營運持續管理

|  |  |
| --- | --- |
| 文件編號： | SC-01-010 |
| 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 | 2024/08/07 | 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](#_Toc135325912)

[第一節 證券商資通安全檢查機制 4](#_Toc135325913)

[第二章 範圍 4](#_Toc135325914)

[第三章 名詞定義 5](#_Toc135325915)

[第一節 營運持續作業 5](#_Toc135325916)

[第二節 通報機關 5](#_Toc135325921)

[第四章 相關文件 5](#_Toc135325922)

[第五章 權責 5](#_Toc135325923)

[第一節 管理審查委員會 5](#_Toc135325924)

[第六章 作業內容 6](#_Toc135325925)

[第一節 營運持續管理體系(Business Continuity Management System，BCMS) 6](#_Toc135325926)

[第七章 輸出文件記錄 7](#_Toc135325927)

# 目的

為確保群益金鼎證券（以下簡稱本公司）營運持續、資訊服務能持續有效運作，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」之規範，特訂定本要點搭配「BP-00-003\_營運持續管理政策要點」明確規範系統之故障復原程序、降低重大實體災害(如地震、火災)及資訊作業故障事件所造成之衝擊，以確保資訊作業等工作項目之持續運作，以達成以下目標。

## 證券商資通安全檢查機制

### 明確訂定（如：電腦設備、通訊設備、電力系統、資料庫、電腦作業系統等備援及回復計畫）故障復原程序，並落實執行且留存紀錄。

### 建立故障復原程序及週期性測試，測試後召開檢討會議，針對測試缺失謀求改進，並留存紀錄。

### 建立證券經紀商之交易主機之備援措施，並依所屬資安分級建置異地備援機房。

### 擬訂營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及其必要之維護，並定訂關鍵業務及其衝擊影響分析，評估核心系統中斷造成之衝擊程度，並依核心系統之復原時間目標(RTO)、資料復原點目標(RPO)，作為恢復核心系統、備份備援規劃及執行復原作業之依據，並已依其所屬資安分級定期辦理業務持續運作演練。應視演練範圍是否涉及第三方，邀請相關廠商參與演練。

### 訂定資訊安全訊息通報機制（如：正式之通報程序及資安事件通報聯絡人），針對與資訊系統有關之資訊安全或服務異常事件依「證券期貨市場資通安全事件通報應變作業注意事項」及「證券商通報重大資安事件之範圍申報程序及其他應遵循事項」辦理，並採取適當矯正程序，留存紀錄。

### 建立個人資料之竊取、竄改、毀損、滅失、或洩漏等資安事故通報機制，立即函報證交所（或櫃檯買賣中心、券商公會）並轉陳主管機關。

### 建立明確訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序。（參考：「SO-09-005\_網路入侵事件作業程序」及「SO-09-005-F01分散式阻斷服務攻擊(DDoS)之應變暨處理措施」）

