資通安全事件通報程序

|  |  |
| --- | --- |
| ◎文件編號： | SO-19-001 |
| ◎文件版次： | V 1.1 |
| ◎發行日期： | 2025/2/13 |

文件修訂履歷

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 發行／修訂版次 | 發行／修訂  生效日期 | 發行與變更說明 | 權責  人員 | 核准  人員 | 備註 |
| V1.0 | 2022/7/11 | 新版文件 | 施雷蜀華 | 簡孝芸 |  |
| V1.1 | 2025/2/13 | 新增重大資安事件定義及其它 | 潘世佳 | 施雷蜀華 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目錄

[第一章 目的 4](#_Toc98255054)

[第二章 範圍 4](#_Toc98255055)

[第三章 名詞定義 4](#_Toc98255056)

[第四章 相關文件 4](#_Toc98255060)

[第五章 權責 4](#_Toc98255063)

[第一節 通報人 4](#_Toc98255064)

[第二節 通報人部門主管 4](#_Toc98255065)

[第三節 通報窗口 5](#_Toc98255066)

[第四節 資訊部主管或其指定代理人 6](#_Toc98255067)

[第五節 事件處理人員 6](#_Toc98255068)

[第六章 作業內容 7](#_Toc98255070)

[第一節 情資或事件判斷 7](#_Toc98255071)

[第二節 事件通報與結報作業 7](#_Toc98255075)

[第七章 輸出文件記錄 8](#_Toc98255076)

# 目的

為建立群益金鼎證券(以下簡稱本公司)資通安全事件之作業準則，特訂定資通安全事件通報資程序（以下簡稱本程序），規範符合事件之內外部通報和結案，以達成以下目標：

### 確保本公司資通安全事件通報流程順暢。

### 確保本公司在接獲資通安全事件及潛在威脅、疑似事件，能確實通報或知悉相應單位，並即時進行應變處置及留存記錄以利後續處理。

# 範圍

群益金鼎證券有關資通安全事件及潛在威脅、疑似事件內部與外部通報等作業均適用。

# 名詞定義

### 資通安全事件：資訊系統之機密性、完整性及可用性受到影響。

### 重大異常事件 : 重大影響客戶權益或正常營運之資訊服務異常事件。

### 重大資安事件：

依臺證輔字第1120503153號來函，證券商重大資安事件之範圍包含以下四類樣態：

### (一)核心系統異常，且開盤期間影響交易達2小時以上未能恢復，或於10日內就同一資安、系統異常事件，通報次數達3次以上者。

### (二)同一資安或系統異常事件，包含同一委外資訊廠商系統異常、及同一基礎設施異常等，自首家證券商通報日起10日內，影響達3家以上證券商者。

### (三)新型態資安攻擊或駭客攻擊事件(例如撞庫攻擊、DDoS攻擊、勒索病毒等)。

### (四)其他重大資安事件：包括但不限於指定案件、重大輿情案件、客戶資料等敏感資料外洩、其他重大影響投資人權益、影響本公司正常營運或影響金融秩序案件等。

### 資通安全事件通報：當發生資通安全事件時，除了組織內部進行管控外，並依證券期貨市場資安事件影響等級分析結果，透過主管機關提供之通報平台(如：證券期貨市場資通安全通報系統、金融資安資訊分享與分析中心(F-ISAC)等)，進行事件、情資等的通報與分享。如屬重大資安事件，應另於七個營業日內向證交所或櫃買中心函報詳細資料。

### 潛在威脅、疑似事件：任何可能造成使用者無法正常使用資訊服務之情況，以及因使用者心理感受而衍生出之意見，均屬之。

### 資訊服務異常事件：參考SO-18-001\_事件管理程序中說明。

### 情資 : 參考SO-16-001\_情資蒐集作業程序中說明。

# 相關文件

### 群益金鼎證券股份有限公司重大事件處理及通報機制管理辦法

### BO-CM-001\_事件通報程序

### SO-16-001\_情資蒐集作業程序

### SO-18-001\_事件管理程序

### SO-06-009\_社交工程管理作業程序

# 權責

## 通報人

公司所有使用者皆應主動通報資通通安全事件及潛在威脅、疑似事件，並協助確認、排除與解決，必要時得進行客戶關懷與結果回報。

## 通報人部門主管

部門主管或其代理人於事件發生時，接收通報人之通報。

## 接受通報窗口

### 客服人員

#### 由資訊部客戶服務處同仁擔任

#### 接受客戶反應問題並協助處理，若反應問題經判斷是資訊服務異常事件，則通報監控室依SO-18-001\_事件管理程序作業進行處理，若是疑似資安事件則通報業務單位所屬主管外，也通知予資安人員、及其他相關主管協助釐清，並向客戶說明事件處理情況與服務現況。

