

Compliance and Risk Management

Risk Management

Shiseido's basic policy of risk management.

Compliance

Here are our activities and promotion systems that will ensure employees act with high ethical standards and compliance awareness.

Shiseido Code of Conduct and Ethics

Shiseido Group Policy on Anti-Corruption

Information Security Management

Measures for cyber security and data protection initiatives of Shiseido Group.

Privacy Protection

Privacy initiatives and data protection initiatives of Shiseido Group.

Protection of Intellectual Properties

Shiseido's activities to protect the Group's various information assets.

Tax Policy

Global Tax Policy and Shiseido Group's Tax Policy in the United Kingdom.

Risk Management

The risk management of the Group is primarily focused on "building trust with multiple stakeholders and achieving our medium-to-long-term strategies." We thus consider risks as "uncertainties" that may impact achievement, both potential threats to business as well as potential opportunities. Based on this approach, we have established a risk management structure and have put into place measures for managing such risks proactively and expeditiously. We manage risk-related information centrally through establishing the Risk Management Department at the Company's global headquarters, which reports into the Chief Legal Officer (CLO), and assigning a Risk Management Officer (RMO) in each regional headquarters to ensure implementation of risk countermeasures across the Group. The Global Risk Management & Compliance Committee, chaired by the Global CEO and composed of Executive Officers/Regional CEOs, meets on a regular basis to discuss risks and countermeasures. In addition to this, we have identified "risk owners" for each risk category to clarify responsibility for countermeasures. Moreover, we have implemented a transparent monitoring and communicative framework within members of the above-mentioned Committee and Directors to regularly discuss and assess our progress in addressing these risks.

Company-wide Material Risk Assessment Result

As part of our Enterprise Risk Management activities, we annually identify and assess group material risks. These material risks are incorporated into the Group's business plan.

In fiscal year 2023, material risks were identified through a holistic approach combining multiple and comprehensive methods. Specifically, the HQ Risk Management Department interviewed and discussed with HQ Executive Officers, Regional CEOs, and Directors for their view on Group risks. Regional risk assessments and input from relevant functions, as well as insight from external advisors, were also taken into consideration. As a result, the Risk Management Department identified material risks affecting the key areas of our medium-term strategy, SHIFT 2025 and Beyond. As shown in Table 1 below, the identified material risks were evaluated with the three metrics: "Impact on business," "Likelihood," and "Vulnerability." Subsequently, prioritization and countermeasures were confirmed through the above aforementioned committee meetings and additional individual meetings. Reflecting our corporate policies, personal health (and safety), company assets, business continuity, and impacts to our company reputation are also considered as critical point of views.

Table 1 <Risk evaluation methodology>

| | |
|---------------------------|---|
| Impact on business | <ul style="list-style-type: none">• Quantitative impact on business performance (e.g. topline sales) in case of manifestation• Qualitative impact on our corporate/brand image and culture |
| Likelihood | <ul style="list-style-type: none">• Likelihood and timing of risk manifestation |
| Vulnerability | <ul style="list-style-type: none">• Preparedness against risk• Controllability of the manifestation of the risk due to external factors |

The total of 20 material risks identified through our risk assessment have been organized into three risk categories: "Consumer and Social-related Risks," "Operation & Fundamental Risks," and "Other Risks," as shown in Table 2 below.

Table 2 <Summary of Shiseido Group material risks> ★: Risks that should be prioritized

| | |
|--|--|
| Consumer and Social-related Risks | <ul style="list-style-type: none"> • Changes in Consumer Values★ • New Technology and Speed of Digital Acceleration★ • Pace of Cutting-Edge Innovation★ • Corporate and Brand Reputation★ • Environment (Climate Change, Biodiversity, etc.) • Diversity, Equity & Inclusion (DE&I) • Natural Disaster, Infectious Disease, and Terrorism • Geopolitical Tensions★ |
| Operation & Fundamental Risks | <ul style="list-style-type: none"> • Corporate Culture and Acquisition/Securing Outstanding People★ • Business Structure Transformation★ • Operating Infrastructure★ • Supply Network • Compliance • Regulatory • Quality Assurance • Governance Structure • Information Security★ |
| Other Risks | <ul style="list-style-type: none"> • Exchange Rate Fluctuations • Business Investment • Material Litigation, etc. |

As a noteworthy point of the risk assessment results mentioned above, the individual risks identified are more interlinked than in the past and interdependency of the countermeasures is increasing. In addition to that, we have identified risks that have increased in levels compared to the previous fiscal year: "Changes in Consumer Values," "New Technology and Speed of Digital Acceleration," "Pace of Cutting-Edge Innovation," "Corporate and Brand Reputation," "Geopolitical Tensions," "Corporate Culture and Acquisition/Securing Outstanding People," "Business Structure Transformation," "Operating Infrastructure," and "Information Security." For details on Business and Other Risks, please refer to the URL link below.

