

## 資通安全管理之資訊揭露

### 一、資通安全管理策略與架構：

#### (一)資通安全風險管理架構：

本公司設置資訊部並依法令規定設置資訊安全專責主管及一名資安人員，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。資訊安全專責主管至少每年一次向董事會報告。

#### (二)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。

#### (三)具體管理方案：

1. 依各部門職掌及職級設定相關資訊存取權限，權限變更時需提出申請經權責主管核准，設置使用者帳號密碼控管。
2. 資訊設備機房實施門禁管制，建立備援主機及資料異地備份，離線備份。
3. 定期更新防毒軟體及病毒碼，設置防火牆管理監測外部網路之風險。
4. 強化全體同仁網路詐騙案例及惡意郵件、釣魚郵件即時宣導，避免同仁誤執行造成損失。
5. 與資安廠商合作，定期檢視資安通告及週報表，針對漏洞缺失盡快修補。
6. 資訊儲存設備報廢時應嚴謹並做記錄，防止資料外洩。
7. 全體同仁應遵守法律，強化資訊安全認知，並簽署勞動契約，其中第三條為契約責任與保密協定。

#### (四)投入資通安全管理之資源：

1. 每年實施災害復原演練，確保發生時能即時反應。
2. 稽核人員每年依據資訊循環內控辦法評估是否確實執行。
3. 採購防毒軟體並持續續約，確保防護效期，強化資訊安全。

### 二、重大資通安全事件：

112年度無重大資通安全事件發生。