Seres Group Information Security Policy

Seres Group Co., Ltd. and its subsidiaries (hereinafter referred to as "Seres" or "the Company") have formulated the *Seres Group Information Security Policy* (hereinafter referred to as "this Policy") to implement laws and regulations such as the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, and the *Personal Information Protection Law of the People's Republic of China*, as well as international standards such as ISO 27001 and ISO 27701.

1. Scope of Application

This Policy has been approved by the Board of Directors, and applies to Seres Group Co., Ltd. and all its subsidiaries, covering Seres's own operations, suppliers, and partners. As the highest supervisory body for matters related to information security and privacy protection, the Board of Directors is responsible for overseeing and regularly reviewing the implementation of this Policy.

2. Principles

The Company strictly adheres to the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, and other relevant laws and regulations, as well as international standards such as ISO 27001 and ISO 27701, establishing comprehensive information security and privacy protection systems.

3. Information Security Management Measures

3.1 Continuous Improvement of the Information Security System

- The Company continuously tracks the latest requirements of laws and regulations and system standards such as ISO 27001:2022, and comprehensively reviews the published information security-related systems in conjunction with changes in business operations. The Company utilizes the PDCA improvement mechanism to continuously strengthen information security management and address security vulnerabilities.

3.2 Data Compliance and Protection

- The Company strictly adheres to the principles of segregation of duties and least privilege, ensuring that only authorized employees have access to critical and sensitive data. This approach aims to mitigate data leakage risks at the source and safeguard data integrity. By signing the *Confidentiality Agreement* and the *Network and Data Security Commitment Letters*, the legal responsibilities and obligations of employees regarding data confidentiality, compliant use, and security precautions are clearly defined.
- The Company clarifies the security requirements throughout the data lifecycle and monitors the implementation of data protection measures through a data monitoring system to promptly identify security issues and respond to potential security threats, continuously enhancing the level of data compliance protection.

3.3 Individual Responsibilities of Employees for Information Security

- The Company clarifies the individual responsibilities of all employees for information security, incorporates information security guidelines into the employee training system, and conducts a series of activities such as cybersecurity and data protection awareness campaigns and interactive quizzes for all employees.
- Relying on the internal office platform, the Company regularly disseminates safety tips and security insights, and provides resources related to data security knowledge, skills training, privacy protection, and other relevant topics through online learning platforms.

3.4 Third-Party Information Security Requirements

- The Company clarifies the security responsibility boundaries and control requirements for third-party partners such as suppliers from the perspectives of cybersecurity, data security, privacy protection, and other security aspects.
- In the cooperation access phase, the Company requires the third-party company seeking cooperation to sign agreements on cybersecurity and data security requirements.
- During the cooperation period, the Company defines the security requirements and standards for products and services provided by suppliers and ensures that suppliers fulfill their cybersecurity and data security responsibilities and obligations
- In the project acceptance and evaluation phase, the Company incorporates cybersecurity and data security evaluation items and regularly conducts information security evaluations to continuously strengthen information security and data protection efforts.

3.5 Information Security Risk Monitoring and Emergency Response

- The Company conducts information security audits through system reviews, special audits, routine inspections, and other methods. For various issues identified during the audit process, the Company clarifies rectification requirements, timelines, and responsible parties, and promotes the rapid implementation of rectifications.
- The Company establishes vulnerability scanning and penetration testing mechanisms to promptly identify and remediate security vulnerabilities, and establishes the Seres Cybersecurity Emergency Response Center (SERES SRC).
- The Company establishes information security emergency response systems, clarifies the classification and grading standards for network security incidents, defines the response and handling procedures for security emergency incidents, and further enhances the efficiency of risk response.
- The Company incorporates information security-related business continuity plans into the overall business continuity management and crisis management framework of the Company, regularly conducts information security emergency response and data backup recovery drills, tests the effectiveness of contingency plans and proficiency of personnel, and forms a closed loop for rectification and updating.

4. Privacy Protection Management Measures

4.1 Incorporating Privacy Protection into the Company's Risk and Compliance Management System

- The Company integrates privacy protection into the group's overall risk control and compliance management system, incorporating it into business process design, system

construction, risk investigation, and other aspects, promptly identifying and rectifying privacy protection compliance risks, and ensuring systematic and comprehensive operation.

4.2 Protection of User Rights and Interests

- The Company collects user personal information based on the principles of lawfulness, fairness, and minimum necessity, and only within the scope necessary for providing products or services.
- Before collecting personal information from users, the Company clearly informs the data subject of the purpose, method, and scope of collection, as well as the channels for inquiring about, correcting, and deleting personal information, and the methods for canceling an account and withdrawing consent. Additionally, the Company ensures that users legally enjoy their legitimate rights and interests, such as accessing, correcting, deleting personal information, and adjusting the scope of authorization. The Company collects and uses personal information only with user consent.
- The Company retains users' personal information within the timeframe stipulated by law and the period necessary to achieve the intended purpose. After exceeding the timeframe, either delete the users' personal information or anonymize it.

4.3 User Information Protection Mechanism

- The Company continuously promotes the Secure Software Development Lifecycle (SDLC) mechanism and the concept of Privacy by Design, integrating user privacy protection into business and products.
- The Company strictly adheres to the principles of segregation of duties and least privilege, ensuring that only authorized employees can access important and sensitive data, thereby reducing the risk of data leakage from the source.
- By signing the *Confidentiality Agreement* and the *Network and Data Security Commitment Letters*, the Company clearly defines the legal responsibilities and obligations of employees regarding data confidentiality, compliant use, and security precautions. Additionally, the Company implements desensitization and encryption processing for critical and sensitive data to ensure the security of data during transmission, storage, and use.
- The Company establishes a security reward and punishment mechanism, imposes penalties for security violations in accordance with regulations, and strengthens employees' awareness of safety compliance.
- The Company develops and drills emergency response plans for network and data security incidents, ensuring a swift and orderly response in the event of potential or actual data breaches, and minimizing the impact to the greatest extent possible.

4.4 Zero Tolerance for Violations and Disciplinary Actions

- The Company implements a zero-tolerance mechanism for user privacy violations, clarifies the definition standards for violations, and formulates severe disciplinary measures. For employee violations of user privacy, the Company imposes sanctions such as notice of criticism, performance deductions, demotion, and termination of labor

contracts according to the severity of the situation. If illegal activities are suspected, cases are referred to the judicial authorities. For third-party violations of user privacy, the Company pursues liability for breach of contract according to the cooperation agreement. If the situation is serious, the Company terminates cooperation and pursues relevant legal responsibilities.

4.5 Implementation Supervision and Continuous Improvement

- The Company regularly conducts internal reviews of policy compliance, continuously improves privacy protection compliance management, and ensures the applicability and effectiveness of policies.
- The Company regularly conducts personal information protection inspections and special audits to promptly identify potential security risks and irregular operations. In accordance with national regulatory requirements, the Company regularly organizes special audits on personal information protection compliance to assess the compliance of internal personal data processing activities and continuously optimize the compliance management system.