At the same time, compliance programs are being or have been prepared for four priority areas: personal data protection, anti-bribery, anti-cartel, and supplier risk reduction.

Incident Response

Shiseido has established the Shiseido Group Crisis Management Policy, a guide for incident response to enable swift and appropriate actions, effective damage control, and early recovery. In Japan, departments in which an incident occurs take initial actions to understand the situation and prevent damage from spreading while promptly reporting to the Risk Management Department. After determining the incident level from the perspectives of severity of damage, possibility of spread, social impact, and other factors, the Risk Management Department assigns members from necessary HQ functions to organize a task force. The task force examines a range of actions to prevent damage from spreading, respond to those affected, and disclose information, while continuously monitoring investigation into cause, progress, and response results and implements reoccurrence prevention measures. Outside of Japan, regional CEOs and RMOs are responsible for leading incident response activities. Significant incidents, such as those which pose a high risk of affecting operations in other regions, are immediately reported to the Risk Management Department at headquarters to enable quick action.

<Shiseido Group Crisis Management Policy>

1. Ensure the safety of employees and their families
2. Preserve company assets
3. Continue operations
4. Earn the trust of stakeholders

Business Continuity Management (BCM)

We have formulated a Business Continuity Plan (BCP) to prepare for major natural disasters and other emergency situations. To enable prompt and appropriate actions by employees according to the BCP in the event of an emergency, we provide regular training and education programs and use the findings from these programs to periodically revise the BCP.

Business Continuity Plan (BCP)

Our BCP is formulated based on the Shiseido Group Crisis Management Policy and the Shiseido Group BCP Concept as described below.

Shiseido Group basic approach to formation of BCP

1. Protecting peoples' lives is the most important thing. Place the highest priority on ensuring the safety of employees and their families and confirm whether they are safe.
After this, when conducting business operations, consider the safety of employees, and prevent secondary disasters.
2. Protect finances, IT systems, buildings, equipment, and other company assets.
3. Perform operations essential to recovery and operations that should be continued in the event of an emergency by the target time, without fail.
4. Through the above, minimize the impact on customers, business partners (clients and suppliers, etc.), shareholders, employees, society, and other stakeholders; prevent damage to corporate value, and earn the trust of society by providing various forms of support to the local community, etc.

Our BCP consists of a "basic plan" serving as a general guide and "action plans" to specifically describe recovery activities to be carried out by each department.

The BCP is designed primarily for natural disasters and other emergency situations, such as large earthquakes, that can seriously affect business continuity. In order to minimize damage and facilitate early recovery, the plan describes "restoration tasks" (necessary actions to restore basic operations) and "business continuity tasks during an emergency" (actions that must be taken to maintain business operations during disaster situations) and sets "recovery time objectives" to complete said tasks. The plan also specifies in phases the information to be collected, items to be decided, and reporting lines. This plan is executed under the leadership of the HQ Emergency Task Force, with members appointed from necessary divisions to address issues related to employees, facilities, communication systems, information disclosure, funding, and consumer relations. The task force undertakes overall management in cooperation with two other special functions: the Product Supply Continuity Task Force (to recover and sustain supply networks) and the SJ Emergency Task Force (to be responsible for Japan Region operations). In addition to the BCP, for sudden and unexpected incidents such as earthquakes, we have separately developed a business continuity plan for emergencies with gradual/long-term impact, such as infectious disease outbreaks, which sets out matters to be considered and implemented by each phase (infectious disease BCP).

HQ Emergency Task Force Drill

The HQ Emergency Task Force Drill is held on a regular basis as training for effective command and appropriate execution of the BCP. Findings from the drill are used to review and revise existing action plans and BCP-related documents. Relevant parties are notified of changes, ensuring the BCP is updated and all are prepared for immediate action.

Emergency education for employees

To promote individual employee awareness and knowledge of emergency preparedness, we run various training and education programs. BCP briefings are given to heads of departments/offices to increase their understanding and ensure swift action by all staff under their leadership in the event of major emergency, under HQ Emergency Task Force instructions. Additionally, safety confirmation drills are conducted for all employees twice a year, and new hire orientation programs include lectures to raise knowledge and awareness of emergency preparedness.

Shiseido Group Policy on Anti-Corruption

Shiseido Group ("Shiseido") hereby establishes the Shiseido Group Policy on Anti-Corruption ("the Policy") by which it will promote efforts to ensure anti-corruption measures and fulfil its social responsibilities.

