

奇瑞汽车股份有限公司负责任人工智能政策

Chery Automobile Co., Ltd.

Responsible Artificial Intelligence Policy

一、前言

I. Preface

作为中国汽车行业的领军企业之一，奇瑞汽车股份有限公司（以下简称“奇瑞”或“公司”）始终将技术创新视为企业发展的核心驱动力。在人工智能技术深刻重塑全球汽车产业的时代背景下，奇瑞积极拥抱 AI 变革，将其融入企业提效、智能制造、供应链管理、客户服务等业务场景，致力于为全球用户提供更安全、更智能、更便捷的出行体验。

As one of the leading enterprises in China's automotive industry, Chery Automobile Co., Ltd. (hereinafter referred to as "Chery" or the "Company") has always regarded technological innovation as the core driver of corporate development. Against the backdrop of artificial intelligence (AI) technology profoundly reshaping the global automotive industry, Chery actively embraces AI transformation by integrating it into business scenarios including enterprise efficiency enhancement, smart manufacturing, supply chain management, and customer service, striving to deliver safer, more intelligent, and more convenient mobility experiences to users worldwide.

奇瑞认识到，人工智能技术的研发与应用伴随着数据安全、隐私保护、算法偏见、伦理风险及环境影响等多重挑战。公司制定本政策，作为人工智能治理的重要制度依据，为人工智能系统的设计、开发、训练、部署、运营及退役提供负责任的治理原则和管理要求，确保技术创新与社会责任并行不悖。

Chery recognizes that the research, development, and application of AI technology are accompanied by multiple challenges, including data security, privacy protection, algorithmic bias, ethical risks, and environmental impact. The Company formulates this policy as a key institutional foundation for AI governance, providing responsible governance principles and management requirements for the design, development, training, deployment, operation, and decommissioning of AI systems, ensuring that technological innovation proceeds in parallel with social responsibility.

二、适用范围

II. Scope of Application

本政策适用于奇瑞汽车股份有限公司及其控股子公司、关联企业中涉及人工智能系统设计、开发、训练、部署、运营及退役全生命周期的业务单元与职能部门，包括人工智能核心技术研发、大模型训练、AI 基础设施与平台建设、AI 驱动的产品创新与客户服务等相关活动。

This policy applies to all business units and functional departments of Chery Automobile Co., Ltd. and its holding subsidiaries and affiliated enterprises that are involved in the full lifecycle of AI system design, development, training, deployment, operation, and decommissioning. This includes, but is not limited to, core AI technology R&D, large model training, AI infrastructure and platform construction, and AI-driven product innovation and customer service activities.

本政策适用于所有使用或接触人工智能系统的全职员工、兼职人员及合同工。公司要求相关人员在人工智能系统的研发、采购、部署、使用和管理过程中遵守本政策要求。

This policy applies to all full-time employees, part-time personnel, and contractors who use or have access to AI systems. The Company requires all relevant personnel to comply with the requirements of this policy throughout the R&D, procurement, deployment, use, and management of AI systems.

本政策所称“人工智能系统”涵盖机器学习、深度学习、自然语言处理、计算机视觉、生成式人工智能（包括大语言模型）等各类 AI 技术及其在汽车全价值链中的应用。

The term “AI system” as used in this policy encompasses various AI technologies including machine learning, deep learning, natural language processing (NLP), computer vision, and generative AI (including large language models, LLMs), as well as their applications across the entire automotive value chain.

