艾訊資訊安全管理

目的

艾訊股份有限公司(以下簡稱本公司)為強化資訊安全管理，提昇資訊安全管理流程之嚴謹度與安全性，依 ISO/IEC 27001:2013 資訊安全管理條文的要求及精神，以持續改善 P.D.C.A. 循環流程管理模式，建立資訊的機密性，完整性及可用性，避免因資訊安全問題造成公司及客戶營運上不必要的損失，確保企業持續營運的目的。

資訊安全政策

- 資訊安全要強化，P.D.C.A 不可少
  為了促使本公司資訊安全管理制度能貫徹執行、有效運作、監督管理、依 P.D.C.A 循環流程管理持續改善，維護公司重要資訊系統的機密性、完整性與可用性，故擬定此資訊安全政策。
- 風險管理勤控管，持續營運最可靠
  本政策旨在降低資訊安全管理與營運風險及電腦病毒危害中斷服務的頻率，加強企業同仁對資訊安全的認知，降低資安事件，強化組織對內外之風險管理，提昇客戶對本公司品質滿意度並達到企業持續營運的目標。

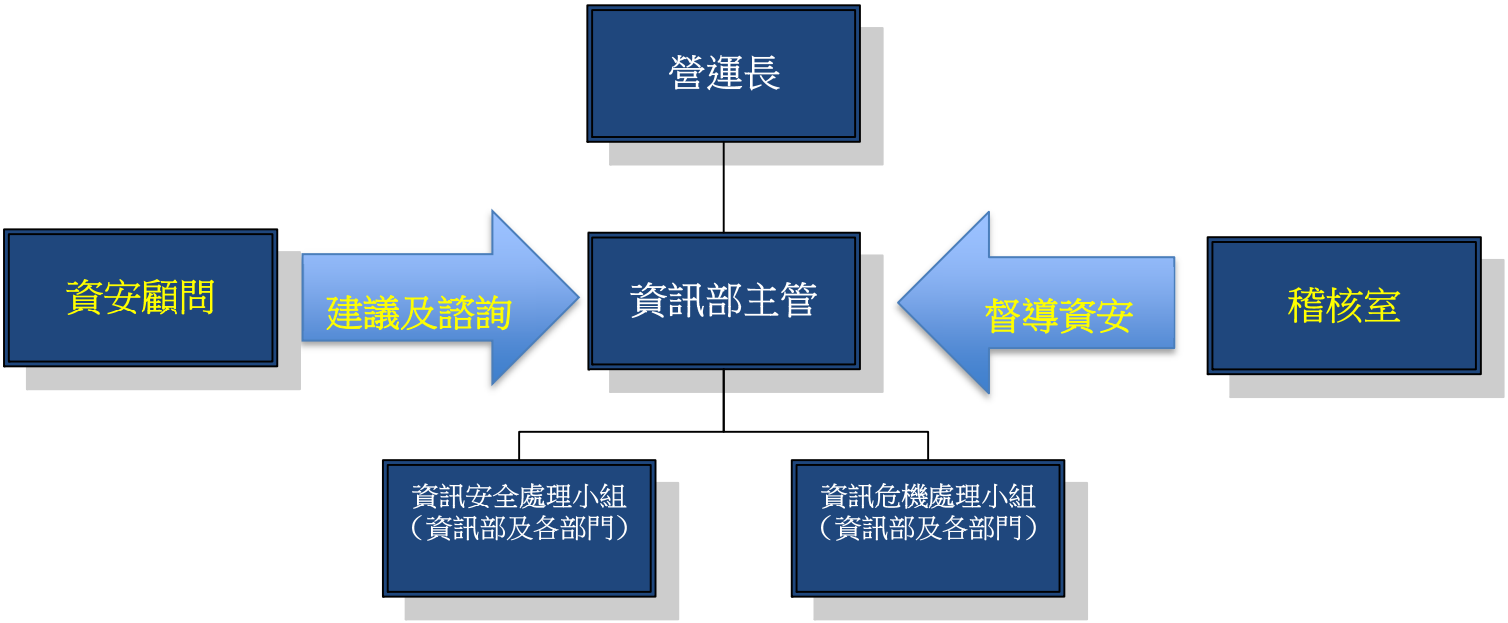
資訊安全風險管理架構

- 組織

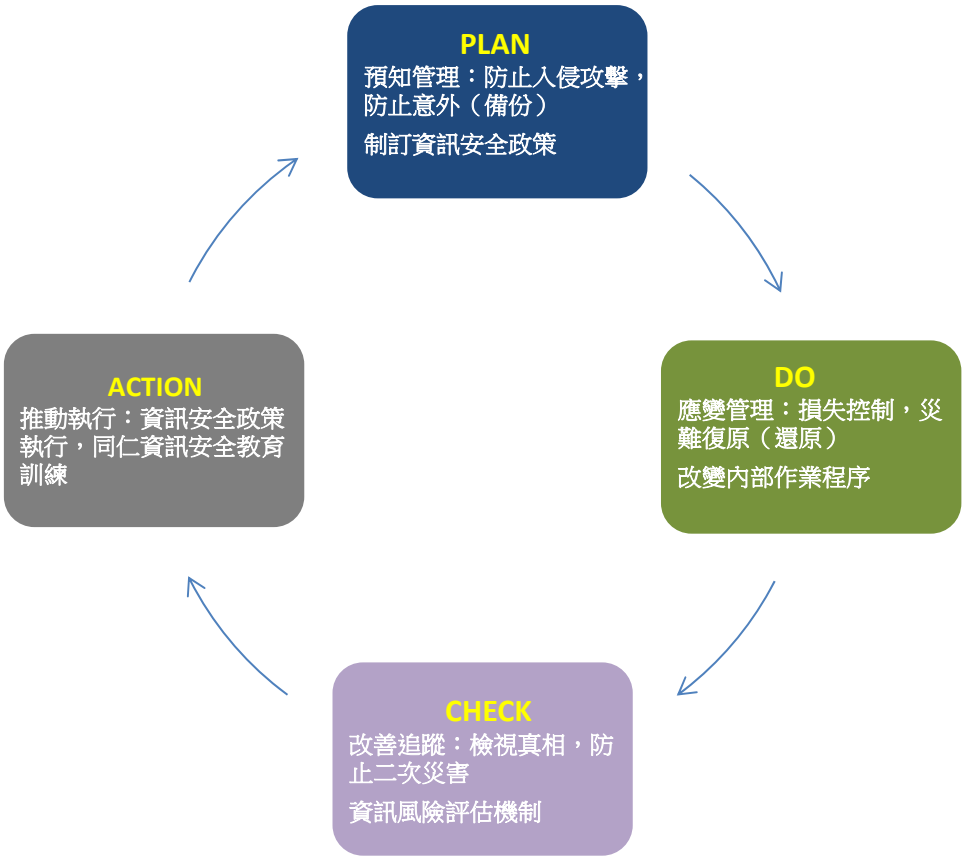
本公司資訊安全之權責單位為資訊部，設置資訊主管一名及專業資訊人員數名，負責訂定資訊安全政策、規劃及執行資訊安全政策推動與落實，並定期向董事會報告公司資安治理概況。已於 110 年 10 月 28 日於董事會報告公司目前資安治理概況。

本公司稽核室為資訊安全監理之督導單位，設置稽核主管一名及專職稽核人員一名，負責督導資安執行狀況，若有查核發現缺失，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，以降低資安風險。

- 資訊安全組織架構



- 組織依 P.D.C.A. 運作模式



- 針對風險管理，本公司掌握三個面向對應及預防風險事件的發生

預防資安事件（事前）	處理資安事件（事中）	調查資安事件（事後）
◆ 防止入侵 ◆ 防毒 ◆ 防意外(備份) ◆ 防外洩	◆ 防止災害擴大 ◆ 停止損失 ◆ 最短時間復原(還原)	◆ 調閱、查核、檢討、持續改善(P.D.C.A.)，風險控制，防止再度發生

