Zhejiang Dingli Machinery Co., Ltd.

Cybersecurity Management Policy

1. General Provisions

To establish and improve the cybersecurity management policy of Zhejiang Dingli Machinery Co., Ltd. (hereinafter referred to as the 'Company'), this policy is formulated in accordance with relevant national standards. It aims to define cybersecurity objectives, effectively manage cybersecurity risks, ensure all employees understand and comply with the relevant provisions of the policy, and enhance the effectiveness of cybersecurity management. This policy applies to all cybersecurity management activities within the Company.

2. Overall Objectives

Through the establishment and improvement of the Company's cybersecurity management policies, enhanced employee cybersecurity training and education, and implementation of appropriate risk control measures, the Company seeks to effectively manage security risks faced by information systems and ensure their stable and normal operation.

3. Cybersecurity Responsibilities

(1) Board of Directors

The Chairman of the Board is responsible for approving the cybersecurity management policy and ensuring its implementation across departments. The Chairman also provides strategic guidance on the cybersecurity of the Company's information systems, makes decisions on major security-related issues, coordinates interdepartmental collaboration on security matters, and supports and promotes the implementation of cybersecurity initiatives throughout the Company.

(2) Cybersecurity Leadership Team

To clarify the organizational structure, roles, and responsibilities for cybersecurity management and promote the organizational development of information system security management, the Company has established a Cybersecurity Leadership Team responsible for cybersecurity efforts. The Corporate Communications Department is designated to implement cybersecurity tasks.

4. Cybersecurity Management

(1) Employee Awareness and Code of Conduct

a.All employees must receive information security training. Each employee must participate in at least one cybersecurity awareness training session per year to ensure an understanding of the importance of cybersecurity and awareness of potential threats.

b.Employees must comply with the Company's information system usage policies. Unauthorized software installation and external device connections are prohibited. Account credentials must be properly managed to prevent disclosure or sharing. Important information and data must be protected from unauthorized access or dissemination.

c.A security incident reporting and response mechanism shall be established, including categorization of incidents and a clear process for reporting suspicious or actual cybersecurity incidents. All employees and stakeholders must understand and follow the incident response procedures.

(2) Technical Safeguards and System Security

a.The Company will centrally deploy network boundary firewalls and intrusion detection systems, harden servers, terminals, and databases, and implement vulnerability repair mechanisms. Access control and encryption will be applied to protect critical data.

b.Regular security audits and configuration inspections will be conducted. All information systems must be regularly updated with patches. Security assessments and controls must be in place for third-party system integration.

(3) Anti-Virus Management

The Company centrally deploys antivirus software. The Corporate Communications Department is responsible for developing protection strategies, while system administrators handle installation, operation, and updates. Unauthorized installation or removal of antivirus software is prohibited. External media or downloaded files must be scanned for viruses. All new devices and those returning from business trips must pass virus checks before connecting to the network. Regular network-wide virus scans will be conducted. Detected virus incidents must be isolated, addressed, and reported immediately.

(4) Violation Handling

Employees who violate this policy will be subject to disciplinary measures ranging from public criticism and job reassignment to disciplinary action, depending on the severity of the violation.

5. Cybersecurity Emergency Response Plan

In the event of major information system incidents, force majeure, or other special circumstances requiring emergency decisions, the Company will initiate its emergency response mechanism.

(1) Emergency Handling

The Company has established a Cybersecurity Emergency Response Team to handle cybersecurity incidents. After an incident occurs, the team will assess the situation, classify the incident (general, major, serious, extremely serious), and initiate the emergency decision-making process. The originating department reports the incident, the Corporate Communications Department convenes the task force meeting, business departments provide updates and assess damage, and the emergency team collectively formulates a

response plan to be executed by the business department. The Corporate Communications Department oversees implementation and prepares documentation. If the incident must be reported to regulatory authorities, the Corporate Communications Department will decide the reporting matters, with the business department preparing materials and other departments cooperating. Final review will be conducted by the Chairman.

(2) Conclusion of Emergency Response

After the emergency is handled, the Company will conduct a thorough investigation, identify weaknesses, propose corrective measures, and determine responsibilities. If third-party responsibilities are involved, experts may be consulted. If the issue is not solely attributable to third parties and the business department fails to remedy it effectively, it may provide explanations and evidence. If the assessment is valid, responsible individuals will be held accountable. If the incident involves terrorism or intentional disruption, and relevant departments fulfilled their reporting and evacuation duties, no further accountability will be pursued, though cooperation with internal investigations is required. Internal participants or accomplices will be handled in accordance with the law and reported to judicial authorities.

(3) Emergency Support

a. Material and Technical Support

The Company will allocate dedicated funds for preventing or responding to cybersecurity emergencies, provide necessary transportation support, and enhance material preparedness for emergency handling. A technical platform for early warning and emergency response will be established to improve incident detection and analysis capabilities. This will gradually enable technical coordination across different networks, systems, and departments in areas such as detection, alerting, response, and reporting.

b. Emergency Drills and Personnel Training

The Company will regularly organize drills to enhance cybersecurity emergency response capabilities. Personnel involved in emergency handling must undergo relevant training to ensure familiarity with working principles, procedures, and necessary skills.

6. Supplementary Provisions

This document is formulated, interpreted, and revised by the Cybersecurity Leadership Team and the Corporate Communications Department.