SHISEIDO

Information Security Report 2024

COO Message

Working from our mission, “BEAUTY INNOVATIONS FOR A BETTER WORLD,” the Shiseido Group will endeavor to enhance our information security measures.

Thank you for taking the time to read the Shiseido Group’s information security report.

Since its founding in 1872, the Shiseido Group has developed businesses around the world in a range of domains, theming its efforts on “beauty.” Now, at the close of the COVID-19 pandemic that began in 2020, we face a period of significant change in both Shiseido business and in the way that the employees of the Shiseido Group work. With the transition to digital technology progressing rapidly, new touchpoints are being established between Shiseido and consumers on a daily basis, both through active developments in e-commerce, and through a range of digital platforms, including social networking and media services such as YouTube, TikTok, X (formerly Twitter), and Instagram. We are also making concrete progress with the creation of new beauty-related experiences, such as the launch of our members-only “Beauty Key” service, which links customer information under a single ID, and the unique “Beauty DNA Program,” which combines AI technology with the skin science research that Shiseido has cultivated over many years. Although the way we work within Shiseido was previously predicated on employees coming to the office, we are now transitioning to a range of working styles that combine working from home with commuting to the office. We are aware that this rapid digitalization and the shift to new ways of living have brought with them an ever-increasing need for information security measures. We discuss issues with management in Japan and overseas, referring to the Cybersecurity Management Guidelines formulated by the Ministry of Economy, Trade, and Industry, and work diligently to implement any information security measures necessary in a timely manner.

The Shiseido Group has set “Becoming number one in the world in the skin beauty domain, as a Personal Beauty Wellness Company” as its goal for 2030. To the end, it is essential that we deploy a globally standard platform of the latest IT and digital technology to support business growth and the creation of customer touchpoints, and further utilize the range of data that this will allow us to acquire. Of course, this is predicated on the protection of our systems and data in a safe, secure environment. By strengthening the information security on which this is founded, we will continue to do our very best to earn and retain the trust of consumers, our clients, and our business partners.

This report looks at the latest initiatives of the Shiseido Group with regard to information security.

Kentaro Fujiwara
Director, Representative Corporate Executive Officer, President and COO
Shiseido Company, Limited

Message from the Officer in charge of Information Security

Executives and employees work together to promote information security measures to ensure that Shiseido Group products and services can be used with peace of mind.

Thank you for your interest in the Shiseido Group's Information Security Report for 2024. I am Atsunori Takano, in charge of information security and information systems at the Shiseido Group.

As stated in the message from President and COO Fujiwara, who has overall responsibility for information security at the Shiseido Group, we are committed to information security and its enhancement as a crucial aspect of our business activities. Especially in recent years, the rapid evolution of technology is closely related to business activities, while on the other hand, various attacks including cyber attacks from outside the company are becoming highly sophisticated.

Face with such circumstances, we have established a system to monitor our defense activities 24/7, incorporating multi-layered defenses from the perspectives of people, process, and data, so that we can properly protect personal information entrusted to us by many consumers, customers, and business partners, as well as our business-critical confidential data.

In terms of people and process, we issue a detailed internal information security report to our head office executives and CEOs in overseas regions every quarter to raise awareness of our activities, and we are working to share and deploy best practices horizontally throughout the Shiseido Group. Of course, we regularly conduct information security training for all employees worldwide and strive to keep them aware of information security as it pertains to their business activities.

In terms of data, we constantly monitor system vulnerabilities and aim to achieve industry-leading benchmark scores through timely remediation of those vulnerabilities and by engaging external organizations to conduct benchmarking of our company.

We are keenly aware that there is no final goal in strengthening and working on information security, and that it is essential to continuously seek improvement. We will continue to introduce our latest initiatives as the Shiseido Group through this report every year. We will work together as a group to ensure that you can continue to trust us in our business activities and utilize our products and services with peace of mind. We would be delighted if read this report helps you to gain an understanding of our information security initiatives.

Atsunori Takano
Executive Officer
Chief Information Technology Officer
Shiseido Company, Limited

