­­­

資產分類與控制

|  |  |
| --- | --- |
| 文件編號： | SC-01-004 |
| 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

第一節 資訊資產管理 4

第二章 範圍 4

第三章 名詞定義 4

第一節 存取 4

第二節 風險 4

第三節 資訊分級 5

第四章 相關文件 5

第五章 權責 5

第一節 資訊資產管理 5

第六章 資訊資產管理作業內容 6

第一節 資訊資產管理 6

第二節 資訊資產之擁有、保管、使用 6

第三節 資訊資產的新增、異動與停止使用 7

第四節 資訊資產群組之分類與管理 7

第七章 輸出文件記錄 22

# 目的

## 資訊資產管理

### 為妥善保護本公司之資訊資產，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，含資訊資產之造冊、清冊維護以及資訊分級標示處理之相關規範，以利後續執行之風險評鑑程序，以確認資訊資產的風險水準及達成以下目標。

#### 證券商資通安全檢查機制

##### 建立資訊資產清冊並加以維護。

##### 訂定資訊分級並作標示處理之相關規範。

##### 建立對本公司自行或委外開發之資訊系統分級標準，資訊系統等級已經區分核心、關鍵與一般系統等系統分級，並訂定每年至少檢視一次資訊系統分級妥適性。

##### 公司應對資訊資產之資料與文件的保存期限進行規範，並於保存期限到期後進行刪除與銷毀。

### 相關風險評鑑程序則依據《SC-01-001\_風險評鑑與管理》，故以此特訂定《SC-01-004\_資產分類與控制》以規定執行作業時應遵循之事項。

# 範圍

凡本公司資訊部內部符合資訊資產定義之事務屬之，包含所提供之資訊服務相關正式環境中的軟、硬體設備及資訊紀錄。

# 名詞定義

## 存取

### 使用資訊資產(硬體設備、軟體、資料、文件)的各種方式，包含取得、使用、保管、查詢、修改、調整、銷毀等。

### 資訊資產：與資訊處理相關之資產皆屬之，包括硬體、軟體、資料、文件、人員等，皆視為資訊資產。

### 資訊資產擁有者：對於資訊資產負有管理權責，得賦予其他人員存取及使用資訊資產權限人員。

### 資訊資產保管者：負責資訊資產相關處理與保管工作人員。

### 資訊資產使用者：可獲得適當授權，得以檢視、使用、存取或異動資訊資產人員。

## 風險

### 威脅(Threats)：在任何狀況下或任何事件，有潛在的機會經由非法存取、破壞、洩密、竄改資料或阻斷服務(Denial of Service)式攻擊，而造成系統傷害或業務中斷者稱之。

### 脆弱點(Vulnerabilities)：為資訊資產本身存在之弱點(Weakness)，但脆弱點不會對資產造成傷害，惟脆弱點可被利用而使資訊資產遭受威脅，導致有害事件發生或造成資訊資產損害。脆弱性若無妥善管理，將促使威脅形成。

### 風險(Risk)：指會造成資訊或資訊資產損害、毀損，或造成資訊服務中斷、品質下降之潛在的可能。

### 風險評鑑(Risk Assessment)：是指透過系統化方式釐清資訊與資訊系統所可能遭遇到的威脅與脆弱性發生的可能性，及資訊服務風險影響的標的與範圍，分析相關衝擊(Impacts)，以及決定風險等級的程序。

## 資訊分級

### 指對資訊資產進行分類，並依照其風險執行分級及標示處理之相關規範。

# 相關文件

### SP-00-001\_資訊安全政策。

### SC-01-001\_風險評鑑與管理。

### SC-01-010\_營運持續管理。

# 權責

## 資訊資產管理

### 管理審查委員會

#### 依資訊資產清冊內容所執行資訊安全風險評鑑之結果，核准資訊資產管理相關要點。

#### 決定資訊安全之風險可接受水準，如確定公司各作業可接受之資訊安全風險等級。

### 資訊安全人員

#### 由資訊安全長指派適當人員擔任。

#### 定期規劃、彙整及檢核資訊資產清冊之完整性，並依循《SC-01-001\_風險評鑑與管理》，將風險評鑑結果呈報管理審查委員會。

#### 依據風險評鑑程序進行相關作業，依循《SC-01-001\_風險評鑑與管理》，協助相關部處進行風險評鑑作業，將對每次風險評鑑結果執行書面的資訊安全風險評鑑報告，並留存相關紀錄。