### 資訊部監控室

#### 由資訊部維護營運處維運一科同仁擔任。

#### 負責監控資訊系統異常告警。

#### 負責公司所有使用者反應問題的釐清及處理。

#### 負責有關資訊服務異常相關事件，例如軟體與硬體異常所造成的資訊處理錯誤或服務中斷，或因傳輸流量受設備損壞或網路不當使用、或遭受阻絕服務（Denial of service）攻擊而引起的異常情形之追蹤與評量等作業。

#### 依SO-18-001\_事件管理程序判斷，如屬重大異常事件 ，或經判斷疑似資安事件則通知予資安人員、客服人員及其他相關主管或處理人員，並向使用者說明事件處理情況與服務現況。

### 資訊部維運人員

#### 由資訊部維護營運處二、三、四科人員擔任。

#### 若接受監控或資安工具異常訊息之告警，若判斷會造成資訊服務異常則應立即通知監控室，若判斷疑似資安事件，則應立即通知監控室、資安人員、事件處理人員、部門主管等。

### 資訊安全人員

#### 由資訊部資訊安全處同仁擔任。

#### 向通報人及其部門主管、事件處理人員等，進行異常狀況和情資之了解與追蹤，必要時得召開會議擬定因應方案、研議後續作為，或進行例外狀況判斷。

#### 向資安長或其代理人進行資通安全事件報告，必要時亦得尋求法遵人員與第三方人員或機關之協助。

#### 經判斷屬重大異常事件或1級以上之資通安全事件時，為向稽核單位及主管機關進行事件通報之總窗口。

#### 依據事件回報狀況排除與處理結果後，與相關主管或人員判斷資訊安全事件結束，並通知事件管理人員進行事件結案。

### 稽核人員

#### 由稽核室人員擔任。

#### 如通報之事件經判斷或會議決議為重大異常事件、1級以上之資訊安全事件等，則會同資安人員，進行主管機關通報。

### 法令遵循人員

#### 由法令遵循暨法務室人員擔任。

#### 如通報之事件涉及個資侵害、損失或疑似事件等，需向警政單位或司法單位備案、說明時之總窗口。

## 資訊部主管或其指定代理人

經判斷屬重大異常事件或資安事件時，應立即向本公司資安諮詢小組組長或其代理人進行通報，並進行事件追蹤、處理與指派專人向主管機關進行通報。

## 資通安全事件處理人員

由維護營運單位、系統開發單位、資訊安全人員及業務單位等所組成。

### 維護營運單位：

#### 由維護營運處人員擔任。

#### 依據SO-18-001\_事件管理程序判斷資訊服務異常事件後，由事件管理人員、事件處理人員、事件通報人員組成，進行事件處理及結案，若是重大異常事件或疑似資安事件則通知予資安人員、客服人員及其他相關主管或處理人員，並向使用者說明事件處理情況與服務現況。

#### 協助就情資或事件內容進行黑白名單比對、作業系統檢視、端點防護、防火牆阻擋、防毒軟體設定、個人電腦設定、郵件或AD規則調整、是否進行DDoS流量清洗或網路區隔等作業。

#### 協助保留受害期間之相關設備紀錄資料(例：主機事件紀錄檔、防火牆紀錄、網站日誌檔、未授權存在之惡意網頁/留言/檔案/程式樣本、移除未授權存在之惡意網頁/留言/檔案、將異常外部連線 IP 列入阻擋清單…等)。

### 系統開發單位：

#### 由資訊部各系統開發單位人員擔任。

#### 協助就資通安全事件、情資等內容進行系統功能或程式編寫方式調整、函式庫或其他套件取用調整等，並依據所授權範圍與專業能力，進行各項改善或加強作業。

#### 依據事件內容協助提供系統資料與佐證紀錄等(例：異常連線行為、異常帳號使用、異常下單交易行為、確認網站資料庫內容是否遭竄改，確認憑證或密碼等各驗證平台與gateway等連線狀態之防護，並適時進行惡意行為阻斷、停用或註銷、移除網站外洩資料等作業)。

