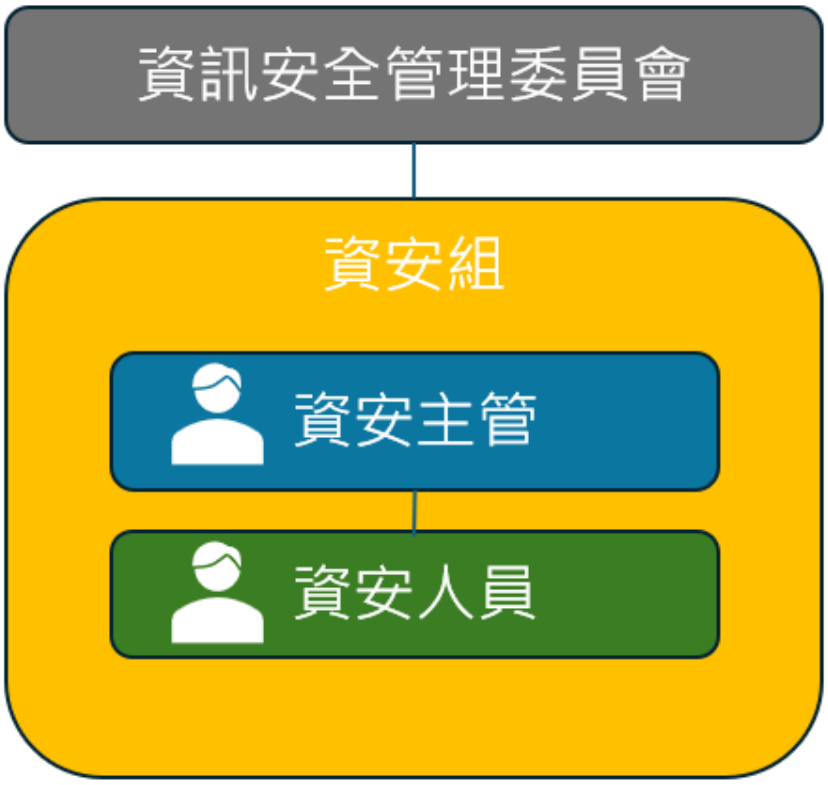
資訊安全風險管理報告

114.12.29

一、 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，特設立資安組，為資安專責單位，包含資安主管及至少一名以上的資安人員，負責資通安全事務的規劃與執行。其中，資安主管至少每年一次於董事會中報告重大議題或規劃。



二、 資訊安全風險管理機制

執行資訊機房、電腦資訊檔案安全、網路安全、郵件安全管理、資訊系統控制存取等管理。

三、 資訊安全政策

- 資訊安全之目標：

建立安全及可信賴之電腦化作業環境，確保本公司資料、系統、設備及

網路安全，以保障公司利益及各單位資訊系統之永續運作。

- 資訊安全之範圍：
  1. 人員管理及資訊安全教育訓練。
  2. 電腦系統安全管理。
  3. 網路安全管理。
  4. 系統存取管制。
  5. 系統發展及維護安全管理。
  6. 資訊資產安全管理。
  7. 實體及環境安全管理。
  8. 資訊系統永續運作計畫管理。
  9. 資訊安全稽核。
- 資訊安全的原則及標準：
  1. 定期辦理資訊安全教育訓練及宣導，包括資訊安全政策、資訊安全法令規定、 資訊安全作業程序、以及如何正確使用資訊科技設施等，促使員工瞭解資訊 安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，並遵守資訊安全規定。
  2. 為預防資訊系統及檔案受電腦病毒感染，對於電腦病毒應採取偵測及防範措施，對入侵及惡意攻擊應建立主動式入侵偵測系統，以確保電腦資料安全之要求。
  3. 為預防本公司遭遇天災或人為之重大事件，將造成重要資訊資產及關鍵性業務或通訊系統等中斷，應建立資訊系統永續運作規劃之政策。
- 員工應遵守之相關規定：
  1. 資訊單位接收帳號申請單後，建立「使用者代號」。
  2. 電腦資料及設備，不得任意破壞、攜出、外借、不正當修改，以維護資料完整性。
  3. 禁止使用無版權軟體。
  4. 進入主機後，若作業結束或長時間不使用機器時，應退出機器，以免資料機密外洩，為別人所破壞或造成當機之困擾。
  5. 電腦設備之擺放位置除以方便為原則外 ，應遠離茶水、咖啡、日曬或潮溼地點，以延長其壽命。
  6. 離職或新舊職務交接時，由資訊單位衡量資料相關性作適當處置。
  7. 電腦設備無法正常作業時，使用者應立即通知資訊單位，以便檢查或維修。

四、 資訊安全具體管理方案:

項目	具體管理措施
防火牆防護	1.防火牆設定連線規則。 2.如有特殊連線需求需額外申請開放。
使用者上網控管機制	1.使用自動網站防護系統控管使用者上網行為。 2.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	1.使用防毒軟體，並自動更新病毒碼，降低病毒感染機會。
作業系統更新	1.作業系統自動更新，因故未更新者，由資訊部協助更新。 2.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。
郵件安全管控	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。
資料備份機制	重要資訊系統資料庫皆設定每日備份。
重要檔案上傳伺服器	公司內各部門重要檔案存放於伺服器，由資訊部統一備份保存。
資安險	本公司客戶主要為企業客戶，無消費者個資保管風險，於評估市面資安險種保險範圍、適用行業等項目後，暫不投保資安險，但因應資訊安全所面臨的挑戰，已導入相關軟硬體,例如防火牆、防毒、入侵防護系統...等，並持續關注資訊環境變化趨勢，並強化公司同仁資安危機意識及資安處理人員應變能力。

五、 資通安全的資源投入

- 本公司設置資安組包含資安主管一名及至少一名以上的資安人員，負責資通安全事務的規劃與執行。其中，資安主管至少每年一次於董事會及季度業務回顧會議中報告重大議題或規劃。
- 針對系統主機的作業系統或重要軟體升級、災害復原演練等重要的資安工作，資安組每季皆會定期檢討規劃與執行進度，並透過不定期的社交工程演練、資安健檢服務等，判斷使用者的資訊安全觀念是否足夠、資訊設備資源投入與系統配置是否存在漏洞，編列資安預算後執行。

六、 緊急通報程序

- 當發生資訊安全事件時，發生單位通報資安組，判斷事件類型並找出問題點，即時處理並留下紀錄。