#### 針對已處分之硬體設備，不定期抽查設備中所有程式及資料檔案皆已清空、無法回復，且經該部處主管覆核。

### 資訊資產登錄人員

#### 由各處指派適當人員擔任。

#### 負責依據資訊安全人員規劃之程序，更新資訊資產清冊。

### 資訊資產相關人員

#### 配合資訊資產登陸人員執行相關作業。

#### 瞭解並遵循資訊資產之相關要點，執行擁有、使用、或保管資訊資產之職責。

### 部處主管

#### 瞭解並遵循資訊資產之相關要點，監督所屬人員遵循資訊資產之相關要點。

#### 針對欲處分之硬體設備，覆核設備中所有程式及資料檔案皆已清空且無法回復。

# 資訊資產管理作業內容

## 資訊資產管理

### 所有資訊資產須經盤點並評估其相對價值及重要性，以建立「SP-00-001\_資訊安全政策」中所定義需保護之資訊資產清冊。

### 資訊資產必須做適當之分類、標示、儲存及保護，並明確劃分其保管責任(例如：明定資訊資產的擁有者、保管者與使用者)，資訊資產之使用、傳遞及保管亦須有對應之控管程序。

### 爲了保護資訊資產免遭受非法公開或濫用，應制定資訊處理和儲存程序，如處理和標記所有媒體、設定存取限制以防止非法存取、維護授權人員存取之正式記錄、保護正在等待輸出的周邊同作資料與其敏感度一致。

### 資訊資產須至少每年盤點一次，資訊資產登錄人員依資訊資產清冊進行盤點，如清冊登錄與現況不符者，經資訊資產擁有者之部處主管確認後，由資訊資產登錄人員更新資訊資產清冊，並得協請資訊資產相關人員配合盤點相關作業。

### 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。

## 資訊資產之擁有、保管、使用

為釐清資訊資產之擁有、保管與使用之權責，確保資產由適當的人員保管及使用，應依資訊資產之機密性、完整性與可用性之標準，指定適當之擁有者、使用者與保管者。相關人員之權責說明如下：

### 擁有者(Owner)： 擁有該資產，對於資訊資產負有最高的權責，得賦予其他人員存取及使用資訊資產的權限，如部門主管、採購單位或其指派之人員擔任。 資訊資產之業務擁有者通常由業務單位權責主管或其指派之人員擔任。

### 保管者(Custodian)： 保管者係指對於該資產需盡保管、保護、保管工作之責任及義務者，得在擁有者授權的情況下，賦予其他人員存取及使用資訊資產的權限。 例如對硬體資訊資產之維護責任，對文件資訊資產進行保存、修改及編輯之工作等。

### 使用者(User)： 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。

## 資訊資產的新增、異動與停止使用

各類資訊資產之新增、異動及停止使用，經申請後由資訊資產擁有者核准後，資訊資產登錄人員彙整存檔及更新資訊資產清冊。

### 資訊資產之異動

#### 以下情形發生時，應進行資訊資產新增之作業：

##### 新購入/移入之硬體設備。

##### 新購入/移入之軟體或系統。

##### 新購入/移入軟硬體設備所增加之系統文件、作業程序等。

##### 新增加/權限異動之作業流程所使用之文件表單。

##### 作業流程變更時所增加之文件表單。

#### 以下情形發生時，應進行資訊資產變更之作業：

##### 各類資訊資產變更擁有者或保管者(即資訊資產之移轉)時。

##### 各類資訊資產變更資訊資產分類群組時。

##### 資訊資產清冊內容(名稱、編號等…)異動。

### 資訊資產之停止使用

#### 以下情形發生時，應進行資訊資產停止使用之作業：

##### 硬體類資訊資產報廢及移出時。

##### 軟體類資訊資產停止使用該系統或軟體時(如因法令資料保存之規定雖已停止使用、仍須保留該軟體之備份時不在此限)。

##### 資料／文件類資訊資產已不再使用且已過法令保存之年限時。

## 資訊資產群組之分類與管理

### 授予資訊資產價值

#### 資訊資產之價值須分別針對資訊資產之內涵(即硬體、軟體、文件/資料、人員等)，依其於機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)三個面向之相對價值作為考量，並列表說明所授予相對價值之判斷依據，以作為資訊安全管理之重要基礎，並據以執行風險分析以選擇適當控管。

