环旭电子信息安全政策

一、目的

环旭电子股份有限公司及其子公司（简称 “环旭电子” 或 “公司”）深知客户将其最关键的技术和运营需求托付给我们。为坚守这份信任并提供始终如一的可靠性，本信息安全政策旨在表明我们对维持安全、有韧性且持续可用的服务的承诺。

我们承诺：

- 通过企业级安全控制措施保护客户数据，防止未授权访问、篡改或破坏。
- 通过主动风险管理和业务连续性措施确保服务连续性。
- 遵守全球标准（如 ISO 27001、TISAX），以达到并超越客户和监管机构的期望。
- 通过定期审查和加强我们的安全态势，提高透明度。

通过实施本政策，环旭电子重申其对卓越运营的执着追求，让客户能够放心地依赖我们的服务。

二、要求与承诺

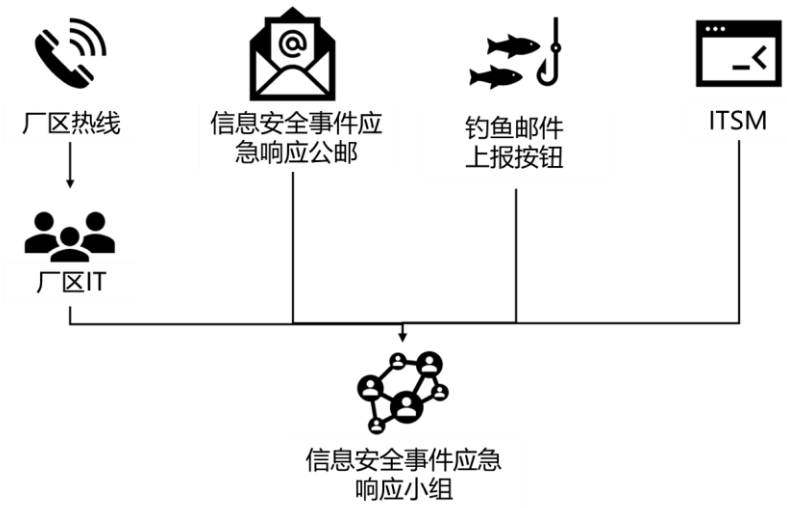
A. 网络安全治理

1. 治理结构
    - 由高级管理层领导的**信息安全指导委员会**，负责监督环旭电子及其子公司的网络安全战略和合规情况。
    - 定期进行**内部审计**和**第三方评估**（如 ISO 27001、NIST），以验证对政

策的遵守情况，并推动我们的信息安全管理体系（ISMS）和信息系统的持续改进。

2. 员工意识与培训
    - 所有员工都对信息安全保护负有责任，包括事件报告和遵守安全协议。
    - 所有职能部门（如 IT、人力资源、法务、供应链管理、行政、质量保证、研发、工程、项目管理办公室）在日常运营中承担与其相关的特定信息安全保护责任。
    - 为信息安全部门提供特定角色的培训（如治理 / 风险 / 合规、安全运营中心运营、安全架构）。
    - 为所有员工提供关于钓鱼攻击、数据处理和事件响应的强制性培训。
3. 数据保护
    - 对数据从创建到处置实施全面的技术和运营控制。
    - 强制性数据分类：所有文件 / 数据库均需标记（如 “机密” “公开”），以实施分层保护。
    - 数据丢失防护（DLP）：实时监控，阻止敏感数据（如个人身份信息、知识产权）的未授权传输。
    - 基于角色的访问控制（RBAC）：根据角色职责，对所有系统执行最小权限访问原则。
4. 风险监控与响应

- 事件报告：为环旭电子员工提供多种渠道，以便及时报告事件。



- 异常检测：用户与实体行为分析工具可对可疑活动（如批量下载、异常访问模式）发出警报。
- 24/7 安全运营中心监控：安全信息和事件管理工具以及威胁情报可实现威胁检测自动化。
- 事件响应：制定及时报告的协议和多种场景的行动手册。
- 漏洞管理：定期扫描和渗透测试，以降低风险。
- breach 通知：根据监管要求（如 GDPR、当地法律）或客户要求，向利益相关者发送包含事件摘要（如已采取的行动、针对未来风险的长期补救措施）的通知。

B. 第三方管理要求

- 第三方（如供应商）在获得访问或处理环旭电子系统或数据的授权之前，必须遵守环旭电子的安全标准，并签署**保密协议**和**隐私保护与信息安全协议**。

- 向供应商传达环旭电子的要求，涵盖从信息安全治理到物理安全的各个方面的**信息安全通知。**
- 审计权：合同中包含合规验证条款。

C. 管理层承诺

- 通过主动的威胁管理，每年实现**零重大漏洞。**
- **持续改进**与业务目标相一致的安全控制措施。