INFORMATION SECURITY | RISK MANAGEMENT

海韻電子工業股份有限公司

SEASONIC ELECTRONICS CO., LTD.

# 資通安全風險管理程序

*Information Security Risk Management Procedure*

版本 v2026.04 發行日期 2026 年 04 月 24 日

# 目　錄

*TABLE OF CONTENTS*


01 目的與適用範圍 P.3
*Purpose & Scope*

02 資通安全風險管理組織與架構 P.3
*Governance & Organization*

03 資通安全政策與風險管理流程 P.4
*Policy & Risk Management Process*

04 具體管理方案與控制措施 P.5
*Management Programs & Controls*

05 資安事件通報應變與危機處理 P.6
*Incident Response & Crisis Management*

06 具體管理方案彙總表 P.7
*Summary of Control Measures*

07 投入資通安全管理之資源及運作情形 P.9
*Resources & Operations*

# 01 目的與適用範圍

*Purpose & Scope*

## 目的

建立系統化流程以辨識、評估並處置資訊資產風險，將風險降低至可接受程度，確保資訊之機密性 (Confidentiality)、完整性 (Integrity) 與可用性 (Availability)。

## 適用範圍

本程序適用對象涵蓋全體員工、委外廠商及訪客；適用之資訊資產包含但不限於下列項目：

- 資通系統與相關設備（伺服器、終端電腦、儲存媒體等）
- 公司內部與對外網路、無線網路及備份系統
- ERP、PLM、人事薪資、Email 等核心應用系統
- 公司營運所產生及處理之各類電子與實體資訊資產

# 02 資通安全風險管理組織與架構

*Governance & Organization*

本公司組織結構設有資訊部，並依下列職責劃分推動資通安全風險管理工作：

| 組織單位 | 職責與權限 |
| --- | --- |
| 董事會 | 督導資通安全與風險管理之執行；稽核發現缺失時，要求受查單位提出改善計畫並定期追蹤改善成效。 |

| 組織單位 | 職責與權限 |
| --- | --- |
| 總經理 | 統籌推動全公司資安風險管理工作，整合跨單位資源並核定相關政策。 |
| 資安長 / 資訊部 | 由資訊主管兼任資安長，配置資訊專責人員，負責電腦網路與系統維護、資訊安全規劃與執行、資產盤點、風險評估及教育訓練。 |
| 稽核室 | 擔任資訊安全監理之查核單位，獨立稽核資安控制措施，確保內部資安風險得以有效降低。 |

## 03 資通安全政策與風險管理流程

*Policy & Risk Management Process*

由資訊部統籌推行並落實各項資通安全作業，核心流程如下：

### 核心業務與權限管控

權限申請須經直屬主管依業務需求審查，並由系統管理者設定程式化控制措施，以符合相關法律、法規與營運要求。

### 資產盤點與風險評估

每年至少一次盤點資通系統，建立並維護資訊資產清冊，內容包含資產類別、威脅、脆弱點與風險等級。

- **資產評價（CIA）**

| 評估面向 | 評估說明 |
| --- | --- |
| **機密性 (C)** | 依資料機密程度區分為低、中、高、極高四個等級。 |
| **完整性 (I)** | 評估資料若遭未授權更動或損毀，對營運產生之影響程度。 |
| **可用性 (A)** | 評估系統能否隨時被授權使用者依需求正確存取與運作。 |

### ● 威脅鑑別與風險處理

比對 CVE 漏洞資訊及廠商安全公告，並檢視設備老化、人為疏失等脆弱點。依「資產重要性 × 發生機率 × 衝擊程度」計算風險值，並區分為下列等級：

| 風險等級 | 分類 | 處理原則 |
| --- | --- | --- |
| C 級 | **高風險** | 必須採取降低、避免或移轉等積極處理措施。 |
| D 級 | **中低風險** | 屬可接受範圍，惟須持續監控與定期再評估。 |

## 系統發展及維護

資安要求（包含機敏資料存取控制、身分驗證、輸入輸出過濾等）必須納入系統開發與維護之需求規格，於設計階段即予以落實。

## 委外辦理管理

委外作業（如設備維護、系統開發等）應簽訂契約並納入保密條款；業務完成後應要求委外廠商提供詳細系統手冊；若有派駐人員，須對其電腦系統使用權限進行適當控管。

# 04 具體管理方案與控制措施

*Management Programs & Controls*

## 網路安全

建置防火牆並定期檢視規則、關閉不必要之服務、自動過濾惡意程式或勒索病毒網站。依網路服務區隔獨立邏輯網域（包含開發、測試與正式作業環境）。無線網路使用前須經安全評估並採用加密通訊協定。

