

114 年度資訊安全政策落實情形報告

(一)資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源：

1.本公司在112年5月8日於行政管理處項下新增「資安部」，並由董事會委任行政管理處協理兼任「資安主管」一職，負責資通安全政策擬定、資通安全風險及資通安全事件等管理作業，資安部並設有1名資深管理師負責資通安全環境之建置、宣導與執行，並向資安主管報告，目前投入2名人力以透過蒐集及改進組織資訊安全管理系統績效及有效性之技術、產品或程序等，共同提升全體員工資安意識。另外，稽核室每年就內部控制制度—電腦化資訊系統循環，進行資訊安全查核，評估公司資訊作業內部控制之有效性。

2.資通安全政策及具體管理方案

公司已訂定「資通安全管理政策暨施行細則」及「電腦化資訊系統循環-資通安全事件管理作業」以落實資安管理，並於內網系統增設「資訊安全事件通報單」，當公司遇到資安事件，同仁能以電子方式及時通報相關單位，資安人員將依影響等級採取不同措施，以降低公司資安風險，期藉由全體同仁共同努力期望達成各控制文件明訂政策目標。

此外，每一年至少執行1次既定災難還原演練，並自107年導入災難還原備份機制後，至今為止已完成了8次記錄。

(1)資通安全政策：

A.網際網路資安管控：內容包含架設防火牆 (Firewall)；定期對電腦系統及資料儲存媒體進行病毒掃瞄；各項網路服務之使用應依據資訊安全政策執行；定期覆核各項網路服務項目之 System Log，追蹤異常之情形。

B.資料存取管控：內容包含電腦設備應有專人保管，並設定帳號與密碼；依據職能分別賦予不同存取權限；調離人員取消原有權限；設備報廢前應先將機密性、敏感性資料及版權軟體移除或覆寫；遠端登入管理資訊系統應經適當之核准。

- C.應變復原機制：內容包含定期檢視緊急應變計劃；每年定期演練系統復原；建立系統備份機制，落實異地備份；定期檢討電腦網路安全控制措施；資訊安全事件通報單。
- D.宣導及檢核：內容包含隨時宣導資訊安全資訊，提升員工資安意識；每年定期執行資通安全檢查，呈報董事長；內外部稽核。

(2)具體管理方案：

公司全體同仁應遵照內部控制制度:電腦化資訊系統循-資通安全事件管理作業。

- A. 平時應定期完善維護系統設備，維持設備正常運作，以減少重大故障的發生機率。
- B. 針對遭遇內部危安（如人為破壞）、外力入侵（如病毒感染、駭客攻擊、非法入侵）、重大突發（如網路系統骨幹中斷）等事件定期作應變演練。
- C. 定期辦理系統弱點掃描、頻寬管理、系統內部安全漏洞檢測（更新、補強），儲備必要之備份資料、程式異地備援。
- D. 以上作業程序所指核心系統為：JDE(ERP)、BPM。
- E. 以上控制重點使用表單:資訊安全事件通報單。

(3)投入資通安全管理之資源

針對以下目的所投入之資源：

- A.端點防護：訂閱最新病毒碼(費用約 4 萬元)每週檢查並更新病毒碼，每季檢查作業系統之更新。
- B.硬體防禦：使用 LEADERS 象限防火牆，訂閱網路防火牆防毒服務(費用約 16 萬元)，保持最新防火牆服務，強化網路資安管理。
- C.安裝控制：確保合法使用授權軟體與防範惡意軟體。
- D.資安案例分享與社交工程演練：114年度宣導共計1次，並隨時接獲可疑案件即進行分析與教育訓練。
- E.備援機制建置：每日備份3次，異地備份1次。

F.災難還原演練：分異地與本地演練，共3人投入演練(114年共1次)。

G.稽核室內部稽核每年至少一次(114年共1次)，委外外部稽核為不定時(114年共1次)。

H.主要系統弱點掃描(112年及114年各1次)。

(二)民國 114 年度因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實：
114 年度本公司無發生重大資通安全事件。

(三)資安強化計劃 (預計 2026 年第一季導入)

1. 資安防護升級，導入TeamT5 EDR及MDR服務

- (1) 伺服器與使用者電腦全面部署”端點偵測與回應”並由資安公司代為管理
- (2) 有效防範勒索軟體及APT進階持續性威脅攻擊
- (3) 大幅提升資安事件偵測率與應變速度
- (4) 所有伺服器已完成測試驗證

2. 備份機制強化，採用分層備份策略確保資料安全

- (1) 本地 + 異地 + 雲端三層備份架構
- (2) 關鍵資料異地保存，抵禦勒索病毒威脅
- (3) 備份頻率提升至每小時一次
- (4) 大幅縮短資料復原時間點目標

3. 儲存系統升級，導入PURE Storage企業級解決方案

- (1) 內建不可變動區與零信任資安機制
- (2) 確保高可用性與快速復原能力
- (3) 支援集團層級資料整合與後續AI分析應用發展