1. Basic Ideas on Anti-Corruption

Shiseido proclaims in its Shiseido Code of Conduct and Ethics that it abides by the laws of each country and region in which it operates, and maintains sound ethical behavior as well as respecting human rights, in order to be the most trusted beauty company in the world. In particular, Shiseido's basic principles relating to business activities are to engage in fair, transparent, and free competition and appropriate transactions. Therefore, Shiseido proclaims in its Shiseido Code of Conduct and Ethics that it will not provide or accept gifts or entertainment that may cause suspicion regarding our fairness, whether or not the provision or acceptance of such items violates applicable laws and regulations, and whether or not the counterparties are public officials or private entities. Corruption is against Shiseido's basic principles, and Shiseido simply will not tolerate any corruption whatsoever. This Policy is Shiseido's promise to engage in the prevention of corruption, as well as to deliver Shiseido's basic principles on anti-corruption, based on the Shiseido Code of Conduct and Ethics with due consideration for the current state of affairs, under which corruption still remains a global issue.

2. Scope and Application

The Policy will apply to all executives and employees of Shiseido. Shiseido also will require its business partners relating to Shiseido's products and services to comply with the Policy.

3. Prohibition Against Bribery

Shiseido does not give, offer, or promise a bribe, in any form, to any person, whether direct or indirect, nor will it receive, request, or promise to receive any kind of a bribe, irrespective of the name given to it, including without limitation political contributions, donations, charitable activities, sponsorship activities, and kickbacks. Shiseido prohibits all of its executives and employees from engaging in the activities above.

4. Measures for the Prevention of Bribery

Shiseido engages in the measures below to prevent bribery, and continues to promote and enhance such measures in implementing the Policy.

■ Development of a System for the Prevention of Bribery

Shiseido has developed and implemented an effective system for the prevention of bribery, including the development of relevant internal rules and procedures, to ensure the thorough prevention of bribery. The measures include the Framework of Empowerment, credit checks on new accounts, and due diligence in acquisitions.

■ Education and Training

Shiseido offers education and training to all of its executives and employees for purposes of preventing bribery, such as familiarizing such executives and employees with the Policy and relevant internal rules.

■ Risk Assessments and Periodic Reviews

Shiseido periodically evaluates bribery risks and monitors the status of operation of the system for the prevention of bribery, and reviews and improves measures relating to, and control of, the prevention of bribery as required with respect thereto.

■ Proper Record Keeping

Shiseido records all transactions and assets accurately and fairly, and in reasonable detail, in its accounting books and records, to thoroughly prevent bribery and to fulfil accountability therefor.

■ Compliance with Applicable Laws and Regulations

Shiseido complies with the laws and regulations and the rules relating to the prohibition against bribery that are applicable in the countries and regions where it conducts its business activities, including the Foreign Corrupt Practices Act in the U.S., the Bribery Act in the U.K., the commercial bribery rules in the PRC, and the Unfair Competition Prevention Act in Japan.

<Revision History> Established in June 2021
Revised in April 2022

Compliance

We have established the Shiseido Code of Conduct and Ethics to ensure that all Shiseido Group employees act with a strong sense of ethics in all business activities based on THE SHISEIDO PHILOSOPHY. We are implementing education and training programs to put the Shiseido Code of Conduct and Ethics into practice and are striving to earn the trust of all stakeholders by ensuring respect among our diverse employees.

In line with the Shiseido Code of Conduct and Ethics, we have established a basic policy and rules to be complied with by the Shiseido Group as a whole and are working to disseminate these internal rules and regulations, together with THE SHISEIDO PHILOSOPHY, to each Group company and business site. We are also preparing an environment in which each Group company and business site can establish detailed internal regulations.

In addition, to promptly detect any conduct that deviates from the Shiseido Code of Conduct and Ethics and various laws/internal regulations, we have established Hotlines/Helplines and are responding appropriately by closely examining the content of such conduct.

Through such activities to raise awareness of ethics and compliance and the systems that support them, we have created a workplace environment in which every employee can maximize his or her potential.

In OUR PRINCIPLES (TRUST8) , which serves as the working principles that every Shiseido employee must follow, we have included "ACT WITH INTEGRITY" as a Key Behavior, calling on all Shiseido Group employees to "demonstrate humble confidence, integrity, and ethical behavior to earn trust from all stakeholders." With this approach, we are striving to achieve both honest and ethical behavior along with business growth.

Structure

We have placed the Risk Management Department at the global headquarters which reports to CLO (Chief Legal Officer), and RMO (Risk Management Officer) at each regional headquarters.

Activities related to corporate ethics and compliance are being promoted across the Shiseido Group with the support of Risk Management Leaders assigned to each affiliate at the global level and Ethics & Compliance Leaders in Japan. Furthermore, by having the CLO coordinate with the legal managers in each region, we are strengthening our compliance system with laws and regulations.

To oversee compliance and risk management for the Shiseido Group, the Global Risk Management & Compliance Committee, chaired by the Global CEO and composed of Regional CEOs and HQ Executive Officers, has been established at the global headquarters.

The HQ/SJ Compliance Committee oversees compliance in the Japan region.

