

資訊安全風險管理架構

本公司資通安全政策為「維護公司資通之機密性、完整性、可用性與適法性，避免發生人為疏失、蓄意破壞與自然災害時，遭致資通與資產遭致不當使用、洩漏、竄改、毀損、消失等，影響本公司作業，並導致公司權益損害」。本公司已於 111 年導入 ISO 27001 資通管理系統，並取得 ISO27001 認證，目前證書之有效期為 111 年 11 月 10 日至 114 年 10 月 31 日。透過 ISO27001 資通安全管理系統之導入，強化資通安全事件之應變處理能力，保護公司與客戶之資產安全。

【資訊安全目的與範圍】

目的:確保本公司資訊安全管理及制度能有效持續運作，並驗證資安管理制度 (ISMS)之活動及其相關結果，是否與預期相符。

範圍:本公司衛星通信系統開發與機房維運作業

對象:本公司衛星通信系統開發與管理相關同仁

【資安風險管理架構】

資安專責單位負責統籌並執行公司資訊安全政策，宣導資訊安全訊息，提升員工資安意識。並定期向資安長、總經理、董事長進行資訊安全成果報告，由資安長向董事會報告資安治理事項，查核評估公司資訊作業內部控制之有效性，以及為保障資訊的機密性、完整性與可用性。

【資訊安全政策與目標】

為加強公司同仁對資訊安全之重視，對客戶展現本公司保護資訊安全的決心，本公司自 111 年度開始導入資訊安全管理制度 (ISMS)。

本公司資訊安全政策聲明為：資安防護，全面保障

【資訊安全控制措施】

1. 資安治理：取得 ISO27001 驗證，執行資安政策管理、資安合規控管並持續進行營運應變演練，保護公司重要系統與資料安全。並以 ISO 27001:2013 版資訊

安全標準及所有本公司資通安全管理制度選定之管控目標與管控措施均列入稽核要項中。包括：

- 資通安全政策、組織、環境及適用性聲明
 - 資通安全風險管理與目標
 - 文件與記錄管制方法與實作
 - 有效性量測、內部稽核及管理審查
 - 改善與持續改進
 - 資通安全政策
 - 資通安全組織
 - 人力資源安全
 - 資產管理
 - 存取控制
 - 密碼學
 - 實體與環境安全
 - 作業安全
 - 通訊安全
 - 系統取得、開發與維護
 - 供應商關係
 - 資通安全事件管理
 - 營運持續管理之資通安全層面
 - 遵循性
2. 風險改善：定期執行資安稽核作業，確保資訊安全落實執行。
 3. 風險控制：投保資安險能保護公司將潛在的各項損失傷害降至最低。
 4. 資安推動：定期進行資安教育訓練及演練，以提升員工資安意識。