- 資訊風險

項目	說明	容忍風險	因應對策	對策方法	容忍剩餘風險
資訊安全風險	◆ 駭客入侵 ◆ 資料外洩 ◆ 電腦中毒	否	◆ 防火牆，防毒軟體，定期更新病毒碼並進行掃毒 ◆ 定期 Windows Update ◆ AD 密碼定期更換 ◆ M365 及 SSL VPN 使用 MFA 手機多因素驗證 ◆ OpenDNS 網頁過濾 ◆ 使用 M365 雲端服務，即使被駭客加密亦可回朔加密前檔案	降低發生機率及降低影響	是
資訊服務中斷風險	因人為或意外災害導致公司主機、網路或其他資訊相關設備無法使用	否	◆ 機房之緊急 UPS 於斷電時約可供應主機約 4 小時之電力 ◆ 使用 M365 雲端服務，即使伺服器設備損壞，員工仍可正常收發 EMAIL 及存取雲端檔案 ◆ 伺服器依備份 321 原則執行備份 ◆ 異地備份	降低發生機率及降低影響	是

具體管理方案

管理面
◆ 加強資訊安全檢核機制(ISMS)：預計 2022 年 3 月評估導入 ISO 27001
◆ 員工資安意識：教育訓練，社交工程演練，資安通報
◆ 資訊安全認證：MIS 取得 CISSP 資訊安全認證，以資訊安全觀點確保企業持續經營
IT 架構
◆ 定期弱點掃描：網路伺服器弱點掃描，預先針對弱點補強
◆ Windows Server 升級：全面升級至 Windows Server 2016 以上
◆ 虛擬主機轉換：Windows Hyper-v 逐步轉換至 VMware vSphere
◆ 雲端服務應用：因應全球集團整合，導入 Azure，初期評估 eRMA 系統
◆ 端點安全升級：評估導入Microsoft MDE 雲端防毒監控服務

資訊安全宣導執行情形

為提升使用者對電子郵件的警覺性，避免因瀏覽惡意電子郵件而影響網路安全、發生個資洩漏事件，公司於 110 年 8 月 30 日對員工進行社交工程演練活動，目的在於透過演練行為，了解大家對於社交攻擊(常見的類型有釣魚信件)的辨別能力，並透過演練來增強同仁的警覺性。