資訊安全政策

本公司為確保資訊資料、系統、設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或毀損等風險，並建立資訊安全管理系統，特訂定資訊安全政策，以確保資訊之機密性、完整性與可用性。

1. 機密性：確保只有經授權的人才能存取資訊。
2. 完整性：確保使用之資訊正確無誤、未遭竄改。
3. 可用性：確保經授權的使用者在需要時可以隨時存取資訊及相關資訊資產。

目標

- 建立組織資訊安全推行小組，負責推動資訊安全工作。
- 評估人員之任免、職務之分派，對離職、休職、停職或調職之人員，應建立控管及人力備援制度；另定期辦理資訊安全教育訓練及宣導，提升人員資訊安全認知及水準。
- 建立資訊資產的管理制度，以有效分配及運用資源。
- 重要設施及特殊場所應加強管制，並定期施以相關維護及保養。
- 提昇電腦網路防禦技術，適時阻絕外界之入侵、破壞。
- 評估資訊資產之安全等級，並賦予相關人員適當存取權限。
- 建立資訊緊急處理機制與營運持續演練計畫，並定期操演、測試紀錄。
- 訂定資訊安全稽核制度，各項電腦系統安全進行定期或不定期之稽核作業，且嚴禁刪除及修改各項稽核紀錄檔案。
- 遵循主管機關各項作業規範及適時更新資訊安全相關法規以符合法令依據。

iSTART

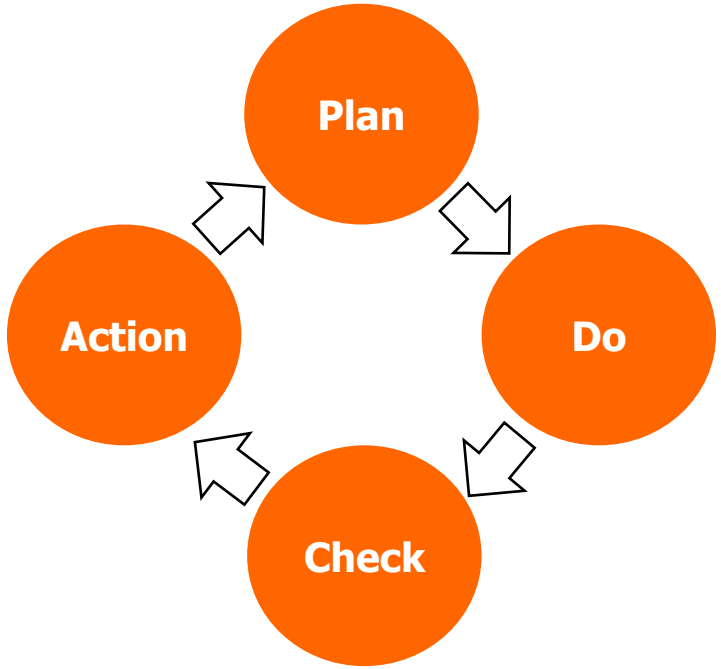
資訊安全風險管理策略及架構

- 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。

PDCA

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

iSTART

資訊安全管理措施

■ 本公司對於資訊安全控管相當重視，在資訊安全方面採用以下具體措施管理：

管理類型	項目	防範目的	相關作業說明
員工	資訊安全宣導	降低中毒及資料外洩機率，強化資安意識	■ 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、資料外洩	■ 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將無法使用網路。
權限	■ 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使用具複雜度之密碼驗證，以避免資料外洩的情況發生。 ■ 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，並且定期執行存取權限覆核，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	客戶專用資料空間	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，由資訊人員上傳到公司提供予客戶下載之專屬空間。