Zhejiang Dingli Machinery Co., Ltd.

Information System Data Security Management Regulations

1. Purpose

To ensure the secure and stable operation of Zhejiang Dingli Machinery Co., Ltd.'s (hereinafter referred to as 'the Company') information systems, protect data security and integrity, and prevent risks such as information leakage, tampering, and loss, these regulations are hereby formulated.

2. Scope

Applicable to all internal information systems of the Company (including ERP, MES, CRM, and other software systems) and all employees and third-party partners.

3. Responsibilities

(1)The Network Information Department is responsible for data security settings of the Company's information systems, including account activation, deactivation, permission settings, and related management and maintenance based on authorization.

(2)The Corporate Communications Department is responsible for the security management and maintenance of company servers, networks, computers, and data backups.

(3)Employees in business departments are responsible for compliant operation of systems within their respective business scopes and must prevent information leakage.

4. Basic Principles

(1)Principle of Least Privilege: Users shall only be granted the minimum permissions necessary to perform their job duties.

(2)Confidentiality: Prevent unauthorized access to and leakage of data.

(3)Integrity: Ensure data accuracy and prevent illegal tampering.

(4)Availability: Ensure timely access to data when legally required.

5. Data Security Management

(1)Data Classification

Differentiate between confidential data (such as customer, supplier, pricing, financial data) and routine business data (such as product material information, production order information).

(2)Data Access and Control

Set permission matrices: important data access is granted only to specific personnel; routine business data access is assigned according to job responsibilities.
Unauthorized data export, copying, or sharing is prohibited. Access to confidential data requires approval by company leadership. Before handling, sharing, or retaining confidential data, specific personnel must obtain consent from relevant stakeholders through signed authorization.

6. Account and Permission Management

(1)Account Creation and Approval

a.New employees must submit a 'System Account Activation Application Form' and obtain department supervisor approval before account activation.

b.Access to confidential data permissions requires approval from the Chairman.

c.Upon employee resignation, the department must promptly notify the Network Information Department, which will immediately deactivate the account, revoke permissions, and keep records.

(2)Permission Allocation Management

a.The Network Information Department assigns permissions based on approved access rights in the application forms.

b.System user accounts and permissions are reviewed and cleaned of redundant accounts every three months.

(3)Password Security Specifications

Password complexity requirements include uppercase and lowercase letters and numbers, with a minimum length of 6 characters. Mandatory periodic password changes are enforced. Simple passwords (such as birthdays or phone numbers) are prohibited.

(4)Audit and Supervision

a.Quarterly inspection of system operation logs to detect abnormal activities.

b.Quarterly information system security vulnerability assessments will be conducted. Identified vulnerabilities will trigger immediate remediation processes.

7. Employee Responsibilities and Violation Handling

(1)Employee Responsibilities

a.New employees must undergo system operation and security training upon onboarding.

b.New employees must sign a 'Confidentiality Agreement,' clarifying confidentiality obligations and consequences of violations. Employees must immediately report security vulnerabilities or anomalies and are prohibited from concealing or handling issues independently.

(2)Violation Handling

a.Minor violations (e.g., password sharing) will result in warnings or fines.

b.Serious violations (e.g., data leakage) may result in suspension or dismissal and legal liability. Third-party cooperation violations will lead to contract termination and legal liability.

c.Illegal actions (such as leaking or selling data) will be handed over to judicial authorities.

8. Supplementary Provisions

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