奇偶科技股份有限公司

資通安全風險管理政策

一、資通安全風險管理架構

(一) 盤點每年需保護關鍵資訊服務。

(二) 進行資安風險評估，將系統服務分散建置於雲端系統及委外管理，或內部自行管理。

(三) 日常營運時定期進行伺服器等設備之檢查，以即時發現問題。

(四) 資安專責單位負責執行公司資訊安全政策，並宣導資訊安全訊息，提升員工資安意識。

二、資通安全政策

因應公司資訊設備除自然損壞外，還需避免內、外部資安事件之威脅。於災害發生時，能迅速應變，在最短時間內回復正常運作，降低事故帶來的損害。

(一) 成立資安單位，訂定資通安全政策及具體管理方案，以確保資通安全。

(二) 個人電腦、伺服器皆需設定密碼，安裝防毒軟體，並定期更新病毒碼。

(三) 應遵守智慧財產權相關規定，確保安裝軟體皆有合法授權。

(四) 重要資料應進行備份，並定期確認備份資料有效性。

(五) 規劃災害復原計畫，以利資安事件發生時快速恢復系統運作。

(六) 為加強員工資訊安全意識，不定期發送電子郵件宣導資訊安全資訊。

三、資通具體管理方案及投入資通安全管理之資源

(一) 加入資安情資分享 TWCERT 聯盟，蒐集資安情資及修補漏洞，並參與資安課程提升資安人員防護能力。

(二) 建構新世代防火牆，結合入侵偵測與防禦、掃毒引擎以多重保護方式有效過濾藏匿於網際網路中的各種病毒、間諜軟體、網路釣魚...有害程式。

(三) 設置電腦主機、伺服器等設備專用機房，對機房執行進出記錄管制、影像錄影監控，機房內部設有獨立空調維持機器於適當的溫度下運轉，並放置滅火器可緊急應變火災發生。

(四) 重要伺服器委託外包專業電腦資訊廠商做代管維護服務。

(五) 依資料性質進行資料備份、與異地存放，定期進行資料還原測試。

(六) 災害復原計畫，定期模擬演練、架設備援用主機及設備，以利災害時能快速恢復系統運作。