#### 機密性(Confidentiality)價值： 機密性的等級分為一般(可公開)、內部使用與限用(或敏感)及機密，分別以數字1、2及3來表示。

#### 完整性(Integrity)價值： 若缺乏完整性保護，所造成資訊資產損害之嚴重程度分別為低、中及高，分別以數字1、2及3來表示。

#### 可用性(Availability)價值： 可用性係對資訊資產使用上的依賴程度，分為低、中及高共3個等級，分別以數字1、2及3來表示。

### 篩選核心系統

#### 應對自行開發或委外開發之資訊系統完成資訊系統分級，並區分核心與非核心系統，且每年應至少檢視一次分級妥適性。參考《證券暨期貨市場各服務事業資通系統安全防護基準參考指引》作為篩選標準：「核心系統：係指**直接提供客戶交易**或**支持交易業務持續運作之必要系統**(如交易系統、報價系統、中台風控、盤後結算系統、帳務系統等維持交易業務之必要系統)，**其餘皆為非核心系統**。」

#### 核心系統應辦理：

##### 對帳號登入失敗紀錄、非客戶帳號登入嘗試紀錄等進行監控及分析，並留存相關紀錄。

##### 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。

##### 評估核心系統可容忍中斷時間。

##### 導入資訊安全管理系統，並通過公正第三方之驗證，且持續維持驗證有效性。

##### 定期(每年至少乙次)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，定期對系統容量進行壓力測試，並留存紀錄。

### 資訊資產群組化：為利於資訊資產管理上的一致性，以及降低風險分析時必須逐項分析之費時，並增進管理之效率，本公司對於所列示之資訊資產予以適當群組化。

#### 硬體(H)分為：

##### 伺服器設備類： ➀H1 伺服器--與營運直接相關\_核心系統、➁H2 伺服器--與營運直接相關\_關鍵系統 、➂H3伺服器--與營運間接相關 、➃H4 伺服器--開發測試

##### 網路設備類： ➄H5 網路設備--與營運直接相關 、➅H6網路設備--與營運間接相關

##### 基礎設備與其他設備類：

##### 、➆H7基礎設備

##### 個人電腦類： ➇H8個人電腦及周邊設備

#### 軟體(S)分為：

##### 應用系統類： ➀S1 與核心營運直接相關軟體、➁S2 與關鍵營運直接相關軟體、➂S3一般軟體、➃S4 IT 管理性作業相關軟體、➄S5 IT 基礎相關軟體

##### 套裝軟體類： ➅S6 辦公室套裝軟體

#### 資料(D)分為：

##### 機密類： ➀D1機密(含高風險個資、直接識別個資、易被詐騙個資)、➁D2機密(不含個資)

##### 內部使用與限用類： ➂D3內部使用與限用 (含間接識別個資)、➃D4內部使用與限用 (不含個資)

##### 可公開類： ➄D5可公開-主管機關、➅D6 可公開等六類

##### 未經細分類之資料，預設層級為「內部使用與限用」

#### 文件(F)分為：

##### 機密類： ➀F1機密(含高風險個資、直接識別個資、易被詐騙個資)、➁F2機密(不含個資)

##### 內部使用與限用類： ➂F3內部使用與限用 (含間接識別個資)、➃F4內部使用與限用 (不含個資)

##### 可公開類： ➄F5可公開-主管機關、➅F6 可公開等六類。

##### 未經細分類之文件，預設層級為「內部使用與限用」。

#### 人員(P)分為：

##### 正式員工：　➀P1 內部人員

##### 利害關係人：➁P2 利害關係人-委外廠商等兩類。

### 資訊資產分類說明、價值判斷標準以及資產之管理

#### 硬體資訊資產分類說明、價值判斷標準以及資產之管理

##### 硬體資訊資產分類說明。

| 盤點群組 | 類別 | 範例 |