三、基本原则与承诺

III. Fundamental Principles and Commitments

3.1 数据隐私保护

3.1 Data Privacy Protection

奇瑞承诺在人工智能系统的设计、开发、训练、部署与运营全生命周期中严格保护个人信息与敏感数据。公司遵守《网络安全法》《数据安全法》《个人信息保护法》《生成式人工智能服务管理暂行办法》等国内法律法规。在开展欧洲市场相关业务时，公司遵守欧盟《通用数据保护条例》（GDPR）及其他适用的数据保护法律，依法保障数据主体的知情、访问、更正、删除、可携带及撤回同意等权利。

Chery is committed to rigorously protecting personal information and sensitive data throughout the entire lifecycle of AI system design, development, training, deployment, and operation. The Company complies with domestic laws and regulations including the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and the Interim Measures for the Management of Generative AI Services. When conducting business related to the European market, the Company complies with the European Union's General Data Protection Regulation (GDPR) and other applicable data protection laws, safeguarding data subjects' rights to information, access, rectification, erasure, portability, and withdrawal of consent in accordance with the law.

公司在 AI 模型相关活动中采用加密技术、匿名化处理、访问控制机制等技术措施保护个人信息；在语料采集前开展个人信息内容风险等安全风险评估和预处理过滤；并通过意见反馈入口、客服邮箱及客服电话等渠道受理个人信息相关投诉和请求。

The Company employs technical measures such as encryption, anonymization, and access control mechanisms to protect personal information in AI model-related activities; conducts security risk assessments including personal information content risk evaluation and pre-processing filtering prior to corpus data collection; and accepts personal information-related complaints and requests through feedback portals, customer service email addresses, and customer service hotlines.

3.2 网络安全防护

3.2 Cybersecurity Protection

奇瑞承诺对人工智能系统建立覆盖研发、部署与运营全流程的网络安全防护体系。公司采取安全开发生命周期管理、数据加密、安全测试、AI 安全事件应急响应及负责任的漏洞披露等防护手段，防范网络安全风险。公司建立全天候安全运营机制（目标覆盖 7×24），并通过定期漏洞扫描与渗透测试持续检验防护有效性。

Chery is committed to establishing a cybersecurity protection system for AI systems that covers the entire process of R&D, deployment, and operation. The Company adopts protective measures including Secure Development Lifecycle management, data encryption, security testing, AI security incident emergency response, and responsible vulnerability disclosure to mitigate cybersecurity risks. The Company has established a round-the-clock security operations mechanism (targeting 24/7 coverage) and continuously validates protection effectiveness through regular vulnerability scanning and penetration testing.

针对生成式 AI 与大语言模型，公司部署输入输出防护机制，防范提示注入、越狱攻击、数据投毒等安全风险，并通过安全基础设施、内容安全服务及安全运营机制，持续提升 AI 系统安全防护能力。

For generative AI and large language models, the Company deploys input/output safeguard mechanisms to defend against security risks including prompt injection, jailbreaking attacks, and data poisoning, and continuously enhances its AI system security protection capabilities through security infrastructure, content safety services, and security operations mechanisms.

3.3 避免偏见与歧视

3.3 Avoiding Bias and Discrimination

奇瑞承诺人工智能系统在设计、训练与运行过程中实现公平且尽可能减少歧视性偏差的结果。公司要求训练数据满足代表性、多样性与完整性要求，建立覆盖性别、年龄、地域、种族、语言、残障等敏感属性的数据审查与清洗机制，并对高风险模型开展偏见审计与公平性测试，保障各类群体均能获得公平合理的 AI 决策结果。

Chery is committed to ensuring fair outcomes and minimizing discriminatory bias in the design, training, and operation of AI systems. The Company requires training data to meet representativeness, diversity, and completeness standards, establishes data review and cleansing mechanisms covering sensitive attributes such as gender, age, region, ethnicity, language, and disability, and conducts bias audits and fairness testing on high-risk models to ensure that all demographic groups receive fair and reasonable AI decision outcomes.

公司通过语料抽检、关键词抽检、歧视类测试题、风险识别标准和标注人员培训等方式识别和降低偏见与歧视风险，并持续完善相关测试和审核机制。

The Company identifies and mitigates bias and discrimination risks through corpus sampling inspections, keyword sampling reviews, discrimination-type test cases, risk identification standards, and annotator training, and continuously improves related testing and review mechanisms.

