Yihai Kerry Arawana Holdings Co., Ltd.

Information Security Policy

Yihai Kerry Arawana Holdings Co., Ltd. (hereinafter referred to as "the Company") is committed to advancing a leading digital strategy within the food industry and enhancing the digitalization level of the entire industry chain in an all-round manner. This policy aims to provide unified guidance and basis for establishing, implementing, operating, and continuously improving the Company's information security management system. It defines the overall direction, implementation methods, and control requirements for information security management, ensuring compliance, confidentiality, integrity, and availability of information and data usage, thereby safeguarding the Company's stable and sustainable operations under stringent information security and data security controls.

1. Scope of application

This policy is a public statement and applies to the entire workforce, including the Company and its subsidiaries, as well as to all individuals who use, own, operate and manage the Company's information technology, including suppliers, contractors, other stakeholders and third-party organizations that provide information processing services to the Company.

2. Key principles

2.1. Strengthen Data Protection

According to the requirements of the Information Security Management System, the Company implements technical, managerial, and procedural measures across various dimensions including human resources, suppliers, assets, networks, applications, and personal information privacy compliance. The Company is committed to adopting advanced technical means to strengthen the security protection capabilities of its network and information systems. This ensures the compliance, accuracy, confidentiality, consistency and integrity of the Company's information and data used in all business activities, while preventing unauthorized access, tampering or destruction.

2.2. Unified Resource and Permission Management

Enable centralized management of public and private cloud computing resources, clarify the scope of permissions for business and operational personnel, promote precision in account and permission management, and avoid resource abuse.

2.3. Safety Risk Monitoring

Establish a company-wide cybersecurity monitoring mechanism for external networks to identify potential external threats and internal anomalies in real time, and set up a rapid response mechanism and incident handling procedures. The Company is committed to promptly notifying affected stakeholders and publicly disclosing response plans in the event of data breaches or other major threats, taking remedial measures in a timely manner, and enhancing overall information security transparency.

2.4. Supplier and Third-Party Information Security Management

The company has established a framework for systematic assessment of supplier information security to conduct regular information security assessments and reviews of suppliers to ensure compliance with supplier information security management and reduce the security risk of information in cooperation with suppliers.

2.5. Business Continuity Management

Conduct tests of information security emergency response mechanisms and incident response procedures at least once a year to ensure their executability and effectiveness.

2.6. Internal Audit and External Review

The Company regularly conducts internal audits of the Information Security Management System and engages external third-party professional agencies annually for assessments to verify the effectiveness of current control measures and compliance in management and operational activities. This aims to identify potential risks, provide relevant alerts, and prevent information security incidents.

2.7. Privacy Protection Management Requirements

For businesses involving the collection of customers' personal data, the Company clearly informs customers of the purpose, usage, retention period, protection measures, and methods for withdrawal of their data, therefore safeguarding customers' right to know and control their personal

data. In collaborations with third parties, the Company adheres to the "Minimum Necessary" principle, ensuring secure and prudent use and processing of third-party data under strict limitations. When government or regulators request data disclosure, the Company must ensure that its responses comply with laws and regulations and the requirements of the jurisdiction involved.

2.8. Information Security Training and Assessment

The Company provides irregular information security and privacy protection training and awareness activities for all employees annually, conducting at least one phishing drill to comprehensively strengthen employees' awareness and capabilities in information and data security protection.

2.9. Establish Reporting Mechanisms

Users of technical resources and information assets who detect suspicious behaviors or potential risks may report them promptly in accordance with Company policies or procedures.

3. Periodic Revision

The Company continuously identifies internal and external environmental factors and, based on the dynamic evolution of information security risks, continuously improves the information security systems in response to market regulatory changes, business development, and technological advancements.

Yihai Kerry Arawana Holdings Co., Ltd.

September 2025