LongShine Technology Group Co.,Ltd

Responsible Artificial Intelligence (AI) Policy

This Policy is formulated to regulate the development, procurement, deployment and use of Artificial Intelligence (hereinafter referred to as "AI") technologies in the operations, product research and development, customer service, smart energy, digital living and corporate operations of Longshine Technology Group Co., Ltd. (hereinafter referred to as the "Company" or "Longshine Technology") and its subsidiaries; promote the safe, compliant, prudent, transparent and green use of AI; prevent risks relating to data security, cybersecurity, algorithmic bias, intellectual property, trade secrets, ethics, compliance and reputation; and safeguard the lawful rights and interests of employees, customers, users, suppliers, business partners and other stakeholders.

1. Principles

The Company adheres to the principles of legal and regulatory compliance, a human-centered approach, safety and controllability, fairness and impartiality, transparency and trustworthiness, traceable accountability, green and low-carbon development, and continuous improvement. It coordinates AI innovation and application with risk prevention and control and promotes the use of AI to support the Company's high-quality development.

The Company believes that AI should serve human wellbeing, customer value and the sustainable development of society. AI shall not be used to undermine human dignity, rights or independent judgment, and shall not replace final judgments or accountability that laws and regulations require individuals, organizations or governing bodies to exercise.

2. Scope of Application

This Policy applies to Longshine Technology Group, its subsidiaries, branches and other organizations under the Company's effective management, as well as all employees, outsourced personnel, interns and other persons under the Company's management who use, develop, procure, access, deploy or operate AI systems, models, tools, interfaces or related services in Company business scenarios.

For purposes of this Policy, AI includes, but is not limited to, machine learning, deep learning, natural language processing, computer vision, speech recognition, recommendation algorithms,

predictive analytics, intelligent customer service, code generation, content generation, intelligent decision support, process automation and generative AI, together with related systems and services. Suppliers, business partners and other third parties providing AI-related products, services or data processing activities to the Company shall comply with this Policy and other applicable Company requirements.

3. Governance Responsibilities

1. The Company maintains an AI governance and accountability mechanism that clearly defines the responsibilities of business departments, R&D and technology departments, the AI Research Institute, Data Governance, Network and Information Security, Legal and Compliance, Procurement Management, Human Resources and other relevant functions, ensuring that AI applications are subject to approval, recording, traceability, oversight and accountability.
2. The business department using AI is responsible for the necessity and appropriateness of AI in the relevant business scenario, the compliance of input content, the use of outputs and related impacts. R&D and technology departments are responsible for technical controls in the design, testing, release, change and operations and maintenance of AI systems. Network and Information Security, Data Governance, Legal and Compliance and other functions conduct security assessments, data compliance reviews, contract reviews, intellectual property management, supplier management, oversight and inspection, and risk response according to their respective responsibilities.
3. AI applications involving major business decisions, customer or user rights, critical business systems, important data processing, externally published content or other high-risk scenarios shall undergo the necessary assessment, approval and review procedures in accordance with Company rules. The Company continuously improves its AI governance framework and supporting processes in response to regulatory requirements, business changes and technological developments.
4. This Policy shall be reviewed and approved by the Board of Directors or the ESG Sustainability Committee authorized by the Board. The Board or its authorized body has overall responsibility for implementation, oversight, periodic review and material amendments to this Policy. Senior management and relevant functions are responsible, according to their respective duties, for implementation, interpretation, communication and day-to-day management.
5. Material amendments, significant AI risk matters and corporate governance requirements shall be submitted to the Board of Directors or senior management for review in accordance with the Company's governance procedures. The Company shall identify the highest approving body for

this Policy or related commitments in its public disclosures so that stakeholders can verify the approval.