Compliance Awareness Enhancement Activities

At each regional headquarters, RMOs (Risk Management Officers) take the lead in implementing training with globally common content to promote the understanding and practice of the Shiseido Code of Conduct and Ethics among all employees. We are also promoting the dissemination of the Shiseido Code of Conduct and Ethics to all employees of the Shiseido Group by encouraging temporary employees and others to participate in training.

Additionally, we regularly conduct the Shiseido Group Engagement Survey to continually monitor the status of compliance with the Shiseido Code of Conduct and Ethics and reflect this in training and various compliance activities.

We are also working to ensure thorough compliance with each regulation by conducting various training and awareness-raising activities on a regular basis at each regional headquarters related to the "Compliance Rules

Regarding Prevention of Bribery" and the "Compliance Rules Regarding Prevention of Cartels," which are detailed regulations within the Shiseido Code of Conduct and Ethics.

We conduct human rights awareness training regarding discrimination in the workplace, and with respect to harassment, training is conducted at least once a year at all Shiseido Group business sites in Japan. We also conduct training sessions to improve communication in various settings to build an open and encouraging workplace culture.

In addition to training for all employees, group training is also provided for Executive Officers, managers, and new employees, with content tailored to the characteristics of each position, job level, and business location.

Hotlines/Helplines for Employees

We offer Hotlines/Helplines for the purpose of detecting and correcting violations against the laws and regulations, the Articles of Incorporation, and rules within the Shiseido Group. The Hotlines/Helplines are operated according to internal rules that specify confidentiality, prohibition of disadvantageous treatment or reprisals against whistleblowers/consulters, elimination of conflicts of interest, and the process for handling whistleblowing and consultations, etc. These internal rules are disclosed via the internal intranet so that employees can view them at any time.

Globally, we have established Hotlines/Helplines at each regional affiliate for employees to voice their concerns about or report on words and/or actions which are or may be unethical or in violation of laws in the relevant countries/regions, the internal rules, and the Shiseido Code of Conduct and Ethics. At the global headquarters, the Shiseido Global Hotline has been established to receive reports directly from any employee in the Shiseido Group.

The hotline system in Japan consists of the Shiseido Hotline that deals with general workplace issues and whistleblowing, and the Shiseido Group Whistleblowing to Audit Committee for reports from Japan and overseas relating to directors, corporate executive officers, executive officers, and hotline staff members*. All these Hotlines/Helplines accept anonymous whistleblowing and consultations.

*The Hotlines in Japan accept whistleblowing and consultations from all persons working for Shiseido Group companies in Japan (directors, corporate executive officers, auditors, executive officers, employees, contract employees, temporary employees, former employees within one (1) year of their retirement, and other protected parties as stipulated in the Whistleblower Protection Act).

<Process for Handling Whistleblowing and Consultations>

The division in charge of the Hotlines/Helplines handles whistleblowing and consultations with due care to protect the privacy of those concerned. It accepts whistleblowing and consultations related to all kinds of improper acts, including discrimination, harassment, and bribery, as well as acts that may be regarded as such. And as necessary, a fact-finding investigation of those involved is launched. If improper acts or the like are revealed, we stop such acts immediately and implement corrective measures and reoccurrence prevention measures rapidly in cooperation with the relevant companies, offices, and divisions/departments. We also take disciplinary action against employees who have been involved in such acts in accordance with employment regulations and internal rules. If any cases of disadvantageous treatment, harassment, etc. toward whistleblowers or consultants are identified, we take appropriate relief/restoration measures immediately in cooperation with the relevant companies, offices, and divisions/departments, and take strict measures including any disciplinary punishment against the persons who have engaged in such disadvantageous treatment or harassment.

If the case may pose a risk to our business management, it is promptly reported to management from the divisions/departments. Any serious compliance-related concern is reported to management of the Global Risk Management & Compliance Committee and/or HQ/SJ Compliance Committee, and we work to eliminate the concern immediately and implement corrective measures and reoccurrence prevention measures rapidly in cooperation with the relevant companies, offices, and divisions/departments.

The number of whistleblowing and consultation cases received through the Hotlines/Helplines and the actual responses to them are reported to the HQ/SJ Compliance Committee and Audit Committee on a regular basis annually for the review, management, and supervision of the appropriate operation of the Hotlines/Helplines. In addition, we evaluate the proper operation and feasibility of the Hotlines/Helplines through reviews by external experts such as outside attorneys and make continuous improvements based on such evaluations.

For business partners in Japan, we have established the Shiseido Business Partner Hotline to receive whistleblowing and consultations regarding violations of human rights and compliance by Shiseido Group companies and employees. For more details, please refer to "Social Data."

Mitigating the Risk of Discrimination/Harassment

In order to identify and reduce risks related to discrimination, harassment, and compliance in the workplace, in addition to accepting whistleblowing and consultations, we assess workplace conditions using the Shiseido Group Engagement Survey, etc., which are periodically conducted throughout the Shiseido Group. For companies, offices, and departments where problems have been identified by the surveys, we propose and implement improvement measures based on the survey results.

