【資訊安全風險管理】

資訊安全風險管理架構

本公司於每年進行資通安全檢查，檢討使用電腦化資訊處理作業，並得於年度結束後向董事會進行報告。主要重點為檢討資訊整體架構、備份完整與可用性、資訊安全措施是否完善，與公司內部安全防護機制是否完備等，並實施具體改善措施，重點如下：

一、現行資訊架構檢討：

資訊電腦與網路日新月異，面對不斷更新之軟硬體及設備，資訊架構必須隨時調整、檢討與強化；公司逐年對於老舊設備訂定計畫汰舊換新，讓既有系統得以持續正常運作，並規畫結合最新虛擬技術降低維護與人力成本。

二、備份機制架構檢視：

備份作業對於資料之保存尤為重要，公司除針對重要系統與資料進行完整備份與差異備份外，亦將部份重要資料進行媒體備份，並將儲存媒體實施異地存放，以保障重要系統資料不至漏失；此外，並逐步規畫與評估硬體備援機制，期能在硬體設備無法修復時得以及時啟動備援硬體，使公司重要系統得以持續運作。

三、網路安全架構改善：

不定期檢視資訊網路安全架構是否完善，如遇具威脅之網路事件，即配合相關資安維護廠商共同研擬應對方案，對於需要增強之防護架構檢討更新強化措施或採購相關設備，以因應突然其來之威脅與衝擊。

四、安全設定方式檢討：

隨時檢視防火牆、郵件過濾規則與病毒碼更新原則，檢討防火牆設備之防護是否有升級之必要；針對年度內曾發生之郵件過濾事件，是否有調整規則之必要；與防毒政策對於網路及內部設備之防護性評估等。

資訊安全政策

公司內部網站中已公佈倫飛資訊使用準則(Twinhead IT Policy)，將有關軟硬體使用、規範及管理方式詳述其中，該政策概分為四大部份。

一、安全政策：

說明公司對於員工帳號安全、郵件、與資訊網路活動之安全控管方式，強化公司資訊網路之安全性。

二、服務政策：

說明資訊單位對於各項軟硬體之管理流程與方式，對於相關系統之問題排除與作法。

三、軟體授權政策：

說明軟體之相關分類，使用授權及相關規範，並定期進行軟體稽核作業，以確保公司內部軟體使用之安全性。

四、資料政策：

說明公司內部有關資料位於不同設備之管理原則與權限，以確保各項資料安全保存於公司內之相關設備。

資訊管理方案

本公司不斷在資訊各環節建置保護措施，以維護公司資訊之安全，並將資訊管理各項方案揭露於年報中，各相關實際作法分述如下。

一、網路安全：

為防止各類網路攻擊，特別建置國外大廠之防火牆設備與系統，透過製定各種阻隔網路攻擊之規則與機制，確實將不同類別之網路攻擊阻擋，使其無法進入公司內網；也特別設定各類上網群組權限，提供不同部門之員工依照業務需求使用，充分降低受到網路攻擊的風險。

二、資訊安全：

各類資訊不斷透過網路傳入公司網路，為防止外來資料之入侵與攻擊，特別建置了郵件過濾防護系統，此系統包含兩層防護，第一層為郵件類型過濾，第二層為郵件防毒過濾，第一層可針對外來郵件設定規則，避免遭受常夾帶病毒檔案或連結之攻擊，並不定期更新相關資訊；第二層則針對可能夾帶病毒類型的郵件進行掃瞄與隔離，待資訊人員確認無風險後始放行該郵件，確實做到雙層防護。

三、員工電腦：

員工機台上皆安裝用戶端防毒軟體，並於每日固定時間連線防毒主機下載最新病毒碼，當電腦有不明中毒檔案時即可發現並隔離，保護員工個人電腦不受到病毒之攻擊，甚至造成資料相關損失。

四、系統控管：

無論系統與資料存放空間，皆有權限之控制與管理，該項權限需透過公司內部電子簽核流程進行申請，申請單將配發給相關資訊人員，由其進入系統進行設定與開放，員工才得以具備進入系統或讀取資料的權限，對於資料之安全性控管可說相當之嚴謹。

五、資訊軟體：

為避免員工不當下載或安裝非經授權及合法購買之軟體，資訊單位於每年不定期進行資訊軟體稽核作業，各部門設置有資訊軟體稽核員，配合資訊單位針對部門內部員工安裝之軟體進行清查與稽核作業，相關資料彙整後即再進行第二次之複查作業，一旦發現有異常情況時馬上通知改善。

六、系統損壞風險：

公司內各重要系統皆進行備份排程，將各類系統之作業系統與資料進行備份，以防系統損壞或無法使用時可進行回復作業。此外，部份系統已經進行虛擬化作業，以防在系統產生無法運作時，可快速將系統復原使用。系統重要備份定期存放於銀行保險箱，以強化異地備援作業，降低系統意外發生之風險。