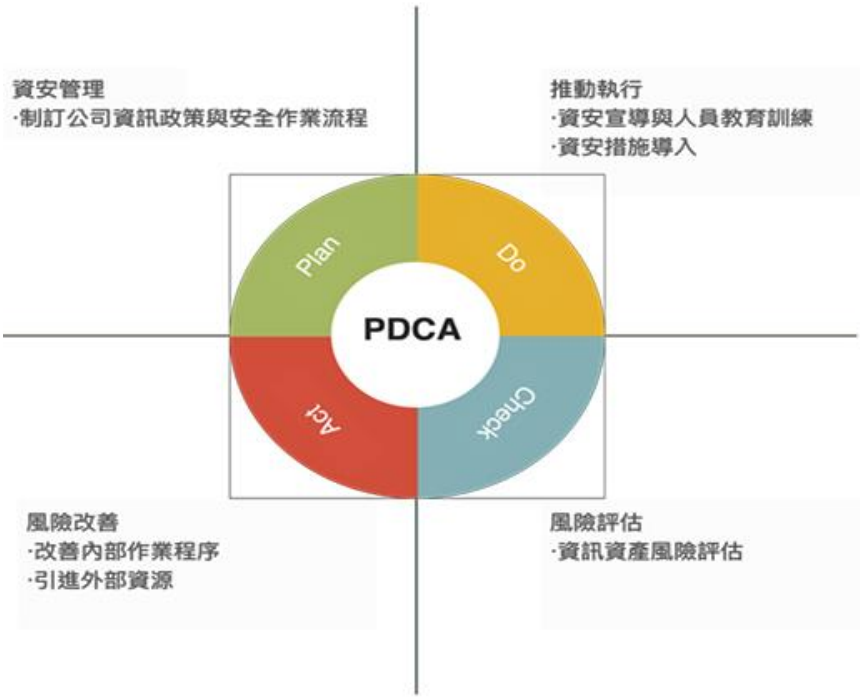
科定企業股份有限公司

2024 年資通安全管理執行情形

一、資訊安全管理架構

1. 本公司資訊安全之權責單位為資訊單位資訊課，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。
2. 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。
3. 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。



本公司於2023/08/09董事會通過設置1位資訊安全專責主管及1位資訊安全專責人員，並定期每年至少一次向董事會報告資通安全管理執行情形。

二、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。為維護本公司資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。期藉由本公司全體同仁共同努力以達成下列目標：

1. 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。
2. 保密面：確保資料機密不洩露，避免不當使用及存取。
3. 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。
4. 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。

三、資訊安全管理方案

為增進本公司資訊安全及穩定之運作，提供可信賴之資訊服務，確保資訊系統之機密性、完整性及可用性，提升用戶端資安意識，實行各項管理作業：

管理事項	作業說明
1. 資訊資產之安全管理	● 資產清冊每年12月定期盤點。 ● 重要硬體資產簽訂更新維護保固作業。 ● 重要系統及資料進行本地備份、異地備份或雲端備份機制。
2. 人員管理及教育訓練	● 持續建立、宣導及推廣新建員工資訊安全認知，以提升資訊 ● 安全新進同仁資訊安全宣導訓練。 ● 不定期各類資訊安全宣導。
3. 實體及環境安全管理	● 資訊機房區域設置有門禁控制，確保只有經過授權人員才許可進入。 ● 資訊相關設備，應適當地進行安置、保護、監控，以降低環境威脅所造成的損害，例如環境溫溼度監控。

管理事項	作業說明
4. 電腦系統及網路安全管理	● 外部及個人電腦網路設備不得私自連接公司網路。 ● 企業級無線網路系統，經系統整合驗證機制始能連線。 ● 重要資料採檔案加密保護機制。 ● 使用專業防毒軟體，並自動更新。 ● 設置新世代網路防火牆，設定連線規則，確保使用安全。 ● 郵件系統垃圾郵件過濾、病毒威脅防護及主機電腦弱點掃描及重大修補程式更新。
5. 系統存取控制安全	● 系統權限依員工職務職能以經權限申請作業後存取。 ● 每年定期進行權限覆核作業。 ● 設置密碼、鎖定及複雜度等原則。
6. 系統發展、開發及維護之安全管理	● 自行開發或委外發展系統，需將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，避免不當危害風險。
7. 營運持續運作	● 每年依公司營運持續計畫進行風險評估及災難復原演練規劃，並依計畫進行系統災難復原演練，確保資訊系統之可用性。

四、投入資通訊安全管理資源及執行情形

目前資訊單位資訊課設置15位人力，負責資訊管理制度、全體公司資訊系統維運及開發、軟硬體網路建置。

為增進本公司資訊安全及穩定之運作，提供可信賴之資訊服務，確保資訊系統之機密性、完整性及可用性，提升用戶端資安意識，實行各項管理作業：

項目	2024年執行情形
資安宣導	於公告系統發布，執行全員資安宣導： 釣魚網站及釣魚信件（05/10、09/18） 新進人員，基礎資安影片觀看
查核作業	資訊組織及職責作業查核（11月）
資安演練	備份系統還原演練（每年至少一次，9月）
聯防組織	台灣 CERT/CSIRT 聯盟資安教育訓練(10月) CERT/CSIRT 聯盟台灣資安通報應變年會(11月)

資安事件：

資安指標	資安客訴事件	外部破壞、竊取資料或病毒威脅事件	資訊系統異常或設備異常影響營運事件
2024年事件統計(件)	0件	0件	1件