Shiseido Group Information Security Policy

This policy applies to all individuals working at Shiseido Group companies—including directors, auditors, executive officers, employees, secondees, part-time workers, temporary staff, and dispatched workers (hereinafter collectively referred to as “Employees”). It serves as the fundamental policy for the rules related to the protection of information assets of Shiseido Group companies (including standards, rules, related regulations, guidelines, various operational manuals, and other internal regulations, hereinafter collectively referred to as the “Regulations”).

I. Purpose

This policy aims to protect the information assets and information systems of Shiseido Group companies from various risks such as unauthorized use, loss, destruction, alteration, leakage, and theft. It also seeks to enhance corporate value through the continuous improvement of information security.

II. Definitions

1. "Shiseido Group" refers to the corporate group consisting of Shiseido Company, Limited and its domestic and international subsidiaries and affiliates.
2. "Shiseido Group Companies" refers to each legal entity belonging to the Shiseido Group.
3. "Information Assets" refers to all business-related records, whether in paper or electronic form, including "Confidential Information" and "Personal Information."
4. "Confidential Information" refers to technical, business, and management information that is useful and not publicly known, as well as information obtained under confidentiality obligations from third parties. This includes information protected as "confidential" under applicable laws and regulations in each country or region.
5. "Personal Information" refers to information that can identify a specific individual, such as name, date of birth, address, phone number, image, or other descriptions. This includes information protected as "personal information" under applicable laws and regulations in each country or region.
6. "Information Systems" refers to the hardware, software, and networks that constitute computer systems.
7. "Information Security" refers to the prevention of and compliance with appropriate use of information assets and systems to ensure their availability, confidentiality, and integrity, and protect the information assets and information systems from unauthorized use, loss, destruction, alteration, leakage, and theft.

III. Information Security Governance Structure

1. The Chief Information Technology Officer (CITO), as the head of information security, holds overall responsibility for the handling of information assets and systems across the Shiseido Group. The CITO oversees the establishment and enforcement of rules related to confidential information management, personal information protection, system management, and security measures, as well as the implementation of safety measures and training.
2. Regional headquarters representatives are responsible for managing information assets and systems within their jurisdictions. They must appoint a regional information security head and ensure the enforcement of relevant rules, safety measures, and training.
3. Department and office heads at each Shiseido Group company are responsible for managing the information assets they handle, including inventory, protection, training, self-inspections, and incident response.

4. Information security committees are held regularly or as needed to maintain and improve group-wide security under a unified policy.

IV. Management of Outsourced Parties

1. When outsourcing operations involving personal information (as defined by local laws), confidential information (as defined by Shiseido Group rules), or operations critical to business continuity or quality, Shiseido Group companies must ensure that appropriate security measures are in place and that the outsourcing party meets Shiseido's security standards.
2. The department entering into the outsourcing agreement must verify the security management system of the outsourcing party at the time of contract and periodically thereafter.
3. If the outsourcing party further subcontracts the work, the contracting department may require prior notification and must verify the subcontractor's security management system as necessary.

V. Education, Inspection, and Monitoring

1. Based on the governance structure in Section III, Shiseido Group companies shall regularly provide appropriate training to employees to ensure compliance with this policy and raise awareness.
2. Regular inspections shall be conducted regarding the management of confidential and personal information, system management, and security measures. Any inappropriate handling shall be corrected.
3. Continuous monitoring shall be conducted to ensure the accuracy of data within information assets and systems, prevent unauthorized access, tampering, or destruction, and ensure access is limited to authorized users. In the event that any anomalies are detected, corrective actions shall be taken.
4. Cyber risks related to information assets and systems shall be continuously monitored. In the event of an incident, prompt and appropriate action shall be taken, and accountability to stakeholders shall be fulfilled in accordance with applicable laws and internal rules.

VI. Specific Procedures

1. Shiseido Group companies shall establish necessary rules in accordance with applicable laws and regulations to comply with this policy.
2. The handling of confidential information shall be governed by rules established by each Shiseido Group company.
3. The handling of personal information shall comply with the "Shiseido Group Privacy Rules," which serve as the common standard across the Group. Companies may also establish specific procedures to comply with these rules and applicable laws.

VII. Obligations of Employees

1. Employees must recognize the importance of protecting information assets and comply with laws, this policy, and related rules.
2. If there is a risk of or actual incident involving unauthorized use, loss, destruction, alteration, leakage, or theft of information assets, employees must immediately report it through the appropriate internal channels and, if necessary, to the relevant authorities.
3. Violations of the above may result in disciplinary action, including dismissal, in accordance with internal rules, employment regulations, contracts, or applicable laws.

VIII. Continuous Improvement of Information Security

1. Shiseido Group companies shall continuously review and improve their information security efforts to maintain and enhance the protection of information assets and systems.
2. Rules and operational structures shall be revised as necessary in response to changes in risks, threats, technology, and laws.
3. Based on the results of training, inspections, monitoring, and incident analysis, preventive and corrective measures shall be implemented to enhance the effectiveness of information security.

IX. Revisions

Revisions to this policy shall be proposed by the Information Security Department of Shiseido Company, Limited and approved by the company's highest decision-making body. However, the CITO may approve revisions related to legal amendments or minor business impacts.

■Revision history

Established on August 30, 2004
Revised on June 15, 2011
Revised on February 1, 2013
Revised on April 1, 2016
Fully-revised on Jan 1, 2018
Revised on November 15, 2021
Revised on November 1, 2022
Revised on March 26, 2024
Revised on June 1, 2025