# 資訊安全管理政策與管理方式

## 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，資訊部人員配置為資訊主管乙名，專業資訊人員四名，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，並定期由稽核室查核資訊安全執行狀況，並向董事會呈報公司資安治理概況。

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，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。

## 資訊安全政策及具體管理方案

1.本公司資訊安全管理政策，包含下列三面向：

(1)制度規範：訂定公司資訊安全管理制度，規範人員作業行為。

(2)科技運用：建置資訊安全管理設備，落實資安管理措施。

(3)人員訓練：進行資訊安全教育訓練，提昇同仁資安意識。

2.管理措施說明如下：

(1)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，並訂有員工使用電腦同意書，內含員工資訊使用安全行為，每年定期檢視相關規定是否符合營運環境變遷，並依需求適時調整。

(2)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，並建置各類資安防護系統，以提昇整體資訊環境之安全。另為確保內部人員之符合公司制度規範，亦設計作業程序和導入資安系統，落實人員資訊安全措施。

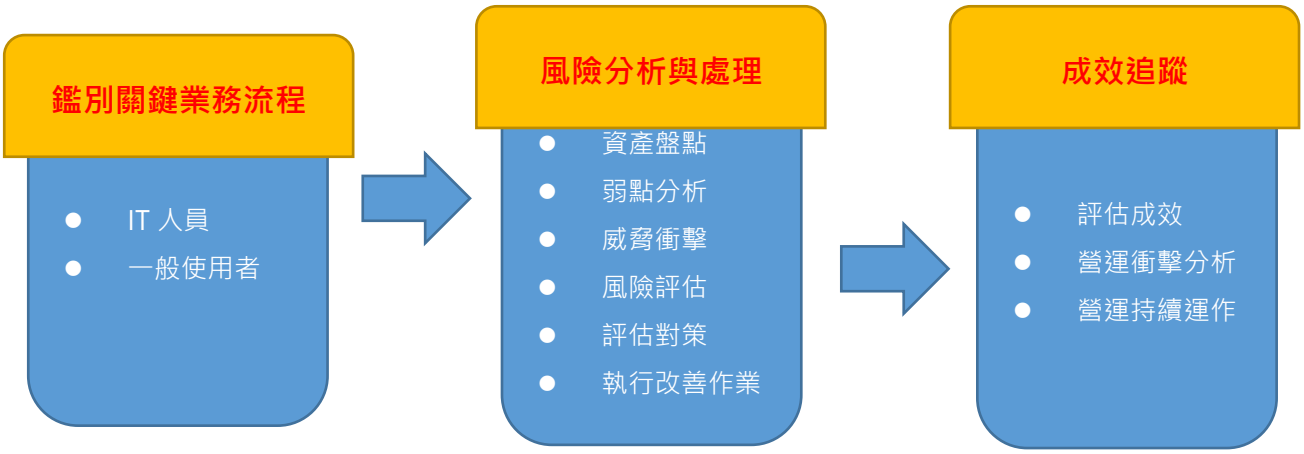
(3)人員訓練：

本公司除鷔近人員教育訓練宣告公司資安政策之外，並建置數堂線上學習 (E-Learining) 資訊安全課程，對內部人員定期實施資訊安全教育訓練課程，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，根據資產價值、弱點、威脅與影響性，分析內部風險水平，並以此風險評估結果制定安全措施強化項目，精進且提升整體資訊安全環境。

1.本公司資訊風險評估程序如下：




2.本公司實施之資訊安全管理措施，包含如下：

| | | |
|---|---|---|
| 權限管理 | 人員帳號、權限管理與系統操作行為管理 | ● 內部人員帳號權限管理與審核 |
| 存取控管 | 人員存取內外部系統及資料傳輸管道之控管 | ● 存取管控措施<br>● 操作行為紀錄 |
| 外部威脅 | 內部系統潛在弱點、病毒管道與防護措施 | ● 伺服器弱點檢測<br>● 防毒系統檢測報告 |
| 系統可用性 | 系統可用狀態與服務中斷之處理措施 | ● 系統與網路狀態監控<br>● 服務中斷應變措施<br>● 資料備份備援措施<br>● 災難還原演練 |

## 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。**