## 電腦與系統安全

各式電腦應及時進行安全修補、安裝並自動更新防毒軟體；電腦均須設定螢幕保護與密碼，並由資訊單位統一管理軟體版權。現有進階控制措施包含 DLP（資料外洩防護）、MDR、防火牆訂閱防護及弱點掃描。

## 帳號與密碼管理

賦予獨立通行帳號並採最低權限原則；職位異動或離職時立即調整權限。密碼設定須達一定強度且加密保存，輸入時不得明碼顯示。

## 資料安全與備份

機房採門禁管制，資料庫每日備份並建立異地備援機制。各部門重要檔案由資訊部統一備份至伺服器；報廢儲存媒體時須徹底銷毀資料至無法解讀。

## 人員安全與教育訓練

處理機密資訊人員須簽署保密協定，各項資訊安全工作須有 2 人（含）以上瞭解，以因應緊急情況。每年至少辦理一次資安教育訓練，並不定期執行電子郵件社交工程演練，以提高員工資安意識

並防止個資外洩。

# 05 資安事件通報應變與危機處理

*Incident Response & Crisis Management*

## 事件通報與緊急應變

發現異常時，依下列流程處置：

**◆ 緊急應變標準作業程序**

**① 偵測異常 → ② 確認受駭設備 → ③ 觀察行為**

**④ 中斷或隔離 → ⑤ 回報主管 → ⑥ 啟動危機處理**

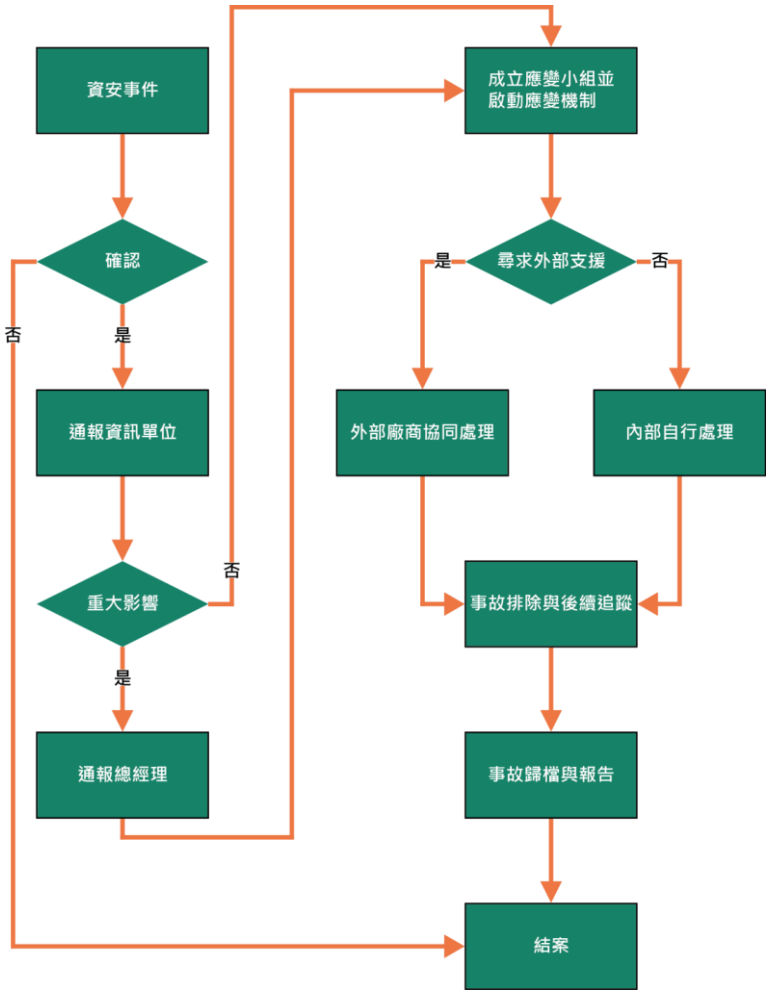
各部門發生資安事件時，應於第一時間通報資訊專責人員並依其指示執行應變措施。

## 危機處理與災害復原

由資訊部與業務主管聯合判定事件影響範圍與損害評估；內部通報由資訊人員執行，外部主管機關通報則依公司「重大資訊處理程序」辦理。處理重點包含降低損害、保護資產、分析原因、撰寫報告並追蹤結案。針對重大業務衝擊威脅，應制定災害復原計劃以確保企業持續營運。

