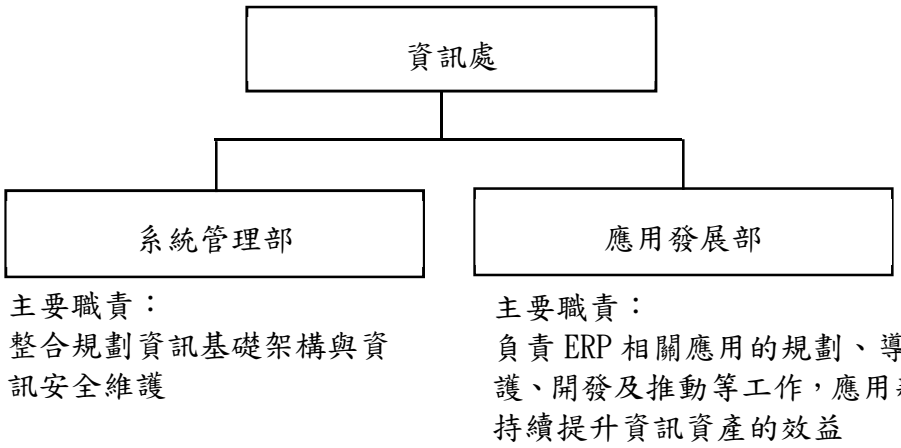
資通安全風險管理

一、資通安全風險管理架構

本公司資通安全之權責單位為資訊處，負責資通安全相關工作之規畫、執行及管理，推展資通安全意識，並直接向公司經營最高主管執行長報告，其架構如下：



二、資通安全政策

為有效推行資訊安全管理制度，以確保資料、系統、設備及網路安全，本公司訂定有資訊應用相關之電腦軟硬體管理規定、系統主機管理規定、及資通安全相關評估辦法，做為資訊安全管理工作之執行、評估及稽核指引，以確保本公司各資訊系統可持續性運作、所屬資訊之完整性、有效性、可用性、及安全性，並落實遵守資通安全相關法律及規定。

三、具體管理方案及投入資通安全管理之資源

本公司在資訊處下設有「系統管理部」(共四位同仁)與「應用發展部」(共五位同仁), 並於 113 年設置資訊安全主管一位及資訊安全人員一位，目前雖未投保資安險，但已制訂資訊安全政策並每年定期檢討。

各項資通安全政策及具體管理方案說明如下：

1. 資通安全管理政策

為確保本公司資訊安全，每年依資通安全稽核查檢表，針對資訊安全政策、組織安全、資產分類與控制、人員安全、實體與環境安全、通訊與作業管理、存取控制、系統開發與維護、營運持續管理、相關法令符合性等事項進行自行評估，並由稽核單位抽樣複查。

2.資通安全管理措施

(1)機房及電力：管制人員進出、進行環境監控、並定期檢測不斷電系統。導入雲端 ERP 系統透過集中數據處理和資源共享，減少對硬體設施需求。降低能源消耗，也減少硬體製造和廢棄時的碳足跡。

(2)主機管理：導入虛擬化容錯移轉之備援架構，以避免故障影響，同時定期完整備份資料及執行異地保存等，訂定明確的管理規範，並依規範定期實施復原演練。

(3)網路管理：內部設置有防護機制，VPN 管制及使用通知，需提出申請經主管及資安長同意，才可開放，VPN 連線需採雙因子認證。對各主要設備皆規畫有對應之備援設備，以減低故障影響，同時租用經認證之網路攻擊防護、垃圾信件過濾及信件病毒過濾防護(中華電信資安艦隊)服務，進行雙重防護。

(4)電腦管制：導入電腦資產管理系統（SmartIT），即時管制全公司電腦，掌握電腦的異動、電腦軟體的合法使用，強制防護軟體的啟用，及報廢的處置。每日更新防毒病毒碼。

(5)帳戶管制:各系統使用權限皆需經申請及簽審核，人員調離職的權限檢視，並每年定期複查驗人員權限。密碼政策為使用者帳號密碼長度最少 8 碼、需具備複雜度、輸入錯誤鎖定、90 天更換密碼且密碼、前 4 次密碼不可重複。

(6)系統發展：針對系統之作業權限、存取管理、功能變更、問題處理等，訂定明確的作業程序與規範。

(7)教育推廣：平時交機使用旋即進行資安觀念宣導，定期執行新人訓練資安宣導，同時不定期公告高風險資訊，提醒員工加強資安觀念。每年執行社交工程演練，提昇風險意識。

(8)組織管理：專職資訊管理部門及人員，並定期向經營最高主管報告執行運作狀況。

3.資訊安全維護作法

資訊安全已為公司營運重要議題，對應資安管理事項及維護作法如下:

(1)每年 1 次向執行長彙報。

(2)製作資安公告，傳達資安防護重要規定與注意事項。

(3)每年至少 1 次執行社交工程釣魚郵件測試。

(4)每年舉辦 2 場新人進員工資安教育訓練。

(5)到職當天簽署”資訊安全保密暨資訊系統合法使用承諾書”。

(6) 每年定期執行內外部稽核，檢視資訊與資安管理系統運作正常合規且持續改善。

(7)汰換防火牆設備以維持韌體版本及防護特徵碼的更新。

(8)每年定期弱點掃描重要系統，更新系統修補弱點。

(9)依循 ISMS 系統，每年執行風險評鑑，投入資源降低風險。

4.資訊安全管理執狀況

(1)導入 SSL VPN 及多因數認證。

(2)通過 ISO27001 資訊安全認證，相關資安稽核無重大缺失。

(3)強化員工資安意識，資安政策／訊息公告宣導 25 次。

(4)完成 2 場新進人員資訊安全管理教育訓練，完訓率 100%

(5)每年定期執行營運衝擊分析，並針對衝擊較高的系統及設施進行災難復原演練。114 年共進行了 16 次災難復原演練。

(6)郵件防護成功阻擋攻擊及垃圾信件總共約 64 萬封。

(7)114 年共製作 25 份資安公告，傳達資安防護重要規定與注意事項。

(8)客戶滿意:無重大資安事件，無違反客戶資料遺失之投訴案件。

(9)共有 308 個人次參與了社交工程演練，整體社交演練違規率為 5.19%。

(10)114 年進行之弱點掃瞄主機數共 21 台，更新系統修補其弱點。

四、本公司於 112 年導入 ISO 27001(2013 版本)資訊安全管理系統，並取得第三方驗證，證書效期為 112 年 8 月 14 日至 114 年 10 月 31 日，並於 113 年 8 月 30 日通過續評審查。且在 114 年 9 月 17 日通過 ISO 27001(2022 版本) 驗證審查，目前證書效期為 114 年 11 月 16 日至 117 年 11 月 15 日。透過 ISO 27001 資通安全管理系統之導入，強化資通安全事件之應變處理能力，保護公司與客戶之資產安全。

五、本公司截至目前為止，未曾發生重大資通安全事件。