4. Data Privacy and Trade Secret Protection

1. The Company respects and protects personal information, important data, trade secrets, source code, customer information, business information and other data protected by law or contract throughout the AI lifecycle, including development, training, testing, deployment, use and operations. The Company strictly complies with requirements relating to cybersecurity, data security, personal information protection, confidentiality management and applicable regulation. For overseas operations or cross-border scenarios, the Company shall also identify and comply with applicable personal information and privacy protection rules, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).
2. The Company applies data classification, minimum-necessary and data-minimization principles, authorized access, de-identification and anonymization, encrypted storage, audit logging and secure destruction to AI-related data. Where appropriate, the Company encourages the use of privacy-enhancing technologies, including differential privacy, federated learning, secure multiparty computation, data masking and anonymization, to reduce the risk of exposure of personal data during AI training, testing and inference.
3. Without authorization or a compliance assessment, personal information, sensitive personal information, customer data, supplier data, employee data, non-public financial information, business plans, contracts, source code, system credentials, vulnerability information, internal meeting materials and other protected information shall not be entered into external AI tools, third-party models or AI services whose security boundaries cannot be verified.
4. When data are used to train, fine-tune or optimize AI models, the Company shall ensure that the data have a lawful source, clear authorization, a specified processing purpose and a controlled scope of use, and shall retain necessary records in accordance with applicable requirements. Scenarios involving personal information subject rights, cross-border data transfer, entrusted processing by a third party or joint processing shall undergo compliance review in accordance with applicable Company rules.

5. Cybersecurity and Information Security

1. The Company incorporates AI systems, models, plug-ins, interfaces, datasets, prompt templates, automated workflows and related services into its cybersecurity and information security management systems and implements controls including account management, identity

authentication, access control, key protection, encryption in transit and at rest, log retention, security monitoring, vulnerability management, incident response, backup and recovery.

2. The Company monitors security risks associated with AI, including prompt injection, unauthorized invocation, data leakage, model hallucination, malicious code generation, content contamination, model misuse, supply chain attacks and deepfakes. For critical systems, external services and high-impact scenarios, the Company conducts security testing, penetration testing, secure coding reviews, adversarial testing, red-team testing or special assessments as necessary, and takes protective, restrictive, isolation, rollback or suspension measures based on the assessment results.
3. For third-party AI platforms, models, cloud services, data services and development tools that the Company procures or uses with business partners, the Company evaluates security capabilities, data processing rules, service stability, audit logs, model updates, vulnerability response, and data retention and deletion mechanisms, and prevents information security and business continuity risks arising from third-party services.

6. Fairness and Bias Prevention

1. The Company monitors bias, discrimination, misleading outcomes and unfair impacts that may arise from AI data, models, rules, training processes and outputs. AI applications shall not improperly discriminate on the basis of ethnicity, race, sex, age, religion, disability, health status, region, occupational status or any other legally protected characteristic.
2. For AI applications that may affect recruitment, performance appraisal, customer service, user rights, supplier selection, credit or risk judgments, resource allocation or the rights and interests of other stakeholders, the Company conducts appropriate assessments of fairness, accuracy, representativeness and impact. Where necessary, it applies human review, threshold limits, sample correction, explanation of results and other corrective measures to prevent unfair outcomes caused by inappropriate AI outputs.
3. The Company identifies algorithmic bias, mitigates training data bias and conducts fairness audits according to the risk level of the AI application. For deployed AI models that may have a material impact, the Company periodically reviews sample coverage, output disparities, error rates and complaint feedback, and records assessment conclusions, corrective measures and responsible departments.
4. The Company encourages accessibility, inclusion and the differing needs of user groups to be considered in the design of AI products and services, so that AI capabilities serve employees, customers, users and other parties in an equal, convenient and understandable manner.

7. Transparency and Explainability

1. The Company values transparency and explainability in AI applications. For AI systems with which users, customers, employees or other parties may interact directly or by which they may be materially affected, the Company provides appropriate labels, explanations or notices according to the scenario so that relevant parties understand that they are interacting with an AI system or that AI is involved in content, analysis, recommendations or decision support.
2. Within an appropriate scope, the Company explains the principal purpose, capability boundaries, data sources, limitations, potential risks and human review methods of AI systems. Necessary records are retained for important AI models, datasets, assessment processes, release approvals, version changes and key outputs. As conditions mature, the Company may use model cards, data documentation, assessment records, user guidance or other methods to improve explainability and auditability.
3. Where an AI output lacks adequate support, contains logical anomalies, has an unknown source, cannot be reasonably explained or clearly conflicts with professional judgment, the Company shall use it with caution and shall not treat it as the final basis for action. AI-generated content intended for external publication or important business use shall undergo appropriate fact-checking, compliance review and human confirmation.
4. The Company shall clearly label or explain AI-generated text, images, audio, video and code, as well as material decision outcomes produced with AI, according to the applicable scenario, enabling users, customers, employees and other relevant parties to distinguish human-created or human-reviewed content from AI-generated or AI-assisted content.

