

資訊安全政策及管理方案

資訊安全管理

資訊安全風險管理架構

- 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，並定期報告公司資安治理概況。
- 本公司稽核室為資訊安全監理之督導單位，該室設置稽核主管乙名，與專職稽核人員數名，負責督導內部資安執行狀況，若有查核發現缺失，旋即要求受查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。
- 組織運作模式-採 PDCA (Plan-Do-Check-Act) 循環式管理，確保可靠度目標之達成且持續改善。



資訊安全政策及具體管理方案

本公司資訊安全管理機制，包含以下三個面向：

(一) 制度規範：訂定公司資訊安全管理制度，規範人員作業行為。

(二) 科技運用：建置資訊安全管理設備，落實資安管理措施。

(三) 人員訓練：進行資訊安全教育訓練，提昇全體同仁資安意識。

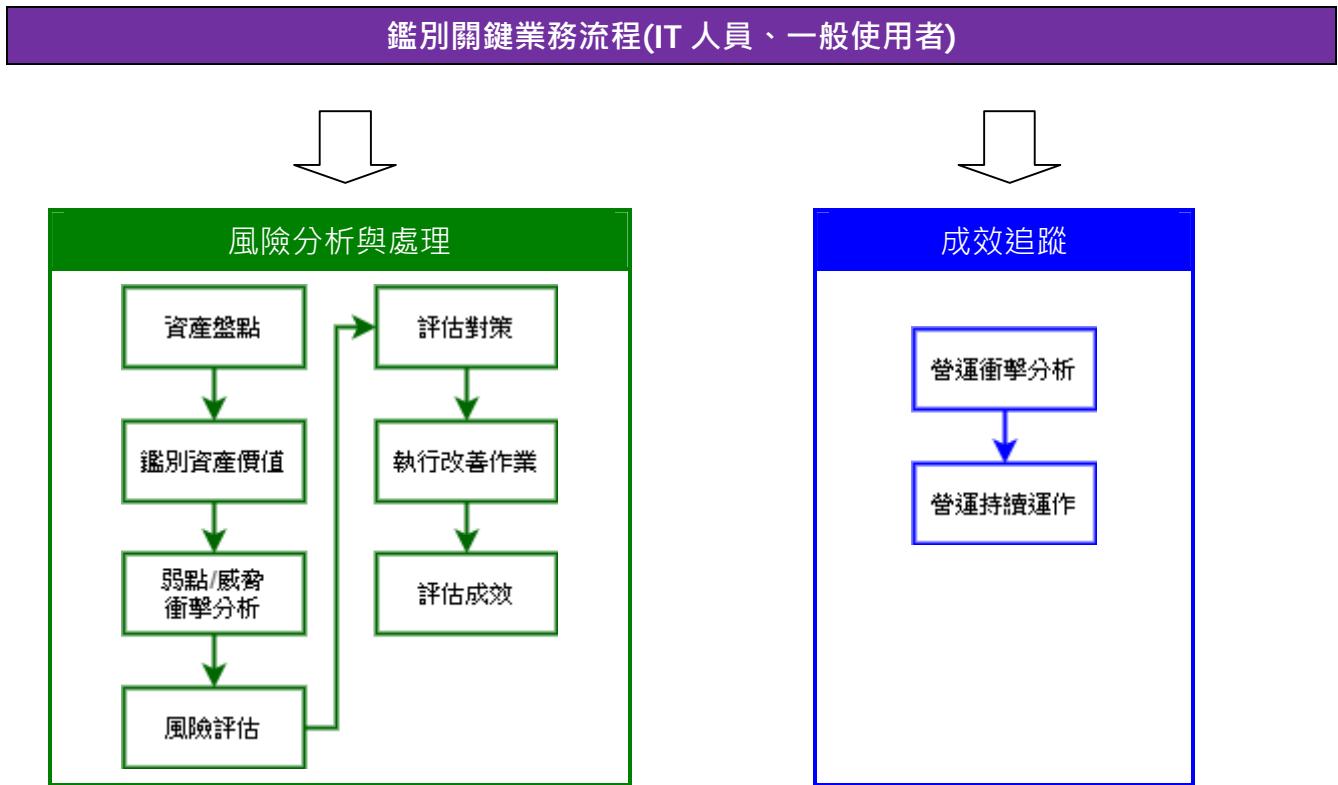
管理措施說明如下：

- 制度規範：本公司內部訂定多項資安規範與制度，以規範本公司人員資訊安全行為，每年定期檢視相關制度是否符合營運環境變遷，並依需求適時調整。
- 科技運用：本公司為防範各種外部資安威脅，除採多層式網路架構設計外，更建置各式資安防護系統，以提昇整體資訊環境之安全性。此外，為確保內部人員之作業行為符合公司制度規範，亦設計作業程序和導入資安系統工具，落實人員資訊安全管理措施。
- 人員訓練：本公司每季定期實施新進人員資訊安全教育訓練實務課程，並建置數堂線上學習 (E-Learning) 資訊安全課程，藉以提昇內部人員資安知識與專業技能。

資訊安全管理措施

本公司定期審視內部資訊安全規範並報告資安治理概況。

本公司資訊風險評估程序如下：



本公司實施之資訊安全管理措施，包含如下：

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 資料外洩管道之控制措施 操作行為軌跡記錄分析
外部威脅	內部系統潛在弱點、中毒管道、與防護措施	主機/電腦弱點檢測及更新措施 病毒防護與惡意程式偵測
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 資料備份備援措施、本/異地備援機制 定期災害還原演練

資安事件通報程序

本公司資通安全通報程序如下，資安事故之通報與處理，皆遵守該程序之規範進行。

