資通安全管理執行情形

(1)資通安全風險管理架構

本公司資訊安全之權責單位為資訊中心，設置資訊主管一名，及專業資訊工程師數名，負責訂定公司資訊安全政策，規劃資訊安全措施，並執行相關之資訊安全作業。

(2)資通安全政策

①維持各資訊系統持續運作

②防止駭客、各種病毒入侵及破壞

③防止人為意圖不當及不法使用

④防止機敏資料外洩

⑤避免人為疏失意外

⑥維護實體環境安全

(3)具體管理方案及投入資通安全管理之資源

①電腦設備安全管理

- 本公司各應用伺服器等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。
- 機房內部備有獨立空調，維持電腦設備於適當的溫度環境下運轉；並放置二氧化碳滅火器，可適用於一般或電器所引起的火災。
- 機房主機配置不斷電與穩壓設備，避免台電意外瞬間斷電造成系統當機，或確保臨時停電時不會中斷電腦應用系統的運作。

②網路安全管理

●與外界網路連線的入口，配置企業級防火牆，阻擋駭客非法入侵，設置DMZ 隔開對外服務，採獨立網段處理。

●廠內設置內部防火牆，廠區分為多個獨立網段，可侷限災害影響範圍。

●台灣、東莞、寧波、印度、印尼 site to site 的連線作業，採用MPLS(MultiProtocolLabel Switching)技術來建置加密連線，建構一個虛擬的、獨立的及安全的路由交換環境，避免資料傳輸過程遭受非法擷取。

●同仁由遠端登入公司內網存取ERP 系統，必須申請VPN 帳號，透過VPN 的安全方式始能登入使用，且均留有使用紀錄可稽查。

●配置上網行為管理與過濾設備，透過DDoS 攻擊的異常流量提供監控與管理、深度封包檢測(DPI)、入侵預防系統(IPS)，可控管網際網路的存取，並屏蔽訪問有害或政策不允許的網路位址與內容，利用TLS / SSL 加密流量檢查、整合第三方身份管理、QoS 頻寬管理強化網路安全，並防止頻寬資源被不當占用。

③病毒防護與管理

●伺服器與同仁終端電腦設備內均安裝有端點防護軟體，病毒碼採自動更新方式，確保能阻擋最新型的病毒，同時可偵測、防止具有潛在威脅性的系統執行檔之安裝行為。

●電子郵件伺服器配置有郵件防毒、與垃圾郵件過濾機制，防堵病毒或垃圾郵件進入使用者端的PC。

④系統存取控制。

●同仁對各應用系統的使用，透過公司內部規定的系統權限申請程序，經權責主管核准後，由資訊中心建立系統帳號，並經各系統管理員依所申請的功能權限做授權方得存取。

●帳號的密碼設置，規定適當的強度、字數，並且必須文數字、特殊符號混雜，才能通過，並規定定期更換。

●同仁辦理離職手續時，必須會辦資訊中心，進行各系統帳號的刪除作業。

⑤確保系統的永續運作。

●系統備份：建置日備份機制的NAS 備份系統，遵守321 備份法則，將資料備份3 份並儲存在2 種不同設備上，定期同步1 份存放異地且實施離線保存。經由複數備份、異地存放方式，降低資料完全漏失的機率，以確保系統與資料的安全。

●災害復原演練：各系統每年實施一次演練，選定還原日期基準點後，由備份媒體回存於系統主機，確保備份媒體的正確性與有效性。

●租用電信公司兩條數據線路，透過頻寬管理設備，兩線路並聯互為備援使用，確保網路通訊不中斷。

⑥資安宣導與教育訓練

●提醒宣導：要求同仁定期更換系統密碼，以維帳號安全。

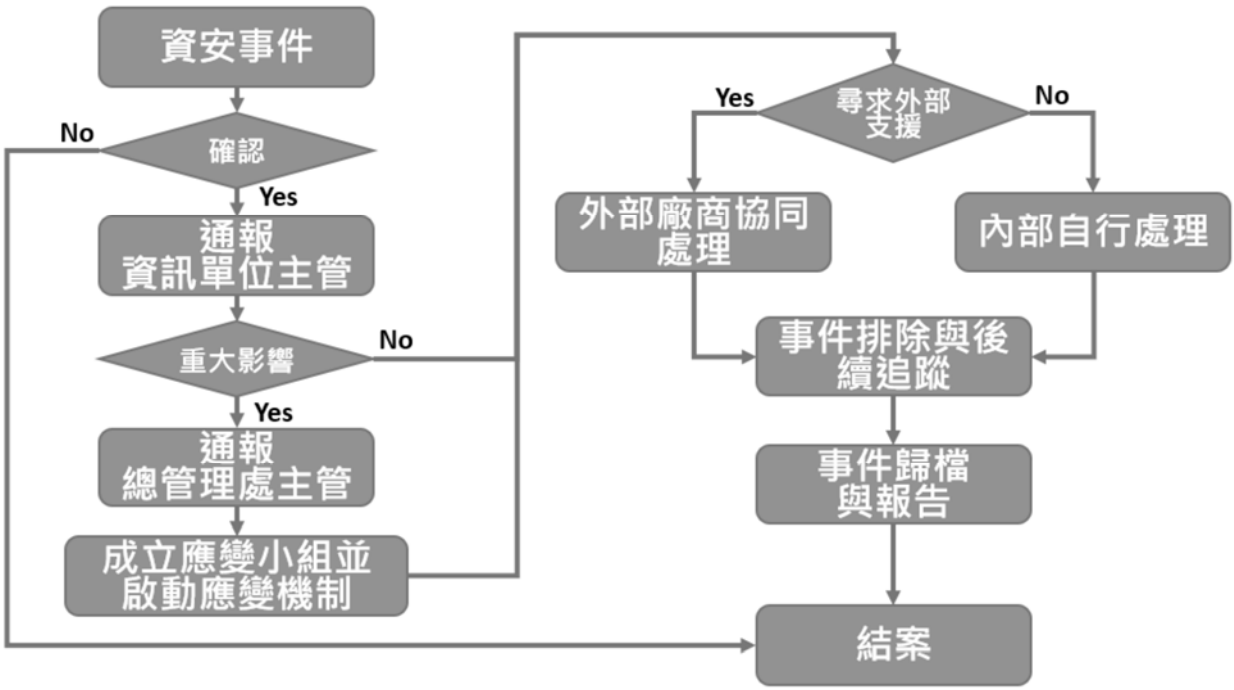
●社交工程演練：每年定期二次全公司社交工程演練，避免不當郵件行為造成資安風險。

●資安新知：每月對內部同仁發送一篇集團內資安狀況與提醒現行資安危害的手法。

●講座宣導：提供新進及在職同仁資訊安全認知教育訓練，以提昇同仁資訊安全意識。

⑦.資訊安全通報

●資安事件之通報與處理，皆遵守下列流程之規範進行，如圖一。



圖一、資訊安全通報與處理流程