

資通安全管理方案及資源

一、範圍

公司之資通資產、電腦、資訊與網路服務相關之系統、設備、資料及人員，包含外包廠商、訪客及其他經授權之人員、服務及設施之管理。

二、管理方式

安全項目	措施
人員安全管理及教育訓練	<ol style="list-style-type: none">1.使用者工作職掌需使用電腦或涉及機密者，應賦予機密維護責任，並進行資訊安全教育訓練。2.使用者應妥善保管帳號密碼，並定期更換密碼，以維持安全性。3.公司對員工實施資訊安全教育訓練。
電腦主機安全管理	<ol style="list-style-type: none">1.存放資訊之電腦主機或伺服器，除作業系統之安全設定外，並強化身分辨識之安全機制，防止非法使用者透過遠端撥接或網際網路傳送資料時，遭截取登入密碼，及防止假冒合法使用者身分登入主機進行竊取或破壞行為。
資料安全管理	<ol style="list-style-type: none">1.保護重要檔案，以防止遺失、損毀、偽造或竄改，儲存於伺服器或轉出、傳出之檔案，系統將自動依檔案之機密程度設定權限。2.依使用者工作職掌，賦予不同資料存取權限，並保存檔案之存取紀錄以備查核，避免資料外洩或不當存取。3.嚴禁使用或開啟無版權、來路不明或內容不確定之軟體及私人可攜式儲存裝置(USB 埠、藍芽、無線網路、可攜式磁碟、記憶卡、隨身碟、外接硬碟、光碟片、智慧型手機……等)。
網路安全管理	<ol style="list-style-type: none">1.網路系統主機伺服器配有備援系統，以備主機無法運作時之用。

	<p>2.網路設備配置不斷電系統，以防電力中斷。</p> <p>3.以防火牆及防毒軟體區隔內部網路與網際網路間之非法連結，阻絕電腦病毒及攻擊性軟體非法入侵與存取資料。</p>
設備安全管理	<p>1.設備地點之防護：設備應設置於適當地點並予以保全，以防環境不安全引發之危險及未經授權存取資料之機會。</p> <p>2.電源供應：資訊設備之設置，應防止斷電或其他電力不正常導致的傷害，並配置不斷電系統。</p> <p>3.設備維護：資訊設備應妥善維護，以確保設備充分運作，維護作業須經授權之人員執行，並記錄維護情形。</p>
環境安全管理	<p>1.全年無休掌控電腦機房運作情形(空調、溫溼度、電源供應、煙霧偵測、火災警報、防水防漏……等自動通報系統，以確保機房安全。</p> <p>2.備援之設備、軟體應存放於距電腦機房以外一定距離以上之安全地點，以達資料保全之目標。</p>