In addition to this, we provide employee training on issues identified from the analysis of the survey results to prevent discrimination, harassment, and compliance risks.

Efforts to Eliminate Anti-Social Forces

The Shiseido Code of Conduct and Ethics states the following: "We do not work with individuals or organizations that engage in illegal activities, such as threatening public order or safety. We also do not respond to any requests for money or support from such individuals or organizations."

In the Japan region, a coordination office is established in the Risk Management Department to effectively gather information and maintain manuals on the intranet on how to cope with such forces. We are taking measures to strengthen its collection of outside information and cooperation with external organizations by coordinating with local police offices and being a member of an organization that promotes the exclusion of anti-social forces.

Information Security Management

1. Policy Related to Information Security

The Shiseido Group (hereafter "Group") establishes "Shiseido Group Information Security Policy" for all people working in the Group to protect and maintain various essential information assets owned by business sites of the Group by setting robust information security. Under this Group-wide basic policy, we strive to manage and operate various information assets.

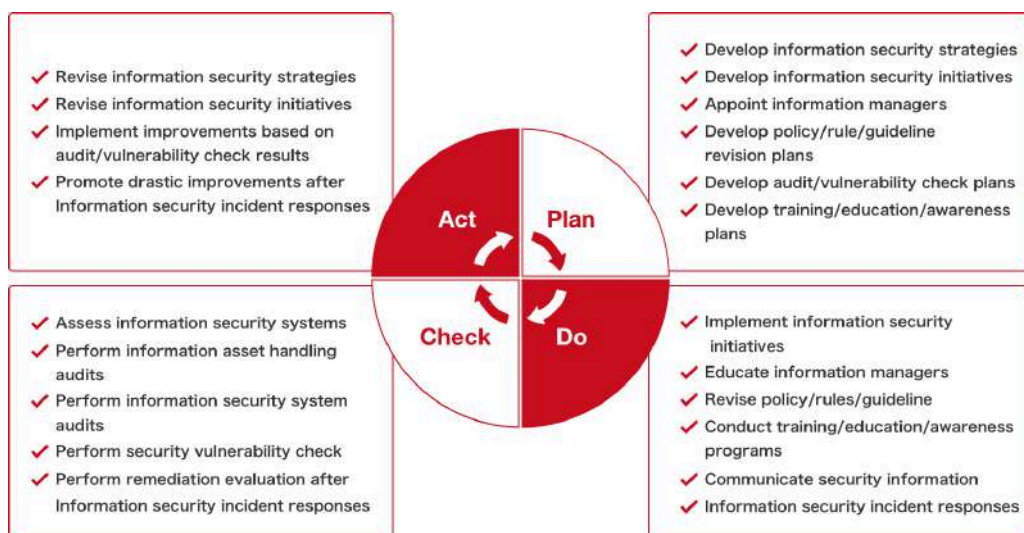
2. Information Security Management Systems

(1) Management structure

In the Shiseido Group, the Chief Information Technology Officer (CITO), the representative executive officer, is responsible for the establishment of the information security management system. More so, the CITO has authority over and is responsible for the establishment and operation of regulations related to confidential information management, data protection, and security measures for information systems, as well as the implementation of safety measures and education and training. In addition, the head of the Information Security Department is responsible for promoting and implementing these measures. Thus, the Chief Executive Officer (CEO) is ultimately responsible for information security.

The representative of each regional headquarter, as the chief administrator for the handling of information assets and systems in the region, is responsible for overall information security, including confidential information management, data protection, security measures on information systems, and education and training. Information security contacts have been appointed in each region, and they are working to maintain and improve the Group's overall information security activities in cooperation with HQ.

The heads of departments of each Group company confirm the protection and management of information assets handled in their departments on a regular basis, provide education and training to employees, and respond to security incidents.



(2) Development of policies and rules

To promote information security management systems, we refer to several major related guidelines or best practices such as the ISO 31000 international standard for risk management, the ISO 27001 international standard for information security management systems, the NIST Cybersecurity Framework of the National Institute of Standards and Technology, the CIS Controls of the Center for Internet Security*, and the Cybersecurity Management Guidelines of Ministry of Economy, Trade and Industry.

Furthermore, specific guidelines and rules have been formulated. These include the above-mentioned "Shiseido Group Information Security Policy," in addition to rules and regulations regarding confidential information management, data protection and security measures on information systems. We are working to promote compliance with these guidelines and rules on a global scale by encouraging the engagement of overseas offices.

To ensure information security in activities involving external business partners, we ask them to observe the "Shiseido Group Supplier Code of Conduct", which includes requirements for proper handling of confidential information and personal information. When outsourcing important operations, we check the information security management systems of the business partners before we execute a service agreement requesting them to take appropriate safety management measures.