| --- | --- | --- |
| **H1** | **伺服器--與營運直接相關\_核心系統** | 其主機上安裝之系統係為影響核心營運作業之系統設備，如定義之核心系統，包含包含系統主機及周邊設備。 例如：   * 證券後台系統(Tandem)、NFTP 3.0 * 國內期貨交易系統(Tandem) * 債券系統(Tandem) * 複委託交易系統(Tandem) * 策略王系統 * 網上發 * 群益超級贏家\ * 掌中財神 * 群益行動贏家 * 全球行情系統 * SOLACE回報系統 * 損益試算系統 |
| **H2** | **伺服器--與營運直接相關\_關鍵系統** | 其主機上安裝之系統係為影響關鍵營運作業之系統設備，如定義之關鍵業務系統，包含系統主機及周邊設備。 例如：   * 風控管理系統 * CRM客戶關係管理 * 興櫃ES帳務系統等 * Fix-Trade造市系統 |
| **H3** | **伺服器--與營運間接相關** | 係指除核心系統/關鍵系統外之系統，其主機上安裝之系統係為非影響核心及關鍵營運作業之系統設備，包含系統主機及周邊設備、提供辦公室自動化或支援系統設備或其提供系統管理/資訊服務管理/安全管理之設備。。  例如：   * 非核心系統 * CRM主機 * WebMail郵件主機 * 一般業務之基礎支援設備，如:Print Server、File Server * 會計主機 * 門禁系統 * 防毒管理主機等 |
| **H4** | **伺服器--開發測試** | 係指除核心系統/關鍵系統外之系統，其主機上安裝之系統係為非影響核心及關鍵營運作業之系統設備，包含IT測試環境內之系統設備。  例如：   * 測試環境伺服器 * AP開發環境測試機 * DB開發環境測試機 |
| **H5** | **網路設備--與營運直接相關** | 提供營運直接相關運作之網路設備，如核心通訊設備及直接影響核心營運作業進行之安全管理設備。  例如：   * Core Switch、Router * 防火牆、Web Application Firewall、DNS   專線使用之加密器 |
| **H6** | **網路設備--與營運間接相關** | 提供營運間接相關運作之網路設備，如端末自動化及一般通訊設備(服務辦公區域)。  例如：   * HiLink與ISDN使用之加密器 * Switch * Router * EDGE Switch |
| **H7** | **基礎設備** | 其它相關一般業務之支援設備。  例如：   * UPS * 發電機 * 滅火器 * 監視器 |
| **H8** | **個人電腦及周邊設備** | 本公司內部經授權所使用之個人電腦，其功用為業務或文書處理用。  例如：   * OA區之個人電腦 |

##### 硬體資訊資產價值判斷標準：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 類別/價值 | 3 | 2 | 1 | 備註 |
| **Availability** | 電腦處理交易不得中斷，有異地備援需求。 | 中斷可容忍時間為1個營業日以下，有每日備份的需求 | 中斷可容忍時間為1個營業日以上 |  |

