MINISO Group Holding Limited

Information Security and Privacy Policy

I. Overview

MINISO Group Holding Limited (hereinafter referred to as "MINISO" or "we") attaches great importance to the confidentiality and security of personal information, and has formulated an information security and privacy protection policy (hereinafter referred to as "the Policy"), which aims to clarify the Company's management requirements and code of conduct in information security and privacy protection.

II. Scope of Application

The Policy applies to all operations of MINISO and its subsidiaries and all personal information processing activities involved, including the personal information processing of consumers, employees, suppliers, etc. We are committed to protecting the privacy of personal data and require franchisees, distributors, service providers and other partners who represent MINISO or participate in activities related to MINISO's business to comply with the Policy.

III. Responsibilities and Obligations for Information Security and Privacy Protection

1. All employees:

- Comply with information security policies and relevant laws and regulations to protect the security of the Company's information assets.
- No unauthorized access, use, disclosure or destruction of the Company's information assets.
- When information security vulnerabilities or abnormalities are discovered, employees may report via email or directly to the relevant person in charge of the IT department, and shall report to the information security management department in time.
- Actively participate in information security training to improve their information security awareness and skill level.

2. Digital Technology Center:

- Digital Technology Center and Legal Department are designated to be responsible for information security and privacy issues, monitor and respond to information security threats, conduct information security vulnerability analysis regularly or when necessary to identify potential security risks in systems, networks, applications or data processing processes, including analysis, verification, documentation, remediation, and final verification of the remediation results.
- At the same time, MINISO imposes information security requirements on third parties with which it cooperates (including suppliers), and all third parties with which it

cooperates are required to comply with relevant regulations on information security management.

IV. Information Security Protection

In order to ensure business continuity related to information security, we apply cutting-edge information security technologies, and carry out situational awareness monitoring, vulnerability scanning and penetration testing on newly launched and operational systems every year, promote information security vulnerability analysis, and build a defense-in-depth information security system. At the same time, we formulate a comprehensive information security emergency plan, clearly define the management bodies, regulations, and emergency response procedures for business continuity, and organize emergency drills regularly to improve our security defense and emergency response capabilities.

V. Personal Information Protection

We have designated the Group Legal Department and the Information Security Team of the Digital Technology Center to jointly oversee privacy compliance. We have established a control mechanism covering the whole life cycle of personal information collection, use, storage and destruction. In accordance with the Personal Information Protection Law, we clearly inform our customers of the reasons for collecting personal information, as well as the purpose, scope, and methods of processing, ensuring that we obtain full and explicit consent and authorization during the collection process. We strictly follow the "data minimization" principle of information collection and implement encryption control over customer information. Users can manage their own personal information, including accessing, reviewing, correcting/supplementing, deleting, and transferring personal information. We also provide channels to exercise personal information rights such as account cancellation, obtaining copies of personal information and requesting explanations of personal information processing rules. MINISO pledges that our personal information processing activities will strictly comply with relevant laws, regulations, and national standards. We undertake not to rent or sell any personal information. Without the explicit consent of our customers, we will not provide or share their personal information with any third parties. For cases where external processing or third-party sharing is necessary to provide specific customer service functions, MINISO has fully informed customers and obtained their explicit consent. Furthermore, MINISO has signed data processing agreements with the respective third parties in accordance with legal requirements to ensure that customer information is handled and protected at the appropriate level. We also ensure the timely deletion of data once the shortest necessary retention period for processing is met. Additionally, we have established robust data backup and disaster recovery mechanisms, as well as information security emergency response plans, to guarantee data availability and

security.

VI. Information Security and Privacy Training

We have established a routine information security training and assessment mechanism, organize dedicated information security training and assessment for all employees every year, targeting key groups such as new employees and customer service teams, and additionally conduct thematic training sessions to comprehensively enhance the awareness of information security and privacy protection of all employees.

VII. Periodic Audit

We embed the information security and privacy protection policy into MINISO's compliance management system, conduct internal audits on the Policy and information management system every year, and invite external independent institutions to audit this policy and information system every year to identify deficiencies and formulate specific improvement plans and measures, and continuously improve the information security system to ensure data integrity and security.

VIII. Supervision and Reporting of Violations

The Digital Technology Center conducts unscheduled supervision and assessment of information security and privacy protection. For issues identified during reviews, it regularly tracks improvement results until rectification is completed, and continuously refines relevant systems and strengthens awareness and education.

We have zero tolerance for violations of this policy, and any violation will be subject to disciplinary action.

We have established a whistleblower protection system and welcome employees and third parties to report any matters that violate laws and regulations, industry standards, or company policies concerning information security and privacy protection. Employees and third parties may choose their own reporting channels. MINISO strictly maintains the confidentiality of the whistleblower's personal information and all materials provided. The specific reporting channels are as follows:

- Official Compliance Hotline: 020-32306713
- Violation Reporting Email: jubao@miniso.com、privacy@miniso.com