8. Human Oversight and Human Intervention

1. The Company keeps humans in the loop for critical matters by maintaining necessary human oversight, human judgment and human intervention. AI-generated or recommended outputs are decision-support tools only and do not automatically replace the responsibilities, judgment or final decisions of employees, management, professional institutions or corporate governing bodies.
2. For major business decisions, financial disclosures, legal and regulatory compliance, information security, data compliance, intellectual property, procurement qualification, material customer or user rights, safe energy operations, product quality, work safety, human resources management and other important or sensitive matters, AI output shall not be the sole basis for a final decision and shall be reviewed, verified, corrected or confirmed by personnel with appropriate authority and expertise.

3. At key decision points, the Company shall identify the human supervisor and define approval, intervention, veto and escalation authority. Supervisors shall be able to access necessary AI inputs, outputs, supporting rationale and operating records and shall promptly correct, reject, escalate, suspend or terminate processing when an AI output is inaccurate, unfair, non-compliant or outside the authorized scope.
4. The Company shall establish mechanisms for human intervention, suspension, termination, rollback and remediation according to the scenario. When an AI system produces anomalous outputs, causes a risk event, generates a complaint or dispute, creates a security hazard, or conflicts with laws, regulations, ethical standards or Company rules, the relevant departments shall take timely action.

9. AI Lifecycle Risk Management

1. The Company manages the full AI lifecycle, including requirements definition, solution design, data preparation, model selection, development and testing, procurement and integration, release and deployment, operational monitoring, version changes, and decommissioning. AI scenarios at different risk levels are subject to corresponding assessment, approval, testing, recording and review requirements.
2. Before an AI system is released or materially changed, the Company conducts necessary assessments of compliance, security, accuracy, robustness, fairness, explainability, business continuity and ecological impact. Generative AI, high-impact automation, integration with critical systems and important data processing are subject to enhanced testing, validation and use restrictions and, where necessary, red-team testing, staged release or pilot operation.
3. During operation, relevant departments continuously monitor AI performance, accuracy, stability, output quality, security incidents, user feedback, misuse and abuse, bias risks and changes in external regulation. Where AI model drift or degradation, declining accuracy, deteriorating output quality or changes in the applicable scenario occur, the Company promptly conducts root-cause analysis and takes corrective action, including reassessment, parameter adjustment, data updates, model rollback, functional restrictions, service suspension or decommissioning.
4. The Company maintains periodic compliance audit and operational review mechanisms for important AI systems, covering approval records, access logs, testing records, model changes, risk events, complaint handling and corrective measures. Appropriate operating and risk response records are retained to support oversight, public disclosure and traceable accountability.

10. AI Use Boundaries

1. The Company uses AI reasonably, proportionately and prudently and establishes clear boundaries for what AI can and cannot do. AI may be used to improve work efficiency, support R&D and testing, retrieve knowledge, prepare initial text drafts, analyze data, automate processes, support customer service, identify risks and optimize operations, provided that its use complies with authorization, data, confidentiality and human review requirements.
2. Employees using AI tools are responsible for input content, prompts, uploaded files, outputs and subsequent use. Without approval, employees shall not use personal accounts, unauthorized external tools or AI services that do not meet Company security requirements to process Company business information, and shall not circumvent Company security policies, access controls, audit logging or approval processes.
3. The Company applies stricter access control and oversight to sensitive AI functions. AI functions involving facial recognition, identity recognition, surveillance technology, biometric processing, automated material decisions, high-impact recommendations or other activities that may materially affect individual rights shall have a clearly identified deploying entity, authorized scope, use scenario, access rights, audit logging, human review and exit mechanism.
4. AI applications shall not be designed, deployed or used to deceive, manipulate, induce or impersonate another person; generate false information; circumvent regulation; compromise system security; infringe intellectual property or personal information rights; misappropriate trade secrets; engage in unfair competition; or pursue any other purpose contrary to laws, regulations, ethical standards or Company rules.

