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個資及資通安全管理政策，由總經理兼任資通安全長，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所有事宜。

(二) 公司資訊安全組織架構

設立資通訊暨個資隱私安全委員會，其成員包含總經理或指定之代理人之主任委員一名與各營運功能面委員數十名，邀請獨立董事列席，每季開會一次，必要時召開臨時會；另依法設置資通安全專責主管及人員十餘員，執行個資及資通安全管理制度所有事宜。

(三) 資通安全政策

已訂定並定期(每年)審查資通安全政策，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，並投保資安險，以降低資安事件衝擊：

1.對外防駭客：建置入侵防禦、網路區隔、防火牆、網頁防火牆，加入資通安全分享與分析平臺 C-ISAC(通訊傳播領域-資安訊息分析分享中心，Communication – Information Sharing and Analysis Center)等聯防組織。

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。