Mengniu Information Security Policy

Mengniu prioritizes information security management, establishing and implementing high-standard principles centered on the core objective of "Enabling Safer Data Utilization." Mengniu continuously enhances systematic information protection and data security frameworks, improves response capabilities to security threats, and rigorously executes security safeguards.

References

This Policy is formulated in strict compliance with the *Cybersecurity Law of the People's Republic of China*, *Data Security Law of the People's Republic of China*, *Personal Information Protection Law of the People's Republic of China*, *GB/T 22239-2019 : Information Security Technology — Baseline for Classified Protection of Cybersecurity*, *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems Requirements*, and ISO/IEC 27002:2022 *Information Security, Cybersecurity and Privacy Protection — Information Security Controls*. In the event of any conflict between this Policy and applicable laws and regulations, the applicable laws and regulations shall take precedence.

Scope

This Policy applies to all departments and employees within Mengniu Group and its subsidiaries.

Contents

1. Information Security Governance

Mengniu has established a four-tiered information security management

organizational structure comprising "Decision-Making Level - Management Level - Execution Level - Support Level." The Decision-Making Level is the Group Information Security Leadership Committee, chaired by the Group President with the Chief Digital Intelligence Officer as Deputy Chair, leading the Group's overarching information security initiatives. The Information Security Team and Data Security Team are responsible for planning and constructing the information and data security governance framework. Security teams of business units, functional departments and subsidiaries, along with all employees, are responsible for implementing specific security measures and cooperating with external experts, risk auditors, and regulatory authorities for supervision and inspection.

2. Information Security Management

Mengniu requires the Group and its subsidiaries to carry out information security management in the following areas:

- Adopt advanced information security technologies, adhere to the principle of continuous improvement, and timely review, modify, and adjust existing security strategies and protective measures to enhance the security management level and maintain the effectiveness of the Information Security Management System.
- Conduct regular internal and external information security audits, actively pursue authoritative information security certifications, and ensure that Mengniu's information security system is subject to supervision.
- Implement full data lifecycle security controls, establish mechanisms to prevent data leakage, ensure that data remains accurate and consistent, and prevent unauthorized access, alteration, or destruction.
- Proactively monitor cyber risks, respond promptly to security incidents, and implement mitigation strategies. In case of data breaches or security threats, maintain transparency with affected parties, take corrective actions, and develop strategies for future risk prevention..
- Following the principle of involving all employees, Conduct comprehensive

information security trainings to raise awareness, and Clarify information security responsibilities and incident reporting procedures. Employees must immediately report any suspected information security issues to the information security department.

- Third-party partners must comply with the privacy and data protection requirements set forth in Mengniu's *Business Partner Compliance Code of Conduct.*

Stakeholder Communication

Mengniu continuously enhances the transparency of its information security efforts and regularly discloses progress updates.

Mengniu actively engages with external stakeholders, ensuring that its information security practices remain at the forefront of the industry, and promptly reviews and updates this Policy as needed.

Policy Supervision and Reporting

The Sustainability Committee oversees the implementation of this Policy. Key initiatives and progress toward targets are reported to the Committee.