資通安全管理

1. 敘明資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。

(1) 資通安全風險管理架構

現有公司內部資通安全工作，由管理部資訊室負責規劃，建置，及持續改善。並且針對系統伺服器，作業系統，網路系統，建置應有的管制及防護機制，並針對異常災變，資料損毀，及機敏資料做好應變防護計畫，以保障公司、顧客、及投資人的利益。

(2) 資通安全政策

建立安全及可信賴之電腦化作業環境。

(3) 具體管理方案

項目	說明
網路防護及 使用者上網控管機制	透過匝道控制器，管控網路存取許可，並且偵測防護惡意入侵及防護外部的網路攻擊。並且透過權限管控給予使用者網路存取權限，並透過紀錄檔案定期排查稽核上網存取紀錄。
郵件安全管控	在使用者接收郵件之前透過郵件匝道器在使用者接收郵件之前過濾郵件，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，防止惡意連結的傷害。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。
資料備份機制	所有系統及資料庫排定自動備份工作。
防毒軟體 及系統程式更新	作業系統及應用程式及防毒軟體會自動更新，降低病毒感染及修補應用程式漏洞。
員工資安教育	每季對員工進行資訊安全教育訓練及測驗與電子郵件社交工程演練，強化員工的資安風險意識。
風險評估及弱點偵測	定期進行系統弱點掃描等檢核機制及檢討改善現有資訊作業環境的資訊安全防護。

(4) 投入資通安全管理之資源

112 年已投入 210 萬進行資訊安全升級，113 年已編列 300 萬預算投入資訊安全的環境改善。

2. 列明最近二年度及截至年報刊印日止，因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實。

本公司最近二年度及截至公開說明書刊印日止尚無因資安問題遭受損失之情形，持續落實資訊安全管理政策目標，保護公司重要系統與資料安全。