## 1.0 資訊安全政策：

### 1.1 定　義：

資訊（有形或無形）是公司的資產，包括資訊資產、實物資產、軟件資產、服務資產、文件、人員等；安全是使用主動或被動方法來保護或維護環境，使其活動不受干擾。因此，資訊安全就是使用一套適當的控制措施，包括政策、實踐、程序、組織結構和軟件功能，以避免因人為錯誤、故意或自然災害引起的風險，以確保公司的資產得到適當的保護。

### 1.2 目　的：

即確保資訊的機密性（只有被授權的人才能訪問信息）、完整性（確保資訊及其處理方法的準確性和完整性）和可用性（確保授權用戶在需要時可以訪問信息並使用相關的信息）。

保護公司資訊資產不被不當使用、洩露、篡改、破壞等，確保資訊收集、處理、傳輸、存儲和流通的安全。

### 1.3 範　圍：

涵蓋電腦技術和人事管理的相關範圍。

(1) 參與人員

涵蓋使用公司資訊資源的公司公務人員、簽約人員和外包供應商人員。

(2) 應用系統

1. ERP 套裝軟件
2.應用軟件及研發所需軟件
3.郵件系統
4. APS、B2B、MES、WMS、HR、CRM、BI、PDM 系統及研發所需各類系統
5.互聯網應用

(3) 硬件設備

各種主機、服務器、個人電腦和筆記本電腦、隨身碟等。

(4) 網絡及其設施和管理軟件

公司總部大樓、廠區和分公司局域網、無線 AP，以及連接辦公室、互聯網專線和數據相關的網絡設施和管理軟件。

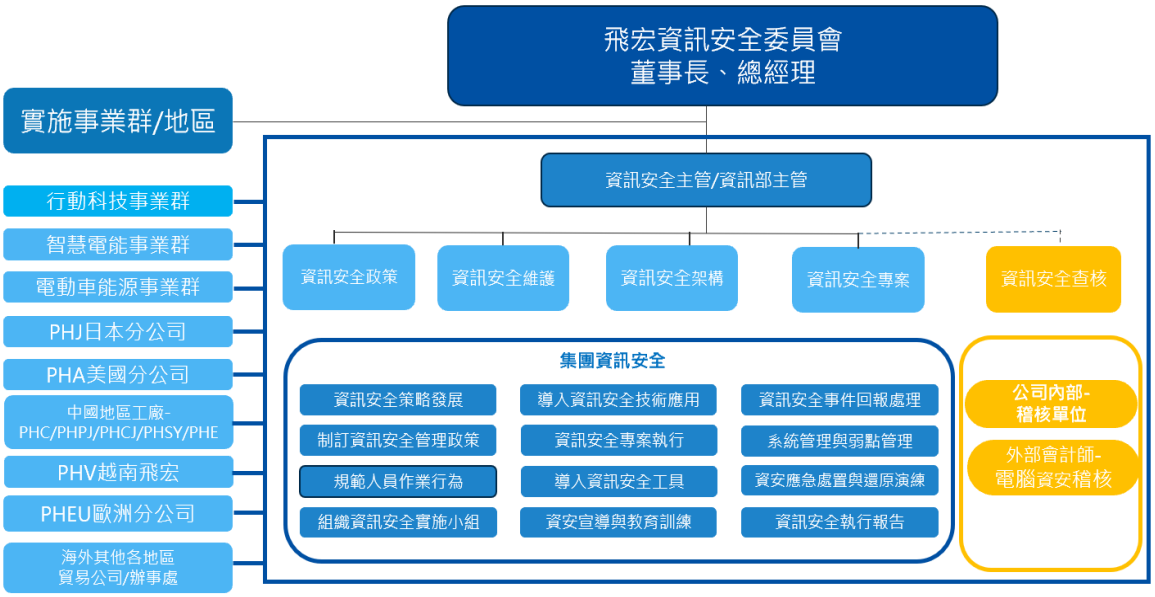
### 1.4 內　容：

- 成立資訊安全委員會，負責推進公司資訊安全工作。
- 相關人員錄用及離職應簽署保密文件，異動或離職時應歸還其資訊資產、新進與現任同仁均須參與資訊安全教育訓練，以提昇資訊安全防護之認知觀念。
- 建立資訊資產的保管制度，有效分配、運用及管理本公司資訊資源。
- 考量建築物之防害、防竊設計，重要設施及特殊場所應加強管制。
- 提昇電腦網路防禦技術，適時阻絕外界之入侵、破壞。
- 評估資訊資產之安全等級，並賦予相關人員適當存取權限。
