資訊安全

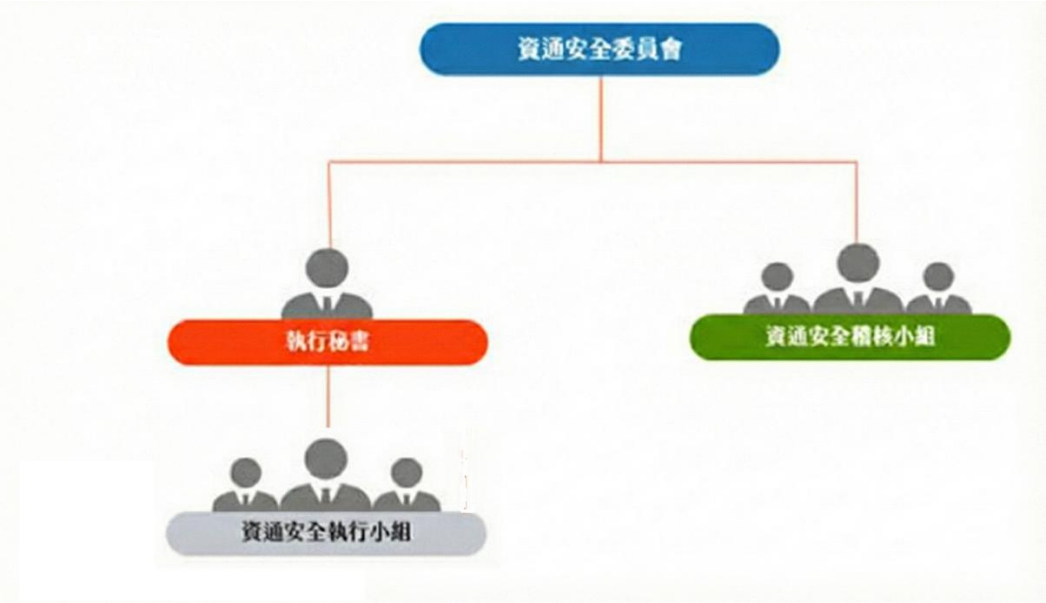
一、資通安全管理策略與架構

本公司視資訊作業為日常營運之重要環節，為確保資料、設備、人員及網路等資產之安全性，已建立完整之資通安全管理策略與架構。

(一) 資通安全風險管理架構

為有效推動資訊安全治理，本公司設有跨部門之「資訊安全委員會」作為最高權力機構，負責統籌資訊安全及保護相關政策制定、執行與風險管理。

1. **組織架構：**
    - **資通安全委員會：** 由總經理擔任主任委員，公司第三階主管擔任委員，並由資訊部最高主管擔任召集人。委員會依需要召開會議，負責制定及評估公司資訊安全政策、監督資安事件之檢討。
    - **執行秘書：** 由資通安全委員會召集人指派專人擔任，綜理、協調及督導委員會決議之資通安全相關業務與執行小組運作。
    - **資通安全稽核小組：**執行資通安全內部稽核，提出稽核報告，追蹤改善情形與缺失矯正。
    - **資通安全執行小組：** 由公司資訊部門擔任常設性資訊安全小組，負責日常資安監控、資訊軟硬體作業及設備維護，辦理資通安全相關教育訓練以及執行資安事件通報及應變處置。



2. 運作機制 (PDCA 管理循環)：
   本公司依據規劃、執行、查核與行動 (PDCA) 的管理循環機制，確保資安管理之有效性：
   - **規劃 (Plan) - 組織與制度：** 成立資訊安全委員會，制定資訊安全準則及編制各項標準作業程序與工作指導書。
   - **執行 (Do) - 資訊安全作業：** 執行資訊安全宣導、教育訓練、資訊分級管理、作業安全控管、防災演練及資安事件證據保全。
   - **查核 (Check) - 分析與檢討：** 進行資安事件與缺失原因分析、資安威脅預警，並追蹤改善進度。
   - **行動 (Act) - 資訊安全考核：** 透過日常查檢紀錄、KPI 審核及內外部稽核，將資安落實於日常作業並內化於組織文化。

(二) 資通安全政策

本公司依據金管會發布的上市上櫃公司資通安全管控指引，制定資訊安全政策。政策目標為確保資訊資產免於因內部或外部、蓄意或意外之威脅與破壞，避免業務資訊遭受竄改、揭露、破壞或遺失。

(三) 具體管理方案

為落實資安政策，本公司採取多項具體管理措施：

1. **網路與作業安全控管：** 建立資訊作業安全控管機制，針對網路存取、設備維護進行規範，並實施資訊分級與管理。
2. **災難復原機制：** 定期執行防災演練，確保資訊系統在遭遇重大事故時能迅速恢復運作。
3. **事件通報與證據保全：** 建立資安事件處理程序，包含證據保全與缺失分析，確保事件發生時能有效應變。
4. **持續改善：** 定期進行日常資安查檢，並透過內部稽核與外部稽核機制，檢視資安管理之合規性與有效性。
5. **外部資安評等監控：** 使用第三方資安平台管理公司對外資安風險，目前分數維持在低風險的 90 分以上，無任何中、高風險。

二、投入資通安全管理之資源

本公司重視資訊安全投資，投入之主要資源如下：

1. **專責組織與人力：**
   - 設置「資訊安全委員會」及常設性「資訊安全執行小組」，由資訊部門專職人員負責日常維運與監控。
   - 設有「緊急處理小組」負責重大事件之即時應變。
2. 教育訓練與宣導：
   為提升全員資安意識，定期舉辦教育訓練及發布資安宣導。近年執行情形如下：
   - **不定時宣導 ：** 透過內部公告發布最新資安威脅預警及應注意事項。

- **2025/ 6/30：** 資通安全通識影片 & 測驗 (課程時數：2 小時)。
- **2025/11/19 ：**『防範內線交易宣導』及『誠信經營、智慧財產權及營業秘密保護』線上宣導課程。

三、重大資通安全事件

本公司於最近年度及截至目前為止，未有因重大資通安全事件（如駭客入侵、病毒感染、資料外洩等）而遭受重大損失或影響公司營運之情事。

四、資通安全風險與因應措施

(一) 資通安全風險評估

隨著數位科技發展，企業面臨之資安風險（包括網路攻擊、勒索軟體、系統漏洞等）日益複雜。儘管本公司已建立防護措施，但無法保證能完全免除所有惡意軟體或駭客之攻擊風險。潛在風險可能包括：

1. **營運中斷：** 若核心系統遭攻擊可能導致業務暫時停擺。
2. **資料外洩：** 機密資訊或個資遭竊取可能影響公司商譽及觸法。

(二) 因應措施

為降低上述風險，本公司採取以下因應策略：

1. **多層次防禦：** 結合防火牆、端點防護、智能安全運營平台及權限控管，建構縱深防禦網。
2. **備份與復原：** 落實資料備份機制及定期防災演練，確保資料可用性。
3. **持續監控：** 透過日常監控與異常警示，提早發現潛在威脅並進行處置。
4. **加入聯防組織：** 加入政府 **TWCERT/CC** 資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊。