

資通安全管理

為強化資通安全之風險管理及維護資訊的機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，故成立資通安全執行小組，負責建置資通安全風險管理架構、訂定資通安全政策及具體管理方案及投入資通安全管理之資源等，並定期檢討資通安全政策，以確保完善的資通安全機制。

(一)資通安全風險管理架構

- 本公司資通安全執行小組(屬集團總經理室)。
- 本公司於2023年6月3日設置資訊安全專責主管及一名資訊安全專責人員。
- 資通安全執行小組定期檢討資通安全管理政策及相關辦法。
- 各單位成員皆依相關辦法確實執行。
- 日常營運時定期進行防火牆、網路設備、伺服器等設備之檢核，以即時發現問題。
- 進行資通安全風險評估，配合稽核單位查核以確保作業之正確性及有效性。
- 遇有錯誤、漏洞與風險立即進行改善，以建構資通安全之持續改善管理循環。

(二)資通安全政策

1.目的

為強化資通安全之風險管理，確保資料、系統、設備及網路安全，特訂定本政策。

2.資通安全目標

- 確保公司資通作業之正確性、可用性、完整性與機密性。
- 避免內、外部資安事件之威脅。
- 於資安事件發生時，公司能迅速應變，在最短時間內恢復正常運作，降低資安事件對公司的後續影響。
- 加強資安訓練，確保營運永續
- 督導全體同仁落實資訊安全管理工作，每年持續進行適當的資訊安全教育訓練，建立「資訊安全，人人有責」的觀念，促使同仁瞭解資訊安全之重要性，促其遵守資訊安全規定，藉此提高資訊安全智能及緊急應變能力，降低資訊安全風險，達持續營運之目標。

3.資通安全管理措施

成立資通安全執行小組，訂定資通安全政策及具體管理方案，落實資

通安全作業循環以確保資通安全。

A.落實資訊安全，強化服務品質

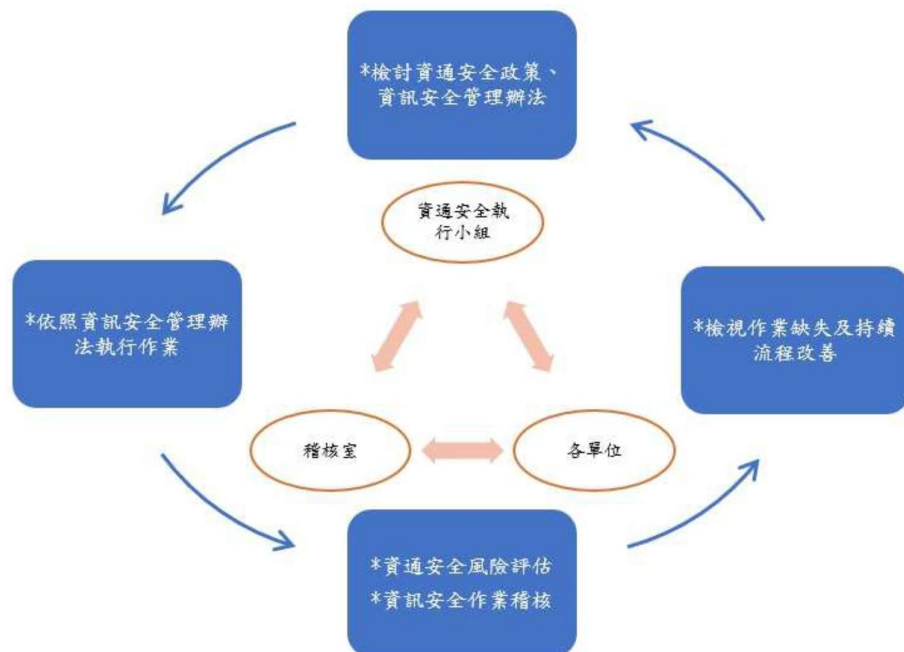
由全體同仁貫徹執行ISMS，所有資訊作業相關措施，應確保業務資料之機密性、完整性及可用性，免於因外在之威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險，選擇適切的保護措施，將風險降至可接受程度持續進行監控、審查及稽核資訊安全制度的工作，強化服務品質，提升服務水準。

B.加強資安訓練，確保營運永續

督導全體同仁落實資訊安全管理工作，每年持續進行適當的資訊安全教育訓練，建「資訊安全，人人有責」的觀念，促使同仁瞭解資訊安全之重要性，促其遵守資訊安全規定，藉此提高資訊安全智能及緊急應變能力，降低資訊安全風險，達持續營運之目標。

C.即時緊急應變，迅速資安復原

訂定重要資訊資產及關鍵性業務之緊急應變計畫及資安復原計畫，並定期執行各項緊急應變流程的演練，以確保資訊系統失效或重大資安事件發生時，能迅速復原，確保關鍵性業務持續運作，並將損失降至最低。



D.審查及修訂

本政策由集團總經理核准後實施，修正時亦同。

(三)具體管理方案

1.本公司之資通安全具體管理方案，由資通安全事件發生時間點區分，可分為事前預防、日常營運維持、資安事件處理。具體管理方案內容如下：

類別	說明	內容
預防外部入侵	安裝防火牆與防毒軟體	設置網路防火牆 伺服器與電腦主機安裝防毒軟體，防毒軟體病毒碼自動更新 每週執行防毒軟體電腦掃描
預防資料外洩	帳號、權限管理	人員帳號審核及管理 定期進行系統權限設定檢核
日常營運維持	資料備份與相關檢核	訂定資訊安全風險管理辦法 依資料性質進行資料備份、異質備份與異地存放 定期進行資料還原測試 定期執行伺服器主機檢核暨系統測試 定期進行資安事件復原模擬演練 定期進行電腦檢核
資安事件處理	資安事件復原計畫	訂定資安事件復原計畫 事後撰寫資安事件復原計畫執行報告進行檢討改善

(四)投入資通安全管理之資源

- 1.建置防火牆，加強公司網路之防護和管控功能。
- 2.以VPN連線方式進行安全性的外部連線管控。
- 3.建置SPAM SQR 進行郵件過濾，減少垃圾信件及抵禦各式郵件攻擊。
- 4.訂定資訊安全風險管理辦法，加強公司內部管控功能。。
- 5.公司電腦均需安裝公司指定之防毒軟體，並自動更新病毒碼。
- 6.建置離線式備份系統，完善備份系統機制。
- 7.相關資訊系統的權限設定和管控。
- 8.導入ISO27001資訊安全管理系統標準，並取得第三方AFNOR驗證，有效期2024/11/21-2027/11/20。

本案已列入 113 年 1 月 21 日第 19 屆第十一次董事會報告事項。