資訊安全風險管理策略及架構

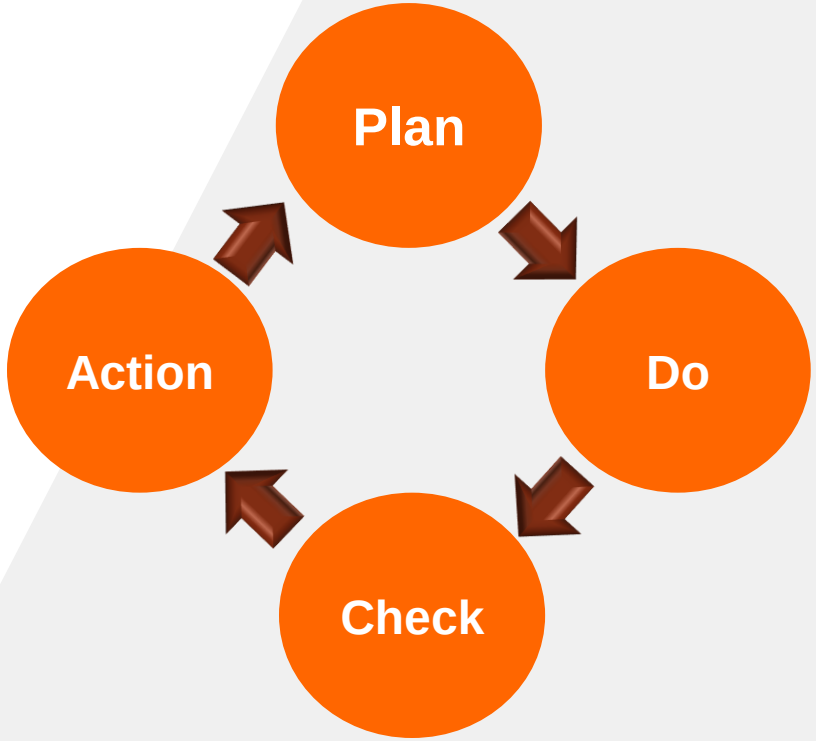
■資訊安全是本公司長期以來重視、關注的重要工作之一，為了確保各項資訊安全管理作業之有效落實，並及早發現不正當之行為以及安全漏洞或威脅，早期識別可幫助阻止不法行為並盡可能減少潛在的風險。

■公司採用 **PDCA (Plan → Do → Check → Action)** 管理循環模式以確保可靠度目標之達成且持續改善。

PACD

資安目標

- 訂定資訊安全管理辦法
- 訂定資訊相關作業程序



推動執行

- 資安政策宣導
- 資安措施導入與實施

風險評估

- 資安風險評估

風險改善

- 改善內部作業程序
- 引進外部解決方法

資訊安全管理措施

■本公司對於資訊安全控管相當重視，在資訊安全保護所採行之具體作法主要以五個方面進行資安管理:

管理類型	項目	防範目的	相關作業說明
員工	資訊安全宣導	預防降低中毒機率	■ 定期對於員工進行國內外重大資安異常事件案例分享。
裝置	防毒軟體 非信任裝置阻檔	預防中毒	■ 系統判定符合規範之電腦才給與網路連接權限 ■ 非經公司許可之電腦設備嚴禁接入公司網路，如有未經許可之設備接入系統將自動進行網路封鎖
權限	雙因素身分驗證 專案權限控管	避免帳號冒用	■ 同仁登入個人電腦需通過雙因素身分驗證(系統帳號密碼+OTP一次性密碼)，以避免帳號被竊取冒用的情況發生。 ■ 各研發專案皆有嚴格權限控管，專案成員需提出表單申請，經主管同意後由資訊管理人員設定存取權限，並且每半年進行一次存取權限覆核，以確保權限管理之正確性。
資料	專業型儲存設備 本地備援架構 異地資料備份	避免資料遺失	■ 專業型儲存設備具有高可用性的備援能力，專案研發 資料皆有權限控管，僅允許授權成員進行存取。 ■ 公司研發資料有完整的定期備份機制。 ■ 採取異地存放，以確保災難發生時的復原能力。
輸出	系統自動化拋轉 專屬加密空間	避免資料外洩	■ 產品交貨給客戶時，需申請表單，經相關主管、業務 ■ 承辦人員同意後，由系統將資料加密後直接上傳到公司提供予客戶下載之專屬空間，不經任何人工作業的介入。 ■ 專屬空間僅允許客戶提供之特定IP設備連線，連線開放時間以一個月為限。