## 通報流程圖

下圖呈現資安事件通報與應變之標準作業流程：




# 06 具體管理方案彙總表

*Summary of Control Measures*

本公司具體管理方案及控制措施彙整如下表，依管理類別分項列示對應之控制重點與作法。

| 類別 | 採行措施 | 具體作法 |
| --- | --- | --- |
| 網路安全 | 網路資源管理 | ■ 關閉網路設備不使用之服務與功能，以降低風險暴露面。<br>■ 建立網路監控系統，及時掌握網路運作情況，及早發現網路失效情形或潛在風險。 |
| | 網路安全管理 | ■ 於公司內部網路與外部網路接界處設置防火牆(Firewall)，並定期檢視防火牆規則以確認設定適當。<br>■ 不定期委由外界專家或自行評估網路系統安全並進行安全修補，提高安全防禦能力。<br>■ 對外連線資訊系統依重要性採取資訊加密、身分辨別、電子簽章等不同安全等級之技術或措施。<br>■ 自動過濾使用者上網可能連結到含有木馬病毒、勒索病毒或惡意程式之網站。<br>■ 如有特殊連線需求，須額外申請並經核准後始可開放。 |
| | 無線網路安全 | ■ 無線網路架設與使用須經審慎之安全評估。<br>■ 無線網路卡與無線基地台間採用加密通訊協定。 |

| 類別 | 採行措施 | 具體作法 |
| --- | --- | --- |
| 電腦安全 | 電腦系統與實體設備保護 | ■ 各式電腦系統應及時進行安全修補。<br>■ 各式電腦軟體及版權集中由資訊單位管理。<br>■ 任何電腦均應設定螢幕保護程式並啟用密碼保護，防止他人未經授權使用。<br>■ 使用任何電腦設備時，注意電源使用不可超過電源負載量。<br>■ 廠商維護電腦主機設備時，應有公司資訊單位人員陪同。 |
| | 防毒軟體 | ■ 公司所有電腦系統均安裝防毒軟體，自動更新病毒碼並定期執行病毒掃描。 |
| | 存取安全 | ■ 每位電腦系統使用者賦予獨立通行帳號，依業務需求採最低權限原則。<br>■ 員工離職或職位調動時，立即取消或調整其帳號權限。<br>■ 定期審查帳號及使用權限狀況，確保符合現況。 |
| | 密碼安全管理 | ■ 所有通行帳號之登錄須設立獨立密碼，並達一定強度設定原則。<br>■ 輸入密碼時，電腦螢幕不得明碼顯示所輸入之密碼。<br>■ 保存密碼之檔案應予加密。 |

| 類別 | 採行措施 | 具體作法 |
| --- | --- | --- |
| 應用系統管理 | 電子郵件使用安全 | ■ 明確規定員工禁止利用公司電子郵件從事工作業務以外活動，並宣導員工不開啟來路不明之電子郵件。<br>■ 啟用郵件過濾及防毒機制，過濾垃圾郵件及可能含有病毒之郵件。<br>■ 個人電腦接收郵件後，防毒軟體將進一步掃描郵件附件是否安全。 |
| | 資料安全與備份 | ■ 機房採門禁管制，限定特定人員方可進入；資料庫每日備份並建立異地備援機制。<br>■ 公司各部門重要檔案存放於伺服器，由資訊部統一備份保存。<br>■ 任何資料儲存媒體報廢時，須徹底銷毀其內資料，直至無法解讀為止。<br>■ 實體機密資料（如紙本檔案、重要合約等）應妥善存放與保管。 |
| | 異常事件處理程序及災害復原計劃 | ■ 針對常見資安事件與異常情況，擬定異常事件處理程序，提升處理時效並降低事件衝擊。<br>■ 依企業持續經營原則，評估並釐清重大業務衝擊威脅事件，據以制定災害復原計劃。 |

| 類別 | 採行措施 | 具體作法 |
| --- | --- | --- |
| 人員安全 | 人員安全管理 | ■ 對公司資訊單位人員之職責進行明確定義。<br>■ 負責資訊安全相關工作或處理機密資訊之人員，須簽署保密協定。<br>■ 各種資訊安全工作須有 2 人（含）以上瞭解，以因應緊急情況之需要。 |
| | 安全認知訓練 | ■ 資訊安全事件應立即公告全體員工。<br>■ 不定期提供員工適當之資通安全認知或教育訓練。 |
| 委外管理 | 委外管理 | ■ 資訊委外時，應與委外廠商簽訂契約並納入保密條款。<br>■ 電腦系統資訊委外業務完成後，應要求委外廠商提供詳細之系統檔案及操作手冊。<br>■ 委外廠商人員如有派駐公司情況，其電腦系統使用權限應予以適當控管。 |

## 07 投入資通安全管理之資源及運作情形

*Resources & Operations*

◆ **資安資源投入重點**

- 針對系統主機之作業系統及重要軟體升級、災害復原演練等重要資安工作，定期檢討規劃進度並追蹤執行成效。
- 透過不定期之社交工程演練及資安健檢服務，評估使用者資訊安全認知是否充分。
- 檢視資訊設備資源投入及系統配置是否存有漏洞，並依評估結果編列年度資安預算後執行。

*—— 文件結束 | END OF DOCUMENT ——*