂定電腦網路安全相關事項之內部公告機制，包含資訊安全政策宣導、防範網路駭客入 侵事件、電腦防毒等。

##### 各電腦主機、重要軟硬體設備等建立專人負責。

##### 本公司網路依用途區分為 DMZ、營運環境、測試環境及其他環境等，並建立適當區隔機制。

##### 個人資料及機敏資料存放於安全的網路區域，不得存放於網際網路等區域。

##### 本公司系統僅開啟必要之服務及程式，未使用之服務功能將確保已關閉。

##### 本公司已建立遠端連線管理辦法，對使用外部網路遠端連線至公司內部作業進行控管及身分認證，留存相關維護紀錄並由權責主管定期覆核。

##### 公司建立防止未經授權設備使用內部網路。

##### 應避免使用生命週期終止(End of Service, EOS/End of Life, EOF)之網路設備擬定汰除計畫。

#### 網路設備安全管理：

##### 建立防火牆。

##### 防火牆有專人管理。

##### 防火牆進出紀錄及其備份至少保存三年。

##### 重要網站及伺服器系統（如網路下單系統等）以防火牆與外部網際網路隔離。

##### 防火牆系統之設定經權責主管之核准。

##### 公司每年定期檢視並維護防火牆存取控管設定，每半年檢視DMZ區之防火牆規則，並留存相關檢視紀錄。

##### 公司交易相關網路直接連線之設備避免使用危害國家資通安全產品。

##### 公司建立網路設備規則應以最小授權及正面表列為原則。

##### 公司應至少每年檢視一次對外網路設備規則，並留存相關紀錄。

#### 網路傳輸及連線安全管理：

##### 網路下單畫面採加密方式（例如：SSL）處理。

##### 公司每日針對核心系統之帳號登入失敗紀錄、非客戶帳號 嘗試登入紀錄等進行監控及分析，發現有帳號登入異常情事 （如密碼輸入錯誤達三次、一定時間內大量帳號登入失敗、 帳戶申請或更新憑證下載異常），即時了解異常原因，並 留存相關紀錄。

##### 公司提供網路下單服務，於網路下單登入時採多因子認證 方式（例如：固定密碼、圖形鎖、下單憑證、綁定裝置、 OTP、生物辨識等機制 ），以確保為客戶本人登入。

#### 多因子驗證:

##### 公司使用多因子驗證應具下列三項之任兩項技術:

##### 公司所約定之資訊，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），公司應確認該設備為客戶與公司所約定持有之設備。

##### 客戶提供給公司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），公司應直接或間接驗證該生物特徵。

#### 身分認證與憑證管理：

##### 網路下單證券商訂定憑證交付程序，避免非本人取得憑證 。客戶申請或更新憑證下載，必須採用多因子（如：下單憑證、綁定裝置、OTP、生物辨識及SIM認證等）驗證方式，且 與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀 錄。（細節請參考「SO-MG-008\_憑證交付作業程序」）

##### 網路下單證券商全面使用認證機制。

##### 公司應於伺服器端驗證客戶交易身分及使用者帳號。

##### 公司對電子交易身分之申請、交付、使用、更新驗證應訂定相關規範。

#### 電腦病毒及惡意軟體之防範：

##### 安裝防毒軟體，並及時更新程式及病毒碼。

##### 定期對電腦系統及資料儲存媒體進行病毒掃瞄（含電子郵件）。

##### 防毒涵蓋個人端（含攜帶型及營業處所內供投資人共用之 電腦等）及網路伺服器端電腦。

##### 勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤特別小心開啟。

##### 為防範電腦病毒擴散，影響電腦安全，本公司訂定電子郵件使用安全相關規定及建立郵件過濾機制。（細節請參考「SO-05-002\_電子郵件作業程序」）

##### 公司建立上網管制措施，以避免下載惡意程式。

##### 公司偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。

##### 本公司定期辦理社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。 （細節請參考「SO-06-009\_社交工程管理作業程序」）

#### 網路系統功能檢查：

##### 定期檢查網路下單系統提供之功能，並留存紀錄。

##### 就提供外部連線使用網路系統偵測網頁與程式異動、記錄並通知相關人員處理。

#### 公司提供API服務規範：公司提供客戶使用用程式介面（API ）服務之申請流程、核可標準及相關控管配套措施相關作業， 依「證券商受理客戶使用用程式介面（ API）服務作業規 範」辦理。

#### 網際網路下單服務品質相關標準： 公司提供網際網路下單業務時，兼顧客戶服務品質，訂定網 際網路下單服務品質相關標準，並包含下列重點如：交易之 安全性、交易之穩定及系統可用性、提供客戶服務。

#### 網路攻擊防護機制導入及安全性檢測

##### 公司依其所屬資安分級定期對提供網際網路服務之核心系 統辦理滲透測試，並依測試結果進行改善。

##### 公司依其所屬資安分級定期辦理資通安全健診（含網路 架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視 、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線 設定檢視）。