##### 硬體資產之管理：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **硬體產之管理控管說明** | | **存取控制** | **存放與保管** | **備援** | **處份：(出售、移轉或報廢)** |
| H1 | 伺服器--與營運直接相關\_核心系統 | 只有獲得授權的人員及供應商，可以進入之機房或管制區域。 | 應存放在具備門禁管制的管制區域。 此管制區域應有溫溼度控制、煙霧偵測及消防等設備。 資產應定期檢查與維護，並應投保適當之保險。 | 應建立適當的異地及同地之備援機制，以避免意外事故發生導致系統無法運作的時間超過可容許限度，而造成公司營運活動中斷。應擬定災難復原及業務持續作業計畫，並定期執行測試及更新計畫。 | 1.移除硬體設備中的所有程式及資料檔案，並會同資訊安全人員檢查覆核是否已經清空且無法回復。 2.資產的出售、移轉、或報廢時應留下適當的紀錄，內容包含設備名稱及編號、日期時間、處份地點以及買受方相關資訊。 3.硬體資產的處份，應遵守本公司資產處理相關法規。 |
| H2 | 伺服器--與營運直接相關\_關鍵系統 | 同上 | 同上 | 同上 | 同上 |
| H3 | 伺服器--與營運間接相關 | 應有適當的實體保護措施，例如限制只有獲得授權的人員及供應商，可進入之機房或管制區域。 | 應存放在有適當的實體保護措施之安全區域，例如限制只有獲得授權的人員及供應商，可進入之機房或管制區域。 | 應建立適當的檢核機制，以避免意外事故發生導致系統無法運作的時間超過可容許限度，而影響公司正常營運活動。 | 1.移除硬體設備中的所有程式及資料檔案，並會同資訊安全人員檢查覆核是否已經清空且無法回復。 2.資產的出售、移轉、或報廢時應留下適當的紀錄，內容包含設備名稱及編號、日期時間、處份地點以及買受方相關資訊。 3.硬體資產的處份，應遵守本公司資產處理相關法規。 |
| H4 | 伺服器--開發測試 | 同上 | 同上 | 同上 | 同上 |
| H5 | 網路設備--與營運直接相關 | 應有適當的實體保護措施，例如限制只有獲得授權的人員及供應商，可以進入的機房或管制區。 | 應存放在具備門禁管制的管制區域。此管制區域應有溫溼度控制、煙霧偵測及消防等設備。資產應定期檢查與維護，並投保適合之保險。 | 應建立適當的異地及同地之備援機制，以避免意外事故發生導致系統無法運作的時間超過可容許限度，而造成公司營運活動中斷。應擬定災難復原及業務持續作業計畫，並適時更新。 | 1.資產的出售、移轉、或報廢時應留下適當的紀錄，內容包含設備名稱及編號、日期時間、處份地點以及買受方相關資訊。 2.硬體資產的處份，應遵守本公司資產處理相關法規。 |
| H6 | 網路設備--與營運間接相關 | 同上 | 同上 | 同上 | 同上 |
| H7 | 基礎設備 | 得視其資產特性採取適當之實體保護措施，例如僅由經授權之人員可以調整監視器之角度。 | 應存放在有適當的實體保護措施之安全區域。 | 得建立適當的備援機制，以避免意外事故發生導致系統無法運作的時間超過可容許限度。 | 1.資產的出售、移轉、或報廢時應留下適當的紀錄，內容包含設備名稱及編號、日期時間、處份地點以及買受方相關資訊。 2.硬體資產的處份，應遵守本公司資產處理相關法規。 |
| H8 | 個人電腦及周邊設備 | 登入需有密碼保護，使用者登出時需鎖定設備。 | 不需特殊存放與保管機制。 | 個人自行備份，並適時更新。 | 1.如果保管機密等級以上資料的個人電腦，需移除硬體設備中的所有程式及資料檔案，並會同資訊安全人員檢查覆核是否已經清空且無法回復。 2.資產的出售、移轉、或報廢時應留下適當的紀錄，內容包含設備名稱及編號、日期時間、處份地點以及買受方相關資訊。 3.硬體資產的處份，應遵守本公司資產處理相關法規。 |

#### 軟體資訊資產分類說明、價值判斷標準以及資產之管理

##### 軟體資訊資產分類說明。

| 盤點群組 | 類別 | 範例 |
| --- | --- | --- |
| **S1** | **與核心營運直接相關軟體** | 自行開發及維護及委外維護，由群益同仁委託外部第三方執行之：  1.影響核心營運作業之軟體  2.包含應用系統、作業系統及資料庫軟體  例如：   * 證券交易系統 * 期貨交易系統(Tandem) * 群益金融網 * 策略王 * 群益行動贏家 * 超級贏家 * 掌中財神 |
| **S2** | **與關鍵營運直接相關軟體** | 自行開發及維護及委外維護，由群益同仁委託外部第三方執行之：  1.影響關鍵營運作業之軟體  2.包含應用系統、作業系統及資料庫軟體  例如：   * CRM客戶關係管理系統 * 興櫃ES帳務系統 * 衍生性商品系統 |
| **S3** | **一般軟體** | 自行開發及維護及委外維護，由群益同仁委託外部第三方執行之：  1.非影響核心營運作業之軟體  2.包含應用系統、作業系統及資料庫軟體  例如：   * Sun Account * E-learning * 期貨交易系統(Speedy) |
| **S4** | **IT 管理性作業相關軟體** | 自行開發及維護之：  1.內部日常作業及系統管理使用之軟體  2.提供辦公室自動化或支援系統(含應用系統、作業系統及資料庫軟體)  例如：   * 人資系統 * 公司內部入口網站 * 客戶關係管理系統 |
| **S5** | **IT 基礎相關軟體** | 自行開發及維護之：  1. IT 基礎設備與網路設備使用之軟體  2.伺服器--開發測試上之應用系統及開發工具 |
| **S6** | **辦公室套裝軟體** | 根據客戶所提供之資訊服務，用於操作實體元件與設備運作之套裝軟體，包含個人使用之辦公室自動化套裝軟體，屬一般固定功能，不另行做修改之應用程式。  例如：   * Windows * Microsoft Office * WinZip |

