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. 資安風險管理架構

本公司資訊安全之權責單位為資訊安全室及應用發展處之作業系統部，資訊安全室負責統籌資訊安全政策、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；作業系統部負責執行資訊安全政策、落實資安管控機制、進行弱點修補等。由稽核室每年就內部控制制度—電腦化資訊系統循環，進行資通安全查核，評估公司資訊作業內部控制之有效性，最近一次查核為民國 111 年 11 月；另外，每年定期進行外部資訊循環查核，確保資通安全有效性。

2. 資通安全政策

為落實資安管理，本公司訂有內部控制制度—電腦化資訊系統循環以及網路資源管理暨內部資訊保護作業要點、資通安全事件危機通報作業要點，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。
- 確保各部門依據職能規範資料存取。
- 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。
- 確保系統漏洞及時防堵。
- 定期執行資安稽核作業，確保資訊安全落實執行。

3. 具體管理方法

網際網路資安管控
• 架設防火牆（Firewall）管控內／外資訊進出 • 定期對電腦系統及資料儲存媒體進行病毒掃瞄 • 各項網路服務之使用應依據資訊安全政策執行 • 定期覆核各項網路服務項目之系統 Log 或流量，追蹤異常之情形 • 定期關注最新電腦病毒疫情、漏洞、弱點等資訊，提早預警與防堵

資料存取管控
• 電腦設備應有專人保管，並設有帳號與密碼管控 • 依據職能分別賦予不同系統／資料存取權限 • 調／離職人員取消相關權限 • 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審核放行
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
• 隨時宣導資訊安全重要性，提升員工資安意識 • 每年定期執行資通安全檢查

4. 本公司每年定期投入資安相關經費，建立基礎防護架構，確保企業營運皆在安全範圍，因此資通安全風險並未對本公司財務業務產生重大影響。
5. 本公司已於民國 112 年設立資安專責單位，包含專責人員一人及專責主管一人。
   - 發布 10 份以上之資安公告，宣達各種資安風險及相關資安規範，共計超過 2500 發送人次。
   - 舉辦 3 場資安相關教育訓練，出席率皆達 98%以上。
   - 針對資訊系統共進行 3 次營運持續演練，確保資訊系統發生異常時能夠儘速恢復服務。
   - 進行社交工程演練，通過率高達 95%以上。
   - 投入約新台幣 200 萬元經費於資安方面，增強公司資安體質。
   - 導入 ISO 27001 資訊安全管理系統，已完成外部稽核，並取得證書。
   - 已舉行一次管理審查會議，並將會議結論於民國 112 年 11 月 1 日董事會報告。

(二)截至民國 112 年 12 月 31 日止，本公司無重大資安事件導致營業損害之情事。