LongShine Technology Group Co., Ltd.

Network and Information Security and Privacy Protection Policy

To safeguard network and information security and users' privacy rights, regulate personal information processing activities, and implement the requirements of the Personal Information Protection Law, the Data Security Law, the Cybersecurity Law and relevant national security standards, Longshine Technology Group Co., Ltd. (hereinafter referred to as the "Company" or "Longshine Technology") has formulated this Network and Information Security and Privacy Protection Policy (hereinafter referred to as this "Policy").

1. Scope of Application

This Policy covers all businesses, products and services of Longshine Technology and third parties such as suppliers and business partners. All Company employees, including, but not limited to, regular employees, interns, outsourced personnel, part-time employees and any other categories of personnel, shall be aware of and understand the Company's network and information security and privacy protection requirements. The Company also requires its business partners and suppliers to comply with this Policy and encourages them to establish similar policies.

2. Key Provisions

This Policy applies to all employees and relevant personnel and establishes requirements for the governance structure and responsibilities, information security management systems and procedures, data lifecycle management, security technology and controls, employee management and training, third-party and supply chain management, protection of personal information subject rights, and security compliance oversight and self-inspection. It also specifies the consequences of violations. This Policy is not only the baseline for corporate compliance, but also a core strategy for building data trust, preventing risks and enhancing competitiveness. Through a systematic management framework, workforce-wide participation and continuous improvement, the Company effectively balances data use and security protection, advances the coordinated development of the Company and society, and supports stable operations and sustainable development.

3. Governance Structure and Responsibilities

1. Network and Information Security and Privacy Protection Management Committee

Members of the Longshine Technology Board of Directors have overall responsibility for the Company's cybersecurity management.

Chair: The Chief Executive Officer of Longshine Technology serves as Chair and coordinates the cybersecurity and privacy protection strategy.

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

Responsibilities: As the highest leadership, coordination and decision-making body for network and information security, the Committee plans and deploys the Company's security strategy and makes and guides decisions relating to major security incidents.

2. Joint Security and Privacy Working Group

The Working Group exercises overall control over the Company's network and information security governance, formulates network and information security principles and policies, and coordinates the Company's network and information security work to ensure effective implementation of the security framework.

3. Dedicated Functions

Security and Quality Management Department: Establishes the security compliance framework; formulates and oversees implementation of data security and personal information protection rules; conducts risk assessments and vulnerability management; manages emergency plans; and safeguards product and service security.

Human Resources Management Department: Develops management rules and procedures for employee personal information security and protects employee privacy.

Process and Systems Department: Implements technical safeguards and protects network infrastructure security.

Administration Department: Manages physical security at office campuses and the security of related software, hardware and facilities.

Legal Department: Conducts legal compliance reviews, handles data subject rights requests and communicates with regulators.

Accounting and Internal Control Department: Conducts personal information protection compliance audits.

4. Information Security Management Systems and Procedures

In accordance with national and local laws and regulations, security standards and technological developments, Longshine Technology establishes and improves management systems and operating

procedures for network and information security, data security and personal information protection. The Company integrates data security and privacy protection into its overall risk management system, risk assessment process and compliance audits; regularly conducts personal information protection impact assessments and personal information protection compliance audits; and ensures that its personal information governance framework and privacy policies are aligned with domestic and international regulations.

5. Data Lifecycle Management

1. Data classification: Maintain a comprehensive data asset inventory, classify data into four levels according to sensitivity, establish processing rules for important data and sensitive personal information, and apply classification-based management and protection throughout the lifecycle.
2. Data collection: Standardize data collection requirements; ensure the accuracy, completeness and lawfulness of personal information collected; collect only the minimum personal information necessary; and obtain the individual's explicit consent.
3. Data transmission: Apply appropriate security measures according to data sensitivity, including encryption, access control and integrity checks, to ensure that the confidentiality, integrity and reliability of data transmission and the availability of network transmission services meet the applicable protection requirements. Conduct internal data security self-assessments for cross-border business. Where the conditions requiring a security assessment for the cross-border transfer of important data or personal information are met, submit the cross-border data security assessment to the national cyberspace authority.
4. Data storage: Encrypt core-level data, store important-level data in a de-identified form, and retain data no longer than necessary for the business purpose. Maintain data backup and recovery management, regularly back up data, and verify the integrity and availability of backups.
5. Data use: Clearly limit the purpose of data use; permit only authorized personnel to use data in approved scenarios; and prohibit processing beyond the authorized scope. Standardize the processing and use of personal information, including entrusted processing, sharing, transfer and disclosure.
6. Data deletion: Use physical or logical erasure technologies to ensure that data cannot be recovered. Apply agreed destruction and disposal requirements to data involving third parties and maintain deletion oversight mechanisms.

