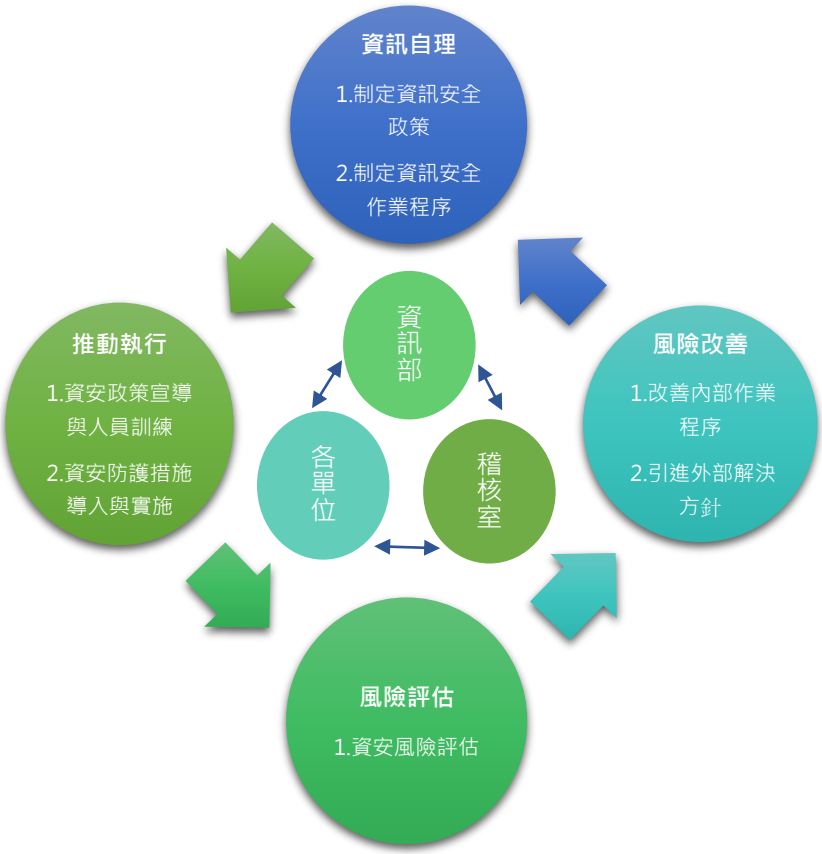
奇偶科技資訊安全執行情形

本公司於 2023 年設立資安管理部門，負責協調公司內部各單位的資訊管理作業，並定期彙報資安治理成果及風險管理措施，為公司長期穩定運營奠定堅實基礎。為防範內外部蓄意或意外的威脅，我們依據《上市櫃資通安全管控指引》制定了內部作業規範，旨在降低新興資訊科技應用及環境變遷帶來的潛在資安風險。

1. **資安部門權責**：資安部由 2 位資安人員成立，為公司資訊安全的主要責任單位，負責制定公司內部資訊安全政策，並規劃與執行相關作業，確保政策有效推動與實施。
2. **稽核室督導責任**：稽核室為資訊安全的督導單位，負責監督內部資安執行情況。若發現問題，稽核室會要求相關單位提出改善計畫並採取具體行動，並定期追蹤改善成效，以有效降低內部資訊風險。



資訊安全政策與管理方針

本公司為應對迅速演變的網路威脅和可能出現的內部安全事件，制定了全面的資訊安全政策與管理方針。資訊安全政策涵蓋公司所有層級的員工、合作夥伴及第三方服務提供者。透過持續的風險評估與管理，於採取適當的技術和管理措施，以確保所有資訊資產的機密性、完整性及可用性，並符合相關法律及法規的要求。

1. **設備防護措施：** 公司內所有個人電腦和伺服器均需設定強密碼並安裝最新的防毒軟體。此舉不僅能防範一般性的病毒攻擊，還能有效抵禦更為

複雜的網路釣魚和勒索軟體攻擊。

2. **合法軟體使用規範：** 公司嚴格遵守智慧財產權相關規定，確保所有安裝的軟體均獲得合法授權。這不僅保護公司免受法律風險，也有助於減少因非法軟體引發的資安問題。
3. **資安意識提升：** 為進一步強化員工的資訊安全意識，公司定期透過電子郵件發送資安資訊，以確保員工能夠識別並應對各種潛在的資安威脅。
4. **先進防火牆與多層次保護：** 公司已建構新世代防火牆，結合入侵偵測與防禦系統以及掃毒引擎，通過多層次的保護措施，有效過濾藏匿於網際網路中的各種病毒、間諜軟體及其他有害程式，保障公司網路環境的安全。
5. **專用機房與物理安全：** 設置專用機房用以安置電腦主機、伺服器等設備，並嚴格執行進出記錄管制、影像錄影監控措施。機房內部設有獨立空調系統，保持設備在適當的溫度下運行，並配備滅火器以應對突發火災事件，確保物理安全。
6. **委外維護與專業支持：** 為了確保伺服器的穩定運行，公司已委託專業的電腦資訊廠商進行伺服器代管維護服務，並與其保持密切合作，以即時應對可能出現的技術問題。
7. **資料異地存放與還原演練：** 根據資料性質進行異地存放和定期還原演練，確保即使在極端災難情境下，公司的核心數據也能安全無虞地進行

恢復。

8. **參與資安情資分享 TWCERT 聯盟：** 為了掌握最新的資安情資，公司已加入 TWCERT 聯盟，並積極參與資安課程，通過修補漏洞和提升資安人員的防護能力，確保我們的系統能抵禦最新的網路威脅。
9. **使用弱點掃描工具：** 公司採用第三方弱點掃描檢測工具，主動在系統或應用程式中發現潛在的資安漏洞。這種預防性措施能夠在漏洞被利用之前進行修補，從而避免可能的安全事故。
10. **產品符合資安標準：** 公司持續將產品送驗，以符合台灣物聯網資安標準，這不僅保障了產品的安全性，還增強了客戶對公司產品的信任。
11. **獲得 TAICS 認證：** GeoVision 成為台灣首家獲得 TAICS（台灣資訊標準協會）認證的科技公司，並於 2018 年 11 月 19 日獲得視訊監控系統安全標準二級認證，這進一步證明了公司在資安領域的領先地位。
12. **建立資訊安全專頁：**在公司官方網站設立資訊安全專頁 (https://www.geovision.com.tw/cyber_security.php)，提供漏洞政策、安全強化指南及相關安全公告。此外，還設置了網路客服信箱 (security@geovision.com)，以便客戶能即時通報漏洞及其他安全問題，並獲得快速響應。

2024 資通安全執行情形

- 資安人力: 資安主管一名及資安人員一名，負責資安架構設計、資安維運與監控、資安事件回應與調查、資安政策檢討與修訂，每年向董事會至少報告一次。
- 投入 2 個人力: 每日各系統狀態檢查、設備異常發信通知、每周定期備份、每月至少一次資安宣導、每年系統災難復原執行演練、每年應對資訊循環之內部稽核、會計師稽核等。
- 投入 2 個人力針對網路應用服務，包含 ERP 和網站系統進行安全開發，保障商業應用安全。