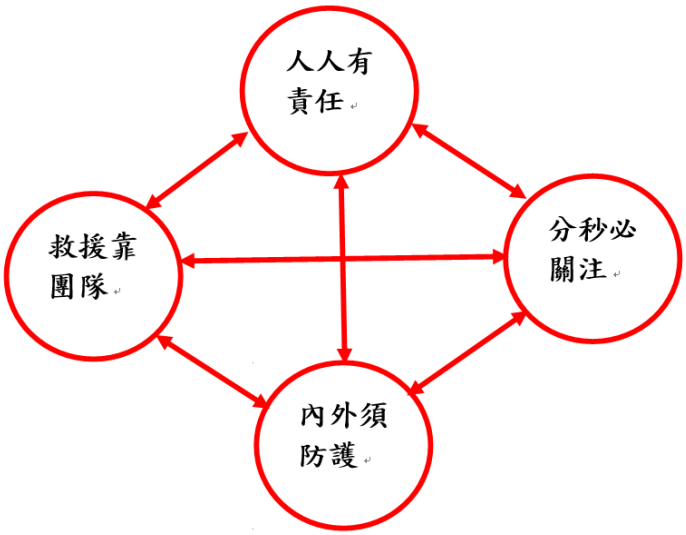
台灣航業股份有限公司
資訊安全風險管理架構

一、資訊安全政策

1. 本公司依「公開發行公司建立內部控制度處理準則」第九條「電腦化資訊系統處理」之規定制定相關內部作業規定，以降低網路環境多樣化所帶來不可預期的資安風險。
2. 資訊安全風險管理流:人人有責任、分秒必關注、內外須防護、救援靠團隊



3. 持續對資訊安全完備治理制度與提升防禦能力，各項資訊作業符合資訊安全，符合資訊安全法令法規。

二、資訊安全風險管理架構

為掌握資訊安全風險管理，應對**資訊安全**事件說明處理方式：

(一)預防管理：定期自主盤點檢驗，從流程與技術多方面著手，主動預防資安事故。

1. 防入侵：主動**防禦來自內外網攻擊**，侵入資訊系統造成破壞。
2. 防意外：主動**預防環境內因素**（故障/跳電／病毒／設備遺失）造成的生產損失。
3. 防外洩：加強誠信宣導，防範公司業務機密訊息、文件外洩。
4. 落實演練：運用演練經驗，在最短時間內恢復正常，維持企業體持續營運。
5. 資訊安全通知流:以電子郵件通知全體員工及業務往來廠商，彼此均加強資訊安全。
6. 防範更新資訊流:每次登入公司內部網域之電腦，更新防毒碼。

(二)事件發生時：

緊急聯絡支援團隊，及時且迅速配合追查破壞原因，立即阻擋、排除破壞，降低損害。

(三)善後處理：追查原因並加強系統防禦功能

1. 避免問題發生：調閱系統紀錄，追蹤問題原因，並予補救，建立新預防措施。
2. 檢測方法再強化：多項檢測，提高網內、外防範機制。

三、具體管理方案

(一)資訊安全基礎

本公司為強化整體資訊安全，每年具體進行多項資訊安全強化專案，範圍包含:

1. 強化網路內、外安全之偵測系統及設備。
2. 提升員工資安意識。

(二)資訊安全落實

資安教育訓練：全體同仁對**資訊安全**認識。新進人員教育訓練必加入資安課程。