##### 軟體資訊資產價值判斷標準：

| 類別/價值 | 3 | 2 | 1 | 備註 |
| --- | --- | --- | --- | --- |
| **Confidentiality** | 其智慧財產權屬或所有權為CSC所有，且該軟體設計規格內容涉及企業持續營運之營業秘密 | 其智慧財產權屬或所有權為CSC所有，未經書面同意，不得由第三方使用 | 其軟體內容不具機密性，如常見套裝軟體、分享軟體、免費工具 |  |
| **Integrity** | 軟體設計規格之不完整，可能造成業務營運之中斷或違反法令之遵循，如線上交易中斷、報表數字未正確表達 | 軟體設計規格之不完整，可能造成作業上之不便，須改以人工作業，如資料傳遞、報表製作等 | 軟體設計規格之不完整，並不影響日常作業 |  |
| **Availability** | 電腦處理交易不得中斷，有異地備援需求 | 中斷可容忍時間為1個營業日，有每日備份的需求 | 中斷可容忍時間為1個營業日或以上 |  |

##### 軟體資產之管理：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **軟體資產之管理控管說明** | | **存取控制** | **存放與保管** | **備援** | **處份：(出售、移轉或報廢)** |
| S01 | 與核心營運直接相關軟體 | 將可存取的帳號及權限減到最少或最小，並關閉不用之預設帳號。其系統存取權限的賦予，應與使用者的角色與職責相符。對於離職或職務調動的人員，其帳號及權限應即時刪除或更新。 | 1.有版權的軟體，其媒體及相關系統文件應集中放置於受保護區域。 2.如有使用安裝之需要，須經擁有者同意，並由保管者紀錄之。 | 應建立應用系統或其他軟體重新安裝及啟動的程序，以便災害發生時可及時復原。應用系統或其他軟體之原始碼及設定資料應有適當的備份機制，以維持最新可用的狀態。 | 1.資產的出售、移轉、或報廢時應留下適當的紀錄，內容包含設備名稱及編號、日期時間、處份地點以及買受方相關資訊。 2.軟體資產的處份應注意是否違反版權及智慧財產權。出售或移轉軟體時，應出具正式的聲明書(特別是針對版權的部份)，以避免因第三方觸犯智慧財產權而引發爭端。 |
| S02 | 與關鍵營運直接相關軟體 | 同上 | 同上 | 同上 | 同上 |
| S03 | 一般軟體 | 將可存取的帳號及權限減到最少或最小，並確保委外開發之維護帳號平時應予關閉或停用。應用系統存取權限的賦予，應與使用者的角色與職責相符。對於離職或職務調動的人員，其帳號及權限應即時刪除或更新。 | 1.有版權的軟體，其媒體及相關系統文件應集中放置於受保護區域。 2.如有使用安裝之需要，須經擁有者同意，並由保管者紀錄之。 | 應建立應用系統或其他軟體重新安裝及啟動的程序，以便災害發生時可及時復原。得視需求取得委外開發之程式原始碼並確認其版本，且原始碼及設定資料應有適當的備份機制，以維持最新可用的狀態。 | 1.資產的出售、移轉、或報廢時應留下適當的紀錄，內容包含設備名稱及編號、日期時間、處份地點以及買受方相關資訊。 2.軟體資產的處份應注意是否違反版權及智慧財產權。出售或移轉軟體時，應出具正式的聲明書(特別是針對版權的部份)，以避免因第三方觸犯智慧財產權而引發爭端。 |
| S04 | IT 管理性作業相關軟體 | 將可存取的帳號及權限減到最少或最小，並確保委外開發之維護帳號平時應予關閉或停用。應用系統存取權限的賦予，應與使用者的角色與職責相符。對於離職或職務調動的人員，其帳號及權限應即時刪除或更新。 | 1.有版權的軟體，其媒體及相關系統文件應集中放置於受保護區域。 2.如有使用安裝之需要，須經擁有者同意，並由保管者紀錄之。 | 應建立應用系統或其他軟體重新安裝及啟動的程序，以便災害發生時可及時復原。應用系統或其他軟體之原始碼及設定資料應有適當的備份機制，以維持最新可用的狀態。 | 1.資產的出售、移轉、或報廢時應留下適當的紀錄，內容包含設備名稱及編號、日期時間、處份地點以及買受方相關資訊。 2.軟體資產的處份應注意是否違反版權及智慧財產權。出售或移轉軟體時，應出具正式的聲明書(特別是針對版權的部份)，以避免因第三方觸犯智慧財產權而引發爭端。 |
| S05 | IT 基礎相關軟體 | 同上 | 同上 | 同上 | 同上 |
| S06 | 辦公室套裝軟體 | 其存取權限的賦予，應與使用者的角色與職責相符。 | 1.有版權的軟體，其媒體及相關系統文件應集中放置於受保護區域。 2.如有使用安裝之需要，須經擁有者同意，並由保管者紀錄之。 | 應確認軟體存放位置，以確保事故發生時可及時取得及復原。 | 1.資產的出售、移轉、或報廢時應留下適當的紀錄，內容包含設備名稱及編號、日期時間、處份地點以及買受方相關資訊。 2.軟體資產的處份應注意是否違反版權及智慧財產權。出售或移轉軟體時，應出具正式的聲明書(特別是針對版權的部份)，以避免因第三方觸犯智慧財產權而引發爭端。 |

