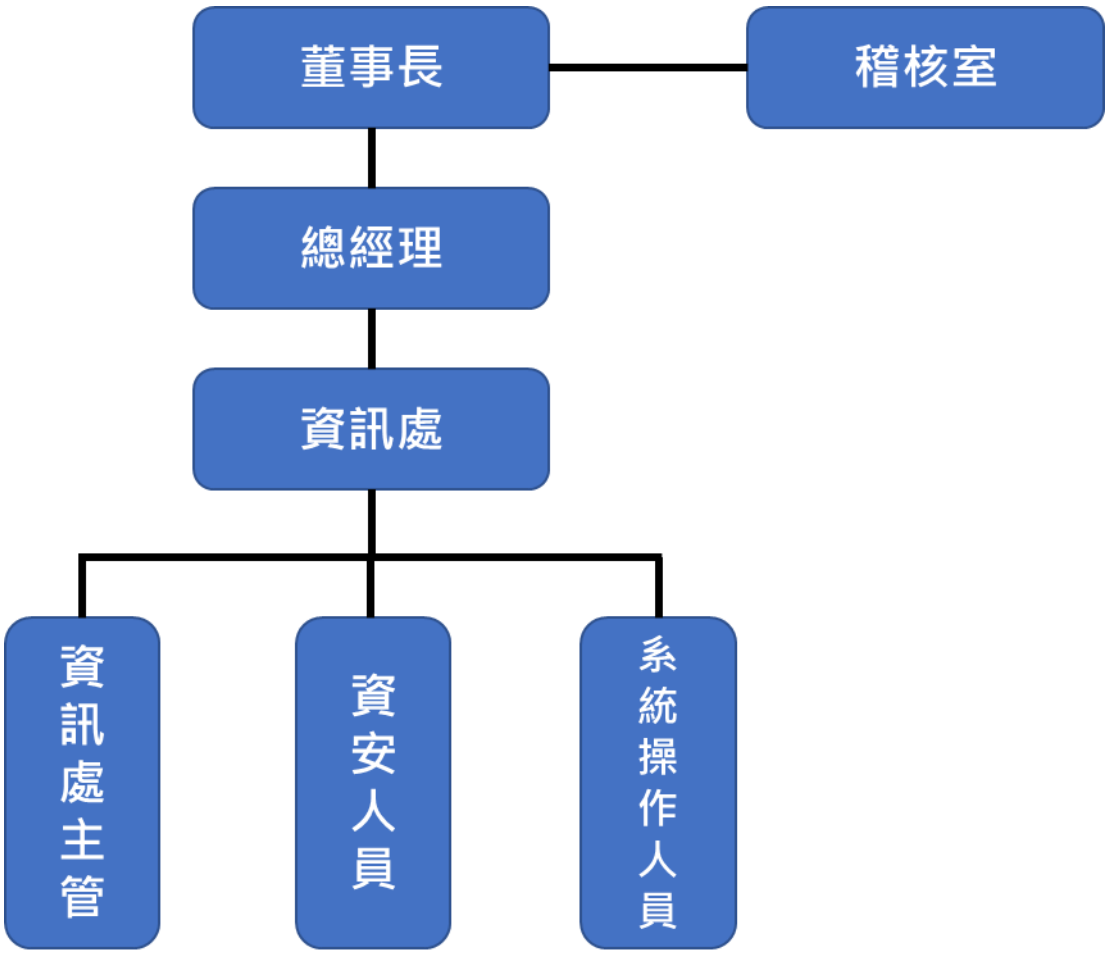
➢ 資訊安全管理架構

本公司資訊安全之權責單位為資訊部，該部設置資訊主管乙名，與專業資訊人員數名，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。

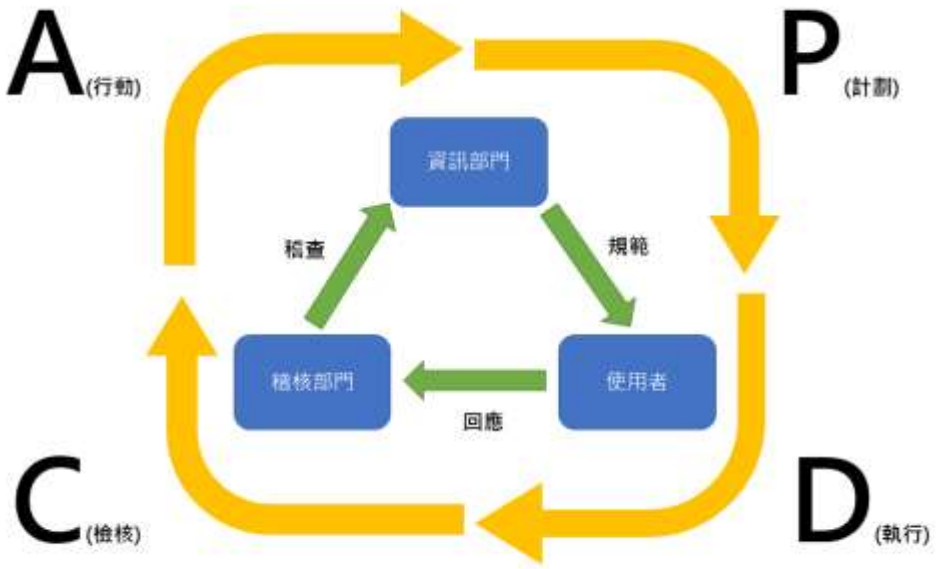
➢ 資訊安全組織架構



➢ 資訊安全目標

- 保障公司資訊軟硬體設備及智慧財產。
- 避免公司營運業資訊及職務機密外洩。
- 尊重智慧財產權，避免公司及同仁觸法之可能。
- 提高穩定安全的資訊作業環境，以提昇整體工作效率。

➢ 資訊安全循環



➢ 資訊安全管理措施

資訊控制	控制說明
程式與資料存取控制	程式設計與開發人員如何控制程式新舊版本等相關規範。
資料輸出/輸入控制	資料輸入與輸出系統如何驗證與避免錯誤資料輸入等相關規範。
資料處理控制	各項操作手冊與電子檔如何更新與保存等相關規範。
機房設備安全控制	資訊機房內外環境、設備實體安全控管等相關規範。
檔案備份作業控制	檔案與生產相關之重要系統的備份方式與時間等相關規範。
資料保存控制	依法律規範須保留與公司內重要研究成果之資料如何保存等相關規範。
系統復原控制	災害發生時該如何應變與避免損失擴大等相關規範。
網路安全控制	公司網路內網與公司外網在使用上該如何防護等相關規範。
作業相關系統使用控制	明訂公司內會使用之資訊服務的使用限制等相關規範。

➢ 112 年度資安風險管理主要措施與執行情形

項目	執行要點
存取管制	● 資料交換方式管控。 ● 資料外洩管控。 ● 操作行為軌跡紀錄。
防毒更新	● 防毒防駭的保護措施。 ● 定時更新防毒軟體病毒碼，降低中毒風險。 ● 防毒軟體版本更新。
防火牆防護	● 防火牆設定連線規則，預設只開放基本上網、郵件連線。 ● 應用服務控管，限制存取。 ● 每月監控分析防火牆防護數據。 ● 更新防火牆韌體。
伺服器及網路設備監控	● 使用 Cacti 將伺服器及網路設備納管。 ● 定期更新納管設備之網路吞吐量及存活情況。 ● 設備斷線立即以電子郵件方式通知管理者。