資訊安全管理

1. 目的

規範資訊安全政策、組織架構、人員角色的區分、權責定義及運作方式，以確保所有的資訊安全管理工作都有明確的負責人，且當資訊事件發生時有正確的處理方式及程序，以維護公司資訊的安全。

2. 適用範圍

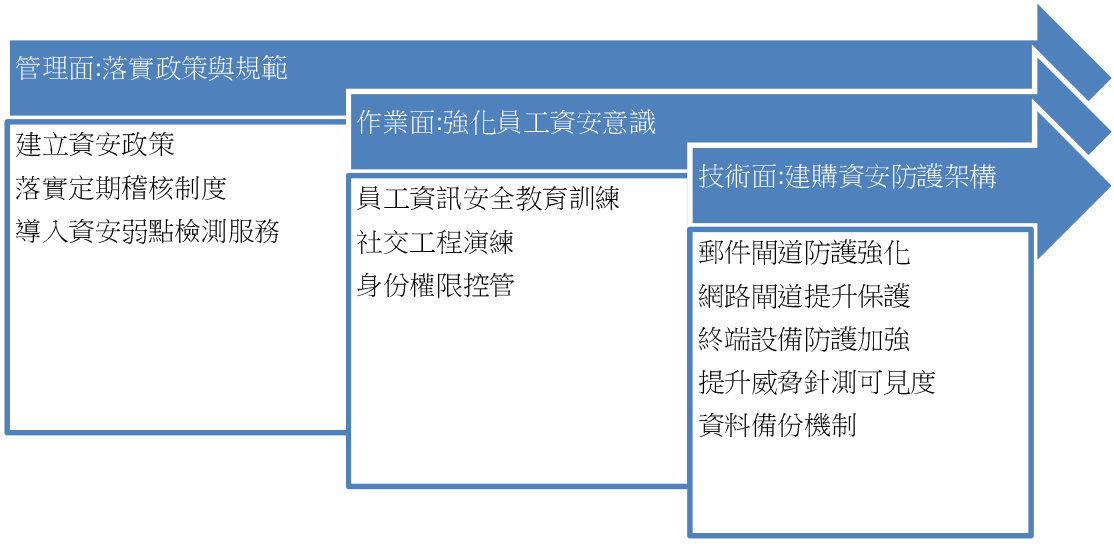
全集團

3. 作業流程

本辦法之訂定是以 ISO27001 資訊安全管理系統為參考範本，分為：

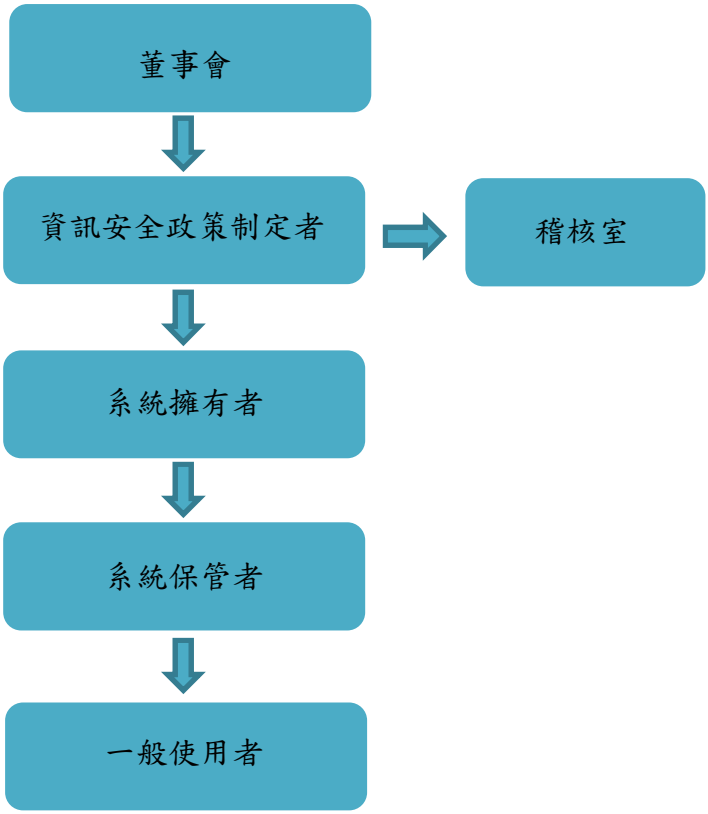
3.1 資訊安全政策

妥善保護公司內部、客戶及供應商之任何資訊，並分為管理面、作業面、技術面實施。



3.2 組織架構

資訊安全是公司每一個部門與人員的責任，上至總經理、各部門主管，下至每位員工，所有人員都應落實公司之資訊安全政策；其組織架構同現有公司組織，並分為：



3.2.1 資訊安全政策制定者

由總經理擔任。

3.2.2 系統擁有者

由各事業部之部主管擔任。

3.2.3 系統保管者

由資訊處人員負責。

3.2.4 一般使用者

在工作上會使用到資訊系統資源的公司內員工。

3.3 資產安全分類與人員安全

資產(料)進行安全分級與人員資訊安全規範，並於每年度進行 2 次資安教育訓練。

3.4 電腦作業

管制環境作業安全、設備進出管制及電腦作業操作記錄控管。

3.5 通訊作業

提供良好穩定性資訊系統服務及資料通訊傳輸安全。

3.6 存取控制

系統存取控管

3.7 系統開發及維護

制定開發流程標準程序

3.8 電腦系統應變及復原計劃

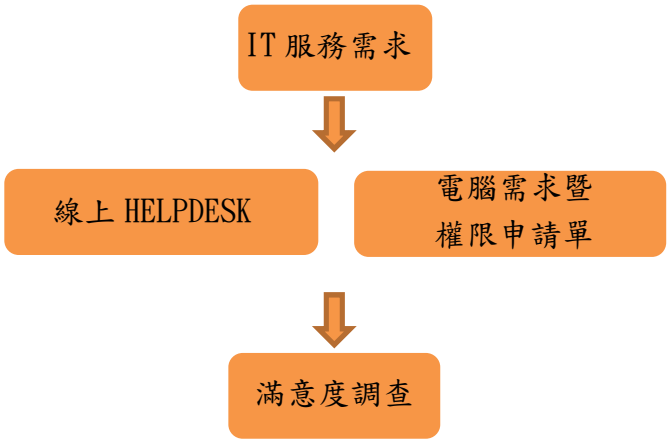
有關火災、地震、颱風等災害，擬定緊急應變計劃並針對電腦設備、系統故障或毀損所造成的損失評估。

3.8.1 災害狀況及影響範圍之評估

災害依狀況輕重不同分級

3.8.2 制定各狀況之解決方案及其復原程序.

3.9 資訊服務流程:



考量公司規模，目前資安規範及作業運作機制已足以防護重要資安風險，未來將依實際需求持續評估後續作法。