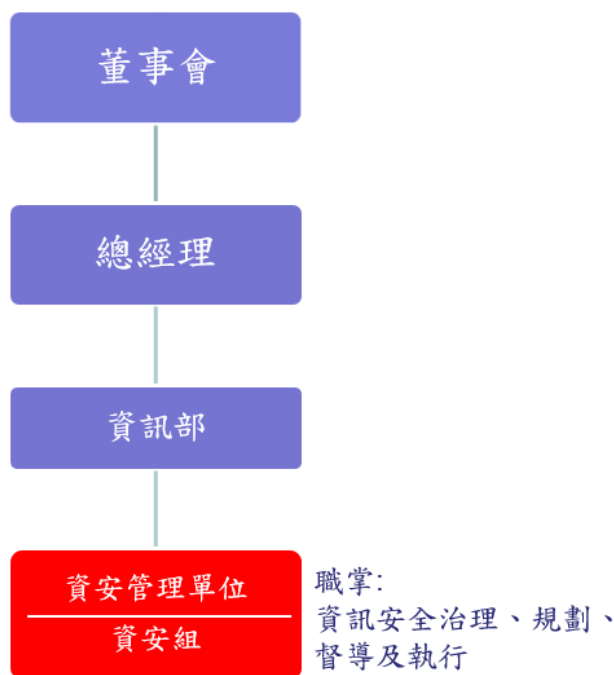


資訊安全

岱宇國際持續對資訊安全精進治理制度與強化防衛能力，所有資訊作業除了符合國際資安標準外，更要符合國、內外資訊安全法令法規，2017年我們加強個資投訴案件的認定，經確認並無侵害顧客隱私權或遺失顧客資料之情事。

資訊安全治理制度

為提升資訊安全管理，2017年7月由資訊部-資安組，負責全公司資訊安全治理、規劃、督導及推動執行，以建構出全方位的資安防衛能力及同仁良好的資訊安全意識。



資訊安全管理機制

岱宇國際的資安策略主軸聚焦資安治理、法令遵循及科技運用三個面向來進行，從制度到科技，從人員到組織，全面性提升資安防護能力。

有鑑於目前資安新興趨勢，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，透過專案的合作，定期關注資安議題並規劃因應計畫，針對不同資安情境，進行 DDoS、ATM 等攻防演練，強化處理人員的應變能力，以期能在第一時間即偵測到並完成阻擋。

資安策略		
資安治理	<ul style="list-style-type: none"> ● 精進管理制度 ● 掌控風險及強化防範 ● 打造聯防體系 	持續精進管理制度，包括強化教育訓練、資訊安全基礎架構設計，並深化保護技術。
法令遵循	<ul style="list-style-type: none"> ● 定期檢視/修訂 ● 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以符合國際資安標準及個海外地區法令。
科技運用	<ul style="list-style-type: none"> ● 內外部資料收集 ● 運用數據分析 ● 預測威脅及決策 	運用新技術，預測資訊安全風險並及早作出安全決策。

資訊安全事件

2019 年 3 月資訊部-資安組發現 dyaco.com.tw 網域郵件被外部郵箱視為垃圾郵件，經查郵件收發紀錄發現有同仁郵件帳號被盜用，起因於密碼設定過於簡易且沒有定期變更密碼，資訊部-資安組立即啟動郵件伺服器安全性檢查，並加強監控機制和提升帳號密碼複雜度規則，全面重新設定所有同仁帳號密碼，與本次事件相關之 3 項強化與精進措施已於當月內完成。