Proya Cosmetics Co., Ltd.

Information Security and Privacy Protection Policy

1. Introduction

This Policy is hereby formulated to strengthen the information security and privacy protection management of Proya Cosmetics Co., Ltd. ("Proya Cosmetics" or the "Company") and safeguard the Company's network security and customer privacy.

2. Scope of Application

This Policy applies to the Company and its subsidiaries and branches within the scope of its consolidated financial statements.

3. Relevant Measures

3.1 Strengthening Information Security Management

3.1.1 Establishing an Information Security Management System

The Company has established an information security governance mechanism with clearly defined rights and responsibilities. The Strategy and Sustainable Development Committee of the Company's Board of Directors is responsible for reviewing information security and data protection plans and supervising and guiding the overall implementation of related work. The Chief Digital Officer (CDO) is responsible for the overall coordination of information security management. The Digital Technology Center is responsible for formulating and implementing information security and data protection plans, ensuring the continuous optimization of product- and system-side security and compliance work, responding to the needs of business departments, and promoting the effective implementation of relevant information security projects.

3.1.2 Formulating Information Security Policies

The Company has formulated comprehensive information security management systems, which clarify the objectives, principles, and requirements of information security management and provide guidance for the Company's information security management.

3.1.3 Strengthening Information Asset Management

The Company classifies, identifies, and evaluates its information assets, clarifies the importance and confidentiality of various types of information assets, and ensures that critical information assets are effectively protected.

3.1.4 Implementing Access Control

Establishing access control strategies: The Company sets different access permissions for different levels of information assets to ensure that employees can only access the information resources required for their work.

Implementing mandatory identity authentication mechanisms: Measures such as usernames and passwords, digital certificates, and other mechanisms are adopted to ensure that only authorized users can access information systems.

3.1.5 Continuously Improving Security Safeguards

Stable operation: Through the power and environment monitoring system and equipment inspection mechanism (daily/weekly/monthly inspections), the Company promptly provides early warnings and eliminates fault risks to ensure the stable operation of equipment such as power supply, fire protection, cooling, weak current, and server storage systems.

Data backup: The Company implements a data protection strategy combining daily local backup and off-site synchronization to address the risk of accidental system or data loss, and verifies the effectiveness of the recovery mechanism through annual disaster recovery drills.

Network security: The Company regularly conducts vulnerability scans and cybersecurity penetration tests and strengthens and remediates relevant risk items.

Compliance audits: The Company regularly conducts technical testing through log detection systems and conducts security and compliance audits on security and privacy protection measures to identify potential security risks.

3.1.6 Strengthening Employee Training

The Company regularly provides information security training to employees to enhance their security awareness and ensure that they comply with information security management rules in their daily work.

3.1.7 Emergency Response Plan

The Company continuously monitors information security risks and potential threats, formulates comprehensive emergency response procedures for information security incidents, clarifies management requirements such as incident reporting, emergency response, and post-incident review, and improves its information security protection capabilities through regular testing and simulation drills.

3.2 Emphasizing Privacy Protection

The Company attaches importance to protecting the privacy of stakeholders such as employees, customers, suppliers, and partners. It complies with relevant laws and regulations within China, such as the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, and the *Personal Information Protection Law of the People's Republic of China*, follows the principles of lawful, legitimate, and necessary collection and use, and takes various measures to protect user privacy.

3.2.1 Providing Dedicated Privacy Protection Organizations and Personnel

The Company has established a dedicated personal information protection team, which is responsible for implementing laws and regulations related to personal information protection and supervising and auditing privacy protection in various business activities to ensure the effective implementation of privacy protection.

3.2.2 Collection of Personal Information

When collecting personal information, the Company clearly defines the purpose, scope, and method of collection, follows the principles of reasonableness, relevance, and necessity, minimizes the collection of users' personal information, and allows customers to choose whether to authorize such collection.

3.2.3 Use of Personal Information

The Company follows the principles of legality, compliance, and security when using users' personal information, and stipulates that such information shall not be used for any other purposes unrelated to the purpose of collection.

3.2.4 Storage of Personal Information

The Company encrypts stored personal information and adopts technical and management measures to prevent risks such as data leakage, tampering, and loss.

3.2.5 Transmission of Personal Information

When transmitting personal information, the Company uses encryption technologies and secure channels to ensure data security during transmission.

3.2.6 Sharing of Personal Information

The Company may share personal information with third parties such as other companies, organizations, and individuals only after obtaining explicit prior consent or authorization, or where required by applicable laws and regulations, legal procedures, competent government authorities, or judicial authorities.