6. Security Technology and Controls

1. For threat monitoring, deploy firewalls, intrusion detection systems (IDS), zero trust architecture, transparent endpoint encryption and other technologies to control inbound and outbound network traffic and prevent unauthorized access and data leakage. Introduce new technologies, such as AI-driven security tools and automated alerting systems, to optimize safeguards; monitor anomalous behavior in real time, including cyberattacks, unauthorized access and indicators of data leakage; and keep controls aligned with evolving security threats and compliance requirements.
2. Conduct regular penetration testing and vulnerability scanning to ensure system security. Maintain an internal security assessment mechanism to analyze system vulnerabilities and deficiencies, develop improvement plans and continuously improve information security systems.
3. Throughout the data processing lifecycle, use data encryption to protect data at rest and in transit and embed integrity verification mechanisms using hash validation, digital signatures and other technologies to ensure data integrity and protection.
4. Implement role-based access control (RBAC) to ensure that only authorized personnel can access important or sensitive data. Record operation logs for important and sensitive data and establish approval processes for data operations so that every operation is appropriately authorized.
5. Conduct regular security drills and post-drill reviews, simulate security incidents, periodically analyze incident causes, and optimize technical measures and control procedures.

7. Employee Management and Training

1. To ensure that all employees understand their information security and confidentiality responsibilities, every employee shall sign a security and confidentiality agreement and a network and information security commitment upon joining the Company, and personnel in key positions shall sign a data security responsibility statement specifying their role-related data security responsibilities. Employees leaving the Company or transferring to another position shall complete the required data handover and have the relevant access rights revoked.
2. Formulate and issue internal rules including the Network and Information Security Management Measures, Data Security Management Measures, Personal Information Protection Management Measures, Employee Security Conduct Guidelines and Fifteen Prohibitions on Network and Information Security to regulate employees' day-to-day conduct and implement internal oversight and accountability mechanisms.
3. The Company regularly provides annual security awareness training and assessments to employees and makes security training a mandatory onboarding course for new employees,

requiring a full passing score on the security examination. Specific arrangements include at least two workforce-wide security awareness training sessions and one workforce-wide session on data security and personal information protection each year. The Company also maintains an assessment mechanism and incorporates information security into departmental and employee performance evaluations.

8. Third-Party and Supply Chain Management

1. Third-party suppliers and other business partners shall hold ISO 27001 certification or equivalent security qualifications, with the certification scope covering the relevant services, to ensure that their security capabilities are appropriate for business needs.
2. Execute project contracts and data security protection agreements that specify the data protection obligations of third-party suppliers and other business partners, including information security, data protection and compliance requirements, and ensure alignment with the Company's security policies and standards. A business partner whose breach of the agreement causes a security incident or data leakage shall bear joint liability for compensation.
3. Strictly implement the Company's Third-Party Supplier Security Management Standards, define the principles governing network and data security conduct by third-party personnel, and strengthen security risk controls and operations. Investigate and address security incidents and violations arising during third-party technical services and ensure timely correction and improvement.
4. Review the cybersecurity and data security capabilities of third-party suppliers annually and regularly conduct spot checks of core controls for key suppliers. Assess and review the activities of third-party suppliers and their personnel to determine whether they meet the security requirements and standards specified in the contract, and terminate the business relationship where requirements are not met.

9. Protection of Personal Information Subject Rights

1. Collect employee and customer personal information in accordance with the principles of lawfulness, legitimacy and necessity; collect only information relevant to the business; clearly communicate the purpose and intended use; and obtain the individual's explicit consent. Personal information shall not be used for another purpose or disclosed to a third party without the personal information subject's consent.
2. Use collected customer personal information only for the Company's normal business operations. Using customer data without authorization for secondary or unrelated purposes is

prohibited. When a business ceases operations, stop collecting and delete personal information to minimize the retention period.