*Center for Internet Security (CIS): An organization established in 2000 by the National Security Agency (NSA), the Defense Information Systems Agency (DISA), the National Institute of Standards and Technology (NIST), and other government agencies, businesses, and academic institutions to work together on Internet security standards.



Structure of Information Security Rules

3.Information Security Enhancement Initiatives

(1) Employee training/education/awareness

The Shiseido Group conducts information security e-learning programs and group sessions on a regular basis to help employees increase their awareness and knowledge of information security. We provide guidance to new graduate and mid-career hires during orientation sessions to instill the importance of information security management in our personnel from the time they start with the Group.

To keep employees updated on information security issues, the latest information is posted on our internal portal.

(2) Promotion of security by design

The Shiseido Group has developed internal systems and processes that enable the Information Security department to be involved in the development of new business or services from scratch so that necessary information security measures can be taken at the planning/designing stage.

(3) Supply chain security

At the Shiseido Group, when outsourcing work that involves the handling of personal information as defined by the laws and regulations of each country or region, the handling of confidential information as defined by the Policy and Rules of the Shiseido Group, or operations that are considered to be significantly related to the business continuity and

quality of goods and services of the Shiseido Group, we appropriately manage and supervise the third parties to ensure the information security of the outsourced work.

(4) Monitoring activities

At the Shiseido Group, we ensure the proper handling of information assets as well as the implementation of appropriate information security measures for information systems development, operation, and management. Assessment on information systems and related operations are performed on the risk basis, where supervision is conducted over improvements to any issue detected. We also conduct security assessments of the factory system environment as needed to ensure information security in production activities.

Also, we periodically perform vulnerability checks on information system infrastructures and application programs, and if vulnerability issues are detected, instructions and improvement advice are provided. In addition, we constantly monitor information security using external threat intelligence services.

For business partners to whom we outsource important operations, we regularly check their information security management systems even after contracts are concluded.

(5) Information security incident response

In the Shiseido Group, the Information Security Department serves as the contact point for incidents related to information security. We respond to incidents by coordinating with relevant internal departments according to the severity of the incidents.

Shiseido has a CSIRT (Computer Security Incident Response Team) , which is an organization that deals with computer security incidents, and conducts activities such as collecting, analyzing, and responding to incident-related information, vulnerability information, and information on predictive signs of attacks. Shiseido has registered with the Nippon CSIRT Association* (Shiseido CSIRT) to share information with relevant agencies and with similar departments at other companies.

The Information Security department works to improve emergency response capabilities through organizing periodic drills (provided more than twice a year by several organizations including the Nippon CSIRT Association and a forensic service provider) and revising associated sections of the manual based on issues revealed through such training opportunities. We also conduct incident response trainings for factories as needed to ensure information security related to production activities.

* Nippon CSIRT Association is an organization that promotes close collaboration and problem solving among CSIRTs at business enterprises.



(6) Third-party assessment

To verify that the Shiseido Group's implementation of its information security initiatives and management systems are appropriate, we enlist external experts to conduct an assessment if necessary. Issues and challenges identified through the assessment are then considered to develop information security strategies and initiatives.

Privacy Protection

1. Privacy Principles

The Shiseido Group (hereafter "Group") is fully aware of the importance of personal information obtained through business activities, considers ensuring the safety of such information to be its social responsibility, and makes sure to implement privacy protection on a Group-wide basis under the "Shiseido Group Privacy Rules," which must be followed by all people working for the Group.

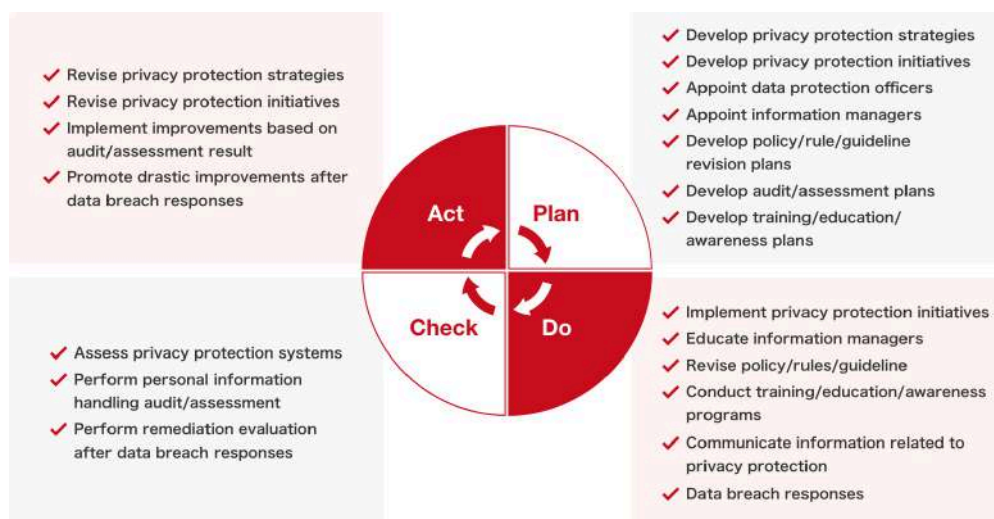
Also, the "Shiseido Global Privacy Principles," which were established as the Group's common privacy principles, as well as each Group company's privacy policies are publicly disclosed.