#### 資料／文件資訊資產分類說明、價值判斷標準以及資產之管理

##### 資料／文件資訊資產分類說明。

| 盤點群組 | 類別 | 範例 |
| --- | --- | --- |
| **D1/F1** | **機密**(含高風險個資、直接識別個資、易被詐騙個資) | 1. 高風險個人資料如含有特種個人資料等狀況  2. 除特定業務承辦人員因職責所需，或經擁有者核可外，不得公開予其餘人員之資料文件。  3. 該檔案中有部分資料性質較為特殊或具敏感性，如任意蒐集、處理或利用，恐會造成社會不安或對當事人造成難以彌補之傷害。  4. 易被詐騙的個人資料，揭露將影響同仁致使遭受詐騙的個人資料或如遭未經授權人員取得易導致當事人遭詐騙。  例如：  人事資料  財會資料  客戶資料 |
| **D2/F2** | **機密**(不含個資) | 可供部分員工使用之資料文件，含機敏資訊，揭露會造成有形及無形之損害。  例如：  營運資料 |
| **D3/F3** | **內部使用與限用**(含間接識別個資) | 僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定個人者，僅含單一個資屬性之姓名、電話號碼、完整地址、電子郵件之個人資料檔案。 |
| **D4/F4** | **內部使用與限用**(不含個資) | 可供所有員工使用之資料文件，惟可能含機敏資訊，揭露會造成有形及無形之損害。  例如：   * 內部公文 * 政策要點 |
| **D5/F5** | **可公開-主管機關** | 例如：   * 公司對主管機關相關資料揭露 |
| **D6/F6** | **可公開** | 例如：   * 公開資訊網站之資料 |

##### 資料／文件資訊資產價值判斷標準：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 類別/價值 | 3 | 2 | 1 | 備註 |
| **Confidentiality** | 除工作職責之所須外，須經擁有者同意後始可使用或閱讀 | 僅簽有保密協定之人員或主管機關可以使用 | 為公開資訊，不具機密性 |  |
| **Integrity** | 其完整性可能影響法令之遵循，如客戶交易額度之累計、財務報表之表達 | 其完整性可能影響決策判斷，如財控績效資料 | 公司不必為其完整性負任何法律責任 |  |
| **Availability** | 該資料若未及時取得，可能直接影響營運業務或法令之遵循 | 該資料若未及時取得，可能導致作業上之不便 | 該資料並無時效性之問題 |  |

