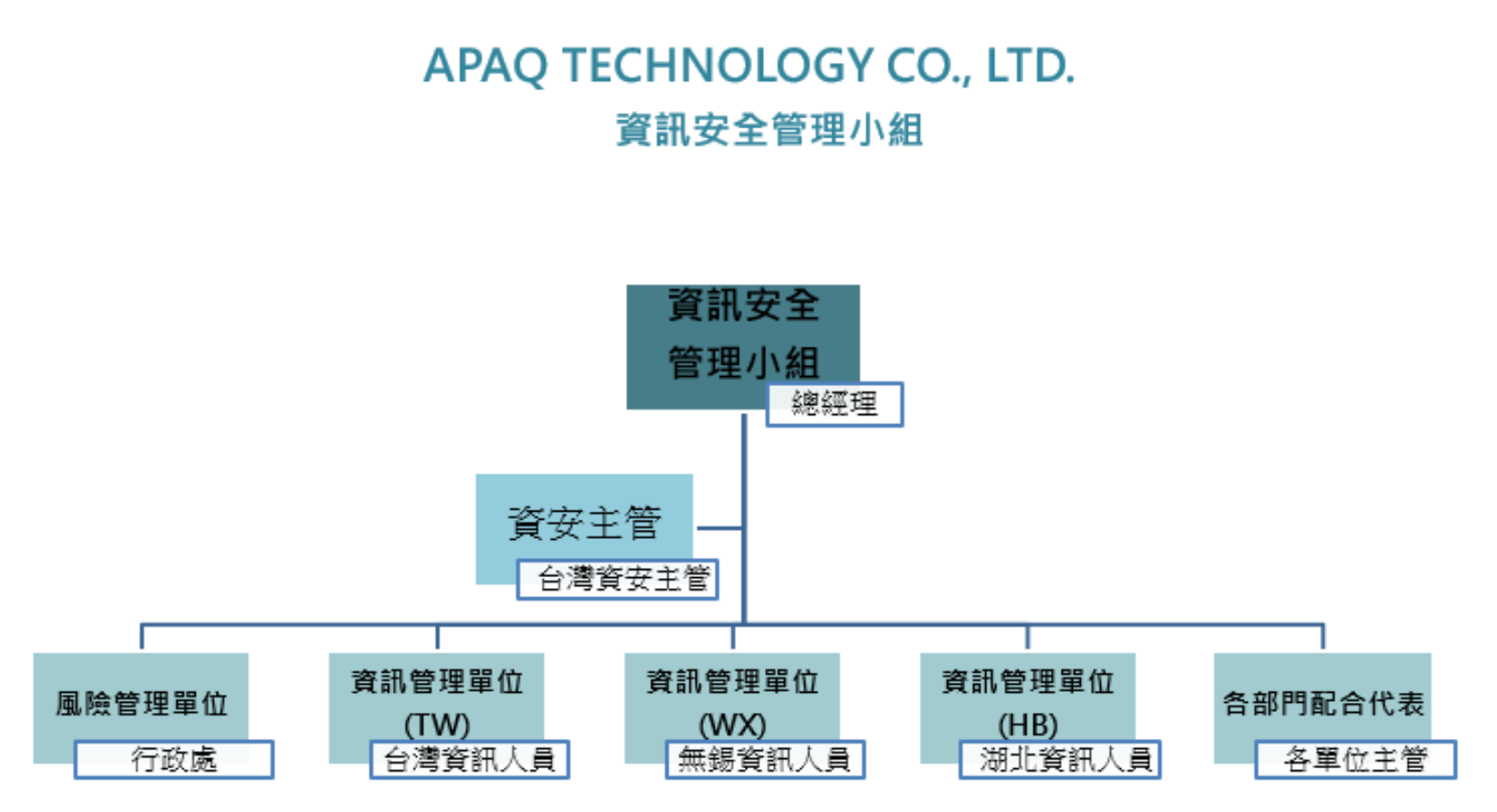
資通安全管理方案及預防措施

◆資訊安全風險管理架構-2024



◆資訊安全

持續對資訊安全精進治理與強化防衛能力，所有資訊作業除了符合內稽內控規範外，更需符合國內、外法規。並確認近三年皆無遺失關鍵技術資訊或顧客資料之情事。

◆資訊安全管理提升

為提資訊安全管理，本公司持續對資訊安全，精進治理與強化資安管理機制。並於2019年度起，建立整體資訊安全管理小組，訂立資訊安全政策以及具體管理方案，負責審視各子公司資安治理政策，監督資安管理運作情形。並定期向董事會報告資安治理概況。全方位規劃，資訊安全治理，規劃，督導及推動執行，建構全面的資安防護能力及同仁良好的資訊安全意識。

◆投入資訊安全管理資源

1. 總設置人數: MIS共五人，資安相關單位人數共計13人。
2. 資料備份次數:每年365次，設備點檢:每年12次，災難還原演練:每年1次。
3. 管理單位會議:每年26次。

◆資訊安全政策

透過資訊安全小組，擬定資安維護作業管理辦法，建立資訊安全運作模式，針對資安維護、治理、風險、同仁意識與宣導，進行全方位的資安管理。

◆資訊安全管理機制

資安策略主軸聚焦法令遵循、資安治理、內部控制，三個面向來進行，從制度到流程管理，從人員到組織，全面性提升資安防護能力。

有鑑於目前資安新趨勢，如DDoS(Distributed Denial of Service)攻擊、勒索軟體、社交工程攻擊、偽冒網站等，每年與國際資安廠商交流，透過資訊共享，針對不同路徑、情境，進行DDoS等威脅，更新防護資訊，以期能在第一時間偵測，並完成阻檔。

