# Longshine Technology Group Co., Ltd.

# Network Information Security and Privacy Protection Policy

Longshine Technology Group Co., Ltd. (hereinafter referred to as “the Company” or “Longshine Group”) has formulated the Longshine Group Network Information Security and Privacy Protection Policy (hereinafter referred to as “this Policy”) to safeguard network information security and protect user privacy rights, regulate personal information processing activities, and implement the Personal Information Protection Law, Data Security Law, Cyber Security Law, and relevant national security standards.

## Scope of Application

This Policy applies to all Longshine Group businesses, products, services, and third-party partners such as suppliers. All employees of the Company, including but not limited to full-time employees, interns, outsourced staff, part-time personnel, and other types of personnel, shall be aware of and understand the Company’s management requirements for network information security and privacy protection. Furthermore, the Company requires its partners and suppliers to comply with this Policy and encourages them to establish similar policies.

## Main Content

This Policy is established for all employees and relevant personnel, covering management structure and responsibilities, security management system regulations, full data lifecycle management, security technologies and control measures, employee management and training, third-party and supply chain management, protection of personal information subject rights, security compliance supervision, and self-inspections. It specifies that violations of this Policy will result in corresponding penalties. This Policy is not only the “bottom line” for corporate compliance but also a core strategy for building data trust, preventing risks, and enhancing

competitiveness. Through a systematic management framework, full participation, and continuous improvement, the Company effectively balances data utilization and security protection, promotes coordinated development between the enterprise and society, and ensures stable operation and sustainable development.

## I. Management Structure and Responsibilities

Network and Information Security and Privacy Protection Management Committee

Longshine’s Board of Directors is overall responsible for the Company’s network security management.

**Chair:** Held by the CEO of Longshine Group, responsible for overseeing network security and privacy protection strategies.

**Members:** Board members, senior management, heads of the Security and Quality Management Department, Human Resources Department, Process and System Department, and business departments.

**Responsibilities:** As the highest leadership, coordination, and decision-making body for network and information security, it is responsible for planning and deploying the Company’s security strategies and making decisions and providing guidance on major security incidents.

### a. Security and Privacy Joint Task Force

Responsible for overall control of the Company’s network and information security governance; formulating network and information security policies; and coordinating and dispatching network and information security tasks to ensure the effective implementation of the security system.

### b. Dedicated Departments

Security and Quality Management Department: Responsible for building the security compliance system, formulating and supervising the implementation of data security and

personal information protection management systems, conducting risk assessments, vulnerability management, emergency response planning, and ensuring product and service security.

**Human Resources Department:** Develops management processes for employee personal information security to protect employee privacy.

**Process and System Department:** Implements technical protection measures to ensure network infrastructure security.

**Administration Department:** Responsible for office campus security and related software and hardware facilities.

**Legal Department:** Handles legal compliance reviews, user rights requests, and regulatory communication.

**Accounting and Internal Control Department:** Responsible for personal information protection compliance audits.

## II. Security Management System Regulations

Longshine Group establishes and improves the Company's network and information security, data security, and personal information protection management systems and related operational procedures in accordance with national and regional laws, regulations, security standards, and technological developments. The Company integrates data security and privacy protection into its overall risk management system and incorporates them into risk assessment processes and compliance audits. It regularly conducts personal information protection impact assessments and compliance audits to ensure the Company's personal information governance framework and privacy policies align with domestic and international regulations.

