

Responsible Artificial Intelligence Policy

Introduction

NIU Technologies (together with its subsidiaries and consolidated affiliated entities, "NIU", "We" or the "Company") recognizes that artificial intelligence ("AI") can support innovation, connected mobility, product development, manufacturing, quality management, customer service and business operations. AI may also create risks to individuals, society, information security and the environment if it is not designed, procured, deployed and used responsibly.

We are committed to the lawful, ethical, secure, transparent and environmentally responsible use of AI. This Policy establishes the principles and governance expectations that apply throughout the AI lifecycle, from design and procurement to deployment, monitoring and retirement.

Scope

This Policy applies to NIU, all of its directors, officers and employees, and any contractors, consultants, organizations or individuals acting for or on behalf of NIU. It covers all AI systems, models and tools developed, procured, licensed, integrated, deployed or used by NIU, including generative AI, AI embedded in products or services, and third-party AI systems and model providers.

All persons within the scope of this Policy are responsible for complying with it and with applicable laws, regulations, contractual requirements and internal controls. Where local requirements are more stringent, the more stringent requirements shall apply.

Core Principles

- **Data Privacy and Data Governance**

We safeguard personal data and other protected information throughout the AI lifecycle. AI systems shall be designed, developed and operated in accordance with applicable data protection laws and NIU's privacy and information governance requirements, including lawful and transparent processing, purpose limitation, data minimization, data quality, appropriate retention and secure disposal.

Personal, confidential or proprietary information shall not be entered into or used to train third-party AI tools unless the use has been authorized and appropriate privacy, confidentiality and security safeguards are in place.

- **Cybersecurity, Safety and Reliability**

We apply security-by-design and risk-based safeguards to protect AI systems and their data against unauthorized access, misuse, manipulation, leakage and cyberattacks. Appropriate controls may include access restrictions, secure

development practices, encryption, testing, monitoring, vulnerability management and incident response.

AI systems shall be tested and monitored in proportion to their potential impact. Material security, safety or reliability issues shall be escalated promptly, and use of an AI system may be restricted or suspended until the issue is addressed.

- **Fairness and Avoidance of Bias**

We seek to prevent AI systems from creating or reinforcing unfair, discriminatory or otherwise harmful outcomes. AI data, design and outputs shall be assessed for potential bias in proportion to the nature, context and impact of the use case. Where relevant, NIU shall use appropriate data quality measures, representative datasets, testing and human review to identify, mitigate and correct bias.

- **Human Oversight and Intervention**

Critical or high-impact decisions influenced by AI shall remain subject to effective and documented human oversight. Authorized persons shall have the authority and practical ability to review, intervene, override, suspend or escalate an AI-generated output or decision. AI shall not make an irreversible or high-stakes decision affecting an individual without meaningful human oversight and an appropriate mechanism for human review.

- **Transparency and Explainability**

We provide transparency appropriate to the context and potential impact of an AI system. Where material, users and affected stakeholders shall be informed when they are interacting with AI, when content has been generated or materially modified by AI, or when an AI-driven outcome affects them.

NIU shall provide understandable information, as appropriate, about an AI system's purpose, capabilities, limitations, relevant data sources and material risks. Decisions with significant effects shall be supported by a meaningful explanation and a route to request human review, subject to legal, security and intellectual property constraints.

- **Accountability and Governance**

The management of the Company oversees this Policy and material AI risks. Each AI system shall have a named business owner accountable for its intended purpose, outcomes, risk decisions and compliance, as well as a designated system owner responsible for lifecycle documentation, testing, monitoring and issue management. Relevant legal, compliance, privacy, information security and other control functions shall support review according to the nature and risk of the use case.

Material AI-related errors, incidents or harms shall be investigated, documented and remediated. Accountability for decisions influenced by AI remains with NIU and the responsible human decision-makers and is not transferred to the AI system.

- **Defined Boundaries and Acceptable Use**

AI systems shall be used only for approved purposes and within documented boundaries covering authorized users, data, functions, capabilities and limitations. Appropriate technical and administrative safeguards shall be used to prevent misuse,

unintended expansion of purpose or operation outside the approved scope. Access to sensitive AI capabilities, including biometric identification, facial recognition or surveillance functions, shall be strictly limited to authorized persons and legitimate, lawful purposes.

- **Environmental Sustainability**

We require AI models and supporting data centers, whether operated by NIU or by third parties, to pursue a low ecological footprint. For material AI use cases and suppliers, NIU shall seek information needed to evaluate, measure and reduce energy use, water use and carbon intensity. We promote efficient model selection, optimization techniques that reduce computational load, energy-efficient infrastructure and the use of renewable energy where feasible.

Environmental considerations shall be incorporated, as appropriate, into AI design, procurement, supplier engagement and lifecycle reviews. Where AI is used to support sustainability outcomes, NIU shall seek to quantify material benefits and adverse impacts using appropriate metrics.

- **Prohibited AI Practices**

NIU shall not develop, procure, use or deploy AI systems that: use subliminal, purposefully manipulative or deceptive techniques to materially distort a person's behavior and cause or reasonably risk harm; exploit vulnerabilities related to age, disability or specific social or economic circumstances; conduct social scoring that results in detrimental, disproportionate or unjustified treatment; or perform unauthorized biometric surveillance or unlawful remote biometric identification.

We also prohibit AI uses that violate applicable law, intentionally facilitate unlawful discrimination, materially undermine human rights, or operate outside the boundaries and safeguards required by this Policy.

- **Implementation and Compliance**

NIU applies a risk-based approach to AI governance. AI use cases shall be identified, documented and assessed before material deployment, with enhanced review and controls for higher-risk applications. Depending on the use case, controls shall include restrictions on access to sensitive capabilities, labeling of AI-generated content and AI-driven outcomes, monitoring for model drift or degradation, regular fairness and bias assessments, and mechanisms for correction, suspension or retirement.

Employees and relevant third parties shall receive guidance or training appropriate to their roles on the ethical and secure use of AI. Persons within the scope of this Policy shall report suspected violations, incidents or harmful outcomes through NIU's established reporting channels and shall cooperate with investigations and corrective actions.

Where an AI-driven decision or outcome materially affects a user or third party, NIU shall provide or enable an accessible and fair channel to request clarification, human review, correction or other appropriate remedy, subject to applicable law. NIU shall not tolerate retaliation against any person who raises a concern in good faith.

Third-party AI providers shall be subject to risk-based due diligence and appropriate contractual or other safeguards. NIU shall consider their privacy, cybersecurity, fairness, transparency, accountability and environmental practices, and may require relevant information, assessments or corrective action.

Review and Update

This Policy has been approved by the management and will be reviewed and updated regularly to reflect changes in applicable laws and regulations, AI technologies, industry practices and NIU's risk profile. Material changes shall be submitted to the appropriate approving body.