資通安全管理之資訊揭露

●資通安全風險管理架構：

本公司設置資訊安全專責主管，為強化本公司之資訊安全管理，並確保資料、系統及網路安全，設立「資通安全部」為資安專責單位，部門內另包含一名資安人員，負責資通安全政策、資通安全管理辦法與資安事務的制定、規劃與執行。資訊安全專責主管至少每年一次向董事會報告重大資安議題、政策或規劃，114/11/11 已向董事會報告 114 年度資通安全執行情形。

●資通安全政策：

訂定「資通安全管理辦法」，強化資訊安全管理，確保所屬資訊資產機密性、完整性與可用性，及提高相關人員資訊安全意識，以提供資訊服務持續運作之環境，並符合相關法規要求。

●具體管理方案：

為達資安政策與目標，建立全面性的資安防護，推行具體管理方案如下：

- 對外：
  1. 定期進行官方網站弱點掃瞄，加以補強及修護，以降低資安風險，建立安全營運平台。
  2. 採購國際知名雲端防毒軟體，與世界同步接軌，防患未然。
  3. 使用高階防火牆，並定期檢視規則與政策，阻擋風險於牆外。
  4. 採用垃圾郵件偵測系統，為郵件防守第一道關卡，有效阻隔駭客郵件。
  5. 已加入 TWCERT/CC 台灣電腦網路危機處理暨協調中心，期能結合政府、企業、學術的公私協力平台，透過情資共享、事件應變協調，提升企業資安防禦能力。
- 對內：
  1. 定期進行社交工程演練，以提升員工日常作業的警覺性，共同維護資訊安全。
  2. 定期進行電腦弱點掃瞄，針對相關問題進行處置，以加強內部電腦防護力，提升資安防禦。
  3. 定期舉辦人員資安教育訓練，內化資安防護的警覺性，以降低資安風險。
  4. 精實資安管理制度，隨著環境變化及法令規範，不斷精進資安管理制度，以應對隨時可能發生的狀況。
  5. 內部發送資安通報，內容包含資通業界時事、資安知識、規範事項宣導，加強人員資訊安全意識。

●投入資源：

- 成立資通安全部，設置一名專責主管及一名資安人員，負責公司資訊安全相關事務的規劃、導入與執行，每週二次內部會議，以提升資通訊安全為要務。
- 採購防火牆、防毒、垃圾郵件過濾等相關系統，強化資訊安全。
- 每年至少一次與資安專業廠商配合，進行官網弱掃、主機弱掃、社交工程演練，以提高整體作業環境的安全性。
- 每年至少舉辦一次員工資安教育訓練。
- 官方網站採用帶有 WAF 功能之資安主機，以確保網站資訊安全。
- 導入使用者行為管控系統，針對技術資料執行檔案加密作業，以確保公司技術機敏資料的安全。