資通安全管理

（一）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

資訊部門負責統籌並執行資訊安全政策，宣導資訊安全訊息，提升員工資安意識，蒐集及改進組織資訊安全管理系統績效及有效性之技術、產品或程序等。由稽核室每年就內部控制制度—資訊循環，進行資通安全查核，評估公司資訊作業內部控制之有效性。

2.資通安全政策

為落實資安管理，公司訂有內部控制制度—資訊循環及資訊機房管理辦法、資通安全檢查之控制，藉由全體同仁共同努力期望達成下列政策目標:

- 確保資訊資產之機密性、完整性。
- 確保依據部門職能規範資料存取。
- 確保資訊系統之持續運作。
- 防止未經授權修改或使用資料與系統。
- 定期執行資安稽核作業，確保資訊安全落實執行。

3.具體管理方案

- 網際網路資安管控。
  - 架設防火牆（Firewall）
  - 定期對電腦系統及資料儲存媒體進行病毒掃瞄
  - 定期覆核各項網路服務項目之 System Log，追蹤異常之情形
- 資料存取管控。
  - 電腦設備應有專人保管，並設定帳號與密碼
  - 依據職能分別賦予不同存取權限
  - 調離人員取消原有權限
  - 設備報廢前應先將機密性、敏感性資料及版權軟體移除或覆寫
  - 遠端登入管理資訊系統應經適當之核准
- 應變復原機制。
  - 定期檢視緊急應變計劃
  - 每年定期演練系統復原
  - 建立系統備份機制，落實異地備份
  - 定期檢討電腦網路安全控制措施
- 宣導及檢核。
  - 隨時宣導資訊安全資訊，提升員工資安意識
  - 每年不定期執行資通安全檢查

4.投入資通安全管理之資源

本公司注重資通安全，持續增加在資安相關之基礎建設與安全防護架構相關軟硬體投資。本公司在 113 年度共計投資資安相關軟硬體費用約為新台幣 223,257 元，足見本公司對資通安全之重視。

（二）列明最近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:

本公司目前無重大資安事件導致營業損害之情事；並持續落實資訊安全管理政策目標，並定期實施復原計劃演練，保護公司重要系統與資料安全。