

## 資訊安全風險管理架構

由資訊部負責統籌資訊安全及相關事宜，擬定相關內部控制程序管理，並定期進行內部資訊安全檢查。

## 資訊安全政策

### (一) 目的：

為建置本公司安全及可信賴的資訊運作環境，維持業務持續運作，降低資訊作業風險，保障資訊服務使用者之權益，建立資訊安全管理系統，規範本程序為最高指導方針，以達成資訊安全管理的目標。

### (二) 範圍：

本公司資訊安全管理範圍，包括本公司所屬各據點資訊作業之相關人員、管理制度、應用程式、資料、文件、媒體儲存、硬體設備及網路設施。

### (三) 目標：

避免資訊系統遭受來自內、外部人員不當使用或蓄意破壞，或當已遭受不當使用、蓄意破壞等緊急事故時，公司能迅速應變處置，並在最短時間內回復正常運作，降低該事故可能帶來之經濟損害及營運中斷。

### (四) 程序：

執行資訊機房、網路安全、系統開發及程式修改、資料安全、資訊保密、智慧財產權、資訊委外等管理。

## 具體管理方法

本公司為防範各種外部資安威脅，除採多層式虛擬網路架構設計外，更建置各式資安防護系統，並採用防火牆大廠品牌，更新防火牆的應用程式防護，且針對人員存取外部有危險的網站時，即刻發出警示，封鎖不讓操作人員進入。

除每台電腦安裝防毒軟體之外，並採集中式防護管理，防範電腦病毒外並能及時將防毒碼更新，且送達資訊部主要網管人員做警示。