3.4 人类参与决策

3.4 Human Oversight in Decision-Making

奇瑞承诺对高风险、不可逆或对个人权益有重大影响的人工智能决策实施人类监督。根据决策风险等级，公司分别采用人类在环（Human-in-the-Loop, HITL）、人类在线（Human-on-the-Loop, HOTL）或人类主导（Human-in-Command, HIC）等模式，由具备相应资质的人员对 AI 输出进行审核、覆写、升级或终止。

Chery is committed to implementing human oversight for AI decisions that are high-risk, irreversible, or have significant impacts on individual rights. Based on the decision risk level, the Company adopts Human-in-the-Loop (HITL), Human-on-the-Loop (HOTL), or Human-in-Command (HIC) modes, with qualified personnel reviewing, overriding, escalating, or terminating AI outputs as appropriate.

公司明确，人工智能不得在未经人类复核或缺乏推翻机制的情况下作出重大或不可逆决策。AI 生成内容应明确提示仅供参考，用户或相关人员应对 AI 输出进行判断、确认和决策；涉及医疗、财务、投资、保险等重大影响情形的，应咨询相关专业人士。

The Company explicitly stipulates that AI shall not make significant or irreversible decisions without human review or without an override mechanism in place. AI-generated content should be clearly disclaimed as for reference only, and users or relevant personnel should exercise judgment, confirmation, and decision-making over AI outputs. For matters involving significant impacts such as healthcare, finance, investment, or insurance, relevant professional advice should be sought.

3.5 透明性与可解释性

3.5 Transparency and Explainability

奇瑞承诺对人工智能系统保持透明与可解释性。公司主动向用户及公众披露 AI 的使用范围、能力边界、数据来源、已知局限与主要风险。当用户与 AI 产品交互时，公司以显著方式告知用户正在与人工智能交互。

Chery is committed to maintaining transparency and explainability for its AI systems. The Company proactively discloses to users and the public the scope of AI usage, capability boundaries, data sources, known limitations, and major risks. When users interact with AI products, the Company prominently notifies users that they are interacting with an AI system.

对 AI 生成文本，公司提供显式标识并提示用户注意确认内容。对影响个人权益的 AI 决策，公司提供与风险程度相称的可解释性信息，包括决策依据、关键特征、置信度水平及申诉路径。公司按照适用监管要求推进算法备案及相关信息披露。

For AI-generated text, the Company provides explicit labeling and advises users to verify the content. For AI decisions that affect individual rights, the Company provides explainability information commensurate with the risk level, including decision rationale, key features, confidence levels, and appeal pathways. The Company advances algorithm registration and related information disclosure in accordance with applicable regulatory requirements.

3.6 问责机制

3.6 Accountability Mechanism

奇瑞为人工智能系统指定责任人，明确其对模型输出、风险决策及合规后果承担责任。公司建立 AI 事件调查与整改机制，对 AI 引发或涉及的错误、伤害、歧视或侵权行为开展根因分析并实施补救措施。

Chery designates responsible persons for AI systems, clearly defining their accountability for model outputs, risk decisions, and compliance consequences. The Company establishes AI incident investigation and remediation mechanisms, conducting root cause analysis and implementing corrective measures for errors, harms, discrimination, or infringements caused by or involving AI.

公司明确 AI 决策的法律责任归属，对其人工智能系统造成的损害依法承担责任，不以“模型自主行为”或“算法结果”为由推卸或免除责任。公司建立快速响应与处理机制、公开沟通机制、责任追究与监督机制，并通过意见反馈入口、客服邮箱及客服电话等渠道受理投诉和求助。

The Company clarifies the attribution of legal liability for AI decisions and assumes responsibility in accordance with the law for damages caused by its AI systems, without evading or exempting liability on the grounds of “autonomous model behavior” or “algorithmic results.” The Company establishes rapid response and handling mechanisms, public communication mechanisms, accountability and oversight mechanisms, and accepts complaints and assistance requests through feedback portals, customer service email addresses, and customer service hotlines.

