資訊安全風險管理架構

資通安全與隱私風險管理組織及權責

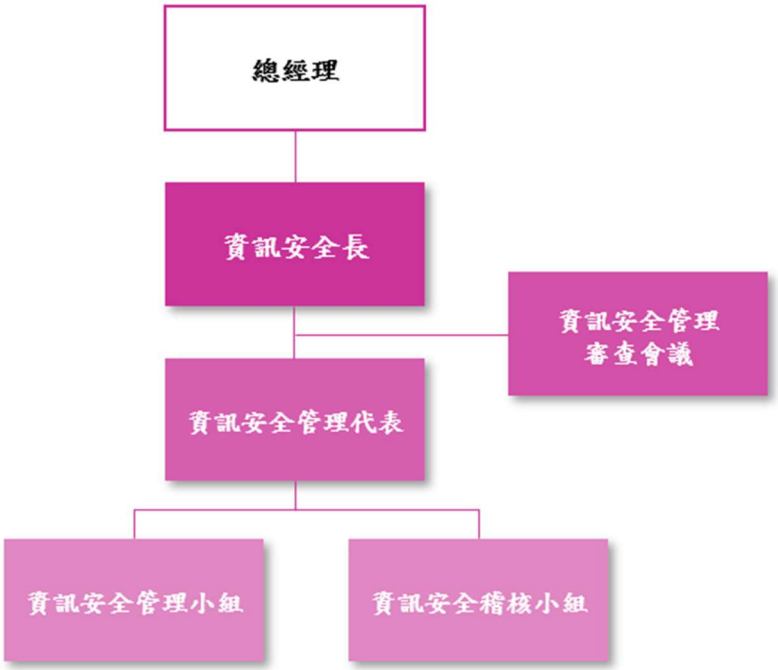
本公司及子公司依據ISO 27001規範與上市上櫃資通安全管控指引，於總經理下設有資訊安全長，負責召開資訊安全管理審查會議，管理、協調、督導及改善本公司及子公司資訊安全管理制度之運行。資訊安全長下設資訊安全管理代表，負責召集各資訊安全管理小組，規劃且執行各項資訊安全管理相關活動，推動落實資訊安全管理制度。資訊安全管理小組以任務編組各司資訊安全管理系統主要功能，以 PDCA(Plan-Do-Check-Act)為方法，依 ISO27001:2022 國際標準及相關的法令法規運營本集團所有資訊安全活動。包含資訊安全事項的執行、資安教育訓練的辦理、資安緊急事件的規範與處理、稽核改善事項的執行等。資安稽核小組另由稽核部門協助督導，包含評估資訊安全管理制度之落實與遵行情形，執行稽核作業，並提出稽核報告及相關建議事項。

資通安全政策

本公司及子公司資訊安全政策目標包含：

1. 建立安全及可信賴之資訊化作業與服務環境，確保本公司資料、系統、設備、網路及雲端服務之安全，以保障本公司業務永續運作。
2. 保護業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。
3. 保護業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。
4. 建立業務永續運作計畫，以確保本公司資訊業務服務之持續運作。
5. 確保各項業務服務之執行須符合相關法令或法規之要求。

資通安全組織圖



具體管理方案與投入資源

本公司除資安專責人員外，投入資通安全管理之資源包含：

1. 資訊安全防護

為確保公司資訊資產之安全，強化縱深防護架構，透過多層級的安全保護，除公司網路防火牆、VPN 閘道，另有帳號與權限管理、郵件防護、防毒軟體等。本公司並全面導入多因素驗證(MFA)、端點防護等系統，確保公司設備免受網路威脅、惡意軟體和未經授權的存取，以保護資料安全，同時維持營運持續性和法規合規性。

2. 資安風險管理

除每年執行資訊資產評估與風險評鑑，持續強化資訊系統防禦韌性，另有資安稽核作業，定期執行弱點掃描，備援與備份演練，重大危機事故演練等。每年辦理電子郵件社交工程演練，透過模擬釣魚郵件等情境提高員工警覺，並評估識別率、回報率與弱點改善成效。並訂定營運持續計畫與定期演練，以確保重要系統、業務於資安事故發生時能於預定時間內恢復作業。

3. 教育訓練與資安證照

每年定期舉辦全公司資通安全教育訓練，114 年完成度達 100%。另資訊安全專責單位人員每年均需接受資訊安全專業與職能訓練，以及各項資安證照的取得。本公司除獲 AWS 與 GCP 雙 Security 專業能力認證外，並取得資訊安全(ISO 27001)及雲端資安(ISO 27017)等國際標準認證的資安認證。本公司及子公司通過不斷優化升級資安策略，持續在日益複雜的威脅環境中保持領先地位，保障客戶的數據安全和業務穩定。

另在個人資料保護方面，本公司積極推行個人資料防護措施，如每年同仁定期個資保護教育訓練。本公司由資安小組負責推動個資保護, 除依據 ISO 27001:2022 資訊安全管理要求，持續強化公司資訊系統資料安全、資料遮蔽與加密、外洩防護、稽核紀錄等措施外。並預計於 114 年下半年度取得 ISO 27701 認證，增強個資隱私保護之管理架構，並落實個人資料保護。

114 年資訊安全與個資保護管理認證	
ISO 27001 資訊安全認證	連續 8 年通過資訊安全領域驗證 (本認證最新有效期自 112 年 11 月 21 日起至 114 年 12 月 08 日)
ISO 27017 雲端服務資安認證	連續 3 年通過資訊安全領域驗證 (本認證最新有效期自 111 年 11 月 18 日起至 114 年 11 月 17 日)