2. Privacy Protection Management Systems

(1) Management structure

The Shiseido Group has privacy protection systems in place under the leadership of the Chief Legal Officer (CLO) and the Legal Department. The CLO has ultimate responsibility for privacy protection and engages in the planning and implementation of related strategies and initiatives while communicating with the management team.

The Chief Information Technology Officer (CITO) is responsible for the implementation and oversight of security measures to protect personal information. In addition, the Vice President of the Information Security Department is responsible for promoting and executing these measures. Representatives of the overseas regional headquarters are responsible for managing the handling of personal information within their jurisdictions. The heads of departments of each Group company confirm the protection and management of personal information handled in their departments on a regular basis, provide education and training to employees, and respond to security incidents.



(2) Development of policies and rules

To promote information security management systems, we refer to several major related guidelines or best practices such as the ISO 31000 international standard for risk management, the ISO 27001 international standard for information security management systems, the NIST Cybersecurity Framework of the National Institute of Standards

and Technology, the CIS Controls of the Center for Internet Security*, and the Cybersecurity Management Guidelines of Ministry of Economy, Trade and Industry.

Furthermore, specific guidelines and rules have been formulated. These include the above-mentioned "Shiseido Group Information Security Policy," in addition to rules and regulations regarding confidential information management, data protection, and security measures on information systems. We are working to promote compliance with these guidelines and rules on a global scale by encouraging the engagement of overseas offices.

To ensure information security in activities involving external business partners, we ask them to observe the "Shiseido Group Supplier Code of Conduct," which includes requirements for proper handling of confidential information and personal information. When outsourcing important operations, we check the information security management systems of the business partners before we execute a service agreement requesting them to take appropriate safety management measures.

*Center for Internet Security (CIS): An organization established in 2000 by the National Security Agency (NSA), the Defense Information Systems Agency (DISA), the National Institute of Standards and Technology (NIST), and other government agencies, businesses, and academic institutions to work together on Internet security standards.

3. Initiatives to Promote Privacy Protection

(1) Employee training/education/awareness

The Shiseido Group conducts e-learning programs and holds group sessions on a regular basis to help employees increase their awareness and knowledge of privacy protection. We provide guidance to new graduate and mid-career hires during orientation sessions to instill the importance of privacy protection in our personnel from the time they start with the Group.

To keep employees updated on privacy protection issues, the latest information is posted on our internal portal.

(2) Promotion of privacy by design

The Shiseido Group has developed internal systems and processes that enable the Legal and Information Security departments to be involved in the development of new business or services from the beginning so that necessary privacy protection measures can be taken at the planning/designing stage.

(3) Supply chain security

At the Shiseido Group, when entrusting all or part of the handling of Personal Information to a third party, we appropriately manage and supervise the entrusted third party to ensure the security management of the Personal Information.

(4) Monitoring activities

The Shiseido Group periodically checks and assesses its information assets including personal information. Also, to check if privacy protection measures have been implemented appropriately in all offices, departments, and affiliates, we conduct a risk-based assessment of their information systems and issue an order for improvement if a problem is detected. As for our business partners to whom we outsource the handling of personal information, we check their information security management systems and operational status thereof on a regular basis even after executing service agreements with them.

(5) Privacy incident response

The Shiseido Group has established a system to respond to incidents related to personal information. In the event of a possible data breach or violation of laws and regulations, the Legal, Risk Management, Information Security, Information Systems, and other departments work together to respond to the incident.

If a privacy incident such as personal information breach occurs, the Group will report to the authorities concerned and data subjects, following the laws and regulations of each country/region.

(6) Third-party assessment

To verify that the Shiseido Group's implementation of its privacy protection initiatives and management systems are appropriate, we enlist external experts to conduct an assessment if necessary. Issues and challenges identified through the assessments are then considered to develop privacy protection strategies and initiatives.

(7) Disciplinary action

Violations of Shiseido Group's privacy principles, policies, and practices may be subject to disciplinary action, including potential termination, in accordance with applicable laws.

Protection of Intellectual Properties

Shiseido Group invests in R&D and marketing to develop innovative technologies and increase our brands' value. Therefore, enhancing our Intellectual Property (IP) value is a crucial activity for our sustainable growth. IP includes intangible assets such as patents, trademarks, copyrights, industrial designs, trade secrets, etc. We protect our inventions, brands, marketing ideas and other IP outcomes properly, as these assets play key roles in our future success. We also respect third parties' IP rights and provide internal trainings for our employees to raise the awareness.

