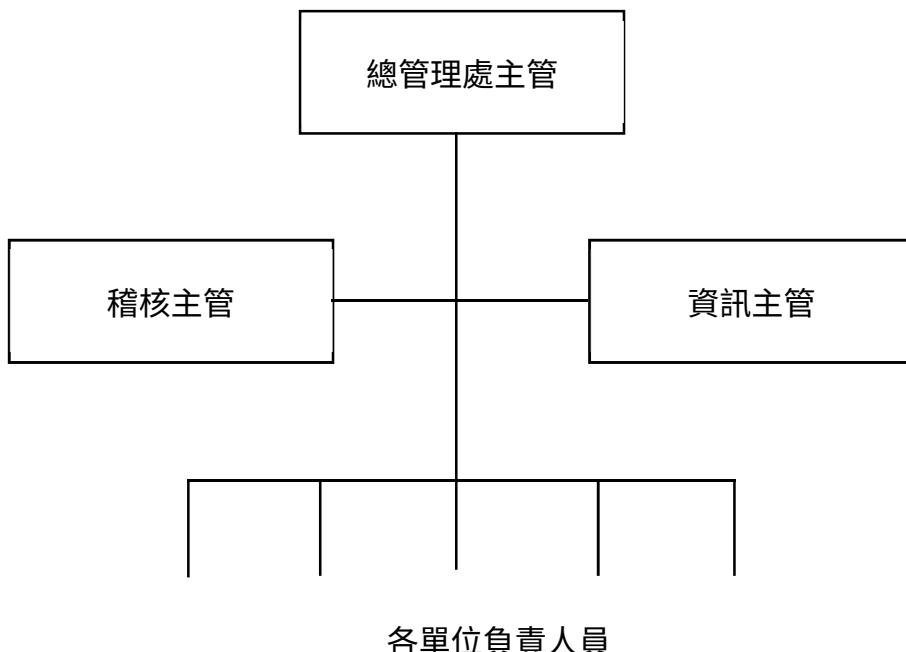


# 資通安全管理策略與架構

## 壹、資通安全風險管理架構

一、資通安全管理單位隸屬於總管理處，資通安全管理架構請參閱下圖，由總管理處最高主管擔任資通安全最高主管、資訊部主管擔任主要執行人員、稽核主管負責作業執行監督，轄下各單位負責人員，負責訂定內部資通安全政策、規劃暨執行資通安全作業與資安政策推動及落實。

## 資通安全管理單位



二、稽核室為資通安全監理之督導單位，負責督導內部資安執行狀況，若有查核發現缺失，旋即要求受查單位提出相關改善計畫，並追蹤改善成效，以降低內部資安風險。

## 貳、資通安全政策遵循說明：

- 一、防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）訂定的規範，並以每半年進行「資通安全檢查控制」九大項目點檢稽核。
- 二、用以規畫（Plan）→執行（Do）→稽核（Check）→矯正預防（Action）方式運行，旨在保護資訊資產的機密性、完整性及可用性。
- 三、為落實保護資訊資產的機密性、完整性及可用性，組織應持續進行：
  1. 提升資安共識，強化資安訓練。
  2. 健全資安防護，確保營運持續。

# 資通安全管理策略與架構

## 參、具體管理方案

### 一、投保資安險

### 二、網路

1. 建置網路防火牆。
2. 強化防火牆與網路的安全，每年簽訂維護合約，即時更新防火牆上的安全防護如：入侵偵測、病毒，網頁等。
3. 內對內、內對外各由不同政策控管來區隔，服務端只開啟該服務端口，禁止非服務端口連接。
4. 外對內有 VPN 的權限控管與服務器端口之控管。
5. 跨廠區的端點經由另一台防火牆控管，另由權限政策來管制防護。
6. 建置防毒系統，電腦端點的防護防止惡意程式與病毒等。
7. 電子郵件過濾病毒、廣告信、網路釣魚信機制。
8. 即時監控網路服務運作狀況。

### 三、備份儲存

1. 建立備份、備援系統。
2. 重要資料實施熱備份。
3. 重要資料實施離線備份。
4. 重要資料實施異地備份。
5. 重要資料備份三份以上。
6. 每日檢查備份狀況。
7. 重要資料每月實施備份資料還原測試。

### 四、人員

1. 每位人員配發專屬帳號及密碼。
2. 定期實施電子郵件社交工程演練。
3. 定期實施資通安全教育訓練及考試，提升員工資安意識。
4. 定期實施電子郵件及防毒的資訊安全宣導。
5. 定期檢查防毒軟體運作情況。
6. 端點防護監控使用者安裝軟體。
7. 定期稽核使用者安裝軟體。

