資通安全風險管理報告

一、 資通安全風險管理架構

資訊部為本公司資安專職單位，資訊主管為資安主管，由資安主管成立跨單位資訊安全推行小組，推動、協調及督導資訊安全各項事宜，直接向總經理或其指定代理人報告。

二、 具體管理方案：

- 落實公司端點裝置資安防護機制：為落實本公司之資訊安全，資訊部門已建置防火牆，進一步阻擋病毒及駭客入侵攻擊公司內部網路，並安裝防毒軟體，加強用戶端防護。
- 落實公司網路資安防護機制：透過 Security Agent，提供入侵偵測及防禦、行為監控、惡意程式防護、網頁信譽評等、未知安全威脅、周邊設備存取控管，確保重要主機安全，並透過其具備之防火牆功能，縮小實體、虛擬與雲端伺服器的攻擊面，提供精細的過濾規則和網路政策，以防止病毒與駭客，因程式未定期更新修補而造成之漏洞攻擊。
- 落實公司資安管理原則：提升密碼安全等級；帳號管理規則依循國家標準 GCB(Government Configuration Baseline)；帳號區隔並賦予最小特權原則(PoLP, Principle of Least Privilege)，設置資安防護斷點；建置重要文件檔案保護機制；建置伺服器網路存取紀錄平台，監控異常事件。
- 資訊部擬視實際需求，評估未來是否投保資安險，以降低發生重大資安事件所造成的營運損失。
- 資訊安全小組則將後續目標，訂定為完備資安相關規範、定期資安評估、取得國際資安認證，並於未來持續強化資安防護機制，同時以教育訓練計畫，對員工宣導與資安相關之重要觀念。

三、 **2023** 投入資通安全管理之內容和資源：

- 2023/04 委請專業第三方公司就本公司資訊架構進行「資通系統風險評鑑」。
- 2023/10 汰換郵件攔截過濾伺服器(Spam Sever)。
- 為防範資安風險及效能提升，採購線上簽核系統更新版本升級套件，並於 2023/11 上線。
- 為解決資安防護及內部網路系統安全與穩定，總公司網路防火牆進行升級，目前進行中，預計 2023 年底前汰換更新完成。
- 增訂「資通安全管控政策」。
- 就電腦通訊設備，增修「緊急復原計畫」，加強並更新各項設備緊急處理程序及應變聯絡窗口及連絡電話。