##### 資料／文件資產之管理：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **資料/文件資產之管理控管說明** | | **原則** | **使用者** | **標示** | **複製** | **保管** | **傳遞** | **後續處理** |
| D1/F1 | 機密（含高風險個資、直接識別個資、易被詐騙個資） | 資訊資產之製作、保管、分發、回收與銷毀，須經資訊資產擁有者(Owner)書面核可，並由資訊資產保管者(Custodian)負責管理。 | 基於業務所需，並經資產擁有者書面核可。 | 於文件首頁或每頁明顯處標示「機密」，每頁標示頁數，並加註後續處理原則。 | 須由資產擁有者之授權核可，方能複製 | 書面文件應放置於上鎖櫃中，使用時保管者應予登錄。電子檔案形式者，僅資產擁有者、保管者及使用者具有存取權限。 | 以書面方式傳遞時，必須密封並註明收件人，嚴禁他人拆封。如以電子方式傳遞，必須事先取得核准，儘可能使用加密保護或防護檢核機制後傳遞。 | 資產擁有者、保管者及使用者皆負有保護其安全之責。作廢時必須以絞碎、燃燒等方式銷毀。 |
| D2/F2 | 機密 (不含個資) | 同上 | 同上 | 同上 | 同上 | 同上 | 同上 | 同上 |
| D3/F3 | 內部使用與限用 (含間接識別個資) | 由資訊資產保管者(Custodian)負責資訊資產之製作、保管、分發、回收與銷毀。 | 允許公司正式員工、已簽訂保密合約之委外廠商或顧問及獲得充分授權之第三者存取。 | 於文件首頁或每頁明顯處標示「內部使用與限用」 | 如複製給委外廠商或第三者時，應做書面簽收。 | 由該資產保管者妥善保管。 | 以公司之電子郵件系統或公文傳遞程序 | 同上 |
| D4/F4 | 內部使用與限用 (不含個資) | 同上 | 同上 | 同上 | 同上 | 同上 | 同上 | 由資產保管者負責其保護及處理。 |
| D5/F5 | 可公開-主管機關 | 無特殊控管程序。 | 公開大眾。 | 無需標示。 | 不需特別控管。 | 書面文件不須特別控管。電子形式公司授權人員存取權限。 | 不需特別控管。 | 不需特別控管。 |
| D6/F6 | 可公開 | 同上 | 同上 | 同上 | 同上 | 不需特別控管。 | 同上 | 同上 |

#### 人員資訊資產分類說明、價值判斷標準以及資產之管理

##### 人員資訊資產分類說明。

| **盤點群組** | 類別 | 範例 |
| --- | --- | --- |
| **P1** | **員工-內部人員** | 例如：   * 資訊部正職同仁、約聘僱同仁 |
| **P2** | **利害關係人-委外廠商** | 例如：   * 委外開發或維護廠商、保全人員等 |

##### 人員資訊資產價值判斷標準：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 類別/價值 | 3 | 2 | 1 | 備註 |
| **Confidentiality** | 可取存各類資料(含機密、內部使用與限用及可公開等資料)。 | 可取存內部限制及可公開資料。 | 可取存可公開類資料。 |  |
| **Availability** | 為維繫正常運作，在該人員無法持續提供服務時，可容忍替換時間為最短。 | 為維繫正常運作，在該人員無法持續提供服務時，可容忍替換時間為適中。 | 為維繫正常運作，在該人員無法持續提供服務時，可容忍替換時間為最長。 |  |

##### 人員資產之管理：

| 類別 | 控管說明 | |
| --- | --- | --- |
| **員工-內部人員** | 原則： | 為包含所有職級之員工，並依管理部人力資源室所頒布相關管理要點進行控管。 |
| **利害關係人-委外廠商** | 原則： | 為非正式員工，因執行委外作業所需，易取得公司內機密之資訊，除依利害關係人對內部資源進行存取時則依循資訊《SC-01-009\_系統開發及維護》、《SC-01-006實體與環境安全》等要點進行控管，。 |

### 

# 輸出文件記錄

### SC-01-004-F01\_資訊資產盤點清冊。