2025 資訊安全報告 總覽

1. 資訊安全管理政策

為保障聯德之產品與服務在開發、生產與交付過程中的資訊安全，防範未經授權之存取、變更、濫用或揭露，並降低因自然災害或資安事件導致之營運中斷風險，本公司致力於建立與維護資訊安全管理制度，確保 關鍵資訊資產之機密性、完整性與可用性。相關管理措施皆遵循適用法令與客戶要求，並結合國際標準如 ISO/IEC 27001 進行持續精進，以強 化外部信任、實踐對客戶與股東的承諾，確保公司核心業務得以穩定、安全且持續運作。2025 年未發生重大之資安事件，也未有接獲侵犯客戶隱私或遺失客戶資料的投訴。

我們重視資訊安全與客戶資料保護，依據 ISO/IEC 27001 國際標準建置資訊安全管理系統(ISMS)並取得驗證。為確保制度有效運作，公司每年至少辦理一次內部自我稽核及一次由公正第三方執行之外部稽核，並每三年進行一次證書重新驗證作業，以持續維持 ISO 27001 認證之有效性。

(1) 維持各資訊系統永續運作

(2) 防止駭客、各種病毒入侵及破壞

(3) 防止人為意圖不當及不法使用

(4) 防止機敏資料外洩

(5) 避免人為疏失意外

(6) 維護實體環境安全

2. 資訊安全管理架構

(1) 本公司資訊部，負責規劃、執行及推動資訊安全管理事項，並推展資訊安全意識。

(2) 本公司稽核室為資訊安全監理之查核單位，若查核發現缺失，立即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低內部資安風險。

3. 資訊安全外部資源取得

類別	資源	說明
專業顧問資源	ISO 27001 輔導顧問	提供資安制度建置與稽核輔導
教育訓練資源	外部資安課程、證照訓練	提升員工資安意識與專業知識
法規與標準資訊	TW/CERT、資通安全網路月報(資通安全署)	取得最新法規、趨勢、資安威脅情報
緊急應變支援	TW/CERT	取得最新資安威脅應變資訊

4. 資訊風險事項報告

風險類別	風險項目/情境	管控單位	風險對策
資訊風險	**資訊安全風險** 因資安架構設計不當或系統、設備、網路、隱私管理機制等控管不足，導致資訊系統遭入侵可能性提高、面臨營運中斷等風險。	資訊部	落實ISO27001資訊安全管理系統，整合及強化資訊安全機制。 落實資訊安全教育訓練及模擬演練作業，提高資通安全智能及緊急應變能力。 設置資安專責主管及專責人員，負責資安防護事務。

5. 資安事件與因應

發生日期	資訊安全事件說明	影響等級	破壞程度	解決日期
2025/10/17	台電進行維護停電作業，計畫性停止機房內部網路及主機服務並恢復正常服務無資料之損失	1	無	2025/10/19
2025/10/25	台電進行維護停電作業，計畫性停止機房內部網路及主機服務並恢復正常服務無資料之損失	1	無	2025/10/26

6. 資訊安全人員教育訓練

日期	課程	時數(hr)
2025/04/08	資訊安全意識、必備知識與責任	2
2025/05/05	資安事件說明及預防措施	2.5
2025/05/05	上市上櫃公司資通安全管控指引說明	1.5
2025/04/15	AI掀起的猶疑遊戲怎麼玩？ 中小企業的資安心法與終局攻略	0.5
2025/04/15	AI 世代下的資安威脅應對策略	0.5
2025/04/15	企業機敏文件保護全攻略	0.5
2025/04/15	地緣政治風暴與企業韌性：在變局中駕馭不確定性	0.75
2025/04/16	18 年了，AD 還在被打：談談微軟安全編年史	0.5
2025/04/16	Generative AI 安全應用情境與架構	0.5
2025/04/16	資安長與未來資通安全領導者的六頂思考帽：全面守護企業資安的創新思維	0.5
2025/04/16	不知不覺，你就變成內鬼	0.5
2025/04/16	漏洞補不完！但更付不起企業失控的風險！一起來探討如何掌握漏洞管理的關鍵吧！	0.5
2025/04/17	別讓威脅情資只是 Big Data：自動化知識圖譜賦能情資關係推理與檢索	0.5

2025/04/17	Wauzh 打造 XDR 資安防護機制經驗分享	0.5
2025/04/17	開源後門程式對開源防禦平台剖析	0.5
2025/04/17	數位鑑識不該是你處理事件應變的重點	0.5
2025/04/17	金箍棒與緊箍咒：解密傳產的數位優化與資安治理策略	0.5
2025/04/17	DevSecOps 和自動化安全檢測的敏捷導入	0.5
2025/04/17	大型語言模型裡面五花八門的攻擊與防禦	0.5