­­­

實體環境與安全

|  |  |
| --- | --- |
| 文件編號： | SC-01-006 |
| 文件版次： | V 1.0 |
| 發行日期： | 2023/11/22 |

|  |
| --- |
| © 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。 |

目 錄

第一章 目的 4

第一節 安全區域管理 4

第二節 資訊設備授權及保護管理 4

第三節 證券商資通安全檢查機制 4

第二章 範圍 4

第三章 名詞定義 4

第一節 安全區域 4

第二節 公共區域 4

第三節 資訊設備 5

第四節 正式環境系統 5

第五節 測試環境系統 5

第六節 所有系統 5

第七節 身分識別與鑑別 5

第八節 數位簽章 5

第九節 公用程式 5

第四章 相關文件 5

第五章 權責 5

第一節 安全區域管理 5

第二節 資訊設備授權及保護 6

第六章 安全區域作業內容 7

第一節 周邊區域 7

第二節 內部區域 8

第三節 管制區域 8

第四節 辦公區域 9

第五節 委外廠商工作區(含測試機房) 10

第六節 公共區域安全保護 10

第七章 資訊設備授權及保護管理作業內容 10

第一節 資訊設備安全 10

第二節 資訊設備之移入移出 11

第三節 公司外之設備安全 11

第四節 資訊設備報廢或再利用之安全防護 11

第五節 業務支援設備安全 11

第六節 系統安全之控管要求 12

第八章 輸出文件記錄 14

# 目的

## 安全區域管理

### 為確保工作區域的實體安全，防範資訊設備未經授權的存取及破壞，依據臺灣證券交易所發布《建立證券商資通安全檢查機制》訂定及落實相關要點，含安全區域範圍、管控及作業要求，以確認本公司實體環境安全。

## 資訊設備授權及保護管理

### 為避免資訊設備遭受損壞以致影響業務之持續運作，並設置適當之防護以保護資訊資產，依據臺灣證券交易所發布《建立證券商資通安全檢查機制》訂定及落實相關要點。

## 證券商資通安全檢查機制

#### 電腦機房建立門禁管制。

#### 設置機房消防設施定期進行檢驗。

#### 將地震、水災等天然災害因素列入實體安全考量因素。

#### 電腦設備之電源供應系統含不斷電設備及發電機。

#### 訂定設備報廢作業程序，報廢前已將機密性、敏感性資料及授權軟體予以移除、實施安全性覆寫或實體破壞，確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄。

#### 建立定期審查資訊機房門禁管制權限之程序。

# 範圍

凡資訊安全管理制度內所屬工作區域活動，對於資訊設備及相關業務支援之實體安全及進出管制等事宜適用之。

# 名詞定義

## 安全區域

### 管制區域：僅限特定人員可以進出與使用內部設施，包含機房、操控室/監控室、 電氣/電池室等受到實體保護管制區域，第三方人員進出須由內部員工全程陪同。

### 辦公區域：各部處之使用區域、各主管辦公室及內部使用會議室等。

### 委外廠商工作區(含測試機房)：位於本公司內部，提供公司資訊人員及委外廠商 開發測試或執行專案之區域。

## 公共區域

### 開放自由使用之區域，如接待區、會客室及接待外賓會議室等。

## 資訊設備

### 包含硬體與軟體，如伺服器、應用系統、資料庫、作業系統、網路設備、組態設定管理等。

## 正式環境系統

### 係指「SC-01-004 資產分類與控制」所定義之正式環境群組，包含應用系統、資料庫、作業系統及網路設備軟體等。

## 測試環境系統

### 係指「SC-01-004 資產分類與控制」所定義之測試環境群組，包含使用於測試之應用系統、資料庫及作業系統等。

## 所有系統

### 係指「SC-01-004 資產分類與控制」所定義之軟體群組。

## 身分識別與鑑別

### 係指使用者存取資訊系統和服務時對其身分進行驗證的機制，如密碼、生物統計學中的指紋鑑定、筆跡鑑定和晶片等硬體標記的使用。

## 數位簽章

### 係指透過公鑰及私鑰的非對稱型密碼技術製作的電子簽章。

