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：

(1)公司設置資訊安全長、設立資訊安全室、資訊安全主管及人員，組織編制四人 (參閱公司組織圖)。

(2)資訊安全室主要負責集團資訊安全之制度規劃與宣導、技術評估、教育訓練、督導及稽核，以強化資安風險管控。

(3)資通安全管理任務：由資訊安全室為推動資通安全管理事宜，以落實資通安全管理控制措施。

2.資通安全政策：

(1)強化人員認知、避免資料外洩、落實日常維運，以確保核心系統管理業務之機密性 (Confidentiality)、完整性 (Integrity)、可用性 (Availability)與適法性(Compliance) 。

3.具體管理方案

(1)資訊安全室組織定期執行資安風險評估，依據風險影響的大小，以及改善風險所需成本以設定優先序，採用規劃、執行、查核與行動 (Plan-Do-Check-Act, PDCA) 的方法，架構多層的資安防禦，並建立資訊安全關鍵績效指標。

(2)加入資安聯防組織，可適時取得外部資安資訊分享及資安事件協助因應管道。

A.台灣資安主管聯盟組織(CISO)

B.台灣電腦網路危機處理暨協調中心(TWCERT/CC)

C.科學園區資安資訊分享與分析中心(SPISAC)

(3)持續進行集團員工資訊安全意識宣導。

4. 資通安全管理作為

(1)定期進行伺服器與個人電腦相關弱點補丁，降低設備暴露的風險。

(2)弱點掃描與滲透測試

A.每年針對集團之網路設備、應用系統及產品進行弱點掃描與滲透測試作業。

(3)年度資通安全教育訓練、釣魚演練

A.對集團員工進行資通安全教育訓練、釣魚郵件辨識宣導、執行釣魚演

練，並分析演練結果訂立改善對策以持續提升全員資安意識。

B.每年對於高階主管會進行資通安全教育訓練，將資訊安全的意識融入日常管理。

(4)透過網路流量可視性，提高對網路安全事件的識別與回應速度。

(5)每週召開資安運營會議，檢討資安事件警報和日誌，識別任何異常活動或潛在威脅，以確保資安監控系統的有效運作。

(6)每年向董事報告資安風險管控及執行狀況，並針對董事之建議進行改善。