新聿科技股份有限公司

2026 年資通安全管理執行情形報告

（2026 年 8 月 10 日董事會呈報）

壹、執行摘要

一、 年度資安目標達成率：

2026 年截至 7 月底重大資安事件發生次數為 0 次，核心系統整體可用性達【99.9%】，均符合年度關鍵績效指標（KPI），有效保障公司營運連續性。

二、 資安治理成熟度：

本公司現階段以「合規防禦」為核心，已具備基礎防毒與防火牆等防護機制。為落實金管會最新《上市上櫃公司資通安全管控指引》之完整規範，本年度已主動完成「資訊安全管理程序書」之重新增修訂作業，健全公司內部資安規章。

三、 核心威脅與對策：

面對日益嚴峻的勒索軟體與關鍵數據外洩威脅，本公司已完成【核心數據異地備份機制】之建置，落實資料多重保障，並將持續優化資安監控與事件應變流程。

貳、資安風險管理架構

一、 組織編制：

本公司依法規與治理需求，設置資訊安全專責主管 1 名，以及資訊安全專責人員 1 名，專責規劃、推動與執行全公司之資通安全政策與防護作為。

二、 運作機制與資安宣導：

（一） 日常落實：本年度常態性落實跨部門資安宣導，定期發布新型網路詐騙與釣魚郵件手法警示，並將資安觀念納入新進員工培訓課程，藉此深化全員防護意識、降低人為疏失之安全風險。

（二） 優化措施：為強化橫向溝通與高階治理架構，本公司規劃自 2027 年起，正式建立「定期資安管理審查機制」，預計每年定期召開跨部門資安審查

會議，由資安專責主管召集，針對內部合規、演練成果及最新安全風險進行實質審查，確保資安政策落實於日常營運。

三、 董事會督導與獨立查核：

本報告依規定每年向董事會進行執行成效報告。安侯建業聯合會計師事務辦理本公司「資訊安全管理作業專案查核」查核範圍涵蓋所針對 2025 年 7 月 1 日至 2026 年 6 月 30 日期間之相關作業，查核結果顯示本公司相關作業均符合內部控制制度，尚無發現重大缺失。此外，內部稽核室已依 2026 年度稽核計畫排定於 2026 年 11 月辦理資通安全管理作業查核，持續追蹤及檢視資通安全管理制度之有效性。

參、資安政策與具體管理方案

一、 制度與國際認證規劃：

本公司高度重視穩健之資訊安全防護。針對導入 ISO 27001 / CNS 27001 資訊安全管理系統標準及取得第三方驗證事項，本年度已由資訊部門與資安人員完成「可行性與效益評估」。

考量現階段營運規模，本公司採取漸進式深化策略，2026 年度首要聚焦於「完善專責編制與落實內部規章」；並規劃於公司掛牌上櫃後之 2 至 3 年內（預計 2028 年度），視整體營運規模與業務需求，適時啟動外部專家輔導與國際標準驗證計畫，以確保公司資安管理持續符合國際先進標準。

二、 技術面防禦成果：

（一） 端點防護：

全公司電腦與伺服器之防毒軟體部署率已達 100%，有效提升對於惡意程式與已知威脅之即時攔阻能力。

（二） 日誌留存（Log Server）建置規劃：

為落實資安事件可追溯性，本公司目前正規劃建置中央日誌伺服器（Log Server），用以集中留存核心防火牆之各項存取紀錄與網路日誌，本案預計於民國 2026 年 9 月底前完成建置，以符合主管機關對於資安軌跡留存之合規要求。

（三） 外部情資通報機制：

本公司已於民國 2026 年 6 月正式加入「台灣電腦網路危機處理暨協調中心（TWCERT/CC）」企業會員，藉此落實外部資安威脅情資之即時共享與早期預警機制，提升公司整體之防禦前瞻性。

三、 管理面與意識提升：

（一） 員工社交工程演練（釣魚郵件測試）成效：

1. 演練數據：

本年度首次辦理全體員工防範惡意電子郵件之社交工程演練，受測同仁之整體開信率為 44%；其中進一步點選惡意連結或下載附件之高風險等級比例為 17%。

2. 盲點分析：

由於本案為公司第一次舉辦，數據反映出部分同仁對於新型態社交工程手法（如：冒充內部公告、假冒外部合作廠商、人事權益通知等）之警覺心仍有不足，人為防線為當前主要需補強之弱點。

