和椿科技股份有限公司

資訊安全政策
及施行管理方案

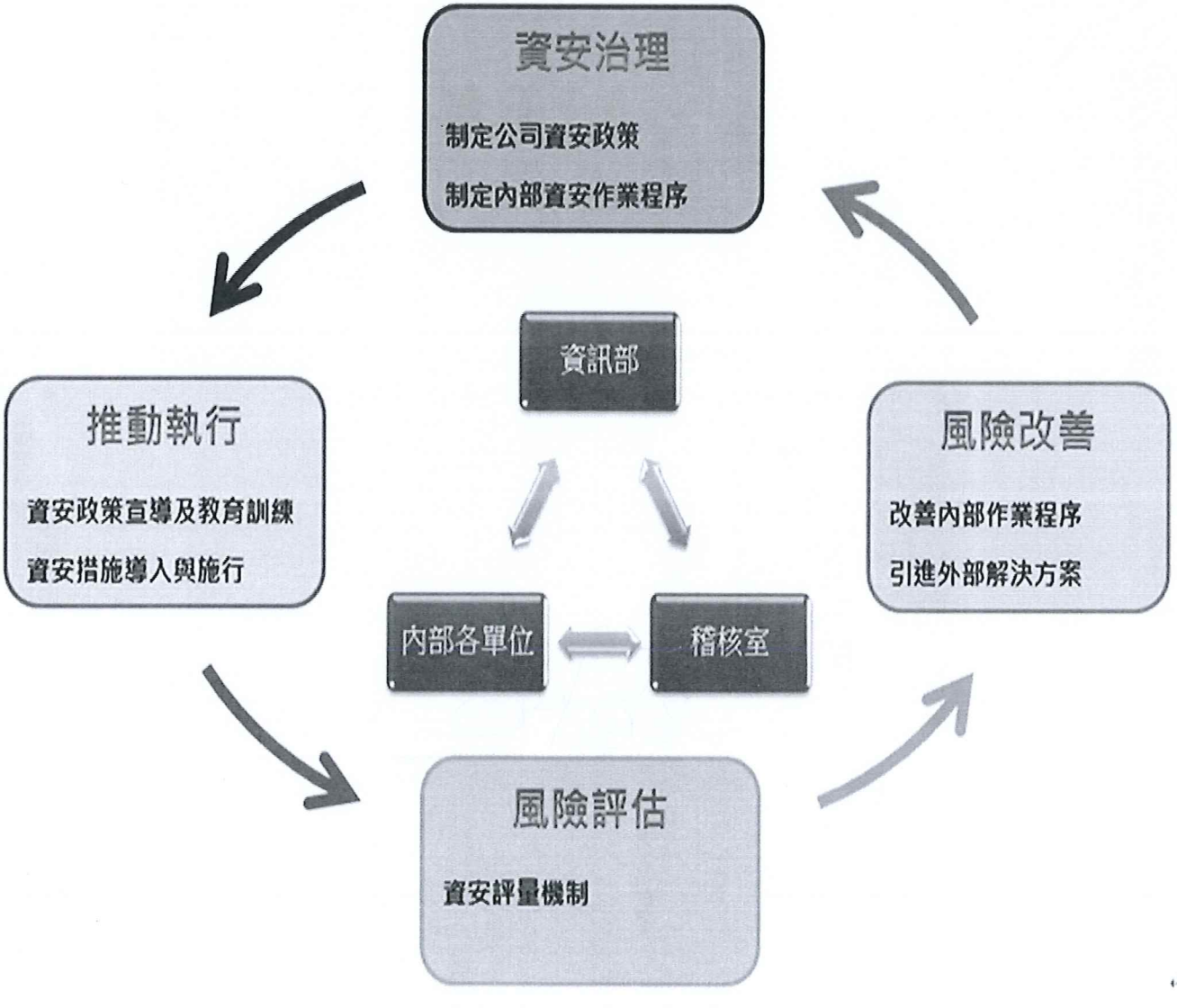
111年

一、資訊安全風險管理架構

本公司資訊安全之權責單位為資訊部，負責規劃、執行及推動資訊安全管理事項，並推展資訊安全意識。

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，旋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。

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



二、資訊安全政策及管理方案

本公司資訊安全管理機制，包含以下三個面向：

1. 制度規範:訂定公司資訊安全管理制度,規範人員作業行為。

2. 科技運用：建置監控軟體，落實資訊安全管理措施。

3. 人員訓練：進行資訊安全教育訓練，提昇全體同仁資訊安全意識。

本公司資訊安全政策：

1. 遵守國家法令訂定相關資訊安全管理規章，對本公司資訊資產提供適當的保護措施，以確保其機密性、完整性、可用性及法律遵循性。

2. 定期評估人為及天然災害對本公司資訊資產之影響，並訂定重要資訊資產及關鍵性業務資訊之防災對策及應變復原計畫，定期演練災害復原計劃，以確保資訊資產之穩定運行，保持本公司業務持續運行。

3. 督導公司同仁落實公司資訊安全防護及配合資訊安全管理措施，確保同仁對資訊安全的防護及認知。

4. 除要求本公司同仁確實遵守公司的資訊安全規定外，亦要求有使用到本公司資訊系統的往來廠商，恪守本公司資訊安全規定，如有違反或造成本公司損失時，將依相關法律追訴究責。

三、資訊安全管理措施

對象	管控類型	相關作業	頻率	說明
員工	權限管理	人員帳號權限管理與審核 人員帳號權限定期盤點	不定期 至少 1次/年	人員帳號、權限管理與系統操作行為之管理措施
員工	存取管控	內/外部存取管控措施 操作行為軌跡記錄 外寄郵件過濾 限定裝置權限管理(包含USB) 遇到較大檔案時公司內部有私有雲提供	即時 即時 即時 即時 即時	人員存取內外部系統及資料傳輸管道之控制措施
系統	外部威脅	主機防火牆沙箱及IPS更新措施 病毒防護與惡意程式檢測	即時 即時	內部防火牆、中毒管道與防護措施
系統	系統可用性	系統/網路可用狀態監控及通報機制 服務中斷之應變措施 資訊備份措施、本/異地備份機制 定期災害復原演練 個人重要資料空間擴大	即時 即時 每天備份，桃園與台北異地 1次/年 即時同步	系統可用狀態與服務中斷時之處置措施