柒、資通安全管理

一、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

(一) 資通安全風險管理架構

本公司依據現行風險管理架構暨運作機制，以董事會為最高決策機制，將資通安全風險納入公司內部整體個資及資通安全管理政策，由總經理率領第一級控管機制，設置資通訊暨個資安全管理處，負責督導及審查資通安全執行、監督及管理事宜；另設置第二級控管機制資通訊暨個資隱私安全委員會，負責督導、審查個資及資通安全管理制度執行所有事宜。

(二) 公司資訊安全組織架構

1.設立資通訊暨個資隱私安全委員會，其成員如下：
主任委員一名：由總經理或指定之代理人擔任。
副主任委員數名：由總經理指派。
委員：主任委員就各營運功能面協調由其最高主管或其指定之代理人擔任。
資通安全官：由主任委員及副主任委員共同遴選任命。

2.會議舉行如下：
定期：平均每季開會一次。
不定期：遇資通安全相關議題時，由資通訊暨個資隱私安全委員會成員、資通安全官提出，經主任委員同意後召開。

(三) 資通安全政策

已訂定資通安全政策，以維護公司業務之永續經營，強化資通安全管理制度，確保資通訊資產之機密性、完整性、可用性及符合相關法規之要求，期有效及合理地降低企業營運風險。

(四) 具體管理方案

採用以下四大管理方案，落實資通安全維護：

1.對外防駭客：建置入侵防禦、網路區隔、防火牆、網頁防火牆等。
2.對內防洩漏：辦理資料外洩防護偵測與缺口補強等。
3.系統規劃建置：納入系統開發安全規範，執行程式碼掃描等。
4.維運監控：建置資訊安全監控中心，檢核與分析系統紀錄，發現異常狀況即時通報與追蹤處理。

(五) 投入資通安全管理之資源：於建設整體經費中分配資通安全預算一定比例。

二、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

未發生重大資通安全事件，故無因此遭受損失與影響，將持續推動資通安全作業，以為預防措施。