除網路硬體結構外，另設置公司內部《資訊安全管理辦法》，自執行面著手，並推動流程管理、意識與宣導工作，以有效從軟硬體面及執行面，降低公司內外部資安風險。

資安策略		
法令遵循	● 精進管理制度 ● 掌控風險及強化規範 ● 定期更新防護資訊	持續精進管理制度，資訊安全架構設計，及時更新防護資訊
資安治理	● 定期檢視 ● 建立合規循環機制	建立合規循環機制，定期檢視及修訂內部作業規範
內控流程	● 流程管理建立 ● 強化資安意識與宣導工作	強化內部流程管理，深化管理意識，於軟硬體之外，實務進行內部資安控管

◆管理方案

為確保資訊安全並妥善管理，本公司訂定資訊管理辦法，並明定相關權責，表單及流程，內容如下:

- 資訊軟、硬體設備購買之規劃與評估
- 資訊環境安全管理之規劃與實施
- 郵件，公網，ERP系統權限管理
- 資訊部門之資產管理，維修，出借或資產移轉處理
- ERP系統問題及帳務問題排除
- ERP系統客制程式及外掛程式管理
- BI報表程式設計
- EPR系統復原
- 電腦軟體版權控制
- 人員外部網路權限管理

◆預防措施

為確保資訊安全並妥善管理，本公司依資訊管理辦法及資訊循環內控制度，預防措施如下：

預防措施-2024	
資訊軟、硬體設備購買之規劃與評估	EDR端點防護、NAS異地備援
外部病毒侵入之防火牆規劃與實施	防火牆設置與病毒碼更新、EDR端點防護
內部檔案-防毒軟體規劃與實施	電腦防毒軟體與病毒碼更新
資訊環境安全管理之規劃與實施	各系統資訊定期備份設置
郵件，公網，ERP系統權限管理	各系統資料訊息權限設置
郵件，公網，EPR系統復原	各系統備份及災難應變設置
電子計算機處理部門之功能與職責劃分	資訊安全之權限設置

◆重大資通安全事件

截至113年度為止，無重大資通安全事件。