Contents

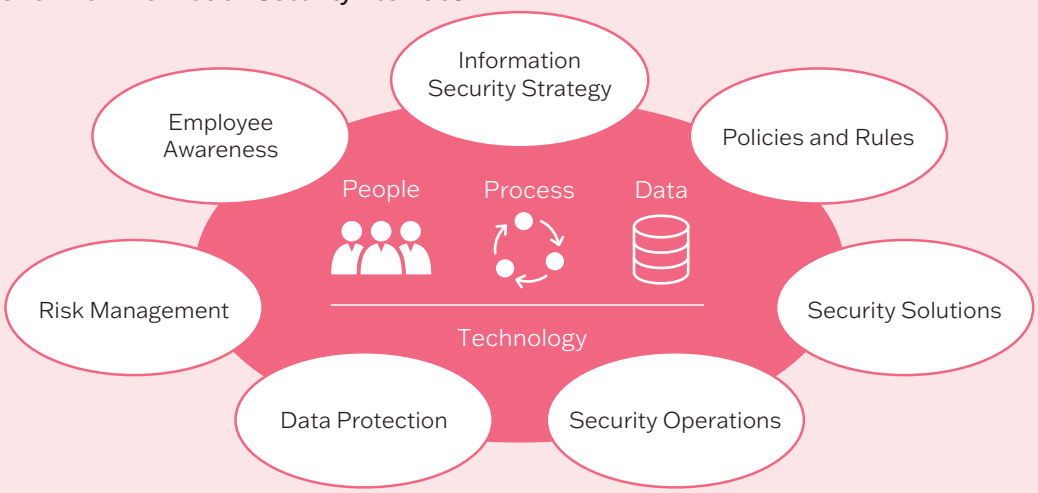
Publication

The Shiseido Group continues to work towards the creation of new value by fusing the latest digital innovations with a diverse range of technologies and insights that lead towards customers' beauty. At the same time, we have been striving to enhance our information systems and information security, aiming to create a better platform that serves as the foundation for these initiatives. This report is part of the information we disclose to our stakeholders and focuses on Shiseido's information security activities. We have edited this document based on the Shiseido Group's Information Security activities, referring to the "Information Security Report Model" issued by the Ministry of Economy, Trade and Industry. To ensure that this report is easy for all stakeholders to understand, we have endeavored to provide readily comprehensible text and visuals for each item.

Reporting period
Generally, fiscal 2023 (January to December 2023)
Subject of report
Shiseido Company, Limited, and Group Companies
Where individual measures, etc., differ from the above, these differences are stated.

Shiseido Website Information Security Management
https://corp.shiseido.com/jp/sustainability/compliance/security.html

Framework for Information Security Activities

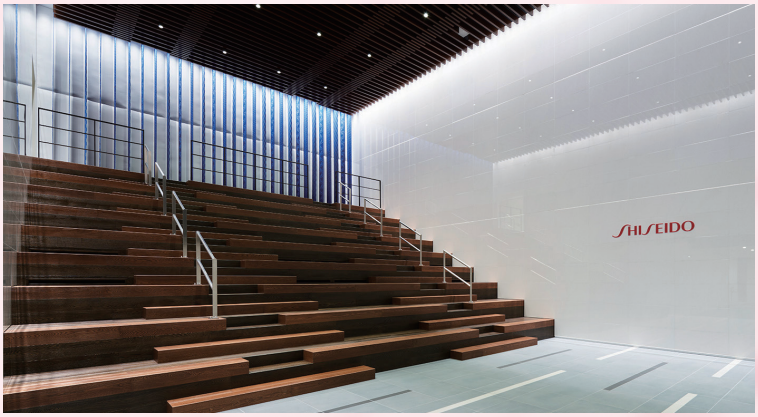


Information Security Governance

Information Security Policy

Protecting the privacy of customers, business partners, and employees is an extremely important responsibility for any company. Moreover, appropriate management of confidential information related to research and development as well as sales and marketing is essential to improving the competitive abilities of a business. Based on that awareness, the Shiseido Group has established the “Shiseido Group Information Security Policy,” which applies to all employees, and is working to manage and operate information assets of all kinds based on a policy that is consistent throughout the Group.

The nature of cyber threats is constantly transforming, set against a background of a changing international situation and legal systems as well as technological progress. Furthermore, in recent years the way people work has changed significantly, with more electing to work from home. We are continuously revising our information security policies to deal with security risks that accompany environmental changes inside and outside the company.



