JL MAG RARE-EARTH CO., LTD.

Information Security and Privacy Protection Policy

Introduction

JL MAG strictly complies with all laws and regulations concerning information security and privacy protection in the jurisdictions where it operates. This policy statement aims to clarify the Company's responsibilities and obligations in information security and privacy protection, ensuring that while pursuing business development, the Company continuously improves its information security management system, safeguards the confidentiality, integrity, and availability of corporate information assets, and supports business continuity and compliant operations.

This policy applies to all employees of the Company, including full-time, part-time, and outsourced employees. The Company encourages suppliers to jointly adhere to the requirements set forth in this policy.

Part 1: Information Security and Privacy Protection Management Requirements

1. Ensuring Integrity and Protection of Data: All data collection, storage, processing, and transmission must comply with laws, regulations, and internal company standards. Comprehensive data classification and grading management shall be implemented, alongside complex password policies and the addition of a two-factor authentication mechanism to prevent data leakage, tampering, or destruction.

2. Continuously Improve the Information Security System: Continuously invest in the latest information security technologies, equipment, and solutions, such as firewalls, intrusion detection systems, data encryption technologies, and security audit systems. Regularly and automatically initiate inspection processes to conduct in-depth analysis of permission configurations and log records for network security equipment, server rooms, and information systems; upgrade protective measures to guard against security risks such as hacker attacks and virus intrusions. Regularly engage third parties to conduct external audits of the information security management system to ensure its effectiveness.

3. Implement Information Security Responsibilities: The Company has established a Leadership Group for Intellectual Property and Trade Secrets, headed by the CEO. Under the leadership of this group, a three-tier information security management structure (decision-making layer, supervision & implementation layer, execution layer) has been established to build a comprehensive and systematic information control system. Clearly define the permissions of IT operation and maintenance

personnel, and promptly revoke relevant permissions upon completion of operation and maintenance tasks. Define the responsibilities of each employee, such as complying with information security operating procedures and consciously protecting company data and customer information.

4. Monitor and Respond to Information Security Threats: Continuously monitor the Company's information and network security status, regularly scan for vulnerabilities, and take measures to promptly repair and remediate any identified information security vulnerabilities and risks. Develop information security contingency plans and regularly test information security emergency mechanisms and incident response procedures.

5. Supplier Information Security Management Requirements: The Company thoroughly reviews the security of suppliers' information and network systems to ensure the integrity and confidentiality of company information is not compromised due to supplier-related reasons.

6. Customer Privacy Management: Implement systematic and process-oriented management of information systems, establish access permissions for customer information, and strictly adhere to the principle of customer information confidentiality. Restrict internal personnel's access scenarios and usage conditions for customer information to maximize the protection of customer information security.

Part 2: Employee Participation

1. Information Security and Privacy Protection Training: Continuously promote information security and privacy protection-related training and awareness activities to enhance employees' awareness of information security.

2. Emergency Response: When potential information security or privacy leakage threats are discovered, they should be reported in accordance with the security risk reporting procedures.

Part 3: Disciplinary Actions

The Company implements a zero-tolerance policy towards any leakage of critical data and user privacy information and will take disciplinary measures against violations of this policy, including but not limited to warning, fine, and termination.