KWANTEX®
KWANTEX RESEARCH INC.
No. 7, Lane 376, Zong-Zeng Rd., Kwanmiao Dist., Tainan City 718012, Taiwan
Tel: 886-6-595 6111 Fax: 886-6-595 5661
E-mail: kwantex@ms18.hinet.net
www.kwantex.com.tw

Information/Cyber Security and Risk Management Policy of Kwantex Research Inc.

Kwantex Research Inc. is committed to establishing a robust information/cyber security and risk management mechanism to protect operational data, client information and business confidentiality. Our goal is to mitigate the impact of security incidents on business continuity, financial loss and reputation, while enhancing our capability to identify and respond to internal and external risks, thereby supporting the long-term stable development of the company.

The implementation guidelines for Kwantex's Information/Cyber Security and Risk Management Policy are as follows:

I. Information/Cyber Security and Risk Management Policy

1. **Confidentiality:** Ensuring that information is accessible only to authorized personnel.
2. **Integrity:** Ensuring that information is accurate and complete, any change is not allowed without permission.
3. **Availability:** Ensuring that authorized personnel have normal access to information and systems when needed.

II. Foundation, Responsibility and Physical Security

1. **Purpose and Scope**
   - 1.1 **Purpose:** To establish a secure and reliable information/cyber environment and prevent data leakage, damage or loss.
   - 1.2 **Scope:** Covers all employees, contractors, external consultants and all hardware, software, network and data assets.
2. **Roles and Responsibilities**
   - 2.1 **CISO (Decision-making):** Responsible for decision-making, resource allocation and policy review.
   - 2.2 **IT Department (Maintenance):** Responsible for technical implementation, system maintenance and daily monitoring.
   - 2.3 **All Employees (Obligation):** Obligated to follow security guidelines, participate in security training and protect company data.
3. **Asset Management**
   - 3.1 Maintain an inventory of assets: Hardware, software and data.
   - 3.2 Data Classification: Manage data based on their importance (e.g., Confidential, Restricted, Public).
4. **Physical and Environmental Security**
   - 4.1 Server Room Access Control: Restrict access permissions to the server room.
   - 4.2 Critical equipment must be equipped with lightning protection, fire protection and Uninterruptible Power Supply (UPS).
   - 4.3 Clean Computer Desktop Policy: Computers must be locked when leaving the workstation, and no confidential documents should be left on the desktop.

III. Technology, Process and Compliance

1. **Access Control Management**
   - 1.1 **Principle of Least License:** Employees shall only have the minimum access rights necessary to perform their duties.
   - 1.2 **Account Management:** Regularly deactivate accounts of resigned or transferred personnel.
   - 1.3 **Password Standard:** Keep personal passwords confidential to prevent leakage.
2. **Network Security Management**
   - 2.1 Firewalls and Intrusion Detection: Deploy firewalls and anti-virus software.
   - 2.2 VPN Encryption: Remote connections must be through encrypted channels (e.g., VPN).
   - 2.3 Unauthorized software or connecting personal devices to the internal network is prohibited.
3. **Backup and Disaster Recovery**
   - 3.1 Regular Data Backup: Perform daily/weekly backups and ensure backup data are isolated from the daily storage space.
   - 3.2 Recovery drills: Conduct disaster recovery drills at least once a year to ensure the availability of backup data.
4. **Incident Response**
   - 4.1 Reporting Process: Report anomalies (e.g., malware, data leakage) immediately upon discovery.
   - 4.2 Corrective and Preventive Actions: Investigate incidents and take corrective measures to prevent recurrence.

President: 

Date: Feb. 3, 2026