## III. Full Data Lifecycle Management

a. **Data Classification and Grading:** Establish a comprehensive data asset inventory, classify data into four levels based on sensitivity, formulate processing rules for important data and sensitive personal information, and implement full-process classified and graded management and protection.

b. **Data Collection:** Standardize data collection requirements to ensure accuracy, completeness, and legality of collected personal information. Collection follows the principle of minimum necessity and obtains explicit user consent.

c. **Data Transmission:** Adopt appropriate security technical measures (including encryption, access control, integrity verification, etc.) based on data sensitivity to ensure confidentiality, integrity, reliability, and availability of network transmission services meet corresponding protection-level requirements. For cross-border businesses, conduct internal data security self-assessments. If conditions for reporting outbound transfers of important data and personal information are triggered, report to the national cyberspace administration for data export security assessment.

d. **Data Storage:** Core-level data is stored encrypted, important-level data is stored desensitized, and storage duration does not exceed business necessity. Implement data backup and recovery management, regularly back up data, and verify backup integrity and availability.

e. **Data Use:** Clarify purpose limitations for data use; only authorized personnel are allowed to use data in limited scenarios. prohibit processing beyond scope. Standardize requirements for processing, entrusted processing, sharing, transfer, and disclosure of personal information.

f. **Data Deletion:** Use physical or logical erasure techniques to ensure data irrecoverability. Implement data destruction/disposal agreements and supervision mechanisms for third-party-related data.

## IV. Security Technologies and Control Measures

a. Threat Monitoring, Deploy technical measures such as firewalls, intrusion detection systems (IDS), zero-trust architecture, and transparent encryption terminals to control data flow in and out of the network, prevent unauthorized access and data leaks. Introduce new technologies (e.g., AI-driven security tools, automated alert systems) to optimize protection measures, monitor abnormal behaviors (e.g., network attacks, unauthorized access, signs of data leaks) in real-time, and ensure alignment with the latest security threats and compliance requirements.

b. Regularly conduct penetration tests and vulnerability scans to ensure system security. Establish an internal security assessment mechanism to analyze system security vulnerabilities and defects, develop improvement plans, and continuously enhance the information security system.

c. Throughout the data processing lifecycle, use data encryption technologies to protect data storage and transmission, and embed integrity verification mechanisms using technologies such as hash checks and digital signatures to ensure data integrity and protection.

d. Implement role-based access control (RBAC) to ensure only authorized personnel can access important and sensitive data. Log operations on important and sensitive data, set up approval processes for data operations, and ensure all operations are properly authorized.

e. Regularly conduct security drills and reviews, simulate security incidents, analyze causes periodically, and optimize technical measures and control processes.

## V. Employee Management and Training

a. To ensure all employees understand information security management responsibilities and confidentiality obligations, all employees must sign security confidentiality agreements and network information security commitment letters upon joining. Key positions must sign data

security responsibility statements clarifying data security responsibilities associated with their roles. Additionally, employees must complete data handovers and revoke relevant permissions upon resignation or transfer.

b. Formulate and publish a series of regulations including the Network and Information Security Management Measures, Data Security Management Measures, Personal Information Protection Management Measures, Employee Security Behavior Guidelines, and Fifteen Prohibitions on Network and Information Security to standardize daily employee behavior, implement internal supervision, and accountability mechanisms.

c. The Company regularly organizes annual security awareness training and assessments for employees. Security training is a mandatory course for new employees, requiring full marks in security exams. Specific arrangements include: at least 2 annual company-wide security awareness training sessions and 1 company-wide data security and personal information protection thematic training. Meanwhile, the Company establishes an assessment mechanism incorporating information security into departmental and employee performance evaluation indicators.

## VI. Third-Party and Supply Chain Management

a. Third-party suppliers and partners must hold security certifications such as ISO 27001 or equivalent, with the certification scope covering the corresponding service content, ensuring their security capabilities match business requirements.

b. Sign project contracts and data security protection agreements to clarify the data protection obligations of third-party suppliers and partners, including requirements for information security, data protection, and compliance, ensuring alignment with the Company’s security policies and standards. Partners bear joint liability for compensation if security incidents or data leaks occur due to their violation of agreements.

c. Strictly implement the Company's Third-Party Supplier Security Management Specifications, clarify management principles for network and data security behavior of third-party personnel, and strengthen security risk control and operations. Investigate and handle security incidents and violations during third-party technical services to ensure timely correction and improvement.

d. Annually review the network security and data security capabilities of third-party suppliers; perform core item spot checks on key suppliers periodically. Assess and review the activities of third-party suppliers and their staff to evaluate compliance with contracted security requirements and standards; terminate cooperation with non-compliant parties.

