Information Security and Privacy Protection Policy

Introduction

NIU Technologies, together with its subsidiaries and consolidated affiliated entities ("NIU" or the "Company"), is committed to protecting information, systems and personal information entrusted to it. NIU shall maintain and continually improve risk-based information security and privacy protection systems designed to preserve the confidentiality, integrity and availability of information, respect individual privacy rights and support resilient business operations.

Scope

This Policy applies across NIU's entire operations and throughout the information and personal-information lifecycle. It applies to all employees, as well as contractors, consultants, temporary workers and other workforce members. Relevant requirements also apply to suppliers, service providers, processors, business partners and other third parties that access NIU information or systems, or process personal information for or on behalf of NIU.

The Policy covers information in any form, including networks, applications, products, services, connected devices and supporting infrastructure; and personal information relating to customers, users, employees, applicants, contractors, business contacts and other individuals. Where applicable law, regulation or contract imposes a stricter requirement, the stricter requirement shall apply.

Responsible Functions and Risk Integration

NIU will designate persons or departments responsible for information security and privacy, with clear escalation channels and authority to coordinate implementation, training, monitoring, audits, incident response and improvement. Information security and privacy will be embedded in group-wide risk, compliance, internal control, product development, procurement, supplier management and incident management processes.

Information Security

- **Integrity and Protection of Data:** NIU shall protect information and systems against unauthorized access, disclosure, alteration, loss, destruction, misuse and disruption throughout their lifecycle. Controls shall include, as appropriate to risk and data classification, asset and data inventories, minimum necessary and role-based access, secure configuration, encryption in transit and at rest, change control, secure development and testing, logging, backup and recovery, retention controls and

secure deletion. Access shall be reviewed and changed or revoked promptly when duties or authorization change.

- **Threat Monitoring and Response:** NIU shall monitor networks, systems, security events, abnormal data activity, vulnerabilities and relevant threat intelligence in proportion to risk. Suspected or actual incidents shall be reported promptly, assessed, contained, investigated and remediated. NIU shall preserve evidence, restore affected services and data safely, address root causes, document corrective and preventive action, and notify affected individuals, business partners, regulators or other authorities when required by law or contract.

- **Workforce Responsibility:** Every member of the workforce is responsible for protecting information, using access only for authorized purposes, following approved procedures, completing required training and promptly reporting suspected threats, vulnerabilities, privacy concerns or incidents. Personnel with privileged, technical, product, procurement, privacy or incident-response duties shall receive additional role based training appropriate to their responsibilities.

- **Third-party Security Requirements:** Before a third party receives access to NIU information or systems, NIU shall conduct risk-based due diligence and establish written security requirements appropriate to the service and risk. Requirements may address authorized use and access, confidentiality, technical and organizational safeguards, incident notification and cooperation, subcontracting, business continuity, audit or assessment rights, remediation, and secure return or deletion of information. NIU shall monitor material third-party risk and may restrict, suspend or terminate access or services where requirements are not met.

- **Continuous Improvement:** NIU shall maintain a risk-based information security framework and continually improve its workforce capabilities, processes, technology and infrastructure. Risk assessments, control reviews, security testing, audit findings, incidents, lessons learned and changes in the external threat and regulatory environment shall inform security priorities and corrective action.

Privacy Protection

- **Privacy Principles and Implementation Measures:** NIU shall process personal information lawfully, fairly, transparently and in good faith. Processing shall have a clear and legitimate purpose, use the minimum information necessary, limit use and retention to the approved purpose and period, maintain appropriate accuracy and security, and support accountability throughout the lifecycle. NIU shall provide clear privacy notices, identify an appropriate lawful basis and obtain consent where required. It shall maintain accessible channels for individuals to exercise applicable rights, including access, correction, deletion, withdrawal of consent, account cancellation, explanation and complaint.

- **Privacy by Design and Risk Assessment:** Privacy requirements shall be incorporated into the design, procurement, development, testing, launch, operation, change and retirement of products, services and processes. NIU shall conduct and document personal information protection impact assessments before processing

likely to create a high risk or material effect on individual rights, including material processing of sensitive personal information, significant automated decision making, entrusted processing, sharing, public disclosure, cross-border transfers or material use of new technology. Identified risks shall be remediated or accepted by an authorized owner before processing proceeds.

- **Suppliers and Other Recipients:** Suppliers, processors, service providers and other recipients that process personal information for or with NIU shall be subject to privacy requirements appropriate to the processing and risk. NIU shall conduct due diligence and, where applicable, use written agreements covering purpose and scope, security, confidentiality, incident notification, rights assistance, subcontracting, retention, return or deletion, audit rights and corrective action. NIU shall supervise relevant processing and may suspend data flows or terminate the relationship if requirements are not met.

- **Privacy Compliance Monitoring and Audits:** NIU shall conduct periodic internal privacy compliance reviews and audits across its operations, including relevant supplier and processor activities. Reviews shall cover governance, lawful basis, notice and consent, minimization, access, sharing, cross-border transfer, retention, security, individual rights, incidents and corrective action. NIU shall also commission qualified, independent third-party audits of privacy policy compliance at intervals determined by risk and when required by law, regulators, a material incident or other significant circumstances. Findings shall be assigned to accountable owners, reported to the appropriate management level and tracked to closure.

- **Privacy Incidents, Complaints and Disciplinary Action:** Actual or suspected loss, leakage, alteration, destruction, unauthorized access, unlawful use or other compromise of personal information shall be reported immediately and handled under NIU's incident response procedures. Privacy inquiries, complaints and rights concerns shall be handled fairly, promptly and without retaliation. NIU has zero tolerance for intentional misuse, concealment, unauthorized disclosure or other material violations of personal information requirements. Violations may result in access restriction, corrective action, mandatory retraining, disciplinary action up to and including termination of employment or engagement, contractual remedies, reporting to authorities and legal action, subject to applicable law and due process.

Review and Update

This Policy has been approved by the management and will be reviewed and updated at least annually and upon any material changes occur. Material incidents, audit findings and assessment results will inform updates.