- 各項電腦系統之新增或變更作業應建立控管制度並完整予以記錄，以備查考。
- 建立資訊安全事件緊急處理機制與災後重建計畫，並反覆操演、測試。
- 建立資訊安全稽核制度，就本公司電腦主機房、各工廠及分公司各項電腦系統安全進行定期或不定期之稽核作業，且嚴禁刪除及修改各項稽核記錄檔案。
- 遵守公司各項操作規範及相關資訊規定。
- 防止公司重要機密文件外洩。

## 2.0 資訊安全風險管理架構：

本公司資訊安全之權責單位為資訊部，該部設置資訊安全主管，及專業資訊人員。
負責規劃、訂定及執行資訊安全策略，並定期檢討資安政策。
資訊安全管理作業執行情形，若有查核發現缺失，旋即要求受查單位提出相關改善計畫與具體作為，
且定期追蹤改善成效，以降低內部資安風險。
且公司配合的外部會計師事務所每年也會定期派人針對資訊單位進行資訊安全的相關稽核並追蹤改善成效。
組織運作模式採定期稽核與循環式管理，確保可靠度目標之達成且持續改善。

## 2.1 成立資訊安全委員會：




## 2.2 資訊安全風險評估：

本公司並未投保資安險，為降低資訊安全風險，採取資訊安全風險評估程序如下。

| 鑑別關鍵業務流程 | 風險分析與處理 | 成效追蹤 |
|---|---|---|
| IT 人員<br>一般使用者 | 資產盤點<br>弱點分析<br>風險評估<br>評估對策<br>執行改善作業 | 評估成效<br>營運衝擊分析 |

## 2.3 資訊安全管理機制：

(1)制度規範：訂定公司資訊安全管理制度，規範人員作業行為。

(2)科技運用：建置資訊安全管理設備，落實資安管理措施。
建置各式資安防護系統，以提昇整體資訊環境之安全性。
為確保內部人員之作業行為符合公司制度規範，亦導入資安系統工具，落實人員資訊安全管理措施。

(3)人員訓練：進行資訊安全教育訓練，提昇內部同仁資安意識。
每年定期實施內部人員資訊安全教育訓練實務課程，並建置數堂線上學習 (E-Learining) 資訊安全課程，藉以提昇內部人員資安知識與專業技能。

