資訊安全風險管理報告

日期:2025/11/7

前言

隨著時代的進步、資訊的發展網路的延伸，資安風險也日漸升高，甚而影響企業的運作或財務、業務的損失。公司對於資安風險，業已建置資訊安全風險營運管理機制因應，如「資訊安全管理辦法」、「資訊設備管理辦法」、「電腦機房管理辦法」、「電腦儲存設備報廢作業辦法」、「電腦化資訊系統作業」及「資訊系統災害復原演練計畫」等相關資訊安全風險管理機制營運，提供所有員工落實遵循，以保障員工，供應商和客戶進行業務接洽時之隱私權保護與資訊安全維護及所有利害關係人之權益，盡職企業社會責任，並輔以相應的內部控制制度、營運管理機制，以茲日常運行，達成公司營運的效果效率、公司經營之成果。

資訊安全策略

本公司的資訊安全政策是以
1、建立符合法規與客戶需求之資訊安全管理規範
2、透過全員認知，達成資訊安全人人有責的共識
3、保護公司與客戶資訊的機密性、完整性與可用性
4、提供安全的生產環境，確保公司業務之永續營運

並以防毒、防駭、防漏三大資安防護主軸為目標，建立防火牆、入侵偵測、防毒系統及諸多內控系統，以提升公司在防禦外部攻擊以及確保內部機密資訊防護的能力。

114 年度資訊安全執行成效

1. 年度投入資訊安全費用相關共計 913 萬元(網路威脅相關 504 萬，帳號權限相關 279 萬，伺服器備援相關 130 萬)
2. 完成關鍵系統弱點掃描，資訊系統原碼報告、主機弱點檢查報告，防止威脅入侵
3. 完成同仁共 615 人次資訊安全教育訓練課程並完成測驗，未通過者年終考績不得為 A 等(含)以上
4. 完成電子郵件社交工程演練，隨機發送 304 人次，無人輸入帳密，防範員工遭受釣魚信件等社交工程作業威脅
5. 完成年度 ERP 權限查核，避免人員組織異動，授權過大和資料外洩的風險
6. 完成年度資訊系統災難復原演練，發揮災難應變能力，確保資訊系統持續營運不中斷
7. 每月資訊安全宣導，加強員工對於資訊安全風險之應變與警覺性
8. SAP 異地備援系統已於 2025 年 4 月完成導入並上線，並且納入年度系統災難復原演練程序，以確保企業營運持續性。
9. 資產管理軟體於 2025 年 1 月完成設置，加強對用戶端進行應用程式與網路行為管控，

規範電腦設備的使用權限，避免員工不當修改系統設定或安裝非授權軟體，確保 IT 系統穩定。

10. 為確保網路服務的連續性與穩定運行，2025 年 9 月啟動機房核心交換機升級至高可用性（HA）架構，以有效消除網路骨幹的單點故障風險。

2025 資安費用明細

網路威脅相關	防毒系統及 APT 駭客防禦系統維護	1,380,000
	弱點掃描及滲透測試服務	410,000
	網路骨幹及安全設備年度維護	1,254,500
	機房核心交換機升級 HA(高可用性)架構	2,000,000
帳號權限相關	遠端連線辦公 SSLVPN 設備年度維護	470,000
	AD 帳號登入權限管控系統年度維護	320,000
	IST 資產管理軟體	2,000,000
伺服器備援相關	郵件主機系統及 SPAM 系統年度維護	640,000
	SAP 異地備援費用	660,000
Total		9,134,500

資安控管機制

資安控管	機制說明	風險控制
特權帳號控管	用戶端電腦本機管理員特權帳號管理系統	防範員工任意安裝非法盜版軟體或惡意軟體入侵
資安意識控管	資訊安全意識加強，減少資安風險	進行資訊安全教育訓練機制，不定期宣導資安風險
周邊裝置控管	用戶端電腦周邊裝置存取管控系統	防範員工使用可移動儲存裝置洩漏機敏資訊
網路存取控管	上網行為管控及威脅偵測系統	防範員工上惡意網站，遭受病毒威脅入侵
社交工程演練	建置社交工程演練作業，防護電子郵件使用安全	防範員工遭受釣魚信件等社交工程作業威脅
資訊外洩控管	用戶端重要檔案進行加密作業	防範機敏資訊外洩及駭客攻擊
系統弱點控管	資訊系統原碼檢測、主機弱點偵測掃瞄系統	資訊系統原碼報告、主機弱點檢查報告，防止威脅入侵
日誌稽核控管	主機日誌管理系統	提供資安事件稽查之相關軌跡日誌查詢
網路威脅控管	導入 IPS（入侵防禦系統）過濾網路流入封包	主動防禦 / 封鎖網路異常行為，避免零時差攻擊
遠端存取管控	提供 VPN 雙因素驗證，管控公司外遠端連線作業	提供員工在公司外連線到公司內部使用資訊應用系統
端點保護管控	端點病毒 / 行為特徵碼偵測管控	針對端點行為特徵碼監控，以避免端點受到攻擊

115 年度預計執行計畫

1. 為確保 IT 系統穩定運行與資料安全，自 115 年起將啟動『使用年限逾七年之系統伺服器』的全面汰換計畫，以有效降低硬體老舊所導致的營運中斷風險。本計畫將採分年分階段實施，首要任務是優先評估及汰換對企業營運具有重大影響性的核心硬體。
2. 啟動硬體資源整合與整併企劃，透過虛擬化或雲端化等技術，實現資源最大化利用。此計畫的效益在於有效減少機房空間佔用、降低電力與維護成本，並藉由集中管理來顯著提升整體 IT 營運效率。執行策略上，自 115 年起我們將優先針對對企業營運具有重大影響性的核心系統，進行資源整併與優化評估。
3. 規劃商業智慧（BI）與視覺化分析報表工具的導入專案，以推動企業數據應用現代化。藉由工具協助營運單位迅速掌握關鍵績效指標（KPI），並透過數據視覺化，優化營運監控與策略制定流程。
4. 取得 ISO 27001 資訊安全管理系統（ISMS）認證，證明本公司的資訊安全控制措施與風險管理能力符合國際規範。此舉將進一步落實資訊資產保護，並確保符合相關法規遵循要求。
5. 每年執行二次弱點掃描及滲透測試，防止威脅入侵。
6. 年度 ERP 權限查核。
7. 年度資訊系統災難復原演練。
8. 電子郵件社交工程演練。
9. 每月資訊安全宣導。

結語

本公司 114 年度無重大資通安全事件，但仍秉持著防範未然之心態持續編列適當的預算強化資訊技術安全，保護公司與客戶之資產安全。