董事會資安治理報告 (2025年11月)

Jim Chiou資訊處

2025/11/06

Agenda

1. 資通安全風險管理架構
2. 資通安全政策與具體管理方案
3. 資通安全管理之資源
4. 執行現況與未來規劃

資通安全風險管理架構

- 依據 ISO/IEC 27001:2022 標準實施，範圍涵蓋 ERP 與 EMS 系統（含基礎架構與終端設備）。
- 2025 Q2 完成 ISO 27001:2022 改版導入2024 Q3 取得母公司及子公司（智能、創博、創博機器人研發中心）之 多站點證書

證書

TÜV NORD Taiwan Co., Ltd.

ISO/IEC 27001
CNS 27001

tuv-nord.com/tw

管理系統依據

CNS 27001:2023 (ISO/IEC 27001:2022)

驗證機構台灣德國北德技術監護顧問股份有限公司特此證明，
依據 ISO/IEC 27006:2015/Amd.1:2020 標準進行的稽核、評估和驗證決定的結果，該組織

新漢股份有限公司
新北市中和區中正路 920 號 9 樓

另有其他場域，請參考附件

將採用符合 ISO/IEC 27001: 2022 標準要求的管理系統並且在本驗證的 3 年有效期間內將對符合性進行監督。

範圍

本公司資訊安全管理活動，包含：

- **新漢股份有限公司資訊處之企業資源規劃(ERP)系統之開發、維護及資訊機房維護。**
- **新漢股份有限公司華亞廠之製造執行系統(MES)管理及資訊機房維護。**
- **新漢股份有限公司三民廠之製造執行系統(MES)管理及資訊機房維護。**
- **新漢智能系統股份有限公司產品設計部之企業資源規劃(ERP)系統及網路設備管理。**
- **創博股份有限公司總經理辦公室之企業資源規劃(ERP)系統及網路設備管理。**
- **創博股份有限公司機器人科技創新中心之企業資源規劃(ERP)系統及網路設備管理。**

依據 2025-02-27 的適用性聲明書，版次 2.0

證書編號 ISMS254
稽核報告編號 IT-371

證書有效期始 2023-03-27
證書有效期至 2026-03-26
重新驗證稽核到期日 2026-02-16
版次3，首次驗證 2023-03-27

請訪問我們的證書資料庫，以驗證此證書的有效性。

台北, 2025-06-30

Liz-Teng Chang

驗證機構之台灣德國北德技術監護顧問股份有限公司

台灣德國北德技術監護顧問
股份有限公司
台北市大安區敦化南路二段
333 號 9 樓 A1 室
tuv-nord.com/tw

Management System
Certification
MS031

TÜV ®
ROC, TW5257, XA

資通安全具體管理方案

- 存取控制: 實施最小權限原則； 定期審查和更新； 實施強密碼策略；多因子認證(MFA)；合規映射(符合 ISO 27001:2022 A.5.18、CRA Secure by Default、IEC 62443-3-3 SR 1.1 要求。
- 操作安全: 加強數據中心和辦公區域的物理訪問控制； 進行容量管理和性能監控；惡意程式防護；多重備份(異地、磁帶備份)。
- 通訊安全: 網絡分段和隔離；NAC控制；外網訪問限制。
- 系統獲取、開發和維護:安全開發流程 (SSDLC)；第三方套件管理；弱點修補；軟體簽章等，滿足CRA有嚴格要求的部分。
- 供應商關係管理: 評估供應商的資安能力； 在合約中包含資安要求；確認是否符合 CRA（特別是工控元件的 CE 標章將納入 CRA 要求）。
- 業務連續性管理: 進行業務影響分析與持續營運演練

NEXCOM

資通安全具體管理方案

- 2026 年度新增要求:
- 符合歐盟 CRA 要求：對 IPC 與嵌入式裝置產品必須具備 secure by design、漏洞管理、產品生命週期安全維護機制。

建立 Product Security Incident Response Team (PSIRT)。

- IEC 62443 全面導入：對 OT 系統與 IPC 機台控制網採用 IEC 62443-3-3 技術控制。 對開發流程導入 IEC 62443-4-1（安全開發生命週期）。
- 零信任架構 (Zero Trust)：逐步導入零信任，針對跨廠區存取、VPN、雲端資源強制身份驗證與持續風險評估。

資通安全管理之資源

- 組織與人力：
  - 政策與合規團隊 2人
  - 資安運營與執行團隊 9人
  - 應變組: 6 人

資安組織架構

- 資安設備：
  - Sophos XGS（防火牆 - 過濾可疑或未經授權的通信）
  - Fortigate （入侵防禦系統)
  - Forescout （網路存取監控與合規性檢查)
  - N-Report （網路風險管理與分析）
  - Tenable Nessus (弱點掃描與分析工具)

NEXCOM

2025 執行現況

- 2025
  - ISO 27001:2022
    - 完成導入並取得證書
    - 取得子母證書
  - Sophos XGS防火牆設備更新
  - 雲、地DLP 導入作業進行中(資料洩漏預防)
  - 重要主機導入EDR進階攻擊防禦
  - 增購UPS 及建立磁帶備份作業
  - 導入社交工程郵件防禦方案
  - 增加(租)台中IDC作為異地備援機房

未來規劃

- 2026
- **配合建立合規地圖 (Compliance Mapping)**
  - 頒布一份「ISO 27001、IEC 62443、CRA 條文合規對照表」：
    - IEC 62443 → 著重工控環境/產品生命週期安全
    - CRA → 著重產品上市前、上市後的安全維護義務
    - ISO 27001 → 著重組織資訊安全管理
- **配合導入SBOM (Software Bill of Materials)功能**
  - CRA 強制要求供應商提供 SBOM，確保可追溯第三方元件漏洞。
- **配合安全更新承諾**
  - CRA 要求產品上市後必須持續提供安全更新（時間通常 ≥ 5 年）
  - **配合建立 PSIRT (Product Security Incident Response Team)**

NEXCOM

未來規劃

- **業務連續性與事件應變 (Business Continuity & Incident Response)**
- **資安事件演練：**模擬勒索攻擊、供應鏈惡意程式、OT 異常行為 → 驗證應變流程。
- **持續營運計劃 (BCP/DRP)：**針對生產製程（如 SMT、IPC 測試線）定義最大可容忍停機時間 (MTPD)。
- **事故通報機制：**CRA 規定「重大資安事件必須於 24 小時內通報主管機關」

2025 Q4 – 2026 Q1

- 配合椰棗，建立 PSIRT 與 SBOM 管理流程

2026 Q2 – Q3

- 協助導入 SSDLC + 自動化資安測試工具
- 協助OT 端部署 NDR/IDS、防火牆強化

2026 Q4

- 完成一次全廠 BCP/資安事件演練(如駭客攻擊、機房斷電火警等)
- 配合建立 CRA 合規報告模板（供歐盟市場產品認證使用）
- 配合對關鍵產品做 **第三方滲透測試 + 認證（IEC 62443-4-1/4-2）**