資通安全管理

1.資通安全管理架構

本公司設有資安主管及資安人員，負責監督資安管理運作情形，以建構出資安防禦能力及同仁良好的資訊安全意識。在網路安全防禦措施方面，已導入網路前端之防火牆、防毒,作為資安防護基礎，內部主機皆佈署防毒軟體，定期更新病毒碼與即時辨識惡意行為特徵，能即時攔截病毒木馬蠕蟲、勒索軟體、文件夾帶之惡意程式等，降低被駭客攻擊損害之風險。

2.資通安全政策

(1)目的

- 增進本公司資通安全及穩定之運作，提供可信賴之資通服務，確保資訊資產之機密性、完整性及可用性，並順利推展本公司各項業務，以符合資通安全管理作業。

(2)範圍

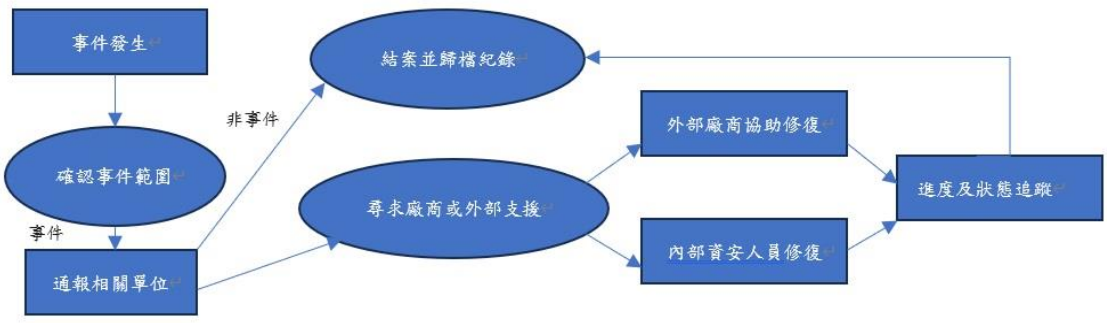
- 本政策適用於本公司同仁、接觸本公司業務資訊或提供服務之廠商。

(3)目標

- 確保本公司相關重要資訊之機密性，保障本公司機密與個人資料。
- 提昇本公司資安防護能力,和持續運作之目標。

(4)策略

- 考量相關規定及企業營運要求，評估資安需求，建立相關程序，確保資訊資產之完整性及可用性。
- 訂定組織分工權責，推行資通安全作業。
- 依照資通安全事件通報應變機制，確保資安事件妥善回應、控制及處理。



3.體管理方案

(1)管制範圍

- 核心資訊設備、電腦設備、相關軟體程式、資料庫及相關資料。

(2)管理作業程序

- 機房不得隨意進出。
- 採購設備需填寫請購單，會簽主管單位核准後，由資訊處進行採購及安裝。
- 不得安裝非法軟體，並安裝防毒軟體，定期作病毒掃描及更新病毒碼。
- 人員離職時電腦相關設備需進行移交手續。
- 設置防火牆，由公司外部進入作業，皆需經由防火牆進入。
- 使用者用暫離電腦時必須鎖定螢幕，電腦不使用時需關機。
- 職員離職或更換工作，其使用帳號密碼應註銷或更新。
- 密碼需定期更新，密碼長度至少 6 位以上。
- 首次使用者帳戶及權限應申請，經部門主管核准，再由資訊部門執行。
- 資料使用權限應有分層授權系統。
- 非指定之財務人員無權使用財務報表系統。
- 密碼不可顯示於電腦螢幕及鍵盤上。

4.投入資通安全管理之資源：

- 端點防護：定期檢查並更新作業系統和病毒碼。
- 硬體防禦：導入 FORTINET 防火牆，強化網路資安管理。
- 設備及軟體盤點：每年盤點一次，確保合法使用授權軟體與確認設備使用狀況。
- 不定時資安案例宣導與強化資安意識。
- 備援機制建置：建構核心設備,備份管理機制，確保資料之安全與可用性。
- 設置資訊安全專責主管 1 人及資訊安全專責人員 1 人。
- 區隔出內部及外部網路。
- 升級郵件伺服器，有效防範釣魚郵件攻擊。
- 升級不斷電系統，避免電壓波動和大樓電力故障造成的危害。