Note: Intellectual properties refer to intellectual property rights (patent rights, trademark, design rights, copyrights, etc.) and business confidentiality (know-how, etc.).

Tax Policy

Shiseido's Tax Policy

Shiseido Group's Tax policy in the United Kingdom

Global Tax Policy

Shiseido Group complies with the laws and regulations in all countries in which we run business. THE SHISEIDO PHILOSOPHY, "OUR MISSION, DNA and PRINCIPLES" and Shiseido Code of Conduct and Ethics sets forth the code of conduct for all employees to ensure our compliance to the law. In addition, we set the global tax policy here to ensure the tax transparency. We aim to maximize the shareholder value by mitigating the tax risk globally.

Tax Principles

Compliance

We fully comply with the international guideline established by the OECD and the tax laws and regulations in all countries in which we run business. Furthermore, we also understand and respect the underlying intentions of the laws and regulations. We will not engage in abusive tax evasion through tax structure without commercial substance or shift profit to countries with low tax rates.

Governance

The discipline for the compliance and accurate tax accounting is set forth in Shiseido Code of Conduct and Ethics and shared with all employees to ensure tax transparency. We will resolve the tax issues by managing the tax risk locally by each RHQ and sharing the tax information globally in a timely manner.

Responsibilities and Organization for the Tax Compliance

Tax compliance is under the responsibility of the CFO. To manage the global tax risk effectively, tax team of global headquarters manages the tax compliance of the group, and CFOs at each regional headquarters manage the tax compliance in their region. Employees with tax expertise are assigned as necessary for the smooth operation of our global tax risk management organization. We provide trainings to employees to raise awareness on the tax compliance.

Maximization of the Shareholder Value

In order to improve the shareholder value, we strengthen the governance and save tax by utilizing tax incentives where applicable in the ordinary course of business.

Transfer Pricing

Our transfer pricing policy is in accordance with the OECD Transfer Pricing Guidelines and the laws and regulations of each country in which we run business. The pricing for the intercompany transaction is determined under the arm's length principle and based on the policy.

Tax Havens

We do not utilize the tax havens to solely avoid tax.

Relationship with the Tax Authorities

We cooperate with the tax authorities and build a good relationship with them.

Shiseido UK Tax Policy

SHISEIDO Group complies with the laws and regulations in all countries in which we run businesses. THE SHISEIDO PHILOSOPHY, "OUR MISSION, DNA and PRINCIPLES" and Shiseido Code of Conduct and Ethics sets forth the code of conduct for all employees to ensure our compliance to the law. In addition, we set the global tax policy to ensure tax transparency. The following document lays out the company's strategy and approach in 2025 for the United Kingdom. We publish this statement to meet our obligation under Paragraphs 19(2) and 22(2) of Schedule 19 of FA2016."

Governance and Responsibilities

The discipline for the compliance and accurate tax accounting is set forth in Shiseido Code of Conduct and Ethics and shared with all employees to ensure tax transparency.

The Chief Financial Officer (CFO) / The Finance Director (FD) and the Group Financial Controller(GFC) is ultimately responsible for Shiseido's overall tax risks. We will resolve the tax issues by managing the tax risk locally by each Regional Head Quarters (RHQ) and sharing the tax information globally in a timely manner.

Tax compliance is under the responsibility of the CFO and/or the FD. To manage the global tax risk effectively, the tax team of Global Head Quarters (HQ) manages the tax compliance of the group, and CFOs and/or the FDs at each RHQ manage the tax compliance in their region. Each RHQ assigns the employees with tax expertise as necessary. We provide trainings to employees to raise awareness on the tax compliance.

Tax Planning

Shiseido's tax arrangements are based on its commercial business and economic activities. Shiseido monitors and reviews its operations in the UK and elsewhere to realign its tax arrangements when necessary to be compliant with the tax rules and regulations.

Globally, we comply with the international guideline established by the Organisation for Economic Co-operation (OECD) and the laws and regulations in all countries in which we run businesses.

Our transfer pricing policy is in accordance with the OECD Transfer Pricing Guidelines and the laws and regulations of each country in which we run business. The pricing for the intercompany transaction is determined based on the policy. We adhere to the UK Double Tax Treaties and the relevant guidance issued by the OECD for international tax matters.

Tax Risk

We aim to maximize the shareholder value by mitigating the tax risk globally.

We will resolve the tax issues by managing the tax risk locally by each RHQ and sharing the tax information globally in a timely manner.

Where there is complexity or uncertainty we may seek support from external advisors.

Relationship with Her Majesty's Revenue & Customs (HMRC)

We seek to build and sustain relationships with government and HMRC that are constructive and based on mutual respect. We work collaboratively wherever possible to resolve disputes and to achieve early agreement and certainty.