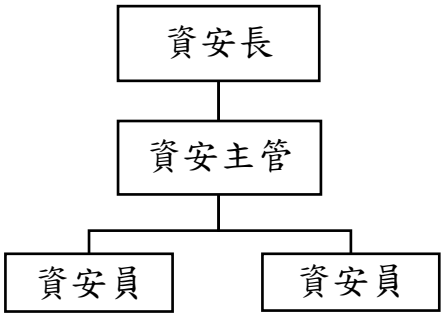
潤泰全球股份有限公司
資通安全管理辦法

2024.11.13 版

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，遵守金融管理委員會，上市（櫃）公司資通安全管理相關規定。

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。

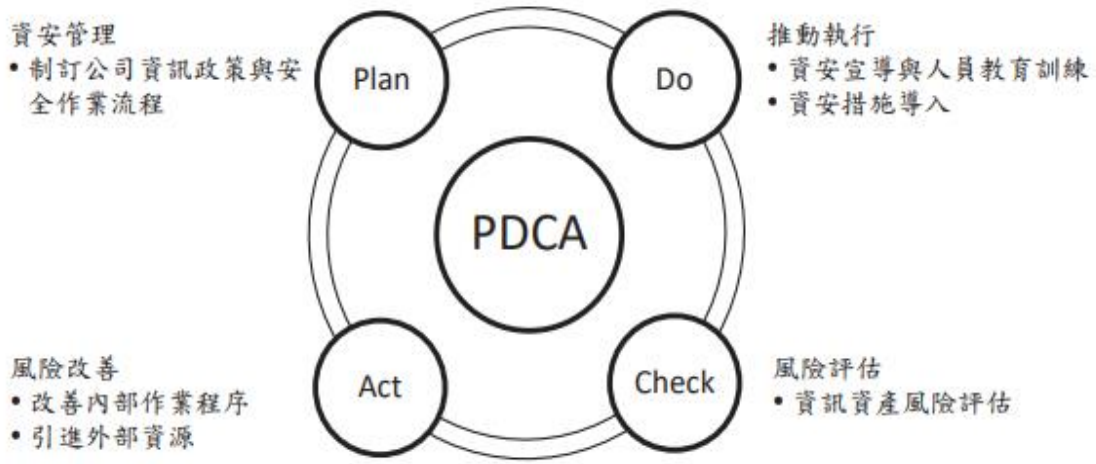


資安政策及目標

訂定資通安全政策及目標，由資安長核定，並定期檢視政策及目標且有效傳達員工其重要性。

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



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：

（一）制度規範：訂定公司資訊安全管理制度，規範人員作業行為。

（二）硬體建置：建置資訊安全管理系統，落實資安管理措施。

（三）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。

資訊安全管理措施：

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。

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。

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。

核心業務及重要性：

資通業務及重要性：

本公司之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
ERP 與財務管理	SAP 系統服務	為公司關鍵基礎設施	無法進行財務管理相關服務	4 小時

本公司之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
人事相關系統	影響行政效率	8 小時
網管系統	無法即時監控網路系統	8 小時
網域、郵件及檔案伺服器	無法正確連線提供服務	4 小時
防火牆	對外網路中斷或無管制連線	4 小時

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。 • 如有特殊連線需求需額外申請開放。 • 監控分析防火牆數據報告。
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。 • 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。
防毒軟體	• 使用多種防毒軟體，並自動更新病毒碼，降低病毒感染機會。
作業系統更新	• 作業系統自動更新，因故未更新者，由資訊處協助更新。
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、垃圾郵件及惡意連結的不安全郵件。 • 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。
網站防護機制	• 網站有防火牆裝置阻擋外部網路攻擊，並採用反向代理、DMZ 防御阻斷等 技术保障對外網站正常運作。 • 防火牆會自動阻斷 IPS、VIRUS、Anti-Bot、Ransomware、DDoS 等攻擊行為。
資料備份機制	• 重要資訊系統資料庫皆設定每日完整備份、每小時差異備份機制。
備份異地存放	• 伺服器與各項重要資訊系統備份檔，分開存放於銀行及異地。
災難復原計畫	• 公司內各部門重要檔案上傳伺服器存放，由資訊處統一備份保存。 • 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，資訊單位重新檢討及修訂系統復原計劃(樣式)， 以提升資訊系統風險管理能力。
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，由資訊處統一備份保存。
資訊中心檢查紀錄表	• 資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。
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。