3. De-identify collected personal information and apply necessary security measures before storage. Establish personal information classification standards and apply appropriate technical measures and controls according to the level and category of personal information. Employees shall obtain approval before being granted access to another person's information, and such access shall be limited to what is necessary for their work.
4. Conduct internal security inspections of privacy policies for online channels developed, built or operated by the Company, including applications and mini programs, and introduce third-party compliance audits for important systems and platforms to ensure lawful and compliant personal information processing.
5. Formulate and issue internal rules and procedures, including the Personal Information Protection Impact Assessment Policy and Personal Information Subject Rights Response Mechanism; establish complete processes for responding to personal information subject rights requests; define responsibilities at each stage; and maintain request intake, handling and complaint management mechanisms for the exercise of personal information subject rights.
6. The Company's privacy policies provide individuals with methods and channels for exercising their rights and clearly describe personal information subject rights, including withdrawal of consent; access, copying and transfer; correction and supplementation; deletion; and restrictions on automated decision-making. They also specify the circumstances in which each right applies and any applicable exceptions.

10. Security Compliance Oversight and Self-Inspection

1. Regularly conduct security compliance self-inspections and, taking into account the Company's business models and product forms, carry out compliance reviews and remediate key issues. Inspect and monitor the network environment, information systems, employee operations, data and information, and third-party supply chains for security risks and hazards, and continuously strengthen the Company's cybersecurity assurance framework and capabilities.
2. Regularly conduct personal information protection impact assessments in accordance with applicable laws, regulations and standards, analyze the potential effects of personal information processing activities throughout the lifecycle on individuals' rights and interests, and apply appropriate personal information security controls to strengthen protection of personal information subjects.

3. Integrate privacy policies into the Company's overall risk management system, develop an overall audit plan, and regularly review the alignment of privacy policies with domestic and international regulations, including the Personal Information Protection Law and the General Data Protection Regulation (GDPR). Establish an independent internal audit team to conduct personal information protection compliance audits through personnel interviews, reviews of management rules, policies, mechanisms and other documentation, and technical inspections, and assess whether any business segment presents a risk of infringing personal information subject rights.
4. For business segments that provide important online platform services, have a very large number of users or involve complex types of business, conduct an external audit or engage an independent third party to perform a compliance audit.

11. Handling of Violations (Zero Tolerance Policy)

1. The Company applies zero tolerance to data leakage; unlawful or non-compliant processing of personal information; infringement of privacy or personal information rights; unauthorized access; use beyond the authorized scope; unauthorized sharing or disclosure; circumvention of audit controls; and failure to report security incidents as required.
2. The Company maintains security incident response and misconduct handling processes. Any data leakage, privacy infringement, non-compliant personal information processing or suspected security incident shall be reported through the Company's process within 24 hours of discovery, and the responsible functions shall assess, contain, investigate, correct and review the incident. The Company also maintains transparency with stakeholders affected by security incidents and proactively informs them of progress in the incident investigation.
3. Employee violations: Where an employee is confirmed to have violated this Policy, applicable laws or regulations, or the Company's information security and personal information protection rules, the Company will impose disciplinary action according to the severity of the violation, including a warning, formal criticism, performance-related deduction, reassignment, demotion or termination of employment. Where the violation causes loss, the Company reserves the right to seek recovery.
4. Management failure: Directly responsible persons and supervising managers who fail to perform oversight responsibilities, conceal an incident, respond improperly or cause the risk to increase will be held accountable in accordance with laws and Company rules.
5. Third-party violations: Where a supplier, business partner, outsourced worker or other third party breaches its contractual obligations or the Company's privacy protection requirements, the

Company may issue a warning, require remediation within a specified period, suspend the business relationship, seek compensation or terminate the relationship, and will incorporate the matter into the supplier's evaluation.

6. Legal accountability: Where conduct constitutes a legal or criminal violation or requires reporting to a regulator, the Company will respond promptly in accordance with laws and regulations and, where necessary, refer the matter to judicial authorities or cooperate with a regulatory investigation.

12. Supplementary Provisions

The Security Management Office is responsible for preparing this Policy, which shall take effect upon approval by the Longshine Technology Network and Information Security and Privacy Protection Management Committee. Where any previously implemented policy conflicts with this Policy, this Policy shall prevail.

The Security Management Office is responsible for overseeing implementation of this Policy and has final authority for its interpretation.