資通安全管理之資訊揭露

一、資通安全管理策略與架構

- 資通安全風險管理架構

  本公司設置資訊處並依法令規定設置資訊安全主管及一名資訊安全人員，負責資通安全、管理、制定政策推動及資安事務的規劃、執行及相關事務處理。

- 資通安全政策

  本公司依據「權限分級、分層防護」的原則制定資通安全政策。

  1.確保公司資訊設備、資訊系統及網路防護運作正常。

  2.確保公司資料完整性避免機密資料外洩。

  3.重要資料應予加密處理，並定期更新密碼，以避免遭挪用或剽竊。

  4.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

  1.使用者帳號管理:所有電腦與電子郵件帳號均設有權限控管機制,並要求定期更換密碼，以防止未授權登入。

  2.資料與系統管理：ERP 系統依工作職掌設定使用者權限，內部檔案以部門別控管存取，未經授權者無法讀取或使用。

  3.備份與異地備援：每日執行必要資料及系統備份，並採用雲端異地備援機制，且定期進行還原測試，以確保備份資料可用性。

  4.外部網路安全：全面設置防火牆並持續更新病毒碼，以防範惡意程式與網路攻擊，維持網路作業環境安全。

  公司亦持續投入資訊安全相關資源，確保內外部資訊系統之穩定與安全運作。

- 投入資通安全管理之資源

  1.定期發布資安公告：每年至少發送 4 則以上資安公告，向員工宣導資安防護之重要規定與注意事項。

  2.稽核查核機制：由稽核人員每年至少一次，依據電腦循環 11 項作業項目及相關法令與內部規章，評估各項作業是否確實執行。

  3.資安防護投資：採購防毒軟體並每三年定期續約一次，確保防護效期不中斷，以持續強化公司資訊安全防護。

二、重大資通安全事件：114 年度無重大資通安全事件發生。