11. AI-Generated Content and Intellectual Property

1. When using AI to generate text, images, audio, video, code, reports, proposals, marketing materials or other content, the Company shall carefully consider factual accuracy, source reliability, copyright, trademarks, patents, trade secrets, portrait rights, reputation rights, data authorization and external communication risks. AI-generated content shall undergo appropriate human review before external publication, submission to customers, inclusion as a contract attachment, entry into a product code repository or use as material for an important internal decision.
2. Employees shall not enter unauthorized third-party works, customer information, materials subject to confidentiality obligations, or code or data subject to license restrictions into AI systems for training, generation, rewriting or dissemination. AI-assisted code, proposals and content shall be reviewed in accordance with the Company's requirements for intellectual

property, open-source compliance, information security and quality management to avoid infringement, vulnerabilities, malicious code, license conflicts or inappropriate content.

3. Where necessary, the Company may label, record or archive AI-generated content and retain relevant review and version records in accordance with laws and regulations, customer contracts, platform rules and Company requirements.

12. Third-Party AI and Supply Chain Management

1. When procuring, integrating or using third-party AI products, models, datasets, plug-ins, interfaces, cloud services, development tools or consulting services, the Company conducts supplier due diligence and qualification assessments proportionate to risk, focusing on legal and regulatory compliance, data security, personal information protection, cybersecurity, model safety, content safety, intellectual property, service stability, environmental impact and ongoing support capabilities.
2. Contracts and business documents involving AI shall, as necessary, specify data ownership, the purpose and scope of processing, confidentiality obligations, personal information protection, restrictions on model training or reuse, security incident notification, audit cooperation, service changes, exit and deletion, intellectual property ownership, liability and other necessary terms.
3. The Company encourages suppliers, business partners and developers to follow responsible AI principles and jointly prevent misuse of AI and adverse impacts on individuals, organizations, society and the environment. Where a third party materially violates laws, regulations, contractual obligations or the Company's AI governance requirements, the Company may require remediation, restrict use, suspend the business relationship or terminate the relationship, as appropriate.

13. Green and Low-Carbon Requirements

1. The Company promotes resource efficiency and consideration of ecological impact in the use, development and procurement of AI. Subject to safety, compliance, quality and business requirements, the Company prioritizes models, platforms, data centers, algorithmic solutions and usage methods with higher energy efficiency, lower resource consumption and lower environmental impact.
2. The Company encourages appropriate model selection, proportionate use, task classification, cache reuse, model compression, edge-cloud collaboration, computing resource optimization, reduction of unnecessary generation and technical optimization that lowers computing load, thereby reducing energy waste, water use and carbon intensity arising from AI operations.

3. For owned or third-party AI data centers, cloud services, model services and computing resources, the Company encourages and progressively promotes energy-efficient infrastructure, green data centers, renewable energy, energy consumption monitoring and carbon emissions accounting to reduce the ecological footprint of AI training, deployment and operations and support the Company's green, low-carbon and sustainable development objectives.

14. Prohibited Uses

1. The Company prohibits the use, deployment or development of AI systems or applications that violate laws, regulations, regulatory requirements, ethical standards or Company rules. Prohibited uses include, but are not limited to, systems that influence another person's independent judgment or behavior through manipulation, inducement or deception; systems that exploit the vulnerabilities of particular groups to mislead or exert improper influence; and systems used for social scoring, social ranking or discriminatory treatment based on improper criteria.
2. The Company prohibits unauthorized biometric surveillance, including biometric identification, facial recognition surveillance, identity tracking and other AI applications that may infringe individual rights, unless lawfully authorized. It also prohibits the generation or dissemination of false information, unlawful or harmful content, malicious code, phishing materials, deepfake content or other content that may harm cybersecurity, public safety, business reputation or lawful individual rights.
3. The Company prohibits the use of AI to circumvent audits, bypass access controls, evade regulation, conceal risks, falsify records, replace required human approval or otherwise violate corporate governance requirements. With reference to the requirements for restricted or prohibited AI systems under international regulatory frameworks such as the European Union Artificial Intelligence Act, the Company prevents the use or deployment of such AI systems through scenario qualification reviews, access controls, audit logging, periodic inspections and enforcement measures.
4. Any person who identifies a prohibited use described above or a material AI risk shall immediately stop the relevant use and report it to the responsible department or relevant control function. The Company will investigate, remediate and determine accountability according to the nature and scope of the event and may review the effectiveness of related preventive controls within an appropriate scope.

