資訊安全政策及管理方案

資訊安全政策目標

有鑑於資安攻擊手法日新月異，如社交工程攻擊、APT 進階持續性滲透攻擊、DDOS 分散式阻斷服務攻擊等，為免於被惡意或意外之入侵、破壞及洩露，致力於強化資訊安全管理，以確保所屬之資訊資產機密性、系統完整性及流程管理、設備及網路安全，以提供資訊業務持續運作環境，避免因資訊安全問題造成營運上不必要的損失。

本公司為有效運用資源，配合資訊安全工作之推行，對於資訊資產其重要性予以不同優先等級之保護，以達到最大資訊安全效果。資訊安全政策旨在確保公司營運順暢、資訊資料完整、企業機密安全，以保障公司本身之信譽。

一、經營面：防範資訊安全風險之威脅發生，減輕資訊安全事件之發生影響。

二、保密面：確保資料機密不洩露，避免不當使用及存取。

三、系統面：提高資訊設備及系統之可用性，確保資訊系統正常運作。

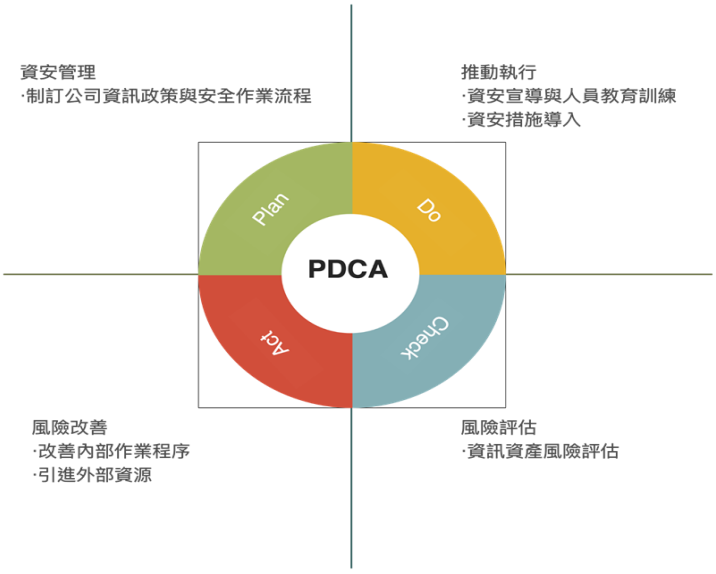
四、意識面：讓全體員工了解於資訊安全制度上應該遵守之責任及義務。

資訊安全風險管理架構

一、本公司資訊安全之權責單位為管理單位資訊部，負責規劃、執行及推動資訊安全管理事項，並推動資訊安全意識及落實管理。

二、本公司稽核室為資訊安全監理之查核單位，若查核發現缺失，即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低內部資安風險。

三、組織運作模式-採 PDCA（Plan-Do-Check-Act）循環式管理，確保可靠度目標之達成且持續改善。



KEDING

資訊安全政策執行方向及管理措施

短期(~2022 年)

一、端點安全

1. 電腦帳號權限管控，避免自行安裝不明軟體。
2. USB 裝置限制使用，禁止任何 USB 儲存裝置讀寫。
3. 作業系統與防毒軟體定期更新。
4. 使用者端通訊軟體的管制。
5. 廠區內智慧型手機的管制。
6. 定期透過教育訓練強化員工資安意識。
7. 定期進行資料的異地備份。
8. 災害復原的流程並定期演練。

二、Web 安全

1. 網頁瀏覽安全管理。

三、網路安全

1. 內部網路存取限制與管理。
2. 公司各據點間網路穩定度確保。

四、身分識別

1. 辦公室、廠區與機房門禁管理。

中期(~2024 年)

一、資安意識加強

1. 定期公告相關資訊安全事件。
2. 實施信件、通訊軟體等社交工程演練。

二、資料外洩防護

1. 強化公司內文件的分級分權管理機制。

長期(~2026 年)

一、委由外部資安廠商進行系統安全檢測。

二、強化 IT 設備與基礎架構。

三、網路容錯叢集架構建立。

四、伺服器異地備份與容錯叢集架構建立。

資安事件通報程序

本公司資通安全通報程序如下，資安事故之通報與處理，皆遵守該程序之規範進行。