## 公用程式

### 用來輔助使用者或系統管理者，易於掌握系統資源。

# 相關文件

### SC-01-004\_資產分類與控制。

### SO-11-002\_機電設備作業程序。

### SO-03-002\_資訊設備攜出入作業程序。

# 權責

## 安全區域管理

### 全體員工與第三方

#### 遵守本公司實體環境與安全要點，於授權使用區域內執行作業

### 安全區域主管

#### 負責公告安全區域及公共區域範圍。

#### 管制區域支援性設備之規劃、設置、管理與檢視。

#### 管制區域門禁進出許可人員清單之檢視。

### 管理部

#### 總務室負責統籌辦理安全設施之設置與管理。

#### 人力資源室負責識別證的核發以及門禁的管理。資訊資產相關人員。

### 維護營運處

#### 制定安全區控制要點並負責規劃安全區域範圍。

#### 確認第三方人員與本公司網路連線時，與本公司內部網路已做邏輯隔離。

### 稽核室

#### 定期檢視設有門禁管制區域的存取許可名單，是否與門禁系統之進出人員清單一致。

## 資訊設備授權及保護

### 業務擁有者 (Business Owner)

#### 得指派權責人員進行資訊設備的維護、保管與處份，及授權資訊資產的存取。

### 資訊資產擁有者 (Owner)

#### 資訊資產擁有者得在業務擁有者授權的情況下，指派權責人員進行資訊設備的維護、保管與處份，及授權資訊資產的存取。

### 資訊資產保管者 (Custodian)

#### 應善盡資訊設備保護之責。

#### 應對資訊設備實施基本清潔及保養。

#### 應為所保管的系統，定期更新重大弱點之修正程式。

#### 應評估系統安全需求與系統功能允許，據以啟動稽核軌跡，並定期檢核。

#### 應定期對無法自動化時間同步之資訊設備執行對時。

#### 應定期監控系統效能及容量使用狀況，如有異常，應留存處理紀錄並陳權責主管覆核。

#### 應取得已公布之技術脆弱性之資訊或定期執行弱點掃描。

### 使用者 (User)

#### 應僅在所獲得之授權內，檢視、使用、存取及更新異動此項資訊設備，並妥善保護所使用的資訊設備。

### 系統管理人員、資料庫管理人員及網路管理人員：

#### 系統、資料庫及網路管理執行單位為維護營運處。

#### 應明確定義作業系統之安全參數。

#### 應於維護之系統上線前，執行適當之強化。

### 帳號管理人員

#### 凡適用範圍內之所有資訊設備或電腦網域中，同時具有兩位以上之使用者，且設有帳號或權限管制之系統，依據經適當授權之帳號權限申請，而設定帳號及權限之人員，即為該資訊設備之帳號管理人員。

#### 帳號管理人員不宜為該資訊設備日常作業之使用者。

### 維護營運處

#### 審核資訊資產存取權限申請文件，並確定其與系統設定一致且適當。

### 維護廠商

#### 定期提出服務報告以供本公司查核。

# 安全區域作業內容

## 周邊區域

### 資訊部辦公場所之規劃

#### 本公司於建設規劃或租賃營業場所時，應注意下列事項：

##### 建築物本體應考慮耐震度及防洪之設計。

##### 建築物內部裝潢應於適當區域採用防火建材。

##### 應設置煙霧感知及消防設備，於重大機電設備所處區域，應另行考量設置適當之消防機制，以避免設備毀壞。

##### 所有可能潛入的風險點（如門口、窗戶）附近應設置適當之監控或警示設備。

##### 應設有門禁管控，用以區隔及辨認第三方人員之身份。

##### 應符合政府之營建及消防法令之規定。資訊安全人員得不定期針對資訊部內之資訊資產進行抽查，以確保資訊資產清冊之完整性。

#### 對非本公司的員工之區隔

##### 非本公司員工（如來賓、委外廠商等）來訪，應先確認身份，並由本公司資訊部同仁陪同，方可進入本公司管制區域內，且不得攜入未經本公司核准之物品（例如： 電腦設備、工具、機械、攝影器材等），若需攜入物品前，應先依據本公司之《SO-03-002\_資訊設備攜出入作業程序》提出申請。

