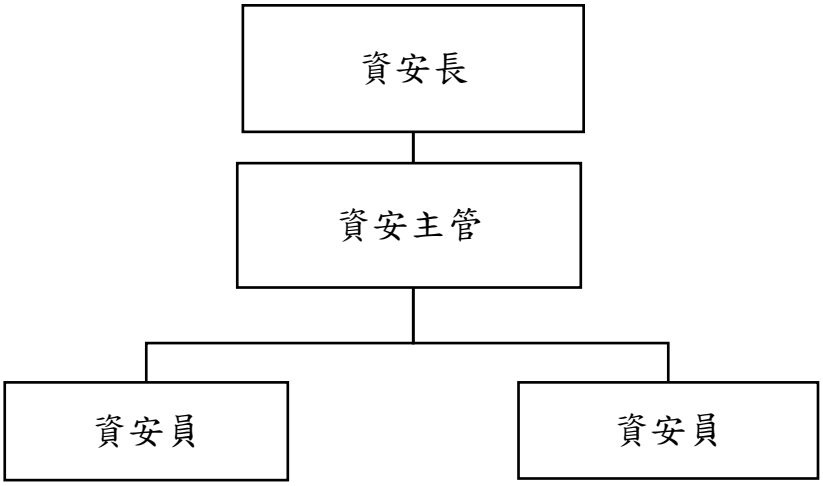
資通安全管理

本公司資通安全權責單位為資訊處，負責訂定安全政策、規劃暨執行安全作業與資安政策推動與落實。

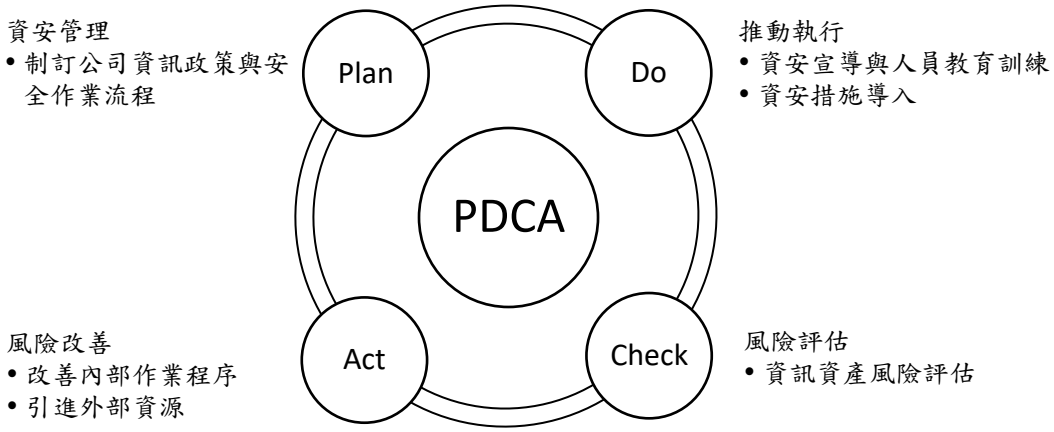
資訊安全組織

為強化本公司之資訊安全管理、確保資料、系統及網路安全，設立資安管理室，為資安專責單位，包含資安長、資安主管及至少兩名以上的資安人員，負責資通安全事務的規劃與執行。其中，資安長至少每年一次於董事會中報告重大議題或規劃。



資訊安全風險架構

主要之運作模式公司採用 PDCA （Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。



一、 資訊安全政策

本公司資訊安全管理機制，包含以下三個面向：

A. 制度規範：訂定公司資訊安全管理制度，規範人員作業行為。

B. 硬體建置：建置資訊安全管理系統，落實資安管理措施。

C. 人員訓練：定期進行資訊安全教育訓練，以提昇全體同仁資安意識。

D.

二、 資訊安全管理措施

(1) 制度規範：本公司內部訂定相關資訊安全規範與制度，以規範本公司人員資訊安全行為，每年定期檢視相關制度是否符合法規與營運環境變遷，並依需求適時調整。

(2) 硬體建置：本公司為防範各種外部資安威脅，除採多層式網路架構設計外，更建置各式資安防護系統，以提昇整體資訊環境之安全性。

(3) 人員訓練：本公司每一年開設資訊安全教育訓練課程，所有同仁每年最少應修習前述課程一次，因工作關係而無法參與前述實體課程者，本公司另設有資訊安全之線上講習課程，藉以提昇內部人員資安知識與專業技能。同仁如未經由前述實體或線上課程完成該年度之資訊安全課程者，資訊處與管理部將列管追蹤，並列為年度考績之檢核項目。

