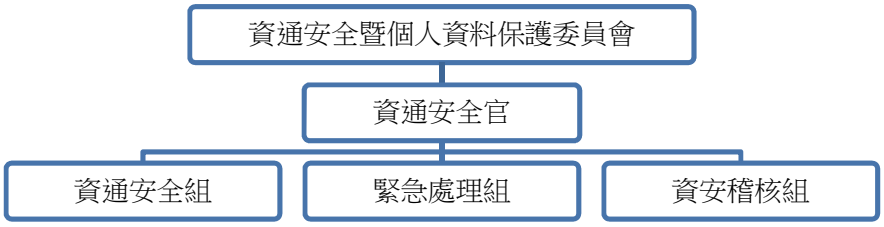
# 資通安全暨個人資料保護政策及管理方案

## 一、 組職架構

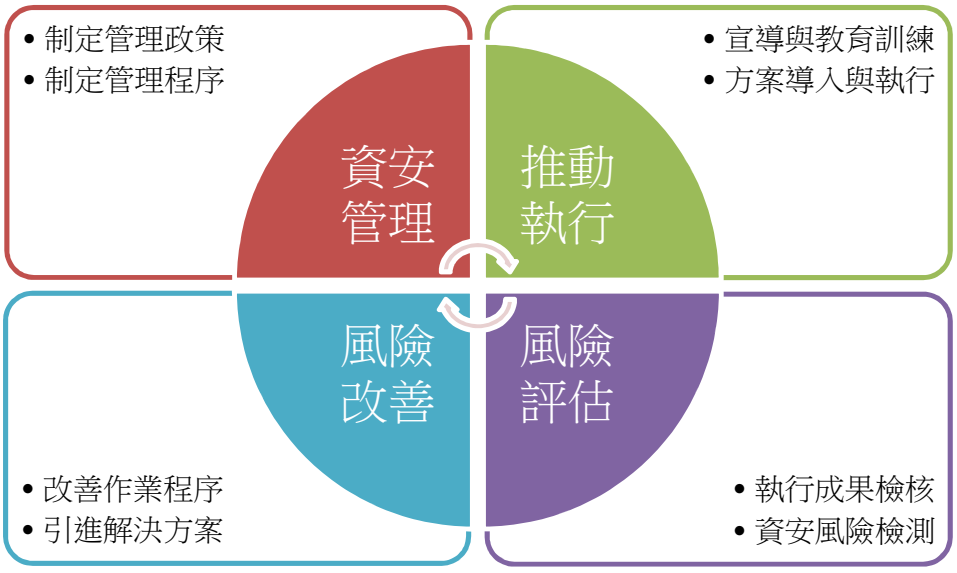
為強化公司的資通安全管理與個人資料保護，確保資料、系統、通信及網路安全，設立資通安全暨個人資料保護委員會。委員會由本公司各單位主管組成。負責資通安全管理制度暨個人資料保護相關事項之決議，並指派專責主管為資通安全官，負責執行與組織團隊包含資通安全組、緊急處理組與資安稽核組。執行成果由委員會每年至少一次向董事會報告。

資通安全組由資通安全官組建，包含專職資通安全管理人員乙名與專業人員數名。負責執行資通安全系統建置，包含網路管理與系統管理。同時持續檢視評估資訊環境變化趨勢，評估資通安全風險與防護，以確保內部資安管理機制持續有效運作。

資通安全稽核負責督導內部資通安全執行狀況，若有查核發現缺失，即要求受查單位提出相關改善計畫與具體措施，且定期持續追蹤改善成效，以降低內部資通安全風險。




## 二、 資通安全組運作模式



# 三、 資通安全暨個人資料保護政策

- 目標

  建立安全及可信賴之電腦化作業環境，確保公司資訊資產(軟體、硬體、電腦資料、資訊環境、人員)之機密性、完整性及可用性，避免遭受來自內、外部的各種威脅損害，使公司資訊系統永續運作，並依照個人資料保護法及其施行細則，提供管理階層對依法保護個人資料之支持與承諾。

