Information Security Management Key Points

At Bairong Inc., we are fully committed to comply with laws and regulations such as the "Cybersecurity Law of the People's Republic of China," the "Data Security Law of the People's Republic of China," and the "Personal Information Protection Law of the People's Republic of China," and prioritize safeguarding customer data and company information. Below are the key measures we have undertaken to ensure information protection and security:

I. Data Security Policy

1. Data Access Control

We have implemented strict data access approval and authorization mechanisms to ensure the principle of least privilege and ensure data access is granted only when necessary.

2. Data Encryption Transmission

We use secure links and encryption protocols such as dedicated lines, VPNs, and HTTPS to safeguard data during transmission.

3. Data Storage

We use secure encryption technologies like AES256 and SHA256 for the storage of important data. Store data in domains and levels according to its security classifications, ensuring physical or logical isolation between different storage domains. We establish reliable data backup and recovery mechanisms and regularly test backup data to ensure its availability and integrity when needed.

4. Data Deletion

We have a well-established process and handling mechanism for data deletion and destruction. Disks containing classified information ("corporate secrets") must be demagnetized before disposal. Disks storing classified or internal-use information must be securely overwritten multiple times before reuse to ensure data cannot be recovered. All operations must be conducted under dual supervision and maintain detailed records of the destruction process for verification and compliance.

II. Data Compliance Management

1. Compliance with Laws and Regulations

We actively cooperate with external regulatory bodies for security supervision.

We identify and document applicable laws, regulations and standards related to information security compliance and maintain a compliance list.

We register critical systems for level protection according to the requirements of the "Cybersecurity Law" ensuring they are created and maintained according to the assessment requirements for level protection.

2. We have built our information security management system with reference to international advanced standards and obtained the ISO27001 Information Security Management System Certification in 2016. In September 2020, Bairong was the first to pass the audit of the domestic authoritative certification body, China Quality Certification, and obtained the ISO27701 Privacy Information Management System Certification.

III. Security Awareness Training

1. Regular Training

We conduct regular training sessions focused on security awareness and data security, covering policy, law, regulation, standard, and other security knowledge protection training. We also conduct specialized data security training for employees in critical or sensitive roles and regularly review and update training materials.

2. Monthly Journal

At the end of each month, we distribute an information security journal to all employees highlighting the latest development and trends in information security current. We use real-world case studies to emphasize the key concerns and best practice in information security, continuously improving employees' information security awareness.

IV. Information Security Emergency Response

1. Emergency Response Mechanism

We have developed a comprehensive information security emergency response framework including detailed emergency plans to ensure rapid response and handling in the event of an information security incident. We conduct regular emergency drills to test and enhance emergency response capabilities, ensuring the effectiveness and operability of emergency plans.

2. Event Reporting and Handling

We have established clear channels for reporting information security incidents to ensure employees can report security incidents promptly. We ensure timely handling of all information security incidents and maintain detailed records of the incidents.

3. Continuous Improvement

We summarize and analyze information security incidents to identify the root causes and implement improvement measures to prevent similar incidents from recurring. And we regularly evaluate and update emergency plans to ensure they are up-to-date with the latest security threats, industry standards and regulatory requirements.

These initiatives highlight Bairong Inc.’s unwavering commitment to information security management, ensuring the security and compliance of both customer data and company information.