Techpoint Inc.

Information Security Policy

Our company is committed to maintaining the information security of its operational environment and serving our customers with integrity. Beyond implementing fundamental and necessary information security control measures, we place emphasis on ensuring that all data and processing activities are securely protected. Our company will strengthen information security management and continuously enhance the **confidentiality**, **integrity**, and **availability** of critical personal and transactional data, effectively implementing information security management practices to improve our service quality.

Our Information Security Statement is as follows:

1. An appropriate organizational structure will be established to execute information security management operations, ensuring compliance with relevant laws and regulations and maintaining the normal operation of the information security management system (ISMS).

2. Job assignments will consider functional segregation, with clear delineation of job responsibilities to prevent unauthorized modification or misuse of information or services.

3. All personnel who use company information for providing information services or executing project work are responsible and obligated to protect the company's information assets they obtain or use, preventing unauthorized access, alteration, destruction, or improper disclosure.

4. All personnel are obligated to protect customer data, including transactional and basic information. Accessing, using, disclosing, or informing unrelated colleagues, vendors, or other customers of such information without authorization is strictly prohibited.

5. The physical security of the computer information environment should be strengthened, including access control for server rooms, air conditioning, uninterruptible power supplies, etc., to prevent unauthorized access, damage, or accidental disasters that may impact normal business operations.

6. All personnel must not privately connect external networks with the company's internal network. Necessary security measures should be implemented to protect both internal and external networks.

7. Security controls should be considered at the initial stages of system development. For outsourced development, control and contractual information security requirements must be strengthened. System development, modification, and implementation must comply with information security management standards.

8. All personnel should remain vigilant and report any occurrence or suspicion of security incidents, vulnerabilities, or non-compliance with the ISMS implementation standards and management procedures, following the established reporting procedures.

9. Business continuity plans should be developed according to business needs and tested regularly to ensure their applicability.

10. The information security organization shall establish information security

objectives based on the information security policy and organizational responsibilities, with review and approval by the Information Security Committee before implementation.

11. The information security objectives should address **confidentiality**, **integrity**, and **availability**, reflecting the requirements derived from the information security policy.

12. This policy shall be reviewed at least once a year by the highest authority of the company's information security organization to ensure alignment with the latest developments in relevant laws, technology, and business operations, thereby ensuring the effectiveness of information security practices.

13. Any matters not covered by this policy shall be handled in accordance with relevant laws and company regulations.

14. This policy shall be implemented upon the approval of the group’s Information Security Manager; any amendments shall follow the same process.