3. 具體補強與改善作為：

(1) 針對性補訓：

已針對本次演練中點選連結之高風險同仁（17%），立即實施強制性之線上資安補強教育訓練與測驗，確保建立正確防範觀念，目前已全數完成補訓。

(2) 制度化管理：

規劃自 2027 年度起，正式將「社交工程演練結果」納入員工年度績效考核（KPI）與考績指標，透過制度引導強化員工資安警覺性，落實全員資安聯防。

(3) 下年度演練目標：

2027 年度規劃辦理至少 2 次演練，並採取「漸進式難度」測試，目標將整體開信率降至 20% 以下，高風險點選率降至 5% 以下。

（二） 全員資安通識教育訓練：

本年度已針對全體在職同仁辦理基本「資安通識教育訓練」，課程涵蓋商務電子郵件詐騙（BEC）防範與日常辦公環境資安規範，全體同仁完訓率達 100%，有效滿足主管機關對公開發行/掛牌公司之年度訓練合規要求。

（三） 資安專責人員專業培訓（合規遵循）：

依據主管機關規範，本公司資安專責人員每年應接受至少 15 小時以上之資安專業訓練。 本年度本公司資安專責主管與專責人員均已積極參與外部專業訓練課程（課程包含：CISSP資安系統專家認證課程、上市上櫃公司資通安全管控指引合規實務解析、參與資安大會等），本年度累計受訓時數已超過15小時，依法完全符合現行主管機關之年度合規訓練要求。

四、 供應鏈資安控管：

（一） 風險評估實施：

鑑於第三方委外風險日益增高，本公司針對主要資訊協力廠商及關鍵供應商，目前正規劃並積極執行外部資安風險評估作業，本案預計於民國 2026 年 9 月底前全面落實完畢。

（二） 機密防護加強：

本公司已全面要求上述關鍵供應鏈合作夥伴簽署「資安保密協定（NDA）」，藉此建立法律防線，有效降低因供應商端延伸之資安漏洞或機密外洩風險，確保公司核心業務數據之安全性。

肆、關鍵資安指標與威脅演練

一、 資安事件統計：

本年度除零星之一般廣告郵件與連線異常通報外，未發生任何損及公司商譽、營運或客戶個資之重大資安事故。

二、 業務連續性演練實績：

（一） 核心系統災害復原演練（DR 演練）實績：

本年度已順利完成核心 ERP 系統之災害復原演練。經實測，系統目標復原時間（RTO）小於 24 小時，資料復原點（RPO）亦控制於 24 小時以內，演練結果均完全符合本公司「營運持續計畫（BCP）」之規範指標。

（二） 勒索軟體專案應變演練規劃：

針對當前嚴峻之駭客威脅，本公司正規劃實施「資安事件專案應變演練」，預計於民國 2026 年 9 月底前完成。本案將實地模擬核心網絡遭受勒索軟體攻擊時之緊急通報、受駭主機隔離、以及備份資料還原流程，旨在確保跨部門應變小組熟練緊急處置程序。

伍、合規情形與前瞻規劃

一、 法規遵循與揭露：

本報告之編製與執行內容，均符合「公開發行公司建立內部控制制度處理準則」之規範，並將依規定配合辦理年報中關於資通安全風險管理、重大資安事件等各項法定資訊之公開揭露事項。

二、 前瞻法規與市場趨勢因應：

本公司持續密切關注並落實國內外最新資安法令與國際趨勢（如：國內《個人資料保護法》之修正條款，以及歐盟《網路韌性法案》（CRA）對於產品安全之嚴格規範）。未來將逐步規劃將安全漏洞管理機制全面納入產品研發與系統生命週期中，以確保本公司之產品與服務能符合未來國際市場之合規高標準。

三、 2027 年度重點工作與預算規劃：

（一） 核心營運系統升級（強化營運韌性）：

本公司預期於 2027 年度進行核心「SAP 系統之版本升級作業」，藉由原廠新版功能深化數據安全防護、優化系統效能，並修補潛在之安全漏洞，從源頭強化核心業務系統之資安防禦與營運韌性。

（二） 資安專責同仁專業培訓：

持續辦理資安專責人員之外部專業技術培訓，輔導參與國際資安證照或最新威脅鑑識課程，維持並持續提升內部專家之專業防護能量，以因應日益複雜之外部黑客威脅。

（三） 資安預算編列：

2027 年度預計編列資安專責預算共計新台幣 650 萬元整。本筆預算將專款專用於維護現有資安基礎防線、支應上述核心 SAP 系統升級之資安相關項目、以及落實專責人員培訓，確保公司在準備掛牌期間之營運安全。