# 資通安全管理策略與架構

## 肆、資通安全應變作業

### 一、目的

為使本公司在發生資通安全事件時之通報及應變機制有所遵循，藉以迅速有效處理事件，特制定本作業要點。

### 二、適用範圍

凡發生於本公司之資通系統、服務或網路狀態，經鑑別顯示可能有違反資通安全疑慮或保護措施失效之狀態發生，而影響資通系統機能運作，構成資通安全之威脅者均屬之。

### 三、工作職責

本公司資訊主管亦為資安判定窗口，發現資通安全事件時，應依事件等級判斷資通安全事件通報及完成應變作業。

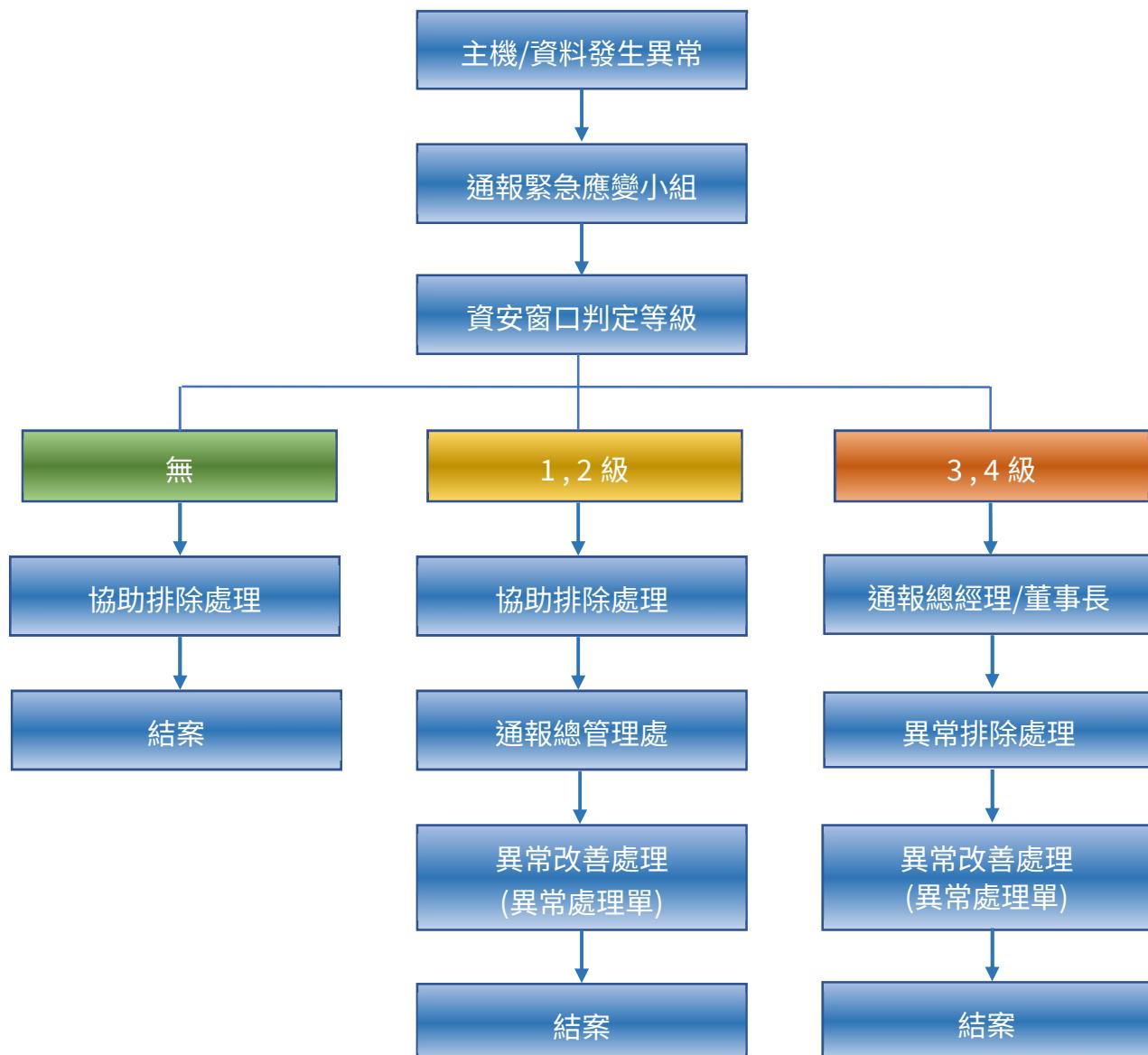
本公司資訊部門為緊急應變小組，負責發生資通安全異常事件時，異常處理及改善。

## 事件等級判斷

| 評估類別<br>影響等級 | 機密性               | 完整性              | 可用性   |
|--------------|-------------------|------------------|---|
| 1 級          | 非核心業務資料遭洩露        | 非核心業務系統或資料遭竄改    | 非核心業務運作遭影響或短暫停頓<br><br><b>(屬單獨電腦等級)</b>                         |
| 2 級          | 非屬密級或敏感之核心業務資料遭洩露 | 核心業務系統或資料遭輕微竄改   | 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。<br><br><b>(屬辦公室區域)</b>        |
| 3 級          | 密級或敏感公務資料遭洩露      | 核心業務系統或資料遭嚴重竄改   | 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。<br><br><b>(屬一級廠處理範圍)</b>        |
| 4 級          | 公司機密資料遭洩露         | 重要資訊基礎建設系統或資料遭竄改 | 重要資訊基礎建設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。<br><br><b>(超過一級廠處理範圍)</b> |

# 資通安全管理策略與架構

## 資安通報機制



### 伍、重大資通安全事件：

最近年度及截至 2025 年止，未有重大資通安全事件。

### 陸、投入資通安全管理之資源(執行情形)：

- 教育訓練執行情形：  
2025 年執行情形：本年度完成教育訓練人數：67 人，完訓率：100%。
- 電子郵件社交工程演練執行情形：  
2025 年執行情形：本年度寄送演練電子郵件 335 封，演練結果點閱連結計 17 筆(百分比為 25%)，開啟附件計 16 筆(百分比為 24%)，輸入機敏資料 8 筆(百分比為 12%)，針對以上同仁特別關心輔導。
- 資安公告：製作超過十份資安公告，傳達資安防護重要規定與注意事項。