##### 因本公司業務需要，由廠商長期派駐本公司之第三方人員，經管理部核發識別證件，出入本公司必須配掛其識別證件，若需攜入物品（例如：電腦設備、工具、機械、攝影器材等），亦需依據本公司之相關規定提出申請。

#### 貨物運送之區隔

##### 貨物、設備及運送人員進入本公司前，應先行進行申請，依本公司相關規定取得同意後，經權責人員檢視無異常狀況後，方可進入本公司。

## 內部區域

### 安全區域之公告 安全區域之規劃應由資訊部維護營運處執行，應於區域異動時公告區域劃分情形，以利相關員工瞭解遵行。

### 門禁管制 各安全區域之進出應設置門禁管制，及適當之身份驗證機制或管控措施，以確保人員須經核准授權後，方可進入各區域。

### 身份識別 使用者係指獲得適當的授權，得以檢視、使用、存取或異動此資訊資產之人員/單位。

### 監視設備之設置 各管制區域應設置必要之監視設備，做為發覺與記錄事件之機制。監視設備之規劃、審核、設置與管理與由資訊部維護營運處負責。

### 門窗管制 各區域之管制出入門戶應儘可能設置自動關閉機制，並應養成隨手關門之習慣。窗戶應盡可能採用強化玻璃，使用完畢後應立刻予以關閉。

### 物品出入管制 本公司員工或第三方人員如應業務需求，需攜入(出)公司及外部電腦資訊暨週邊設備、工具、機械、磁片、光碟等物品時，均應由本公司員工依《SO-03-002\_資訊設備攜出入作業程序》核對相關表單。

## 管制區域

### 管制區域進出管理

#### 進出管制區域的大門應有門禁隔離設施以防止未經授權的存取，如使用門禁刷卡裝置、警報裝備、門鎖，或使用人工值守的接待區域等，確保僅有經過適當授權的人員始可進入，門禁管制應由專人控管權限，且應適當記錄，紀錄至少保留五年。

#### 人員調（離）職或申請期間屆滿時，應註銷其通行權限並繳回門禁卡。

#### 人員進入管制區域之門禁權限應經申請程序，並由專人控管權限，並留存紀錄，紀錄至少保留五年。

#### 因業務需要，如設備維護，而獲臨時授權進入管制區域之第三方人員，應經業務單位及資訊單位主管核准始得進入，交由機房管理員、機房操作員或業務承辦人簽名確認，工作時應由本公司員工陪同與監督，若無法全程陪同，則應留存監控錄影紀錄，且任一進出皆應確實填寫《機房進門禁進出管制表》，詳載入出之時間、目的及處理事項，並應至少保留五年。