##### 公司依其所屬資安分級建立資通安全威脅偵測管理機制（ 含括事件收集、異常分析、偵測攻擊並判斷攻擊行為）

##### 公司依其所屬資安分級建立入侵偵測及防禦機制。

##### 公司依其所屬資安分級設置用程式防火牆。

##### 公司依其所屬資安分級辦理進階持續性威脅攻擊防禦措施 。

##### 核心系統身分驗證機制應防範自動化程式之登入或密碼更換嘗試，非核心系統宜防範自動化程式之登入或密碼更換嘗試。

#### 帳號登入或異常態樣通知： 公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣即通知客戶，並留存紀錄，避免非客戶本人登入情事：

##### 密碼輸入錯誤或帳戶被鎖定。

##### 申請或更新憑證。

##### 變更基本資料。

##### 異常來源或行為嘗試登入等

##### 密碼申請異動或補發時。

#### 異常IP登入之監控與預警： 公司對異常及不明來源IP連線進行監控分析及留存紀錄，如有發現下列情形，設有警示機制，並定期檢視以確認機制有效運作：

##### 同一來源IP登入不同帳號達一定次數以上。

##### 同一帳號在一定時間內由不同國家登入。

##### 發現異常來源（如金融資安資訊分享與分析中心F-ISAC公布之黑名單或國外IP）嘗試登入。 （細節請參考「SC-01-009\_系統開發及維護」）

### 電腦系統及作業安全管理

#### 電腦設備之管理： 為確定電腦設備維護內容，與廠商訂有書面維護契約，做完 維護時留存維護紀錄並由資訊單位派人會同廠商維護人員共 同檢查。

#### 電腦作業系統環境設定及使用權限設定：

##### 電腦作業系統環境設定及使用權限設定經有關主管核示， 並由系統管理人員執行。

##### 電腦系統檔案異動前後皆有完善之備份處理措施。

##### 公司建立系統最高權限帳號管理辦法（含作業系統及用系統），如需使用最高權限帳號時須取得權責主管同意，並留存相關紀錄。

##### 公司建立並落實個人電腦、伺服器及網路通訊設備之安全性組態基準（如密碼長度、更新期限等），核心系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。

##### 公司透過網際網路使用帳號登入系統時，採用多因子認證機制。 （細節請參考「SC-01-009\_系統開發及維護」）

##### 資通系統內部時鐘應定期與基準時間源進行同步。

##### 公司應依其所屬資安分級對核心系統重要組態設定檔案及其他具保護需求之資訊進行加密或以其他適當方式儲存。

##### 公司應依其所屬資安分級訂定對核心系統之閒置時間或可使用期限與核心系統之使用情況及條件(如：帳號類型與功能限制、操作時段限制、來源位址限制、連線數量及可存取資源等)。

#### 電腦媒體之安全管理：

##### 重要軟體及其文件、清冊抄錄備份存於另一安全處所。

##### 重要之備份檔案及軟體若儲存於與電腦中心同一建築物內， 鎖存於防火之房間或防火且防震之防火櫃中。

##### 存放備份資料之儲存媒體，於其標籤上註明存放資料之名 稱及保存期限。

##### 建立機密性及敏感性資料媒體之相關處理程序，防止資料洩露或不當使用。

##### 建立回存測試機制，以驗證備份之完整性及儲存環境的適當性。

##### 公司應依據系統特性與資料復原點目標（RPO），考量備份頻率、儲存媒體類型（光碟、外接硬碟、磁帶）、資料類型（虛擬機映像檔、系統源碼、資料庫與組態設定檔等）、備份類型（完整備份、增量備份與差異備份）、備份方式（網路同步寫入、網路非同步寫入與離線備份）等，制定適當之資料備份機制，如採離線備份應依備份類型建立適當的備份基準(baseline)，以確保資料可正確回存。

##### 公司制定資料備份機制時，宜考量「3-2-1備份原則」，至少製作三份備份；將備份分別存放在兩套獨立不同儲存設備；至少一份放在異地保存。

#### 電腦操作管理：

##### 操作人員確實依規定操作程序執行。

##### 操作日誌詳實記載並逐日經主管核驗，操作人員不可與主管為同一人。

##### 系統主控台所留存之紀錄，經專人檢查訊息內容且定期送主管核驗。

##### 證券經紀商配備經營業務所需、且有適足容量之電腦系統。

##### 證券經紀商之電腦系統訂定定期（每年至少一次）由內部或委託外部專業機構評估電腦系統容量及安全措施之機制與程序 ，定期對系統容量進行壓力測試，並留存紀錄。（細節請參考「SC-01-009\_系統開發及維護」）

## 相關控制管理要點

### SC-01-007-001資料備份與媒體管制管理

### SC-01-007-002電子化資訊服務控制管理

### SC-01-007-003網路暨通訊安全管理

### SC-01-007-004可用性管理

### SC-01-007-005容量管理

### SC-01-007-006威脅情資管理

### SC-01-007-007偽冒案件處理辦法

# 範圍

適用於本公司資訊環境所使用之網路與通訊相關事宜，包含網路服務及提供網路服務的硬體、軟體與週邊設備等；威脅情資則為資訊部有關情資蒐集作業均適用。

# 名詞定義

無

# 相關文件

參閱第一章第二節，相關控制管理要點。

### SC-01-007-001資料備份與媒體管制管理

### SC-01-007-002電子化資訊服務控制管理

### SC-01-007-003網路暨通訊安全管理

### SC-01-007-004可用性管理

### SC-01-007-005容量管理

### SC-01-007-006威脅情資管理

### SC-01-007-007偽冒案件處理辦法

# 權責

參閱第一章第二節，相關控制管理要點。

### SC-01-007-001資料備份與媒體管制管理

### SC-01-007-002電子化資訊服務控制管理

### SC-01-007-003網路暨通訊安全管理

### SC-01-007-004可用性管理

### SC-01-007-005容量管理

### SC-01-007-006威脅情資管理

### SC-01-007-007偽冒案件處理辦法

# 作業內容

參閱第一章第二節，相關控制管理要點。

### SC-01-007-001資料備份與媒體管制管理

### SC-01-007-002電子化資訊服務控制管理

### SC-01-007-003網路暨通訊安全管理

### SC-01-007-004可用性管理

### SC-01-007-005容量管理

### SC-01-007-006威脅情資管理

### SC-01-007-007偽冒案件處理辦法

# 輸出文件記錄

### 無。