3.7 授权使用与功能边界

3.7 Authorized Use and Functional Boundaries

奇瑞为人工智能系统制定授权使用政策或同等管理要求，明确规定其可执行与禁止执行的任务清单、能力边界、输入输出约束，以及升级与熔断规则。公司通过护栏、能力限制、沙箱环境、速率限制、内容过滤及权限分级等技术手段，防范功能漂移、越权使用及任务蠕变。

Chery establishes authorized use policies or equivalent management requirements for AI systems, explicitly defining the lists of permitted and prohibited tasks, capability boundaries, input/output constraints, and escalation and circuit-breaker rules. The Company employs technical and procedural safeguards including guardrails, capability restrictions, sandbox environments, rate limiting, content filtering, and permission tiering to prevent functional drift, unauthorized use, and task creep.

公司严禁将通用人工智能工具应用于未经授权的高风险决策场景。公司 AI 服务的使用范围应限定于经授权的内部运营、企业提效、汽车营销、出行交通、汽车专业知识问答、车主服务、售后服务、购车政策等场景，并明确禁止用户从事反向工程、恶意注册、竞争性应用开发、危害网络安全等行为。

The Company strictly prohibits the application of general-purpose AI tools to unauthorized high-risk decision-making scenarios. The Company’s AI services shall be limited to authorized scenarios including internal operations, enterprise efficiency enhancement, automotive marketing, mobility and transportation, automotive domain knowledge Q&A, vehicle owner services, after-sales service, and vehicle purchase policies, and explicitly prohibits users from engaging in reverse engineering, malicious registration, competitive application development, and activities that compromise cybersecurity.

3.8 低碳生态足迹

3.8 Low-Carbon Ecological Footprint

奇瑞承诺持续降低自有及第三方人工智能基础设施与模型的能源消耗、水资源使用及温室气体排放。公司持续测量并减少 AI 训练与推理阶段的能耗、水耗与碳强度，并通过模型蒸馏、量化、剪枝、稀疏化、混合专家模型、参数高效微调及推理缓存等算法优化技术降低算力需求。

Chery is committed to continuously reducing the energy consumption, water usage, and greenhouse gas emissions of its own and third-party AI infrastructure and models. The Company continuously measures and reduces energy consumption, water usage, and carbon intensity during AI training and inference phases, and reduces computational requirements through algorithm optimization techniques including model distillation, quantization, pruning, sparsification, Mixture of Experts (MoE), parameter-efficient fine-tuning (PEFT), and inference caching.

公司要求第三方 AI 数据中心与模型供应商提供其 PUE、水源使用效率及可再生能源占比，并将其纳入采购评估标准。公司未来计划建立 AI 算力碳排放核算体系，并适时对外披露 AI 相关能耗和碳排放数据。

The Company requires third-party AI data center and model providers to disclose their Power Usage Effectiveness (PUE), Water Usage Effectiveness (WUE), and renewable energy ratio, and incorporates these metrics into procurement evaluation criteria. The Company plans to establish an AI computing carbon emissions accounting system and disclose AI-related energy consumption and carbon emission data.

3.9 禁用人工智能系统

3.9 Prohibited AI Systems

奇瑞明确承诺不开发、不采购、不部署任何违反欧盟《人工智能法案》第 5 条所列的禁用人工智能系统，包括但不限于：基于人脸识别的监控系统、社会评分系统或未经授权的生物特征识别系统。公司承诺不将 AI 技术应用于上述禁用场景。

Chery explicitly commits to not developing, procuring, or deploying any AI systems that violate the prohibitions listed in Article 5 of the European Union Artificial Intelligence Act, including but not limited to: surveillance systems based on facial recognition, social scoring systems, or unauthorized biometric identification systems. The Company commits to not applying AI technology to any of the above prohibited scenarios.

