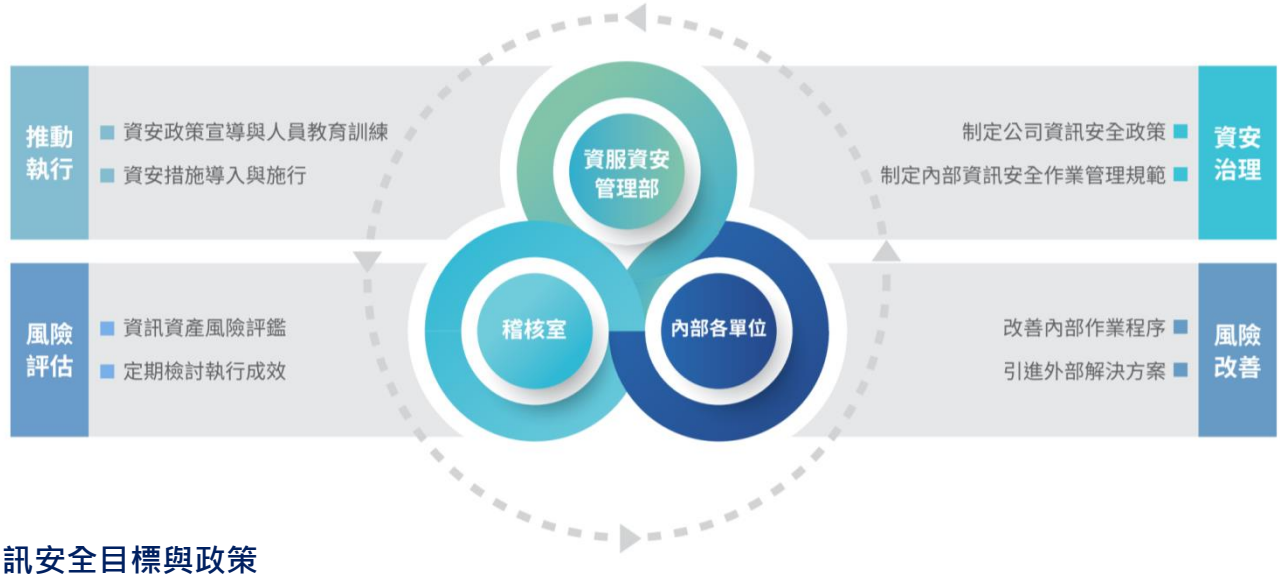
資訊安全政策與管理方案

資訊安全風險管理架構

本公司資訊安全之權責單位為資服資安管理部，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實，並每年至少一次向董事會報告資訊安全執行計畫與執行情形，以確保內部資安管理機制持續有效運作。組織運作模式採用PDCA（Plan-Do-Check-Act）循環式管理，建構完整的資安管理系統，以有效防範資訊安全事件發生，確保達成資訊安全目標，並持續優化改善。



資訊安全目標與政策

資訊安全目標

透過適合集團業務型態之資訊安全政策的訂定，並投入適當資源，以達到確保資訊的機密性、完整性與可用性。

1. 確保資訊機密性，落實資料存取控制，資訊需經授權人員方可存取。
2. 確保資訊的內容正確且完整，避免未經授權之修改。
3. 確保資訊系統之可用性，提供業務營運之所需。
4. 確保資訊作業均符合相關法令規定要求。

資訊安全政策

1. 加強集團資訊系統及網路環境安全，防止電子機密資料洩漏。
2. 建立資訊安全事件應變處理程序，避免傷害擴大。
3. 辦理資安教育訓練，強化全體同仁對資訊安全之認同與防護知識。
4. 推動資訊安全管理制度，落實集團資訊安全管理作業，並定期檢討執行成效，達成全面資訊安全之目的。

具體管理方案

在資訊安全強化部分，除確保備份及異地存放作業正常運作、採用防火牆、入侵偵測系統、資料外洩防護(DLP)、防毒牆及防毒軟體等資安措施外，更導入網路攻擊防禦系統來偵測進、出網路上之進階威脅和針對性攻擊，如惡意程式、幕後操縱 (C&C) 通訊以及標準資安防護所無法偵測的隱匿駭客活動，以提升資安等級。

2019年資訊系統故障率為0.311%，可用度為99.689%，最主要故障發生原因為：(1)Storage韌體Bug，(2)資料庫主機負荷過重，(3)虛擬主機系統底層異常。均已採取相對應解決方式：(1)檢視所有Storage韌體版本並更新，(2)資料庫採雙主機，並已讀寫分流機制降低負荷，(3)更新虛擬主機底層版本，以降低未來資訊系統故障率。

資訊安全管理措施		
類型	說明	相關作業
權限管理	人員帳號、權限管理與系統操作行為之管理措施	• 人員帳號權限管理與審核 • 人員帳號權限定期盤點
存取管控	人員存取內外部系統及資料傳輸管道之控制措施	• 內/外部存取管控措施 • 機敏資料外洩管控 • 操作行為軌跡記錄
外部威脅	內部潛在弱點、中毒管道與防護措施	• 主機/電腦弱點防護及更新措施 • 病毒防護與惡意程式檢測 • 源碼檢查/滲透測試 • 網路威脅監控
系統可用性	系統可用狀態與服務中斷時之處置措施	• 系統/網路可用狀態監控及通報機制 • 服務中斷之應變措施 • 資訊備份措施、本/異地備份機制 • 定期災害復原演練