

## 資通安全管理

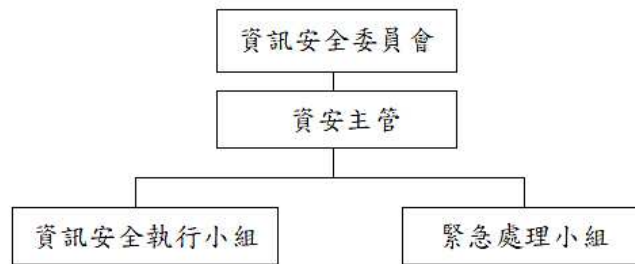
### (一) 資通安全風險管理架構

#### 1. 企業資訊安全治理組織

為落實本公司資訊安全，108 年成立「資訊安全委員會」(簡稱資安委員會)任務組織，負責推動與統籌資訊安全管理系統之建置及維運事宜。

稽核室將資通安全檢查列入每年年度稽核計畫之項目，並定期向董事會呈報資訊安全稽核報告。

#### 2. 資訊安全組織架構



資訊安全委員會職掌：

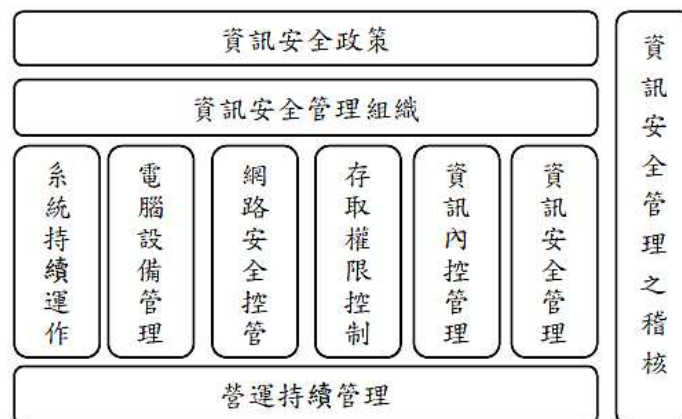
- (1) 資訊安全委員之組成：依據公司組織架構，直屬於總經理的單位，其單位之最高主管為資訊安全委員之組成。
- (2) 資安主管：  
資訊安全委員會設置資安主管 1 人，得由資訊部門最高主管兼任。
- (3) 資訊安全執行小組：  
含資訊安全人員，負責規劃及執行各項資訊安全作業。
- (4) 緊急處理小組：  
各項關鍵業務流程負責人擔任組員。

### (二) 資通安全政策

#### 企業資訊安全管理策略與架構

公司內部已建立資安相關依循的規範，針對電腦設備、網路環境、軟體系統等皆有權限設定及安全控管。系統架構也強化備援及備份機制，確保系統在遭遇資安事件後能快速並順利恢復運作。

公司定期進行內部資訊安全管理稽核與審查，針對缺失部份進行矯正並採取預防措施，強化資訊安全機制及防護等級。



### (三) 具體管理方案

#### 1、電腦設備安全管理

- 伺服器等主要設備均設置於專用機房，機房門禁採用感應刷卡進出，且保留進出紀錄存查
- 電腦設備安裝端點防護軟體，病毒碼自動更新，確保能有效偵測病毒，強化惡意軟體行為偵測。
- 機台設備入廠上線前需經過掃毒程序，防止內含病毒或惡意軟體的機台進入廠內。

#### 2、網路安全管理

- 連外網路設置防火牆控管、連外伺服器安裝端點防護及入侵偵測軟體，偵測並阻擋外部入侵及攻擊行為。
- 內部網路設置攻擊行為偵測設備，及早偵測內部網路電腦異常感染行為，快速找出感染源。

#### 3、存取權限控制

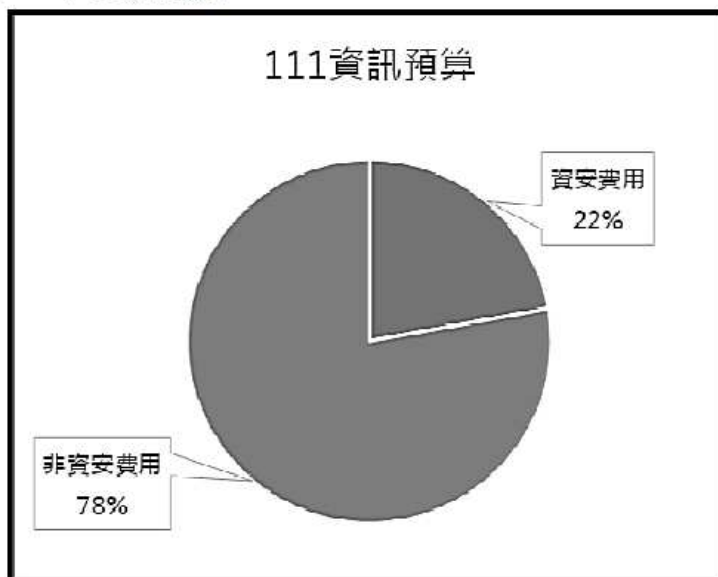
- 使用單位依所需之資訊功能、電腦應用系統及程式使用提出權限申請，並經單位主管及資訊單位主管根據其工作職責及系統授權表核准後，由系統管理者設定其使用權限。
- 重要文件資料限制權限存取及加密控管。
- 人員調職、離職時，資訊單位依異動資料適時修改或取消其帳號及使用權限，確保資訊安全。

#### 4、系統的持續運作

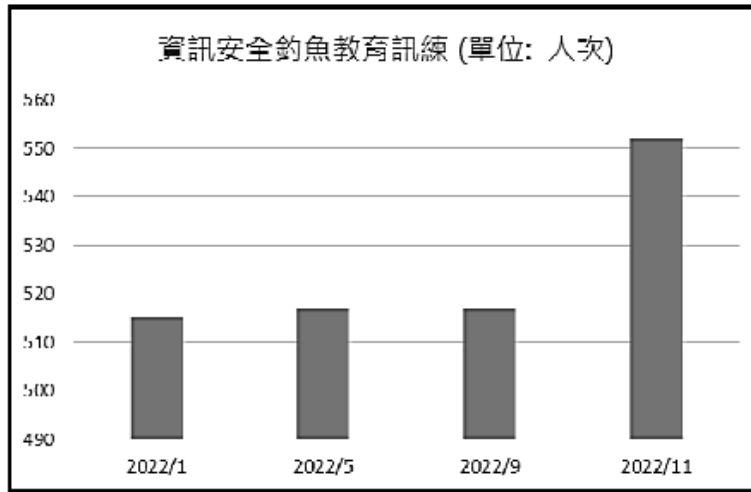
- 機房主機配置不斷電與穩壓設備，並連結公司的發電機供電系統，防止停電或供電異常造成之系統損壞。
- 建置即時異地備援架構，當本地端機房因災害失去功能時，可由異地端備援主機及儲存設備啟動相關服務。
- 強化資料備份及復原機制，除每日排程進行儲存媒體備份外，亦啟用儲存裝置的定時 Snapshot(快照)功能備份，加強系統復原完整度及效率。

### (四) 投入資通安全管理之資源

#### 1. 111 年度資訊預算



## 2.111 年度共進行 4 次電子郵件社交工程演練



3.所有新進員工皆完成資訊安全教育訓練。

4.為降低資安事件造成之損失，本公司於 111 年度協同母公司力成集團購買資安保險，總保障額度為 USD500 萬元。