項　　目	具體管理方式
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。
遠端存取管控	• 因疫情或業務需要遠距辦公，依內控表單流程核准使用。 • VPN 通道採加密連線、多重身分驗證、授權存取限定、Idle 自動斷線、及流量 進出病毒掃描技術及保留操作軌跡等方式控管。 • 每年不定期透過資安教育訓練宣導遠距離使用相關網路風險。
資通系統掃描	• 對資通系統進行資安檢測掃描作業。
參加情資分享組織	• 加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊。

資通系統或服務委外辦理之管理

本公司委外辦理資通系統之建置、維運或資通服務之提供 時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

（一）選任受託者應注意事項

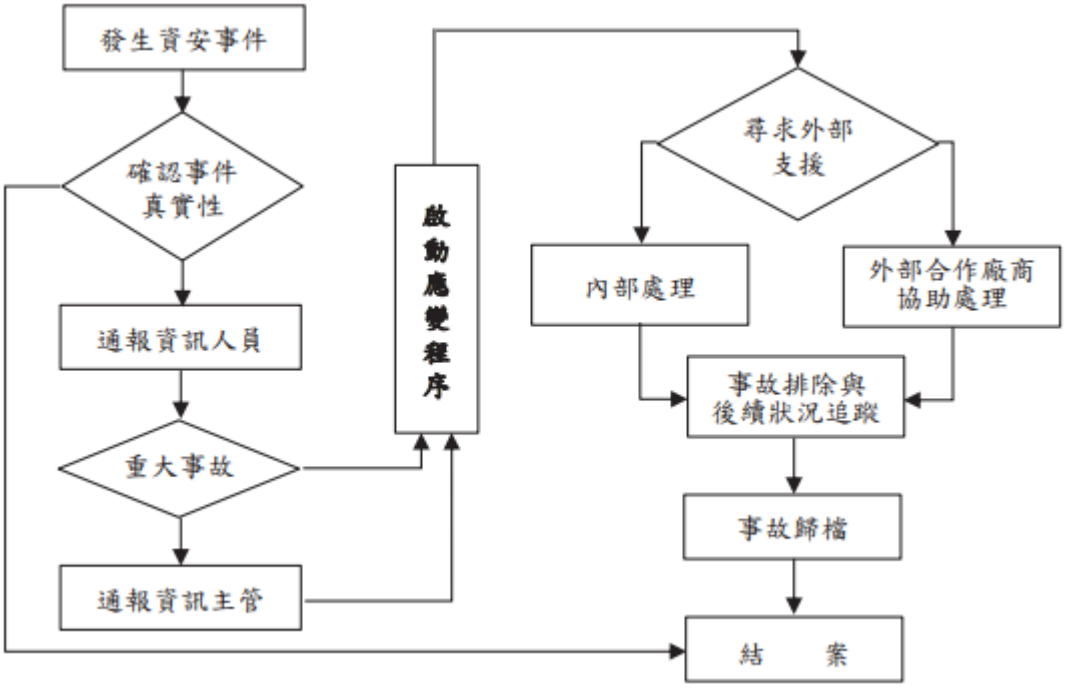
1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施。
2. 受託者應配置充足且經適當之資格訓練或具有類似業務經驗之資通安全專業人員。

（二）監督受託者資通安全維護情形應注意事項

1. 受託者執行受託業務，需簽屬保密協定，違反資通安全相關法令或知悉資通安全事件時，應
   立即通知委託機關及採行之補救措施。
2. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資
   料。
3. 本公司應定期或於知悉受託者發生可能影響受託業務之資通安全事件。
4. 基於資安管理要求，對委外廠商訂定資安稽核權。

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。



如遇重大資安事件，除內部通報處理流程，配合法規主動上報相關單位，並於年報敘明資安事件損失及及可能影響及因應措施。