環旭電子資訊安全政策

一、目的

環旭電子股份有限公司及其子公司（以下簡稱「USI」或「本公司」）深知客戶將其最關鍵的技術與運營需求委託給我們。為維護此信任並提供無可妥協的可靠性，本資訊安全政策體現了我們對維持安全、具韌性且持續可用的服務的承諾。

我們承諾:

- 通過企業級安全控制措施保護客戶數據，防止未經授權的訪問、篡改或中斷。
- 通過積極的風險管理和業務連續性措施確保服務的連續性。
- 遵守全球標準（如 ISO 27001、TISAX），以達到並超越客戶和法規的期望。
- 通過定期審查和增強我們的安全狀態來提高透明度。

通過實施本政策，USI 重申其對卓越運營的承諾，使客戶能夠放心地依賴我們的服務。

二、要求與承諾

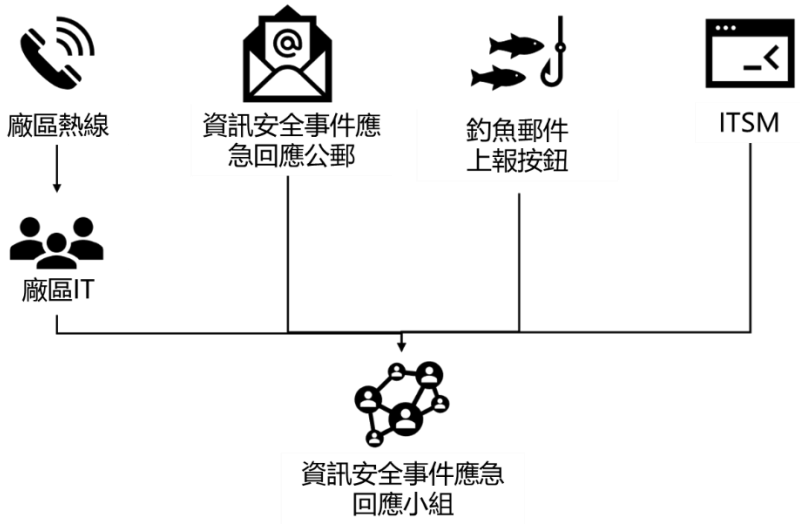
A. 網路安全治理

1. 治理架構
    - 由高級管理層領導的**資訊安全指導委員會**，負責監督 USI 及其子公司的網路安全戰略和合規情況。
    - 定期的內部審計和第三方評估（如 ISO 27001、NIST）驗證對政策的遵守情況，並推動我們的資訊安全管理體系（ISMS）和資訊系統的持

續改進。

2. 員工意識與培訓
    - 所有員工共同承擔資訊安全保護的責任，包括事件報告和遵守安全協議。
    - 所有職能部門（如 IT、人力資源、法律、供應鏈管理、行政、品質保證、研發、工程、專案管理辦公室）在日常運營中承擔與其相關的特定資訊安全保護責任。
    - 為資訊安全部門提供特定角色的培訓（如治理 / 風險 / 合規、安全運營中心運營、安全架構）。
    - 為所有員工提供有關釣魚攻擊、數據處理和事件回應的強制性培訓。
3. 數據保護
    - 對從創建到處置的數據實施全面的技術和運營控制。
    - 強制性數據分類：所有文件 / 資料庫均需標記（如「機密」、「公開」），以實施分層保護。
    - 數據丟失防護（DLP）：實時監控，阻止敏感數據（如個人身份信息、知識產權）的未經授權傳輸。
    - 基於角色的訪問控制（RBAC）：根據角色職責，對所有系統執行最小權限訪問原則。
4. 風險監控與回應

- 事件報告：為 USI 員工提供多種渠道，以便及時報告事件。



- 異常檢測：用戶與實體行為分析工具可對可疑活動（如批量下載、異常訪問模式）發出警報。
- 24/7 安全運營中心監控：安全信息和事件管理工具以及威脅情報可實現威脅檢測自動化。
- 事件回應：制定及時報告的協議和多種場景的行動手冊。
- 漏洞管理：定期掃描和滲透測試，以降低風險。
- 違規通知：根據監管要求（如 GDPR、當地法律）或客戶要求，向利益相關者發送包含事件摘要（如已採取的行動、針對未來風險的長期補救措施）的通知。

B. 第三方要求

- 第三方（如供應商）在獲得訪問或處理 USI 系統或數據的授權之前，必須遵守 USI 的安全標準，並簽署**保密協議**和**隱私保護與資訊安全協議**。

- **資訊安全通知**向供應商傳達 USI 的要求，涵蓋從資訊安全治理到物理安全的各個方面。
- 審計權：合同中包含合規驗證條款。

C. 管理層承諾

- 通過積極的威脅管理，每年實現**零重大漏洞**。
- **持續改進**與業務目標相一致的安全控制措施。