### 本公司辦理下列資安防護事宜：

#### 指定人員及部門統籌並協調聯繫各有關部門。（參考：《BP-00-001\_企業持續營運管理要點》及《BP-00-003\_營運持續管理政策要點》等規範管理之。）

#### 定期評估核心營運系統及設備，對評估結果採取適當措施，並提報董事會，以確保營運持續及作業韌性之能力。

#### 於永續報告書、年報、財務報告或公司網站，揭露年度內公司持續核心營運系統及設備營運所需之資源及落實於年度預算或教育訓練計畫等項目。

### 公司應辨識風險情境，就各項風險情境當災害發生造成資訊作業異常或中斷時，擬定各系統之應變、減災或復原措施 相關作業流程。

### 核心系統原服務中斷時，應於可容忍時間內，由備援設備或其他方式取代並提供服務。

### 公司資訊委外作業如涉及核心資通系統與資通服務，資訊服務供應商應定期提供資通系統與資通服務之回復計畫，回復計畫可以災難復原計畫、備援演練、營運持續計畫等形式呈現。

# 範圍

本委員會應執行之各項活動及本公司資訊部提供之資訊服務相關事宜皆適用之。

# 名詞定義

## 營運持續作業

### 資訊服務異常暨資安事故：導致資訊資產毀損或遺失以致危害本公司或客戶權益之事件，或導致本公司主要資訊作業營運中斷之事件。

### 資訊作業營運持續計畫：為避免主要資訊作業遭受意外事件而中斷營運所研擬之計畫。

## 通報機關

### 主管機關：金融監督管理委員會證券期貨局

### 函報機關：證券交易所、櫃檯買賣中心或券商公會

### 外部專家包含主管機關、司法與警察單位、資訊安全與資訊科技服務顧問及其他相關組織機構等提供專業意見諮詢，或相互交換資料。

# 相關文件

### SP-00-001\_資訊安全政策

### SC-01-002\_資訊安全政策

### SO-18-001\_事件管理程序

### SO-19-001\_資通安全事件通報程序

### SO-09-005\_網路入侵事件作業程序

### BC-00-002\_危機處理小組管理要點

### BP-00-003\_營運持續管理政策要點

### BO-MG-002\_營運衝擊分析程序

### BO-MG-004\_營運持續管理演練作業程序

### BO-MG-008\_系統異地復原暨演練程序

### PIMS-P-01個人資料管理目標與政策

# 權責

## 管理審查委員會

### 為營運持續管理體系運作之最高監督單位。

### 營運持續管理體系管理審查事項。

### 委員會溝通方式

#### 本公司各管理體系作業管理之最高機構，負責本公司管理體系之政策審核、管理系統建置作業及相關活動之督導，內容如下：

##### 討論並議定全公司各管理體系之重大事項。

##### 依照本公司之各管理體系的策略方向，發展、修訂與公布管理政策及要點。

##### 聽取及覆核營運持續及資訊安全風險評估報告，並根據該報告之結果，決定營運持續及資訊安全之可接受風險水準。

##### 依據本公司之營運需求、法令異動、營運持續、資訊安全需求、技術變遷及可接受風險水準等因素，審議及公布管理體系政策、管理體系組織及相關要點。

##### 議定各功能單位營運持續與資訊安全之職務與責任。

##### 針對本公司各項系統之復原順序、資源分配與外部專家進行溝通與協調，與各部門有關營運持續與資訊安全事務達成一致共識。

##### 監控並檢討重大安全事件應變處理與改善措施，與安全事變報告及事件調查結果。

##### 聽取營運持續、資訊安全及個人資料管理之落實、威脅變化、安全評估等相關評估或措施。

##### 檢討與處分各管理體系違失事項。

##### 檢討並改進現行管理體系，以提高其運作效率及有效性。

##### 了解管理體系運作相關人員必須具備之職能，並提供相關人員所需之教育訓練課程。

# 作業內容

## 營運持續管理體系(Business Continuity Management System，BCMS)

### 程序書「BO-MG-008\_系統異地復原暨演練程序」已明確訂定（如：電腦設備、通訊設備、電力系統、資料庫、電腦作業系統等備援及回復計畫）故障復原程序，並落實執行且留存紀錄。

### 程序書「BO-MG-008\_系統異地復原暨演練程序」、「BO-CM-002\_人員疏散程序」、「BO-CM-003\_風災水災應變暨處理程序」、「BO-CM-004\_地震應變暨處理程序」、「BO-CM-005\_火災應變暨處理程序」、「BO-CM-006\_重大疾病或傳染病處理程序」、「BO-CM-007\_危機溝通程序」、「BO-CM-008\_電力中斷應變暨處理程序」、「BO-CM-009\_異地辦公室啟動暨資訊系統切換程序」、「BO-CM-010\_保險理賠採購招募程序」建立故障復原程序及週期性測試，並於測試後召開檢討會議，針對測試缺失謀求改進，並留存紀錄。

### 程序書「BP-00-003\_營運持續管理政策要點」及「BP-00-003-F02\_營運持續管理策略」建立證券經紀商之交易主機之備援措施。

### 程序書「BO-MG-004\_營運持續管理演練作業程序」建立營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及其必要之維護，並定訂關鍵業務及其衝擊影響分析，並已依其所屬資安分級定期辦理業務持續運作演練。

### 本要點、「SO-19-001\_資通安全事件通報程序」及「BO-CM-001\_事件通報程序」訂定資訊安全訊息通報機制（如：正式之通報程序及資安事件通報聯絡人），針對與資訊系統有關之資訊安全或服務異常事件依「證券期貨市場資通安全事件通報應變作業注意事項」辦理，並採取適當矯正程序，留存紀錄。

### 程序書「PIMS-P-01個人資料管理目標與政策」已建立個人資料之竊取、竄改、毀損、滅失、或洩漏等資安事故通報機制，立即函報證交所（或櫃檯買賣中心、券商公會）並轉陳主管機關。

### 程序書「SO-09-005\_網路入侵事件作業程序」及「SO-09-005-F01分散式阻斷服務攻擊(DDoS)之應變暨處理措施」建立明確訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序。

# 輸出文件記錄

### 無。