CyberSecThreat Corporation Limited.

Information Security Policy Statement

To ensure the effective implementation, operation, supervision, and continuous management of our ISMS (Information Security Management System), and to maintain the confidentiality, integrity, and availability of our company's critical information systems, we have issued this information security management policy.

This policy aims to provide clear guidelines for employees in their daily work. All employees are obligated to actively participate in promoting the information security management policy to ensure the safe operation of our company's personnel, data, information systems, equipment, and network. We expect all employees to understand, implement, and maintain this policy to achieve the goal of continuous information operation.

"Implement information security, enhance service quality";

"Strengthen security training, ensure continuous operation";

"Prepare for emergencies, quickly recover from disasters";

"Reasonably use personal data, prevent data leakage."

- Implement information security, enhance service quality

  All employees must implement ISMS and ensure the confidentiality, integrity, and availability of business data. Appropriate protective measures should be selected to reduce risks to an acceptable level, continuously monitor, review, and audit the information security management system to enhance service quality and improve service standards.

- Strengthening security training, ensuring continuous operation

  Supervise all employees to implement information security management work, conduct appropriate information security education and training annually, establish the concept of "information security, everyone's responsibility," and promote the importance of information security. This will improve information security intelligence and emergency response capabilities, reduce information security risks, and achieve the goal of continuous operation.

- Prepare for emergencies, quickly recover from disasters

  Develop emergency response plans and disaster recovery plans for critical information assets and key business operations and regularly conduct drills to

ensure rapid recovery in case of system failure or major disaster events. This ensures the continuous operation of key business operations and minimizes losses.

- Reasonably use personal data, prevent data leakage

  Classify and evaluate personal data to ensure legal requirements and protective measures are in place. Establish access control mechanisms, use encryption and security measures during data transmission and disclosure, regularly evaluate the compliance of entrusted parties, and sign contracts and agreements with them to ensure data security. Strengthen employee education and training to enhance data protection awareness. Establish monitoring and review mechanisms to continuously monitor the use, access, and transmission of personal data, and promptly detect and respond to abnormal activities or security incidents. Ensure that personal data can be safely and permanently deleted when no longer needed.