資訊安全政策

- 本公司各項資通安全管理規定必須遵守政府相關法規之規定。
- 定期實施資通安全教育訓練，宣導資通安全政策及相關實施規定。
- 建立主機及網路使用之管理機制，以統籌分配、運用資源。
- 新系統及設備建置上線前，須將風險、安全因素納入考量，防範危害資通安全之情況發生。
- 建立資訊機房實體及環境安全防護措施，並定期施以相關維護及保養。
- 明確規範網路系統之使用權限，防止未經授權之存取動作。
- 訂定資通安全管理制度內部稽核計畫，定期檢視資通安全管理制度範圍內所有人員及設備使用情形，依稽核報告擬訂及執行矯正預防措施。
- 訂定營運持續管理備援/備份還原之演練，確保公司業務持續運作。
- 本公司所有人員負有維持資通安全之責任，且應遵守公司相關之資通安全管理規範。
- 資安政策之評估與審查應至少每年評估及審查一次，以反映管理政策、政府法令、新科技技術及公司業務等之最新發展現況，確保資通安全管理制度的可行性及有效性，以維持營運和提供適當服務的能力。

iSTART

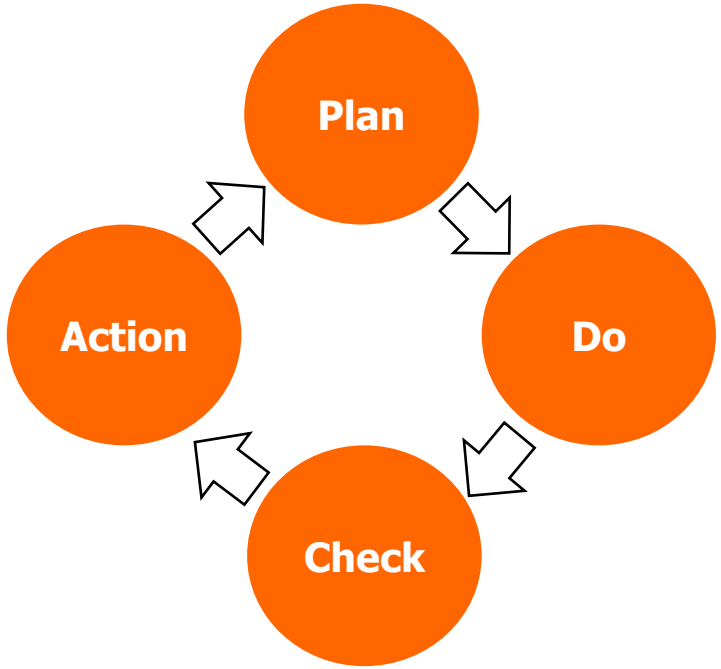
資訊安全風險管理策略及架構

- 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。