(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： 本公司強化資訊安全管理，確保所屬資訊資產之可用性、完整性及機密性，以提供本公司業務持續運作之資訊環境，並不定期進行資訊安全檢查。

2.資訊安全政策： 為落實資安管理，公司訂有資訊安全管理程序與資訊管理控制作業，以期望達成下列政策目標： (1)資訊處理單位之功能及職責劃分。 (2)應用系統維護管理。 (3)電腦作業管理。 (4)備份及回復作業。 (5)網路安全管理。

3.具體管理方案及投入資通安全管理之資源： 擬定資安計畫以逐年推動資訊安全政策，導入資訊安全制度與流程規範，並持續架構完整資訊安全技術防護措施。

(1)網路及電腦系統安全管理：AD(網域管理)已完全取代單機作業，且 AD 政策預計調整近似 ISO27001 相關規範。

(2)文件管理系統：重要資料均上傳於系統中，並設定存取權限。文件管理系統仍在調查規劃中。

(3)網際網路資安管控：防火牆均已架設和調整，目前正常運作中，常規比較病毒掃描。2025 年全面使用新型防毒軟體 WithSecure。

(4)2025 年起，核心系統-完整備份並常規實施還原演練、演練週期從一年兩次更新為一季一次。

(4)資料存取管控：資料存取權限控制及遠程登入資訊系統控制。推動端點控制系統，以利事前預防、事後舉證使用者行為，目前仍持續規劃中。

(5)資訊安全宣延：不定期宣導資訊安全資訊並執行資通安全檢查，一年兩次課程，加入 ChatGPT 實用教學。資訊人員依職別外訓資訊安全相關，再對內部召開資訊安全宣延課程和不定期抽檢人員資訊設備。

(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，如無法合理估計者，應說明其無法合理估計之事實： 最近年度及截至年報刊印日止，本公司無因重大資通安全事件導致損失之情事。