Seres Group Code of Ethics and Responsible Application of Artificial Intelligence

Seres Group Co., Ltd. and its subsidiaries (hereinafter referred to as "Seres" or "the Company") have formulated the *Seres Group Code of Ethics and Responsible Application of Artificial Intelligence* (hereinafter referred to as "this Code") in accordance with the national *Ethical Guidelines for the New Generation of Artificial Intelligence* and the ISO 42001 Artificial Intelligence Management System standards, taking into account actual business scenarios such as intelligent driving and intelligent cockpits, to regulate the entire lifecycle of artificial intelligence (AI) development, procurement, deployment, and operation.

1. Scope of Application

This Code has been approved by the Board of Directors, and applies to Seres Group Co., Ltd. and its subsidiaries, and third-party partners such as suppliers. All parties shall comply with this Code to uphold the bottom line of technological ethics, prevent technological risks, safeguard user rights and interests, data security, and social public interests, and promote the deep integration of artificial intelligence and the new energy vehicle industry, achieving innovative and compliant collaborative development.

2. Commitment

2.1 Data Security and Privacy Protection

- Respect for Data Privacy in AI Development and Use: During the development, training, and continuous optimization of AI systems, the Company strictly complies with relevant regulations on personal information and privacy protection stipulated in applicable laws and regulations. The Company collects users' personal information solely within the scope necessary for providing products or services, adhering to the principles of lawfulness, fairness, and minimum necessity, and clearly informs users of the content of the information collected and its usage scenarios.
- Strict Control of Sensitive Data: The Company strictly limits the application scenarios and access permissions of sensitive AI capabilities such as facial recognition, biometric monitoring, and precise location tracking, utilizing them only in statutory or explicitly user-authorized scenarios. The Company strictly adheres to the principles of segregation of duties and least privilege, ensuring that only authorized employees can access important sensitive data. The Company implements desensitization and encryption measures for important sensitive data to ensure its security during transmission, storage, and use.

2.2 Cybersecurity

- Ensuring AI System Cybersecurity: The Company establishes AI security protection mechanisms and conducts regular network security assessments, verifications, and emergency drills to prevent risks such as model theft, data tampering, and malicious attacks, ensuring the stable and controllable operation of AI systems.

2.3 Content Security

- Ensuring AI System Content Security: The Company establishes AI content security filtering and protection mechanisms to ensure that AI-generated content is legal and compliant.

2.4 Fairness, Transparency, and Explainability

- Avoiding Potential Bias and Ensuring Fairness: During the development and continuous iteration of AI models, the Company takes effective measures to monitor and eliminate algorithmic bias based on factors such as race, gender, region, age, and socioeconomic status. The Company regularly conducts fairness and bias assessments on deployed AI models to ensure that their decision-making logic does not result in discriminatory treatment in diverse real-world scenarios.
- Ensuring Transparency and Explainability of AI-Generated Results: Adhering to the concept of "defining safety by scenario," the Company extends safety protection to dimensions such as privacy protection. In scenarios involving user-oriented system operations or user-critical rights and interests, the Company ensures that the output of AI systems is reasonably understandable and technically interpretable, guaranteeing that users have a basic understanding of the purpose and logic of AI decisions. The Company proactively discloses to users, regulatory agencies, and stakeholders the application scenarios, core functions, data sources, decision-making logic, and potential risks of AI systems. For text, images, audio, and video content generated by AI, the Company uses methods such as electronic watermarking, digital certificates, or prominent identifiers for clear labeling.
- Clearly Defining the Scope of AI Authority: The Company ensures that AI operates controllably within permitted boundaries under the framework of laws and regulations. The Company clearly defines the operational authority boundaries, triggering conditions, functional thresholds, and exit mechanisms of AI in various operational scenarios. Furthermore, The Company divides the scope of AI system authority according to risk levels and strictly prohibits accessing data and performing operations beyond the authorized scope.

3. Actions

3.1 Human Supervision and Intervention

- Ensuring Human Involvement in Critical Decision-Making Processes: AI systems serve only as auxiliary tools. Key decisions (such as handling high-risk scenarios in intelligent driving, determining major user rights, and performing critical operations in production safety) are ultimately confirmed by humans. It is strictly prohibited for AI to make autonomous decisions on high-risk matters. All AI systems are equipped with convenient and operational human intervention interfaces to ensure quick manual control in the event of AI anomalies, risk warnings, or user objections. The Company clearly defines the process and responsible parties for human intervention to ensure timely and effective intervention and eliminate the risk of loss of control of AI system.
- Detecting and Correcting Drift or Performance Degradation in AI Models: The Company establishes monitoring mechanisms for the entire lifecycle of AI models, tracks model

performance changes in real-time, promptly detects and corrects issues such as accuracy drift, performance degradation, or drift reinforcement that arise over time, and regularly conducts model health assessments to ensure the continuous, stable, and compliant operation of AI systems.

3.2 Green, Low-Carbon, and Sustainable Development

- Requiring Low Ecological Footprint for Self-Owned or Third-Party AI Data Centers/Models: AI models/tools developed in-house or procured from third parties must exhibit low energy consumption and high efficiency, reducing computing power consumption and carbon emissions. In the AI data center, model training, and application stages, the Company strictly adheres to low-carbon and environmental protection requirements, prioritizing energy-efficient computing power and green energy sources.
- Proactively Reducing the Ecological Footprint of AI Data Centers/Models: The Company collaborates with suppliers and other partners to develop low-carbon AI technologies. Through measures such as model lightweighting, computing power scheduling optimization, and waste heat recovery and utilization, The Company continuously reduces the ecological footprint of AI throughout its entire lifecycle and regularly quantifies the impact of AI initiatives on sustainable development outcomes.

3.3 Employee Training and Capacity Building

- Integrating AI Ethics, Compliance Requirements, and Security Standards into the Employee Training System: The Company regularly conducts specialized AI training for all employees who interact with, develop, manage, and maintain AI systems. The training content includes AI ethics guidelines, data privacy protection, algorithmic drift prevention, emergency response procedures, etc., to enhance employees' ethical awareness and compliance capabilities.

3.4 Appeals Process and Accountability

- Establishing a User Complaint Process for AI Decision-Making: The Company provides users and affected third parties with a channel for complaining about AI decision-making, clarifies the requirements for accepting, verifying, responding, and rectifying user complaints, conducts independent verification of complained matters, and promptly corrects unreasonable AI decisions, safeguarding the legitimate rights and interests of users.
- Establishing and Improving Accountability Mechanisms: The Company clarifies the responsible parties for each link of AI research and development, deployment, operation and maintenance, and use, establishes a comprehensive accountability system, and investigates the responsibilities of relevant parties in accordance with laws and regulations for adverse results, safety accidents, or rights and interests damages caused by AI models/tools.