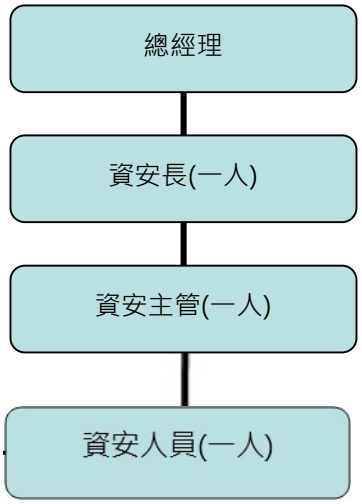
朋程科技股份有限公司

資通安全風險管理情形

一、 資通安全架構

總經理室所轄之資訊室負責資訊安全管理業務。



二、 資通安全政策

(1) 所有資訊作業相關措施，應確保資料之機密性、完整性與可用性，防止敏感性資料與機密性資料外洩與遺失。
(2) 資訊安全事件或可疑之安全弱點，應即時依程序通報反映，並予以適當調查及處理。
(3) 資訊資產應予適當保護，並採行合宜之備援回復措施及作業，以防止未經授權或因作業疏忽對資產所造成之損害。備援回復作業應確認資料之完整與一致性。
(4) 本政策應定期評估檢討，適時反映政府法令、資訊技術發展及公司相關業務需求，以落實資訊安全作業。

三、 具體管理方案及投入資通安全管理之資源

(1) 由稽核室擬定相關內部控制程序管理及定期進行內部稽核，並定期向審計委員會及董事會報告查核結果，以確保本公司資訊安全相關政策及作業之落實。
(2) 自 2022 年起採用委外租賃欣盟企業資安保全服務，提供重大威脅事件即時通報 / 每周中高風險通報 / 每月資產風險報告。
(3) 與資安廠商每年 Q3 全面重新評估風險並提出改善方案，2023 年已導入端點防護及 EDR 方案，2024 年預計更換自建郵件防護為雲端郵件防護服務。
(4) 本公司每年對員工實施「資通安全相關教育訓練及宣導」，每年每位員工完成至少 2 小時資通安全相關教育訓練及宣導。
(5) 資通安全委員會每年定期召開至少二次會議，2025 年度於第一季及第三季召開會議，並至少每年一次向董事會告，最近一次提報董事會日期為 2025 年 5 月 7 日。

四、 本公司取得資訊安全 TISAX 標章

本公司已通過由 ENX 協會認可的第三方稽核機構（SGS Taiwan Ltd.）依據 VDA ISA 標準進行的資訊安全評鑑，並於 2025 年 11 月正式取得 TISAX 標章：

- 等級：TISAX Level 2（AL2）
- 類別：Confidential / Information High（資料與資訊安全）
- 有效期限：至 2028 年 10 月 13 日

TISAX（Trusted Information Security Assessment Exchange）是汽車產業的資訊安全驗證標準，由 ENX 協會監督與管理。其目的是確保汽車供應鏈中的企業在處理客戶資料、設計圖、原型及技術資訊時，具備符合國際標準的資訊安全管理能力。

●TISAX 核心重點

項目	說明
主要目的	驗證汽車產業供應商的資訊安全管理能力，確保機密資料受到保護。
稽核標準	根據 VDA ISA（德國汽車工業協會資訊安全評鑑），並參考 ISO/IEC 27001、27002、GDPR 等國際標準。
評鑑方式	Level 2 採遠端真實性檢查，確保自我評估內容的合理性。
標章用途	可於 ENX Portal 上分享給指定客戶(如車廠或合作夥伴)，作為資安合規依據。

TISAX 標章的重要性

TISAX 標章已被多家國際車廠（如 BMW、Porsche、Mercedes-Benz）列為供應商合作的必要條件。取得該標章代表公司已符合歐系車廠對資訊安全的要求，作為客戶及外部稽核單位信任依據，同時展現公司在機密資料保護及資安管理上的成熟度與持續改善能力。

說明 TISAX Information Security AL2 認證與 ISO 27001 的對應關係及其優勢：

1. TISAX 與 ISO 27001 的關係

- TISAX（Trusted Information Security Assessment Exchange）由歐洲汽車工業協會（VDA）依據 ISO/IEC 27001 標準開發，專為汽車產業供應鏈設計。

- ISO 27001 是其核心基礎，TISAX 在此基礎上增加「可驗證性」與「特定風險防護」要求。

2. TISAX AL2 的安全特性

比較維度	ISO 27001	TISAX AL2 (高保護需求)
核心標準	ISMS 通用要求	完全涵蓋 ISO 27001 核心控制項
稽核深度	著重管理流程與文件化	強調控制措施成熟度與落地執行
特定防護	通用資訊安全	增強原型設備保護及第三方資料隱私
認可機制	證書式	交換平台稽核結果，由權威機構嚴格審核

3. TISAX AL2 的優勢

- **成熟度評分制**：採 0–5 級模型，確保資安措施穩定可預測。
- **供應鏈信任度**：為全球汽車大廠（如 Mercedes-Benz、BMW、Volkswagen）強制要求的標準，對數據與硬體安全管控更具體。

4. 結論

- TISAX AL2 不僅涵蓋 ISO 27001 核心控制項，更在資料保護與供應鏈風險管理上提供更高透明度與落地能力。
- 取得 TISAX AL2 認證即代表我司具備處理高敏感資訊的能力，其資安等級與 ISO 27001 相當，在物聯網設備管理等領域更具針對性。