- 政策實施要點

  1. 人員管理及資訊安全教育訓練。
  2. 電腦資訊系統安全管理。
  3. 網路安全管理。
  4. 系統存取管制。
  5. 系統發展及維護安全管理。
  6. 資訊資產安全管理。
  7. 實體及環境安全管理。
  8. 資訊系統永續運作管理。
  9. 資訊安全稽核。
  10. 個人資料保護暨安全維護。

- 資通安全與個人資料保護的原則與標準

  1. 定期辦理資通安全教育訓練及宣導，包括資通安全政策、法令規定、資通安全作業程序與如何正確使用資訊科技設施等。促使員工瞭解資通安全的重要性與各種安全風險，提高員工資通安全意識，並遵守資通安全規定。
  2. 為預防資訊系統及檔案受電腦病毒感染，對電腦病毒、入侵及惡意攻擊，建立主動病毒偵測、主動式入侵偵測及防範措施，以確保電腦資料安全之要求。
  3. 為預防天災或人為之重大事件，造成重要資訊資產、關鍵性業務或通訊系統等中斷，應建立資訊系統永續運作規劃之政策。
  4. 資通安全與個人資料保護納入公司年度稽核計畫之稽核項目。
  5. 本公司應依法蒐集、處理及利用個人資料，以保護當事人權益，並促進個人資料之合理利用。

- 員工應遵守之相關規定

  1. 資訊部依帳號申請單建立”使用者代號”。
  2. 電腦資料及設備，不得任意破壞、攜出、外借與不正當修改，以維護資料完整性。
  3. 禁止使用無版權軟體與來路不明軟體。
  4. 作業結束或長時間不使用機器時，應退出機器，以免資料機密外洩或遭他人破壞。
  5. 電腦設備之擺放，應遠離茶水、咖啡、日曬或潮溼地點，並保持設備整潔與線路梳理以延長其壽命。
  6. 離職或新舊職務交接時，由資訊單位衡量資料與權限相關性作適當處置。
  7. 電腦設備無法正常作業時，使用者應立即通知資訊單位，進行檢查與維修。

- 資通安全政策修正

  1. 資訊環境發生重大改變與趨勢變化時，重新檢視資訊安全政策。
  2. 每年定期重新檢視資訊安全政策，確認相關規範是否符合需求。

# 四、 具體管理方案

本公司資通安全相關管理方案如下：

| 項目 | 管理方案 |
| --- | --- |
| **防火牆防護** | ✓ 防火牆設定連線規則。<br>✓ 有特殊連線需求需額外申請開放。<br>✓ 備份系統日誌與連線紀錄並保存一年以上。 |
| **防毒軟體** | ✓ 使用防毒軟體，並自動更新病毒碼，降低病毒感染機會。 |
| **郵件安全管控** | ✓ 自動郵件掃描威脅防護，事先防範不安全的附件檔案、釣魚郵件與垃圾郵件，並擴大防止惡意連結的保護範圍。<br>✓ 防毒軟體於個人電腦接收郵件後進行掃描內容與不安全的附件。<br>✓ 自動備份每封寄件與收件郵件。 |
| **資料備份機制** | ✓ 重要資訊系統、資料庫與檔案伺服器設定每日備份。<br>✓ 備份資料除本地備份外，一律進行異地備份。 |
| **人力資源安全管理** | ✓ 定期進行資訊安全教育訓練。<br>✓ 建置雙因子確認機制與反饋管道。 |
| **環境安全管理** | ✓ 外部儀器設備與新進設備需經資訊安全人員檢查並登記。<br>✓ 外部儲存媒體使用需經過資訊安全人員檢查並登記。 |
| **網路管理** | ✓ 防護系統自動控管使用者上網行為。<br>✓ 自動過濾使用者可能連結到木馬、勒索病毒...等的惡意網站。 |
| **協力廠商管理** | ✓ 對協力廠商進行評鑑與審查。<br>✓ 協力廠商確實簽屬保密協議。 |
| **資安事件通報** | ✓ 依事件等級依序回報主管單位。<br>✓ 詳實記錄事件發生過程與數據，後續進行檢討改善。 |
| **檔案上傳伺服器** | ✓ 使用者重要檔案一律存放於伺服器，由資訊部統一備份保存。 |
| **個人資料保護** | ✓ 宣導並教育訓練本公司之個人資料保護政策。<br>✓ 定期檢視單位業務流程之個資風險。 |
| **資通安全稽查** | ✓ 定期查核整體資訊安全管理系統。<br>✓ 定期對資通安全管理作業進行自評查核。 |
| **資安險** | ✓ 本公司主要客戶為企業客戶，無消費者個資保管風險，經評估市面資安險種、保險範圍與適用行業等項目後，暫不投保資安險。為因應資訊安全所面臨的挑戰，已導入相關軟硬體,例如防火牆、防毒、入侵防護系統…等，同時持續關注資訊環境變化趨勢，強化同仁資安危機意識及資安處理人員應變能力。 |
| **資安聯防組織** | ✓ 本公司已於 111 年 12 月正式加入台灣資安聯盟組織(TWCERT/CC)<br>✓ 持續追縱本國最新相關資安風險資訊，進而對本公司進行相關資安防護。 |