### 資訊安全人員：

#### 資訊部資訊安全處人員擔任。

#### 接受之重大異常事件或疑似資安事件通報，進行判斷與評估，必要時通報主管機關或協同至警局備案。

### 業務權責單位：

#### 由群益金鼎集團各業務單位人員擔任。

#### 依據事件通報單位，由總公司業務單位進行權責管理與業務指派，以協助事件釐清、處理與解決(例如：客戶清單、狀況回報等)。

#### 必要時得進行客戶關懷與結果回報，並將事件處理結果告知客戶；或協同至警局報案或備案。

# 作業內容

## 情資或事件判斷

### 通報人員應於接獲客戶回報，或自行發現時，經初步判斷屬於資通安全事件，因於資訊事件通報系統進行通報，及回報其部門主管。

### 接受通報窗口，應於收到通報後，針對內容進行初步分類，以判斷是否為資訊服務異常事件，或是疑似資安事件等，及需不需要立即通報相關主管及資安人員。

### 接受通報窗口如獲異常異常訊息之告警，若判斷是疑似資安事件則應立即通知資安人員、事件處理人員、部門主管等。

### 資安人員依接受之資通安合事件通報，進行下列判斷與評估：

證券期貨市場資安事件影響等級3 個級別：

（一）3 級事件：符合下列任一情形者，屬 3 級事件：

1. 敏感資料遭洩漏。

2. 核心業務系統或資料遭嚴重竄改。

3. 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回 復正常運作。 （二）2 級事件：符合下列任一情形者，屬 2 級事件：

1. 核心業務一般資料遭洩漏。

2. 非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料 遭輕微竄改。 3. 非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內 回復正常運作；抑或核心業務運作遭影響或系統停頓，於可容 忍中斷時間內回復正常運作。

（三）1 級事件：符合下列任一情形者，屬 1 級事件：

1. 非核心業務一般資料遭洩漏。

2. 非核心業務系統或資料遭輕微竄改。

3. 非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復 正常運作。

4. 接獲恐嚇或威脅，但尚未發生資安攻擊事件。

## 事件通報與結案作業

### 事件偵測、調查、排除及恢復：依SO-18-001\_事件管理程序辦理。

### 重大異常事件或疑似資安事件：經判斷如屬重大異常或疑似資安事件，得由資安或相關人員召開臨時性會議，邀集通報人、通報人部門主管、資訊部主管或其指定代理人、事件處理人員等，進行因應方案與後續作為之研議，或進行例外狀況、誤判等之判斷。

### 重大資安事件：經判斷或會議決議為SO-18-001\_事件管理程序所定義之A~C級事件、1級以上之資通安全事件或情資項目(例：0級事件、偽冒應用程式、釣魚信件、冒名…等)或重大資安事件者，由資安人員會同稽核室人員進行以下作業：

#### 視情況提供情資予F-ISAC進行資訊分享。

#### 依據「證券期貨市場資通安全事件通報應變作業注意事項」進行事件分類與異常狀況判斷是否需進行主管機關通報；30分鐘內應於「證券期貨市場資通安全通報系統」進行初步事件通報作業，如釐清事件確認誤報者，則可“取消通報“；若非誤報則需於查明事件後儘速辦理“正式通報“，並於事件處理完成後進行“解除通報“。

#### 如屬臺證輔字第1120503153號來函界定之重大資安事件類型，本公司應填具「證券商重大資安事件通報單-初步(正式)通報作業」，並於七個營業日內填具「證券商重大資安事件通報單-結案通報作業」向證交所或櫃買中心函報詳細資料，包括事件發生時間、事件發生原因、事件分類、對證券商及投資人造成之影響、有無敏感資料外洩、處理措施、恢復情形、事件後續處理進度、投資人糾紛處理、改善情形及相關預防措施等。

#### 如需尋求警政資源協助者，由資安人員、法令遵循人員及事件主管等至警局報案或備案。



### 如事件屬重大異常事件、SO-18-001\_事件管理程序所定義之A~C級事件或經判斷為1級以上之資通安全事件，所有應變處理皆需保存相關記錄及文件。

# 輸出文件記錄

### 無。