公司承诺不使用以下禁用人工智能系统：

The Company commits to not using the following prohibited AI systems:

- 使用潜意识、操纵性或欺骗性技术实质性扭曲个人行为的系统；
- Systems that deploy subliminal, manipulative, or deceptive techniques to materially distort the behavior of individuals;

- 利用年龄、残疾或特定社会经济脆弱性实质性扭曲个人行为的系统；
- Systems that exploit vulnerabilities related to age, disability, or specific socioeconomic situations to materially distort the behavior of individuals;
- 基于社会行为或个人特征对自然人进行跨场景社会评分并造成不公正或不相称后果的系统；
- Systems that evaluate or classify natural persons based on their social behavior or personal characteristics across contexts, resulting in unfair or disproportionate outcomes (social scoring systems);
- 未经授权授权的实时远程生物特征识别系统。
- Real-time remote biometric identification systems in public spaces that are not authorized by law.

四、治理架构与职责

IV. Governance Structure and Responsibilities

为确保本政策有效实施，奇瑞建立多层次的人工智能治理架构，明确各层级职责与权限。公司法定代表人承担 AI 治理最终责任，并在安全评估报告上签字确认；安全评估负责人承担 AI 治理管理责任，监督 AI 安全合规；AI 研发部门负责政策制定与技术实施，承担 AI 核心技术研发相关职责；安全运营工作小组负责安全运营与事件响应，实时监控 AI 系统运行；信息安全部门负责线上实时监看和运营等相关工作。

To ensure the effective implementation of this policy, Chery establishes a multi-tiered AI governance structure with clearly defined responsibilities and authorities at each level. The Company's legal representative bears ultimate responsibility for AI governance and signs off on safety assessment reports; the Safety Assessment Director assumes management responsibility for AI governance and supervises AI security compliance; the NEXTAI Intelligent Research Institute is responsible for policy formulation and technical implementation, undertaking responsibilities related to core AI technology R&D; the Security Operations Working Group is responsible for security operations and incident response, monitoring AI system operations in real time; and the Information Security Department is responsible for online real-time monitoring and operational oversight.

本政策经公司执行管理层审核认可，作为公司 AI 治理的重要政策文件。各相关业务单元、职能部门和人员应按照本政策要求落实人工智能治理职责。

This policy is reviewed and approved by the Company's executive management, and serves as a key policy document for the Company's AI governance. All relevant business units, functional departments, and personnel shall implement AI governance responsibilities in accordance with the requirements of this policy.

五、公开披露、复审与更新

V. Public Disclosure, Review, and Updates

公司通过官网公开发布本政策，文件名称中明确包含“人工智能”或“AI”字样，以便利益相关方识别。本政策每年进行一次复审，并在每两年或遇法规、技术、业务发生重大变化时重新审议批准。

The Company publicly releases this policy through its official website , with the document title clearly containing the terms “Artificial Intelligence” or “AI” to facilitate identification by stakeholders. This policy undergoes annual review and is subject to re-evaluation and approval every two years or upon the occurrence of significant changes in regulations, technology, or business conditions.

公司依法推进生成式人工智能服务备案、安全评估及相关管理体系建设，并根据技术发展、法规变化及业务需求对本政策进行修订。重大修订将经公司执行管理层审批后发布，并在公司官网同步更新。

The Company advances generative AI service registration, safety assessments, and related management system development in accordance with the law, and revises this policy based on technological developments, regulatory changes, and business needs. Major revisions shall be published upon approval by the Company’s executive management and simultaneously updated on the Company’s official website.

六、附则

VI. Supplementary Provisions

本政策自发布之日起施行，如本政策与国家法律法规存在冲突，以国家法律法规为准。

This policy shall take effect from the date of publication . In the event of any conflict between this policy and national laws and regulations, the national laws and regulations shall prevail.

奇瑞汽车股份有限公司

Chery Automobile Co., Ltd.