#### 因工作需求，需攜出入電腦資訊暨週邊設備等物品時，應依《SO-03-002\_資訊設備攜出入作業程序》塡寫表單，需詳載攜出入物品之、時間、目的及處理事項，經權責主管核准後始可攜出入，並將相關紀錄留存至少五年。

#### 門禁進出許可人員清單應由維護營運處主管至少每半年檢視乙次，以確認進出許可授權之適當性，並留存相關紀錄。

#### 每日應查核門禁管理執行情形，並作成紀錄，呈報主管簽核。

### 管制區域作業規範

#### 管制區域空間

##### 管制區域出入口應保持暢通。

##### 危險或易燃材料儲存應與管制區保持安全距離，並設置卸載區，提供設備裝載及拆卸，以避免粉塵、易燃物品及蟲害侵擾。

##### 管制區域應保持清潔，禁止於管制區域內吸煙及飲食。

##### 堆放及儲存在管制區域內之大宗物品，如電腦零組件，應放置於規定地點，並排列整齊，且不得堆置不必要之廢棄物品。

#### 管制區域支援性設備

##### 管制區域應設置停電緊急照明設備、專用之消防系統與搭配設置不斷電設備，並定期保養及檢測。

##### 消防設備、空調設備與監視設備等支援性設備之規劃、設置、管理與檢視由總務單位負責。支援性設備檢測保養作業之執行頻率至少每年乙次。

##### 管制區域應設置必要之監視設備，監控範圍應包含機房出入口與重要資訊設備，並針對重要與非常出入口裝設警報器或偵測系統，以作為警戒或記錄資訊安全事件之機制，監視紀錄至少保留一年。

#### 管制區域內不得從事監控以外之照相、錄影、錄音及其他記錄行為，如必要時應經總經理或其授權人核准後方可進行。

#### 應每日檢測及監控機房之基礎設施運作狀況，並作成紀錄。如發現異常，應即時通報處理。

#### 機房設備之異動需求，除緊急事件外，應事先申請核准並留下異動紀錄。

#### 管制區域內機櫃應予上鎖，以避免人為破壞或人員誤觸。

#### 離開管制區域時，應確認門窗已確實關閉並鎖上。

#### 應每年清查機架設備，並作成相關紀錄備查。

## 辦公區域

### 辦公室的安全保護

#### 具有資料複製功能之設備(例如：影印機、傳真機、掃瞄機等…)，不應放置於公共區域及委外廠商工作區，並應設置使用相關控管規定，以規範內部人員方可使用。

#### 辦公區域對外門窗平日應儘可能關閉並上鎖，避免未經核准的侵入活動。

#### 第三方人員於辦公區域工作時，應受本公司監督。

### 辦公區域作業要點

#### 列印、影印或傳真收發機密性文件時，應立即領取，並同時取走原始文件，不可任意棄置，以避免機密資訊外洩。不再使用之文件，應立即銷毀。

#### 無人領取之傳真機、影印機、印表機原始文件或列印文件，應由專人定時整理收取並代為保管，以防範相關文件遭未經授權人員取走。經保管超過一星期以上仍無人領取者，應立即銷毀。

#### 會議結束應立即清理會議室白板與桌面資料，以防範未經授權人員竊取、窺視或破壞。

#### 個人辦公桌面應維持清潔，下班前應將業務上使用之文書歸檔整理，並依據資訊資產之分類原則，將屬機密等級文件放置於上鎖的文件櫃中。

#### 個人作業不再使用之機密文書資料，應使用碎紙設備或其他無法還原原始資料之銷毀方式進行銷毀。

#### 嚴禁員工於外界之公佈欄或新聞媒體等公開資訊場所，張貼、散佈、提供任何未經本公司授權之一切資訊，不論其性質是否機密或業務相關。

## 委外廠商工作區(含測試機房)

### 委外廠商工作人員須遵守上述辦公室的安全保護，及管制區域與辦公區域作業要點。

### 與本公司網路連線時，須經由資訊部維護營運處確認與本公司內部網路做邏輯隔離。

## 公共區域安全保護

### 機密與內部限閱等級之文件禁止任意放置於公共區域。

### 本公司之分機表及通訊錄等，具有聯絡資料及身分之文件，應避免放置或張貼於公共區域。

### 避免於公共區域討論業務及工作內容。

# 資訊設備授權及保護管理作業內容

## 資訊設備安全

### 資訊設備之存放

#### 正式環境資訊設備應置於具有門禁管理、空調、電源供應穩定、防火、耐震與抗洪之管制區域內，避免非法存取或破壞行為。

