資訊安全風險政策及執行情形

1 資訊安全政策：

1.1 確保本公司資料、系統、設備及網路通訊安全，阻絕外界之入侵、破壞。

1.2 確保系統資訊帳戶存取權限與系統之變更均經過公司規定程序授權處理。

1.3 落實銷毀程序，已報廢之電腦儲存媒體應加以銷毀避免資料意外暴露外流。

1.4 監控資訊系統之安全狀態與活動紀錄，有效掌控並處理資訊安全事件。

1.5 維護資料與系統之可用性與完整性，發生災害或受破壞時，可回復正常作業。

2 資安網路架構本公司資訊單位專責資訊安全，定期向資訊主管會報資安管理運作情形。公司之內部系統皆位於虛擬網路之中，外部網路受隔離無法直接進入，並且採用多重網路安全防禦系統，位於網路前端之防火牆、入侵防禦連線篩檢系統、郵件內安全控管系統負責過濾網路進出連線的內容，能防禦外部網路攻擊，並即時封鎖最新惡意軟體、有害之網路連結、垃圾電子郵件等威脅。位於內部之主機及端點皆由中控台佈署防慣軟體，隨時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，有效降低被駭客功擊損害之風險。

3 系統帳號生命週期管理與權限帳號管理依各業務範圍、職權分別設定使用者之帳號及權限，資料之存取皆需透過簽核流程經各權責主管申請並核准後始能使用與變更。使用者一旦離開原職務，立即撤銷該使用者之帳號與權限，以防範未經授權之使用。

4 資料存取紀錄稽核備存能紀錄系統檔案文件存取之軌跡記錄、往來郵件等資料，進行歸檔保存。報廢程序完成之電腦均執行硬碟拆解破壞以符合法規遵循的管理制度及資安政策。

5 資訊系統持續運作系統與文件皆採取每日、每週及每月之本地備份，每月之備份資料再傳輸到異地做異地備份，並每年定期執行系統資料復原測試演練，以確保資訊系統之正常運作及資料保全，可降低無預警天災及人為災害造成之資料損失風險。

6 資訊部門執行作業依本公司規定程序均能落實執行，確保資料完成性與安全性，風險評估結果尚屬良好，最近年度科技改變對公司資訊安全並無重大不利影響且無重大營運風險。

7 資訊部門執行作業依本公司規定程序均能落實執行，確保資料完成性與安全性，風險評估結果尚屬良好，科技改變對公司資訊安全並無重大不利影響且無重大營運風險。

8 本公司於 110-112 年度投入資通安全管理相關之費用(EX：防火牆、防毒軟體、SIEM、資安防禦系統及安全性資料管理..等)。

年度	金額
110	$2,788,148
111	$ 907,500
112	$2,352,740