【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。

本年度於 **112 年 3 月 16 日第十三屆第八次董事會**中報告資安風險管理架構及執行概況。

資訊安全政策

1.遵循 ISO 9001 資訊規範與標準：

相關資訊規範與標準以遵循 ISO 9001 之資訊服務管理程序為原則，如遇政策需新增、修訂或廢止有關內容時，承辦之資訊單位將以電子簽核系統申請 ISO 文件/表單處理申請單，將所要修正之內容述明於摘要處後，進行會簽單位之簽核流程，提供公司內部作為相關參考。

2.外部資訊稽核制度：

每年或不定期由委外稽核單位，針對資訊系統及內外部網路架構進行檢視；內容包含了資訊部門之組織架構、職責分工、委外資訊作業、應用系統架構、財務報表運用處理、網路與伺服器硬體架構…等，並檢視年度重要之資訊計劃與專案，以確保資安相關活動之合理性。

3.資訊安全管理政策：

公司制定倫飛資訊使用準則 (IT Policy)，為有效管理相關電腦與資訊資源之使用規範，內容涵蓋員工個人使用之工作機台、無線網路使用規範、電子郵件與網路瀏覽之管理、防毒管理機制與作法、軟體合法授權使用與稽核、檔案權限管理與授權…等，以有效維護公司內部資訊環境。

4.內部資訊稽核制度：

資訊單位配合公司稽核單位於每年進行資訊安全內部稽核，填具資訊安全內部稽核檢查表，針對使用者電腦系統帳號密碼、防毒軟體之運行模式、外部網站與網頁瀏覽之安全性及相關之控管措施予以調查，協助資訊部門進行檢視，以強化內部資安控管機制。

具體管理方案

1.實體防火牆（Firewall）管理：

採用硬體防火牆管理，進行外部網路相關攻擊之阻絕方式，防火牆中皆已規劃及運用資訊單位所訂定之資訊策略，來不斷監控內外部的資訊活動，並扼止相關異常資訊活動，以保護內部資料的安全。

此外，並結合內部 AD (Active Directary)伺服器，制定公司內部使用者之網路瀏覽權限，避免使用者進行違規之網路瀏覽活動導致內部檔案或資料被竊取或遭病毒感染。

COVID-19 疫情期間更規劃使用防火牆之既有 VPN（Virtual private network）功能，得以使兩岸三地及國外地區之使用者，可隨時取用公司內部資源，提升整體之工作效率。

2.郵件安全管制措施：

各類資訊不斷透過網路進行交換，為防止外來資料的入侵與攻擊，專門建置了郵件過濾流程與系統；此系統包含兩層防護；第一層使用了郵件類型過濾（IMSVA），第二層為垃圾郵件過濾（Mail Sweeper），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，並不定期更新病毒資訊；第二層則補強第一層之功能，將判定為垃圾郵件之信件進行掃瞄與隔離，待確認無風險後始放行該郵件，確實做到層層的防護。

3.防毒管理機制：

公司所有工作機台皆於使用前預先安裝使用者端防毒軟體（Officescan），此作為可於使用者存取異常檔案文件時，即時將有問題之檔案文件予以隔離或刪除，以避免同仁電腦中毒產生後續感染或問題；此外，伺服器端亦不定期自動更新病毒碼，於系統管理者設定之時間，自動更新使用者端相關資訊，達到防止病毒入侵之最好效果。

4.系統與檔案文件權限管理：

公司將各部門重要檔案文件儲存於 NAS 檔案伺服器中，並定時進行備份作業；使用者需要使用相關系統或瀏覽檔案時，必須具備應有的權限，否則是無法使用系統或瀏覽文件的。

而權限需經過電子簽核系統（Business Process Management）中之需求申請單，並經過部門主管等之簽核後，方可由系統管理人員開放權限與使用。

5. 台北總部/高雄廠均已建置 OSSIM 資安平台，進行內部監控及檢測：

本公司建置 OSSIM 資安資訊和事件管理平台，用於監控和管理組織的資訊安全狀態，幫助公司識別、監視、回應和管理安全事件，以提高資訊安全性。

OSSIM 功能包括資訊收集和整合、事件分析、資訊安全監控、威脅情報彙整、定期報告和即時警報，以及安全設備整合，並由多種資訊源收集安全事件和日誌數據，包括防火牆、入侵檢測系統 (IDS)、入侵預防系統 (IPS)、操作系統、應用程序和網路設備，並提供事件審計和分析功能，利用內置的安全資訊和事件管理 (SIEM) 功能來幫助分析人員檢測潛在的安全威脅和攻擊模式，以實時的資訊安全監控，讓安全團隊能夠查看網路和系統的當前狀態，以識別異常活動，整合多個威脅情報源的數據，協助安全專業人員及早識別新的安全威脅和漏洞。

資通安全管理資源

1.編列相關預算

資訊部門於每年底檢視當年度執行成果，並探討各項資訊基礎建設、虛擬化效益、重點資訊系統維護升級等重要指標，訂定次年度之相關改善專案，以強化與提升公司之資訊能力。

本年度已編列 2024 年預算，將會進行資安釣魚測試及測後教育訓練會議。

2.系統功能性委外以強化維護

公司多項營運作業系統除資訊部門負責部份維護作業外，亦配合相關委外維護廠商共同維護，如電話交換機系統、企業資源規劃 ERP 系統、BPM 電子簽核流程系統、GPM 綠色供應鍊管理系統、人事薪資系統、門禁管制系統等，皆逐年編列預算，遇系統產生異常狀況時，可即時到場維修服務。

3.資訊單位人力資源

資訊部門人力六名，專責需求整合分析、ERP 系統規劃管理維護、電信網路與資安設備管理維護、簽核流程系統管理維護等及產線需求客製及電信網路硬體設備管理與維護；並配有**資安專業人員兩名**，分配配置於台北總部與高雄廠，以期即時應對於不同工作地區所發生之資安事件。