#### 資訊設備之保管者應善盡保護之責。

#### 第三方放置於本公司之資訊設備應由各保管單位負責保護管理。

### 資訊設備之維護

#### 資訊設備之保管者須實施基本清潔及保養，僅被授權的維護人員才能對設備進行修理和維護。

#### 與營運直接相關之資訊設備應與廠商簽訂維護合約，並要求廠商定期檢修

#### 各資訊設備之使用、操作、定期維護應依據供應商之標準作業手冊執行之，除經授權之廠商維修人員及資訊部門維修人員外，其他人員不可擅自進行拆卸或維修資訊設備。

#### 資訊設備維修應以在本公司就地維修為優先，如需整組設備送修，應將存放機密性資料之硬碟予以拔除或徹底刪除其內容。若上述無法執行，則應取得廠商之保密同意書。

#### 重大的資訊設備應購置適當之保險，保險之項目應涵蓋潛在可能的威脅，包含火險、颱風險、地震險等。

## 資訊設備之移入移出

### 本公司所有資訊設備的移入與移出，設備及物品之進出須經資訊資產擁有者核准，包含移入及移出之日期皆須適當記錄，由維護營運處主管覆核。

## 公司外之設備安全

#### 若可移動的資訊設備或儲存媒體內存資料之機密性(Confidentiality)等級評定為3時，除異地備份媒體外，禁止攜出至公司以外之場所。

#### 應制定媒體備份相關管理要點《SC-01-007\_通訊與作業管理》，以保護異地存放媒體的安全。

#### 本公司同仁攜帶可移動的資訊設備或儲存媒體(包含筆記型電腦、個人數位助理PDA、可讀寫CD裝置、外接硬碟…等)到本公司以外之場所使用時，若資訊設備或儲存媒體內含公司機密資料或客戶資料，攜出時應妥善保管以避免設備遺失造成資料外洩。

#### 在外使用之可移動的資訊設備或儲存媒體，應設置密碼保護以確保資料的安全，當內存機密等級以上之資料時，應考量於設備中加設加密機制。

## 資訊設備報廢或再利用之安全防護

### 資訊設備報廢時應依本公司《SC-01-004\_資產分類與控制》相關規定辦理。

### 各資訊設備經評估不堪使用或不擬使用時，應由資訊資產擁有者指派人員進行設備之破壞，使該設備上原存在之本公司資料或資訊不可再利用，方可進行處份或變賣。

### 資訊設備進行移交或變賣時，應將原屬於該單位之機密性資料或資訊以低階格式化、重寫資料方式予以消除或實體銷毀，方可移轉。

## 業務支援設備安全

### 電力供應

#### 重要資訊設備應設置不斷電系統(UPS)，確保電力供應之持續性。不斷電系統之電力供應，必須足以支援緊急應變處理時，啟動切換備援電力或關機之所需。

#### 計算電源容量時，除電腦設備外，其他業務支援設備如空調、給水、照明等，應分別計列。

#### 機電設備應考量其周圍環境，如排水設備、散熱設備及噪音排除等因素之配合。

#### 使用電氣及不斷電設備應注意下列事項，並作成保養維修紀錄：

##### 電氣設備保養維護詳細辦理流程請參照《SO-11-002\_機電設備作業程序》。

##### 發電機應備足燃料，燃料應與發電機、電氣或不斷電設備適當隔離。

#### 高壓電、不斷電設備、發電機、機電設備等支援設備之設置地點應禁止閒雜人等進出，並設有實體門禁控管。

### 空調設備

#### 設置空調設備時應考量下列因素：

##### 應計算空間之容積、環境之密封性、隔離材料(牆壁或玻璃)之散熱性及電腦機器之散熱量。

##### 所使用材料須具有不易燃性。

##### 空調設備須有足夠之備援。

#### 使用空調設備注意事項以及保養維修細節請參照《SO-11-002\_機電設備作業程序》。

## 系統安全之控管要求

### 正式環境系統安全要求

#### 系統安全要求

各主要資訊設備（如應用軟體、系統工具、資料庫及系統主機）應依照機密性等級需求，訂定安全參數設定，並應注意以下事項：

