麗臺科技資訊安全管理

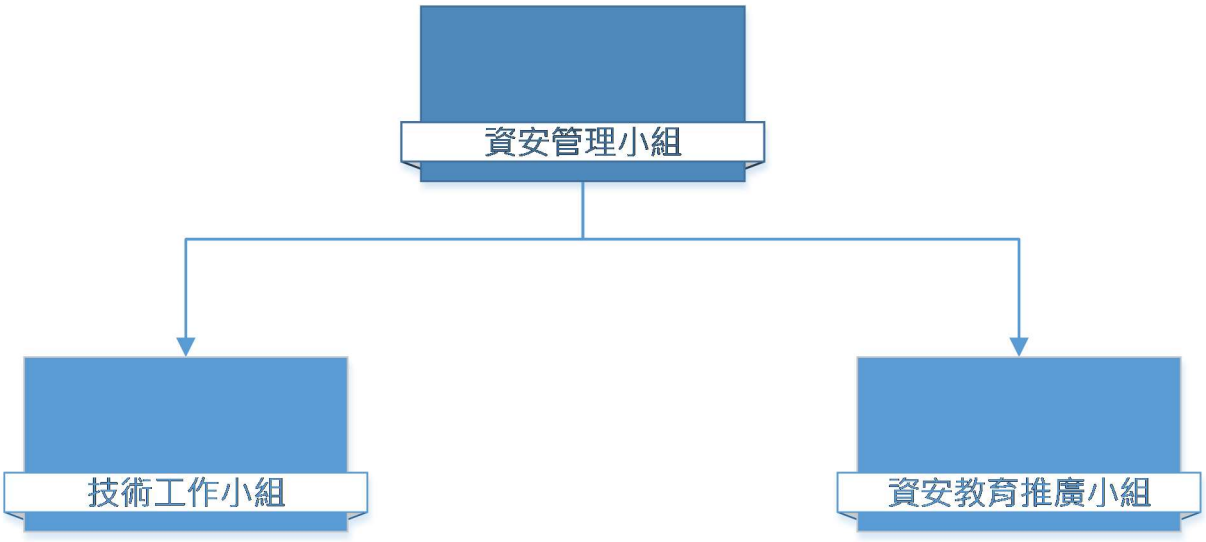
目的

因應全世界資訊安全的潮流趨勢，面對數位化及行動化日益複雜的應用環境，以及維護麗臺科技股份有限公司（以下簡稱本公司)的創新及營運，建立資訊的機密性，完整性及可用性，避免任何類型的資安威脅與破壞，為了確保企業持續營運，提供員工與客戶一個安全可信賴的環境與永續使用。

一、風險管理架構

- 資訊安全組織架構

本公司資訊部門為電腦中心，設置資訊主管一名及專業資訊人員數名，負責訂定資訊安全規範、規劃及執行資訊安全技術支援工作，並定期宣導資訊安全觀念，降低資訊安全風險。



- 針對風險管理，本公司使用三個面向對應及減少風險的影響程度

風險管理計畫	風險事件處理	風險對策改善
導入適當的控制措施	及時與正確的處理	檢討與持續改善
防毒、防駭機制 防資料外洩 弱點掃描、偵測與回應 備份機制	減少影響範圍，防止擴大 及時還原，恢復運作	依缺失進行檢討 提出改善計畫 納入風險管理

二、公司資訊安全政策

節錄本公司制定之資訊安全政策規範，依下列項目做實際控管

- 帳號與密碼原則

  制定較嚴謹之密碼原則，定期更換密碼，並嚴禁將密碼交付他人使用…

- 資訊硬體使用

  嚴禁攜入與使用非公司資產之資訊設備…

- 資訊軟體使用

  嚴禁員工自行安裝任何未經電腦中心安裝或同意之非授權軟體…

- 檔案管理

  個人公務檔案、實體機密文件與檔案文件資訊的儲存設備，須妥善保管，不得讓人輕易存取…

- 郵件管理

  來歷不明、有質疑性郵件勿開啟並立即刪除…

- 網路使用

不得試圖冒用、竄改配發 IP、私自接續公司網路環境、架設無線發收設備等以擴張使用…

- 定期發布資安政策、案例與宣導

定期在公司內部網站或以郵件方式發佈相關資安政策、發生案例、宣導等，員工應隨時注意並配合遵守…

三、具體管理方案

2020~21 年本公司執行的具體方案，並持續加強改進

- 更新與提升 IT 基礎架構

1. 購置新伺服器硬體與軟體，並更新伺服器與用戶端作業系統到最新版本
2. 導入弱點掃描系統，減少因漏洞而產生的資安問題
3. 網路設備更新，增加備援線路與設備，避免因單一設備或線路損壞而影響公司營運

- 強化備份機制

1. 購置新款備份方案
2. 制定新備份、還原與災難演練 SOP
3. 設置主機備援機制，減少災難後停機的時間

- 加強員工資安概念

現在的資安事件不只是外部入侵，越來越多是由內部員工設備感染，進而引發大規模資安事件

1. 定期發布資安政策、案例與宣導

2. 員工資訊安全教育訓練，不只是在公司，在任何地方都應提高資安意識

- 評估導入資安相關認證

2021 年評估與協助相關部門導入 ISO27001:2013，並分析資訊安全管理現況與 ISO27001 標準規範的差距，作為規劃資訊安全管理架構之重要依據