(4)政策檢討：推動資訊安全持續改善，確保企業永續經營。

## 2.4 資訊安全管理具體措施：

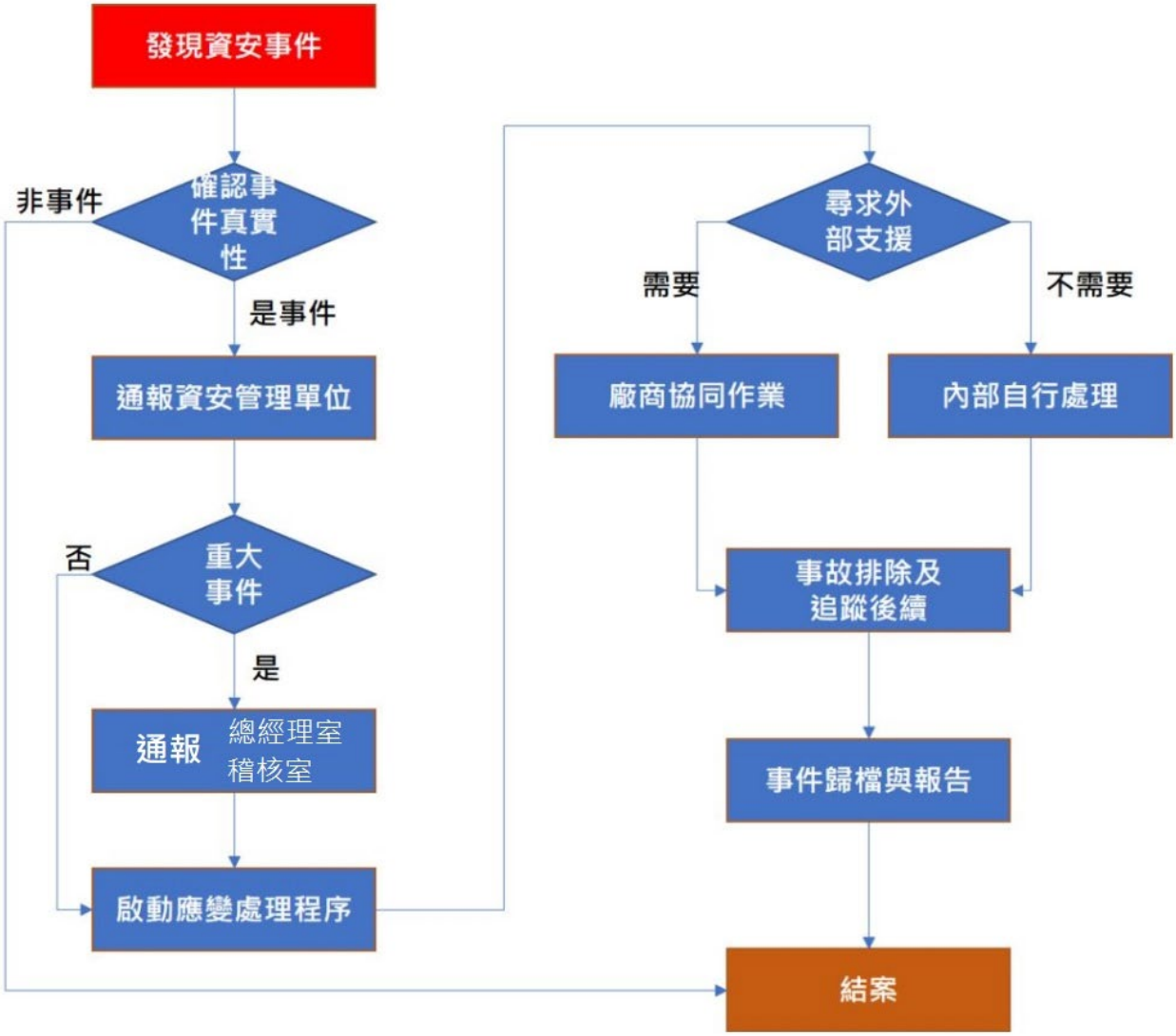
| | | |
|---|---|---|
| 權限管理 | 人員帳號、權限管理與系統操作行為之管理措施 | 內部人員帳號權限管理與審核 |
| 存取控管 | 人員存取內外部系統及資料傳輸管道之控制措施 | 內/外存取管控措施<br>資料外洩管道之控制措施<br>操作行為軌跡記錄分析 |
| 外部威脅 | 內部系統潛在弱點、中毒管道與防護措施 | 主機/電腦弱點檢測及更新措施<br>病毒防護與惡意程式偵測 |
| 弱點分析 | 針對 PC 與伺服器系統弱點掃描與檢查、修補措施 | 定期演練 |
| 社交工程演練 | 針對人員存取外部郵件訊息強化資安措施 | 定期演練 |
| 教育訓練 | 針對使用者同仁定期宣導資安觀念 | 定期演練 |

2.5 資訊安全管理方案

採用 PDCA（Plan-Do-Check-Act）循環流程管理模式，確保可靠度目標之達成且持續改善。

| | |
|---|---|
| Plan | 資安管理：製訂公司資訊政策與安全作業流程 |
| Do | 推動執行：資安宣導與人員教育訓練、資安措施導入 |
| Check | 風險評估：資訊資產風險評估 |
| Act | 風險改善：改善內部作業程序、引進外部資源 |

2.6 資訊安全事件通報程序：




3.0 相關文件：

3.1 電子資訊管理程序(PHG-C2-AI01)

4.0 相關表單：

4.1 資訊安全事件通報處理記錄單