
資訊安全政策

壹、資訊安全風險管理架構

為強化本公司之資訊安全管理，本公司資訊安全之權責為資訊單位，設置資訊主管乙名，與數名專業資訊人員，負責統籌和執行各項資訊活動，訂定內部所有資訊管理辦法暨相關作業，宣導資訊安全訊息，提升員工資安意識，落實各種資訊循環，資訊安全查核，以及貫徹資訊安全機制的作為。

貳、資訊安全政策

為保障公司、員工的權益，落實公司內部資訊安全管理辦法，為此建立可信賴的資訊安全作業環境，以確保資訊資產之機密性、完整性，及設備、網路的安全，維持資訊系統之持續運作原則，特訂定本政策。

參、資訊安全具體管理方案

1. 同仁帳號、密碼與權限應善盡保管與使用責任並定期換置。
2. 重要資訊系統或設備應建置適當之備援或監控機制並定期演練，維持其可用性。
3. 個人電腦應安裝防毒軟體並定期確認病毒碼之更新，並禁止安裝與使用未經授權軟體。
4. 資訊安全定期進行風險評估，如有需要則列入年度預算計畫表，落實各項資安措施，提升作業安全。
5. 郵件安全管控：設置郵件掃描防護系統，在使用者接收到郵件之前先針對有疑慮及不安全的附件檔案、垃圾郵件進行隔離，防止惡意郵件進到公司內部。
6. 防火牆防護：設置防火牆連線規則。
7. 全體人員應遵守法律規範與資訊安全政策要求，主管人員應督導資安遵行制度落實情況，強化同仁資安認知及法令觀念。

肆、投入資通安全管理之資源

本公司不定期以時事案例作為資通安全宣導，為加強資訊安全，未來將編列適當預算強化資訊技術及安全維護。