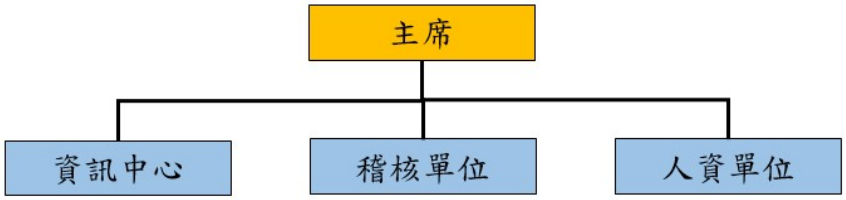
興采實業資通安全管理架構

1. 組織

1.1 資訊安全組織：

- 本公司公司設立『資訊安全組織』，統籌資訊安全及相關政策制訂、執行風險管理與查核。



- 主席:由資訊安全專責主管擔任，負責核准公司資訊安全政策、提供資源與審查重要資安措施，除定期向管理階層報告資通安全執行情形，確保運作之適切性及有效性外，每年至少一次向董事會彙報資安相關重大議題及管理成效。
- 資訊中心: 至少設有資訊安全專責人員一名。
  - 制定資訊安全政策和計畫，確保公司的資訊安全符合相關法規和標準，並監督整個資訊安全組織的運作。
  - 監視公司的資訊系統和網路，發現並回應安全事件，維護系統和網路的安全。
  - 評估公司的資訊安全風險，制定相應的風險管理策略和程序，減少公司面臨的風險。
- 稽核單位:包含外部稽核和內部稽核，定期或不定期進行測試公司的資訊系統和應用程式，檢測安全漏洞和弱點，並提供相應的解決方案，定期追蹤改善情形。
- 人資單位:負責提供資訊安全培訓和教育，提高員工的安全意識和技能，以降低公司面臨的內部安全風險。

2. 資訊安全風險管理機制

2.1 風險識別：

- 通過定期的風險識別活動，識別可能對資訊安全造成威脅的因素，包括內外部因素，如自然災害、網絡攻擊等。

2.2 風險分析：

- 對已識別的風險進行深入分析，包括風險的可能性、影響程度、風險優先級等評估，以確定其對組織的潛在影響。

2.3 風險控制：

- 基於風險分析的結果，制定相應的風險控制措施，包括技術控制、政策措施等，以減輕風險。

2.4 風險監控：

- 建立風險監控機制，持續追蹤已實施的風險控制措施的有效性，及時調整和優化。

2.5 風險回顧：

- 定期回顧風險管理過程，檢討和更新風險評估，以確保風險管理措施的適用性和有效性。

3. 資訊安全政策

- 詳見「興采實業資通安全政策」。

4. 資通安全具體管理方案

4.1 資料分類與處理：

- 制定明確的資料分類標準，並確定相應的處理程序，包括敏感資料的加密、存儲等。

4.2 系統訪問控制：

- 確保僅授予相關人員必要的系統訪問權限，並建立相應的訪問審計機制，以追蹤和審查系統訪問記錄。

4.3 事件監控與應變：

- 建立事件監控系統，並制定應變計劃以應對安全事件和事故，並確保相關人員具備應變所需的培訓和資源。

5. 投入資通安全管理之資源

5.1 人力資源：

- 確保有足夠的資安專業人才參與資通安全管理活動，並提供持續的專業培訓。
- 本公司目前規劃聘任資安顧問,輔導資訊安全改善政策並擬訂改善計畫,以取得資訊安全認證為目標。
-

5.2 技術資源：

- 提供必要的資安工具、技術支援以及相關的安全設備和軟體，並保證其持續更新和升級。

5.3 財務資源：

- 分配足夠的預算以支持資通安全管理活動，包括培訓、技術更新等方面，並確保合理的資源分配。

6. 資通安全風險評估

6.1 定期評估：

- 定期進行全面的資通安全風險評估，包括內部和外部威脅的評估，以確保風險評估的準確性和全面性。

6.2 風險評估報告：

- 撰寫風險評估報告，明確評估結果和提出改進建議，並確保報告得到相應人員的審批