USI Information Security Policy

I. Purpose

Universal Scientific Industrial Co., Ltd., and its subsidiaries (USI or the Company) acknowledge that our clients entrust us with their most critical technological and operational needs. To uphold this trust and deliver **uncompromising reliability**, this Information Security Policy establishes our commitment to maintaining **secure, resilient, and continuously available services**.

We commit to:

- **Protecting client data** through enterprise-grade security controls to prevent unauthorized access, tampering, or disruption.
- **Ensuring service continuity** via proactive risk management and business continuity measures.
- **Complying with global standards** (e.g., ISO 27001, TISAX) to meet and exceed client and regulatory expectations.
- **Promoting transparency** through regular reviews and enhancements to our security posture.

By implementing this policy, USI reaffirms its dedication to **operational excellence**, enabling clients to rely on our services with confidence.

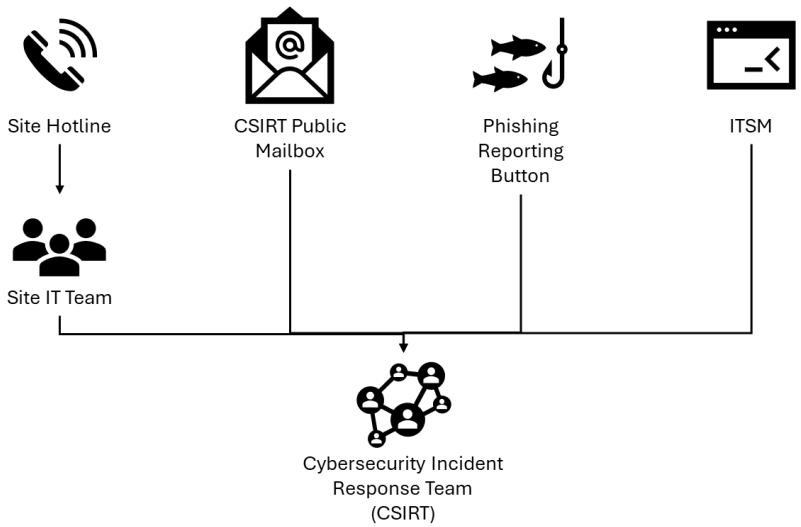
II. Requirements and Commitments

A. Cybersecurity Governance

1. **Governance Structure**
    - The **Information Security Steering Committee**, led by senior leadership, oversees cybersecurity strategy and compliance across USI and subsidiaries.
    - **Regular internal audits** and **third-party assessments** (e.g., ISO 27001, NIST) validate adherence to policies and drive continuous improvement of our Information Security Management System (ISMS) and information system.
2. **Employee Awareness & Training**
    - **All employees** share responsibility for information security protection, including incident reporting and adherence to security protocols.

- **All functions** (e.g., IT, HR, Legal, SCM, GA, QA, RD, Engineering, PMO) take their specific information security protection responsibilities related to their daily operation.
- **Role-specific training** for the Information Security Division (e.g., Governance/Risk/Compliance, SOC operations, Security Architecture).
- **Mandatory training** covering phishing, data handling, and incident response for all staff.

3. **Data Protection**
   - **Comprehensive technical and operational controls** for data from creation to disposal.
   - **Mandatory Data Classification**: All files/databases labeled (e.g., Confidential, Public) to enforce tiered protections.
   - **Data Loss Prevention (DLP)**: Real-time monitoring to block unauthorized transfers of sensitive data (e.g., PII, IP).
   - **Role-Based Access Control (RBAC)**: Least-privilege access principles enforced for all systems based on role responsibility.
4. **Risk Monitoring & Response**
   - **Incident Reporting:** USI employees are provided with multiple channels to report incidents promptly.



   - **Anomaly Detection**: UEBA tools alert suspicious activities (e.g., bulk downloads, unusual access patterns).
   - **24/7 SOC Monitoring**: SIEM tools and threat intelligence automate threat

detection.

- **Incident Response**: Defined protocols for timely reporting and playbooks for multiple scenarios.
- **Vulnerability Management**: Regular scans and penetration tests to mitigate risks.
- **Breach Notification**: Stakeholders are notified with incident summary (such as action taken, long-term remediation for future risk) according to regulatory requirements (e.g., GDPR, local laws) or client requirements.

B. Third Party Requirements

- Third parties (e.g., suppliers) must comply with USI security standards and sign **NDAs** and **Privacy Protection and Information Security Agreement**, before accessing or processing USI system or data is authorized.
- **Information Security Notice** communicates USI requirements, from information security governance to physical security, to suppliers.
- **Right-to-Audit**: Contracts include clauses for compliance verification.

C. Management Commitment

Objectives:

- **Zero major breaches** annually through proactive threat management.
- **Continuous improvement** of security controls aligned with business goals.