## VII. Protection of Personal Information Subject Rights

a. Collect personal information of employees and customers following the principles of legality, legitimacy, and necessity. Only collect information related to business purposes, clearly inform the purpose and use of collection, and obtain explicit user consent. Without consent from the personal information subject, it shall not be used for other purposes or disclosed to third parties.

b. Collected user personal information is only used for the Company's normal business operations. Monitoring user data for secondary or unrelated purposes is prohibited. Cease collection and delete personal information after business operations stop, ensuring minimization of personal information storage time.

c. Store collected personal information after de-identification and necessary security measures. Formulate personal information classification and grading standards, and adopt appropriate technical measures and control processes based on different levels and categories of personal information. Internal employees require approval to access others' information, granted only for work necessities.

d. Conduct internal security checks on privacy policies for online channels such as apps or mini-programs developed or operated by the Company. Introduce third-party compliance audits for important system platforms to ensure lawful and compliant personal information processing.

e. The Company formulates and publishes internal regulations and operational procedures such as the Personal Information Protection Impact Assessment System and Personal Information Subject Rights Response Mechanism, establishes complete processes for responding to personal information subject rights, clarifies division of responsibilities at each stage, and sets up application acceptance and handling mechanisms for rights exercise, as well as complaint management mechanisms.

f. The Company's privacy policy ensures individuals are provided with methods and channels to exercise their rights, clarifies the content of personal information subject rights (including withdrawal of consent, access, copy, portability, correction, supplementation, deletion, and restriction of automated decision-making), and stipulates applicable scenarios and exceptions for each right.

## VIII. Security Compliance Supervision and Self-Inspection

a. Regularly conduct security compliance self-inspections. Perform compliance self-checks and key issue rectification based on the Company's business models and related product forms. Inspect and monitor the network environment, information systems, employee operations, data information, and third-party supply chain for potential security risks, continuously strengthening the Company's network security assurance system and capabilities.

b. According to laws, regulations, and standards, regularly conduct personal information protection impact assessments, analyze potential impacts on personal rights throughout the

personal information processing lifecycle, and adopt appropriate personal information security control measures accordingly to effectively enhance the protection of personal information subject rights.

c. Integrate the privacy policy with the Company’s overall risk management system, develop overall audit plans, and regularly check the consistency of the privacy policy with domestic and international regulations (e.g., PIPL, GDPR). Establish an independent internal audit team to conduct personal information protection compliance audits, using methods such as personnel interviews, review of management systems, policies, mechanisms, and technical verification to supervise and inspect whether various business sectors pose risks to personal information subject rights.

d. For business sectors providing important internet platform services, having a huge user base, or involving complex business types, conduct external audits or commission external third parties for compliance audits.

## IX. Violation Handling (Zero-Tolerance Policy)

a. The Company establishes security incident response procedures and violation handling processes. Any data breach or violation must be reported within 24 hours, and actions taken based on severity include:

b. Employee violations: Penalties such as warning, fine, demotion, or termination of labor contract depending on the severity.

c. Management negligence: Hold directly responsible persons and supervising leaders accountable.

d. Third parties: Warning, accountability for compensation, termination of cooperation.

e. Legal accountability: Cases constituting crimes will be transferred to judicial authorities.

## X. Supplementary Provisions

a. The Security Management Office is responsible for drafting this Policy, which takes effect after approval by the Longshine Group Network and Information Security and Privacy Protection Management Committee. Any previously implemented policies inconsistent with this Policy shall be superseded by this Policy.

b. The Security Management Office is responsible for supervising the implementation of this Policy and holds the final right of interpretation.