##### 資訊設備管理人員應明確定義對該類型資訊設備之系統參數設定，並據以執行。

##### 購置或建置時應依據相關之資訊安全控管要點，要求廠商對系統予以強化；新購或新建置之資訊設備，應要求廠商提供系統安全控管參數設定標準，以做為訂定資訊安全控管要點參考依據。

##### 應依據不同工作需求，明確訂定可以存取的系統資源內容，包括系統操作人員、系統管理人員、網路管理人員、應用系統開發人員、安全管理人員等等，以作為授權之依據。

##### 應遵照最小安裝原則執行安裝，並減少不必要的安裝與啟動項目。

##### 公司交易相關網路直接連線之設備應避免使用危害國家資通安全產品。

#### 終端機登入程序

登入程序應該將公開的系統資訊減至最小限度，避免爲非法用戶提供資訊。登入程序應考量以下控制：

##### 登入時電腦螢幕上應該顯示警告消息，說明進入的系統是專用系統，不允許非法存取。

##### 在登入過程未成功之前不顯示系統或應用程式的名稱及版本資訊。

##### 登入發生錯誤時，系統不應說明係帳號或密碼錯誤。

##### 登入逾時，系統應自動終止。

##### 成功登入完成後，應儘可能顯示以下資訊：

###### 上一次成功登入的日期和時間。

###### 自從上次成功登入後登入失敗的時間及位址。

#### 機密性系統的隔離

#### 機密性等級為3的應用系統，應在獨立的電腦運算環境下執行，與一般辦公室網路及網際網路作邏輯隔離，並應有適當的防火牆保護。

#### 無人看管之資訊設備

##### 無人看管的個人主機或終端機應限定其存取資料之路徑、連線方式及使用之服務。

##### 供多人使用之電腦主機或終端機應設定登入控管，如帳號登入機制，以確保僅經授權之人員可以使用。使用結束後應予登出主機或終端機。

#### 系統公用程式之安全

系統之公用程式如下所列應予以控管，並禁止非資訊設備保管者或被授權人員使用。

##### 帳號暨群組管理。

##### 網路參數設定。

##### 系統參數設定。

##### 稽核原則變更。

##### 批次作業建立。

##### 系統資訊變更，如主機名稱與時間。

##### 系統處理程序變更，如停用或變更執行中之程序。

#### 連線時間限制

#### 除監控用電腦外，應設定15分鐘以內啟動密碼保護之螢幕保護程式或自動登出機制。

### 測試環境系統之控管要求

#### 系統安全要求

##### 應由資訊設備保管者據以執行適當作業系統安全參數之強化，以加強系統安全。

##### 應至少每月檢視乙次是否有重大弱點之修正程式並視需要予以更新。

#### 連線時間之限制

應設定15分鐘以內啟動密碼保護之螢幕保護程式或自動登出機制。

### 電子商務安全

### 電子商務包括使用電子資料交換（EDI）、電子郵件和透過公共網路如 Internet 線上交易。電子商務易受網路威脅的攻擊，可能會導致詐欺、合約糾紛以及資訊遭修改或外洩等風險。應考慮以下控制重點保護電子商務不受這類威脅：

#### 驗證 (Authentication)：

##### 顧客和本公司需建立身分驗證機制，以確定交易對象之身份 (例如：使用憑證進行網路下單交易)。

##### 客戶使用網路下單登入時，應採雙因子認證方式 (例如：下單憑證、綁定裝置、OTP、生物辨識等機制)。

##### 應提供客戶定期更新密碼之機制並要求客戶使用優質密碼並進行管控。

#### 授權 (Authorization)：應設立交易額度授權的相關機制。

#### 交易之不可否認性：例如數位簽章的使用。

#### 報價資訊 (Pricing Information)：各股報價資訊的正確性以及完整性。

#### 訂單交易 (Order Transactions)：客戶網路下單流程的機密性(如：SSL)及完整性(如：憑證)檢查。

#### 檢查 (Vetting)：檢查網路下單客戶之交易額度、信用額度、保證金、是否簽署電子交易保證書等。

#### 訂購要求 (Ordering)：須設立相關檢核機制確保網路下單交易資訊的機密性和完整性，並確保避免交易資料遺失，或重複交易。

# 輸出文件記錄

### 無。