For third parties with whom personal information is shared, the Company requires them to process personal information as per confidentiality and security measures no less stringent than those required under this Policy.

3.2.7 Destruction of Personal Information

Unless otherwise provided by laws and regulations, the Company shall retain personal information only for the shortest period necessary to achieve the purpose of processing. After the retention period expires, the Company will delete the relevant personal information in accordance with applicable laws.

3.2.8 Protection of User Rights

The Company respects and safeguards users' rights to be informed, to make choices, to make

corrections, and to request deletion, among other rights, and provides convenient channels for user appeals and complaints.

3.2.9 Training and Communication

The Company regularly provides employees with training on privacy protection knowledge to enhance their privacy protection awareness and capabilities.

3.2.10 Accountability

The Company adopts a "zero tolerance" attitude toward violations of privacy protection requirements, and establishes mechanisms for investigating and determining privacy violations and pursuing accountability. For violations such as employees' unauthorized collection, use, or disclosure of private information, the Company will take corresponding disciplinary measures in accordance with relevant management systems and the circumstances of the violation.

3.3 Responsible Use of Artificial Intelligence

In the lifecycle management of artificial intelligence (AI), the Company will follow the following principles to ensure that technology is used for good, risks are controllable, and responsibilities are traceable.

3.3.1 Protecting Private Information

The Company strictly complies with data protection regulations and embeds privacy protection into the development and application of AI. Before inputting data into AI systems, especially third-party generative AI tools, the Company desensitizes, anonymizes, or encrypts sensitive personal information to prevent data leakage and unauthorized secondary training.

3.3.2 Ensuring Information Security

The Company incorporates AI systems into its overall information security management framework, implements access control and encrypted transmission for models and interfaces, and regularly conducts vulnerability scans. When procuring third-party AI services or models, it includes suppliers' cybersecurity capabilities within the scope of due diligence and gives priority to service providers certified under ISO/IEC 42001 (Artificial Intelligence Management System), ISO 27001 (Information Security Management System), and other standards.

3.3.3 Preventing Potential Bias

The Company recognizes that AI systems may produce discriminatory results due to imbalanced training data, defects in algorithm design, or differences in application scenarios. During model development, the Company uses data from diversified sources to the extent possible, and regularly conducts systematic reviews of model outputs to ensure the fairness of AI output results.

3.3.4 Applying AI Scientifically and Prudently

When using AI to assist decision-making, the Company requires decision-makers to fully

understand the operating logic of the system and the basis of its outputs, and retains human authority to review, question, and intervene in final conclusions.

3.3.5 Ensuring Transparency and Explainability

The Company strictly fulfills its AI labeling obligations. In various AI application scenarios, the Company explains AI involvement to relevant parties in a clear and understandable manner and strives to improve the explainability of AI system operations so that stakeholders can understand the basic logic of AI-generated results or decisions.

3.3.6 Establishing an Accountability Mechanism

In accordance with the principle of "whoever is in charge is responsible," the Company clarifies the management responsibilities of business departments, functional departments, and relevant service providers throughout the AI lifecycle. All relevant parties shall properly perform technical management, security assurance, compliance review, and supervision and inspection according to their respective responsibilities. Where adverse consequences arise due to non-compliant applications or management omissions, the Company will pursue accountability in accordance with relevant systems.

3.3.7 Defining the Boundaries of AI Capabilities

The Company clearly defines the applicable scenarios and capability boundaries of AI technology, formulates an AI prohibition list and restriction rules for high-risk areas, and ensures that the application of the technology always complies with laws, regulations, and business ethics.

3.3.8 Reducing the Environmental Footprint of AI

The Company takes the environmental impact of AI into consideration in procurement decisions, gives priority to suppliers with low PUE, low energy consumption, and use of renewable energy, and, on the basis of meeting actual needs, prioritizes the use of efficient algorithms and lightweight models to reduce inference energy consumption and minimize the negative environmental impact of AI applications.

4. Others

This Policy is formulated by the Strategy and Sustainable Development Committee of the Company's Board of Directors, which shall be responsible for its interpretation.

Matters not covered in this Policy shall be handled in accordance with relevant laws, regulations, and normative documents.

This Policy shall take effect on the date it is reviewed and approved by the Company's Board of Directors. The applicability of this Policy shall be assessed every three years or when major changes occur.

Proya Cosmetics Co., Ltd.

August 2026