# 五、 資通安全投入資源

本公司持續投入資源於資通安全事務，每年增加預算進行軟硬體設備的更新與強化，包含防火牆、防毒、防駭與入侵偵測等，並積極投入端點的防護與情資監控分析。同時設置專責主管乙名、專職人員乙名與數名資通訊專業人員，規劃並改善資通安全管理制度，定期執行災難還原演練、針對重要系統資料，每周進行多個異地資料備份、保管與測試。

另外在提升資通安全意識與個人資料保護方面，全面進行資通訊安全暨個人資料保護課程講習，同時每月會進行資通安全宣導，在發現可疑郵件與行為時立即通告全體同仁加強注意，另依據時下內外部威脅最新狀況進行不定期的宣導與教育訓練，在資安大環境的趨勢下，本公司加入資安聯盟組織(TWCERT/CC)，針對國內最新資安風險，對公司資通安全事務進行必要防護機制。

本公司於資通安全管理事項及投入之資源方案如下：

專責人力：設有專職單位「資通安全暨個人資料保護委員會」，負責資訊安全規劃與稽核事項，持續維護強化資通安。

客戶滿意：無重大資通安全事件，無違反客戶資料遺失之投訴案件。

教育訓練：所有新進員工到職前皆完成資訊安全教育訓練課程；年度完成 1 次資通安全教育訓練。

資安測試：年度進行 1 次滲透測試與弱點偵測；年度共計執行 3 次社交工程釣魚郵件測試

系統備份：重要資料進行 3 地備援，且異地備援距離資料所在地 40 公里以上；年度進行 1 次災難復原演練。

資安公告：每年製作超過 12 份資安公告與宣導，傳達資通安全防護的重要規定與注意事項。

董事會報告：最近一次報告於 2023 年第 4 季董事會進行匯報。

資安通告：設有專門資安通報管道「soc@ezconn.com」提供給員工、客戶與供應商進行資安通報。

# 六、 資通安全事件

本公司明訂資通安全通報及處理流程，資通安全事件由緊急處理組通報窗口進行應變並訂定事件等級。當發生資通安全事件時，依事件等級通報上層主管與主管機關。

緊急處理組需於目標時間內排除及解決資通安全事件，並於事件處理完畢後進行分析，並擬出對策與矯正措施，以防事件重複發生。

近四年無發生資通安全事件及相關損失。

| 資通安全事件 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|
| 因資通安全事件導致資料遺失 | 0 | 0 | 0 | 0 |
| 因資通安全事件損失的財務 | 0 | 0 | 0 | 0 |
| 資料外洩事件數量 | 0 | 0 | 0 | 0 |