GCL Technology Holdings Limited

GCL Technology Information Security and Privacy Protection Policy

Chapter I: General Principles

Article 1 Purpose

To strengthen the information security and privacy protection management system of GCL Technology Holdings Limited (hereinafter referred to as "GCL Technology," or "the Company"), clarify management requirements and responsibilities throughout the data processing lifecycle, prevent risks of data leakage and misuse, and support the stable operation and compliant development of the Company's business, this policy is formulated in accordance with relevant national laws and regulations.

Article 2 Scope of Application

This policy applies to all full-time employees, labor dispatch employees, interns, and outsourced personnel (hereinafter referred to as "employees"), as well as any third party (including but not limited to customers, suppliers, agents, distributors, service providers, and third-party intermediaries) that accesses, processes, or uses the Company's information assets in any form.

Article 3 Definitions

1. Data: Any information, in electronic or non-electronic form, generated, collected, stored, transmitted, or used by the Company in its business management activities, including but not limited to business data, financial data, personnel data, customer and supplier information, and intellectual property.
2. Personal Information: Any information recorded electronically or by other means that can identify a specific natural person, either alone or in combination with other information.

3. Data Security: The state in which data is effectively protected and legally utilized through necessary measures, with the capability to ensure continuous security. Its core objectives are to protect the confidentiality, integrity, and availability of data.
4. Privacy Protection: The protection of personal information involving personal dignity and privacy, preventing unauthorized collection, use, processing, transmission, provision, disclosure, and other related actions.

Chapter II: Specific Provisions

Article 4 A dedicated team has been established to advance information security and confidentiality, ensuring unified and standardized management of privacy and data security matters.

Article 5 The Company is committed to continuously improving its information security system, including upgrading information infrastructure, applying information security defense technologies, and enhancing emergency response capabilities, to strengthen system resilience and risk response, ensuring that security measures evolve to effectively address dynamic risks.

Article 6 The Company strictly protects the integrity of all business data through technical and managerial measures such as encrypted storage, access control, backup, and recovery, preventing data tampering, loss, or damage, and ensuring accuracy, availability, and security throughout the data lifecycle.

Article 7 To ensure the correctness, consistency, and security of data, The Company continuously strengthens information security governance and control measures, including access permission settings, audit logs, and anomaly reporting mechanisms, effectively preventing unauthorized access, tampering, or destruction during storage, transmission, and processing. Sensitive information is accessible or modifiable only by authorized personnel.

Article 8 The Company integrates information security and privacy protection into its overall compliance and risk management framework, establishing a comprehensive information security monitoring system covering networks, systems, terminals, and user

behavior. This system continuously monitors and identifies potential threats (including cyber attacks, data breaches, malware, etc.). Through emergency plans, incident response mechanisms, and regular drills, The Company ensures rapid handling of security incidents, effectively controlling risk impact and maintaining stable business operations.

Article 9 The Company has established an information security incident notification and emergency response mechanism, routinely monitoring information security threats and anomalous activities and taking swift action. For major information security incidents, internal procedures are strictly followed, with continuous follow-up on corrective measures and risk reassessment. Relevant stakeholders are promptly informed of the incident impact and handling progress to maintain transparency and trust.

Article 10 Information security and privacy protection are the shared responsibilities of every employee. All employees must fulfill their corresponding information security obligations according to their roles, strictly adhering to The Company's information security and privacy protection policies and related regulations. Any data security incident (including leakage, loss, or tampering) must be reported immediately to direct supervisors and the GCL Technology Information Security Management Structure Leading Group.

Article 11 The Company has developed an information security management plan covering all employees and regularly conducts information security training and awareness activities to enhance overall security awareness and ensure compliant operations.

Article 12 The Company also imposes clear information security maturity requirements on suppliers and external partners, specifying confidentiality agreements, information security responsibility clauses, and information security incident notification and emergency collaboration mechanisms in contracts. Necessary assessments and audits are conducted based on risk levels to comprehensively safeguard information supply chain security.

Article 13 The following violations will be handled according to the severity of the circumstances: If an information security or customer privacy incident occurs but remedial measures are taken promptly, or if the leaked information does not cause serious consequences or economic losses, a warning and financial penalty will be imposed, with

the department head bearing joint responsibility; If authority is used to compel others to violate regulations, assist in stealing, probing, or soliciting the Company's confidential information, or if negligence or intentional actions cause an information security or customer privacy incident with serious consequences or significant economic losses, the employee will be dismissed and may be required to compensate for economic losses. Severe cases will be subject to legal action.

Article 14 The Company regularly conducts internal and external audits related to information security and privacy protection and optimizes management practices based on audit results.

Article 15 The Company will periodically review and update this policy, making adjustments in response to revisions in relevant laws and regulations, technological evolution, and trends in information security and privacy protection management.

Chapter III: Supplementary Provisions

Article 16 This policy is ultimately interpreted by the Sustainability Center of GCL Technology Holdings Limited.