

資通安全管理

(1) 資通安全風險管理架構

本公司由管理部負責統籌規劃、執行及推動資訊安全管理事項，宣導資訊安全訊息並提升員工資安意識，蒐集及改進組織資訊安全，公司資訊安全系統可行性之技術評估等。配合內部控制制度，進行資訊安全查核，評估公司資訊作業內部控制之有效性。

(2) 資通安全政策

為落實資訊安全管理，依據內部控制制度處理準則已制定「資通安全檢查」及「個資安全保護管理準則」之相關作業程序，包括建置防火牆及使用權限及記錄，確保電腦網路系統及網路傳輸資料安全，管理個人資料之保護及利用，以控管公司資訊安全風險。

(3) 具體管理方案及投入資通安全管理之資源

1. 檔案安全：依備份類別設定備份時程表，定期備份資料。
2. 設備安全：電腦機房裝設空調、防水及除濕等設備，以控制溫度及濕度，機房有緊急動力不斷電系統裝置，以防止發生臨時停電造成資料毀損。
3. 電腦病毒之預防及處理：主機系統安裝伺服器專用防毒軟體，確保主機資料安全，電腦安裝合法版權之防毒系統，使用者不得任意將外來磁片及檔案或電子郵件存入、安裝到公司電腦系統中，隨時監控外來檔案及定期更新防毒病毒碼。
4. 系統安全監控：建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，保護連網作業，防止未經授權的系統存取，造成機密資料之外洩，對於跨公司之電腦網路系統，加強網路安全管理，並且對內安裝防毒軟體，設置對外之網路防火牆。
5. 分工及權限：使用者密碼設定避免使用容易被識破及猜測的密碼並定期更改密碼。依各業務範圍、權責分別設定使用者之帳號及權限，使用者一旦離開原職務，應立即撤銷該使用者之帳號及權限。

本公司已於112年11月10日設置資安主管1名及資安人員1名，並購置防毒軟體(每月授權費約3000元)，每月檢查主機系統、會計系統、資料庫及防火牆等，軟體及資料檔案每月執行備份作業，以控管公司資訊安全風險。。