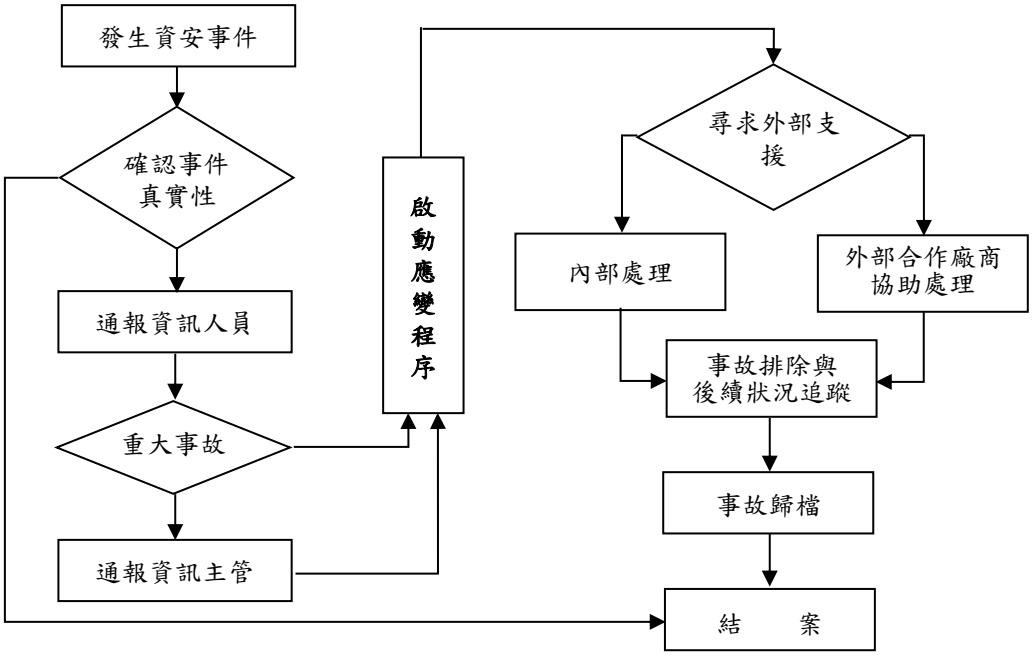
三、 本公司目前資訊安全相關具體執行措施如下：

項目	**具體管理方式**
防火牆防護	• 防火牆設定連線規則。 限定各項服務，如網站、FTP、郵件依權限存取網路可使用範圍 • 如有特殊連線需求需額外申請開放。 如有使用者有 80、443 標準 PORT 以外需求，如視訊會議、遠端存取需求 、FTP 下載需依上網權限單提出申請。 • 監控分析防火牆數據報告。 每週防火牆系統產出資訊安全分析報告，由資訊專責人員彙整
使用者上網控管機制	• 使用自動網站防護系統控管使用者上網行為。 限定使用者依權限存取網路可使用範圍，並自動阻擋色情、遊戲、比特幣 、賭博等違規網站。 • 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。 過濾系統會自動過濾有威脅網站，有毒附件及程式等，並攔截可能威脅。
防毒軟體 RGP-06-12	• 使用多種防毒軟體，並自動更新病毒碼，降低病毒感染機會。 由資訊單位建立執行排程更新病毒碼，並檢視更新狀況
作業系統更新 RGP-06-12	• 作業系統自動更新，因故未更新者，由資訊單位協助更新。 由資訊中央整體派送更新，達到整體控管及時更新之目的

項目	具體管理方式
郵件安全管控	• 有自動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附 件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。 郵件進出有防火牆及 SPAM 系統預先過系統威脅郵件，確保安全性 • 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。 電腦預裝防毒軟體會自動掃描安全附件
網站防護機制	• 網站有防火牆裝置阻擋外部網路攻擊。 防火牆系統會自動阻擋 IPS、VIRUS、Anti-Bot、Ransomware 等各種 型態攻擊。
資料備份機制 RGP-06-08	• 重要資訊系統資料庫皆設定每日完整備份、每小時差異備份。 資訊備存作業如有異常狀況時，經判定為系統設定問題者，應及時予以 調整。
備份異地存放 RGP-06-08	• 伺服器與各項資訊系統備份檔，分開存放於銀行。 RGP-06-8 檔案安全作業
重要檔案上傳伺服器	• 公司內各部門重要檔案上傳伺服器存放，由資訊單位統一備份保存。 重要檔案資料皆放置在中央檔案主機系統，並且每天進行備份作業。
資訊中心檢查紀錄表 RGP-06-09	• 訊中心檢查紀錄表紀錄機房溫溼度、資料備份、防毒軟體更新、網路流量等紀錄。
災難復原計畫 RGP-06-11	• 作為資訊系統發生系統性異常時復原的依據，以降低資訊系統風險。 • 資訊單位每年研擬災難回復備存演練計劃(樣式)，辦理演練作業，並保留演練紀錄。 • 演練結果未達預期成效時，資訊單位應重新檢討及修訂系統復原計劃，以提升資訊系統風險管理能力。
資產電腦報廢程序	• 配合資訊安全實施，加強電腦等資訊設備報廢管理，避免報廢資料外洩風險。 • 電腦資訊設備報廢，資訊單位需填寫資料報廢清冊填寫說明。
郵件對外授權管理機制	• 對外發送郵件，如有機敏性資料或需代表公司等需授權郵件，可經由資訊單位設定各層級主管，審查內容後放行發送郵件。

四、 資安事件通報程序

本公司資通安全通報程序如下，資安事故之通報與處理，皆遵守該程序之規範進行，詳見下圖：



五、 資通安全相關實施情形：

1.教育訓練課程：

2023 年參與資通安全相關講習與課程(如：工研院資安情搜集與分析、數位發展部資安將帥班、跨域資安強化產業推動班、資安領袖工作坊…等)共計 60 人次、120 小時。

2.機器設備、系統更新情形：

隨著科技網路進步，公司仰賴網際網路進行業務往來，為了提高效益逐步走向 E 化，但隨之產生的內部及外部攻擊威脅，嚴重威脅公司運行，需建置新防火牆系統保障企業資訊的安全性，避免資料破壞及外洩發生，影響公司及客戶權益。

潤泰全球現有網路架構錯綜複雜且運行多年，設備均老舊及缺少內部防火牆系統，若發生資安事件無法有效防禦威脅。更換舊網路設備及增添資安設備於樓層間區隔網路資料流，有效過濾病毒及木馬威脅等。

於潤泰全球樓層及主機伺服器群中，新增加防火牆系統，隔離網路廣播封包，並借 IPS、Anti-Virus、Anti-bot、DDos、Threat-Emulation 各種安全模組有效防禦資安威脅。

本案2023年相關費用支出共計新台幣1,519千元。