15. Objections, Appeals and Review Mechanism

1. Where an AI-generated result, AI-assisted analysis or AI-influenced decision may materially affect an employee, customer, user, supplier, business partner or other affected party, the Company supports the relevant party in raising an objection, submitting an appeal or requesting review in accordance with applicable rules.
2. The Company conducts human review according to the specific scenario and, as necessary, provides an explanation, corrects the result, performs a supplementary assessment, suspends application, reprocesses the matter or takes other necessary action. In handling objections, appeals and reviews, the Company protects personal information, trade secrets and lawful rights and prevents improper treatment arising from an appeal or feedback.
3. Where AI causes or may cause an error, harm, discrimination, improper denial of service, restriction of rights or another adverse impact, the Company shall establish an intake channel, identify the department responsible for investigation, specify handling timeframes, corrective measures and feedback methods, and ensure that accountability and the resolution process are traceable.

16. Implementation Mechanisms and Performance Metrics

1. The Company embeds responsible AI requirements throughout the AI lifecycle, including system design, R&D, procurement, deployment, operations, iteration and decommissioning, and develops implementation plans, operating standards, checklists and assessment requirements appropriate to the business scenario. Implementation mechanisms may include access restrictions for sensitive AI functions, distinct labeling of AI-generated content, model performance monitoring, algorithmic bias assessments, ecological footprint management, objection and appeals processes, employee training and periodic compliance audits.
2. The Company establishes performance and impact tracking mechanisms for important AI projects. Subject to data availability, financial accounting rules and disclosure approval requirements, it tracks AI-related investment in the latest reporting year; revenue growth, cost reduction and efficiency improvements attributable to AI; return on AI investment; and AI's contribution to sustainability objectives such as carbon reduction, resource efficiency, customer service quality, reduction of risk events and employee training coverage.
3. AI-related performance metrics shall be jointly verified by business departments, Finance, Data Governance and relevant functions to avoid overstating AI contributions or double counting. Metrics eligible for public disclosure shall be reported using verifiable methodologies in annual reports, sustainability reports, the Company's website or other formal publications. For metrics

not yet ready for disclosure, the Company shall continue to improve calculation methodologies, internal records and verification processes.

4. Based on its AI management maturity, customer requirements, regulatory trends and external rating requirements, the Company may evaluate the introduction of third-party assessments or external assurance to continuously improve the credibility and verifiability of its AI governance mechanisms.

17. Training and Continuous Improvement

1. In response to business development, technological progress and regulatory change, the Company continuously improves its AI governance mechanisms and provides training, as appropriate, on AI compliance, security, ethics, data protection, intellectual property, review of generated content and responsible use, enhancing employees' awareness and capability to use AI appropriately.
2. For personnel engaged in AI R&D, data processing, security management, product operations, customer service, procurement management, Legal and Compliance and other key roles, the Company may establish role-specific training, user guidance, checklists or operating procedures. Training may cover AI ethics principles, data privacy, cybersecurity, algorithmic bias, human oversight, labeling of generated content, prompt security, trade secret protection, intellectual property and examples of violations.
3. The Company shall record training topics, target audiences, participation and improvement feedback in accordance with the training plan and incorporate training on ethical AI use and security protection into the continuous improvement of AI governance. The Company will promptly remediate, optimize and continuously improve issues, risks and deficiencies identified in the use of AI.

18. Supplementary Provisions

Relevant Company functions are responsible for preparing and administering this Policy, which shall take effect upon review and approval by the Board of Directors or the ESG Sustainability Committee authorized by the Board. Where existing Company rules on AI, data security, cybersecurity, personal information protection, information disclosure, trade secrets, intellectual property, procurement, compliance, human resources or other matters conflict with this Policy, the stricter requirement shall apply. Where laws, regulations, regulatory rules or customer contracts impose a higher requirement, that requirement shall apply.

Relevant Company functions are responsible, according to their respective duties, for communication, interpretation, implementation oversight and periodic review of this Policy. Unless otherwise provided by the Company, any exception not covered by this Policy shall be submitted to the appropriate governing body for approval in accordance with the Company's approval process.

This Policy takes effect on the date of issuance and shall be publicly disclosed through the Company's website, annual report, sustainability report, integrated report or other formal corporate publication. When referring to this Policy in an external rating, questionnaire or stakeholder communication, the Company shall identify the location, page number or URL of the public disclosure. Internal drafts, emails and unpublished presentations do not constitute supporting evidence of public disclosure.

The Company will amend and improve this Policy as appropriate in response to laws and regulations, regulatory requirements, technological developments, business practices, external rating requirements and stakeholder feedback.