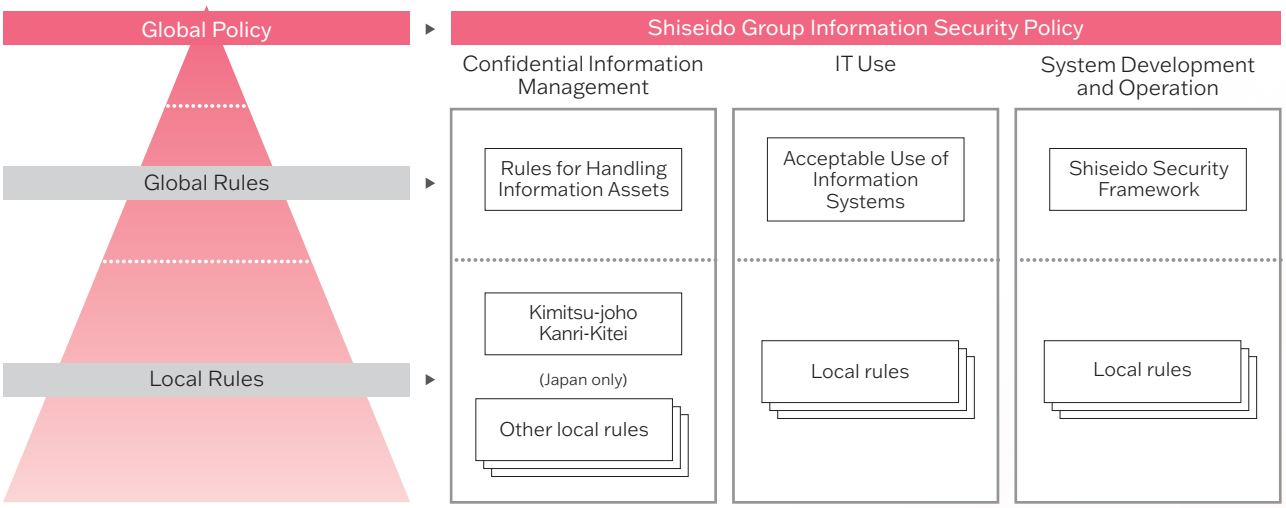
Policies and Rules

The Shiseido Group has established a set of group-wide rules for management areas such as confidential information management, use of information technology, and system development and operation. These are treated as global rules that are complied with at all sites, including our offices overseas.

Conversely, information security also requires dealing with the legal frameworks, business practices, and system environments of each region. Accordingly, we have put in place local rules at each regional headquarter and Group company to promote management that reflects the actual conditions in each country and region.

When creating our policies and rules on information security, we referred to the ISO 31000 international standard for risk management, the ISO 27001 international certification standard for information security, the NIST Cyber Security Framework from the United States National Institute of Standards and Technology (NIST), CIS Controls from the Center for Internet Security*, the Cybersecurity Management Guidelines from the Ministry of Economy, Trade and Industry, and established best practices.

*A United States organization established in 2000 with the goal of working to standardize internet security in cooperation with business, academic institutions, and government agencies such as the National Security Agency (NSA), Defense Information Systems Agency (DISA), and NIST.



Management Framework

Group-wide Management

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 Operating Officer (COO), the representative executive officer, is ultimately responsible for information security.

Additionally, we have established an Information Security Department within Shiseido headquarter. Semiannually, this department reports to the Risk Management Department on the status of incidents occurring, and shares information through this department with the Board of Directors.

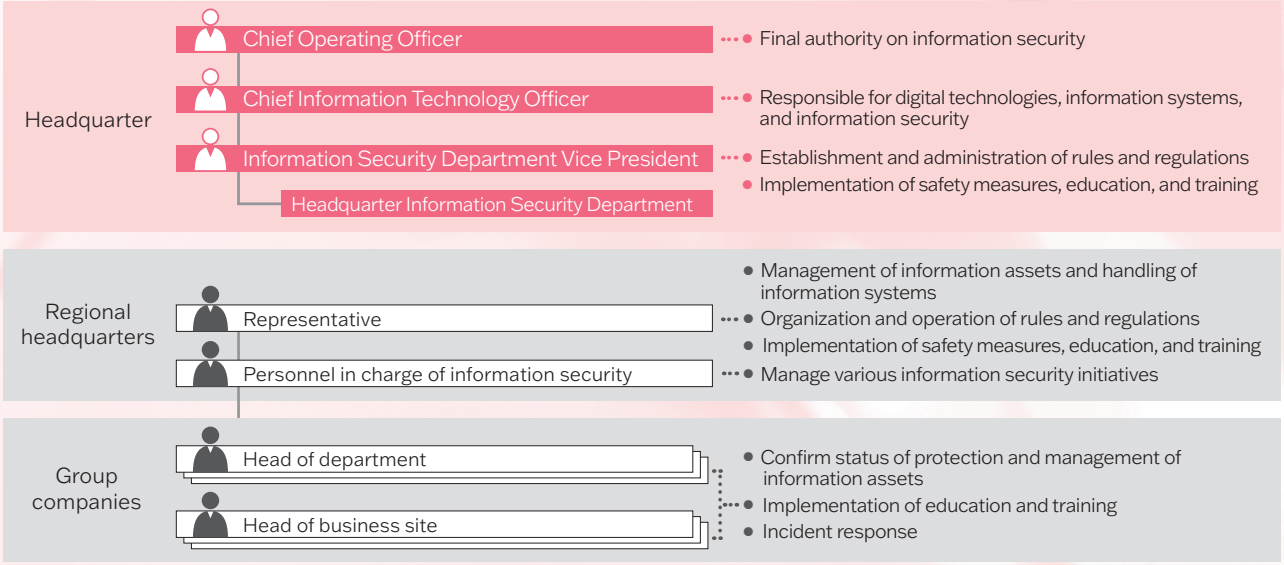
Management at Regional Headquaters

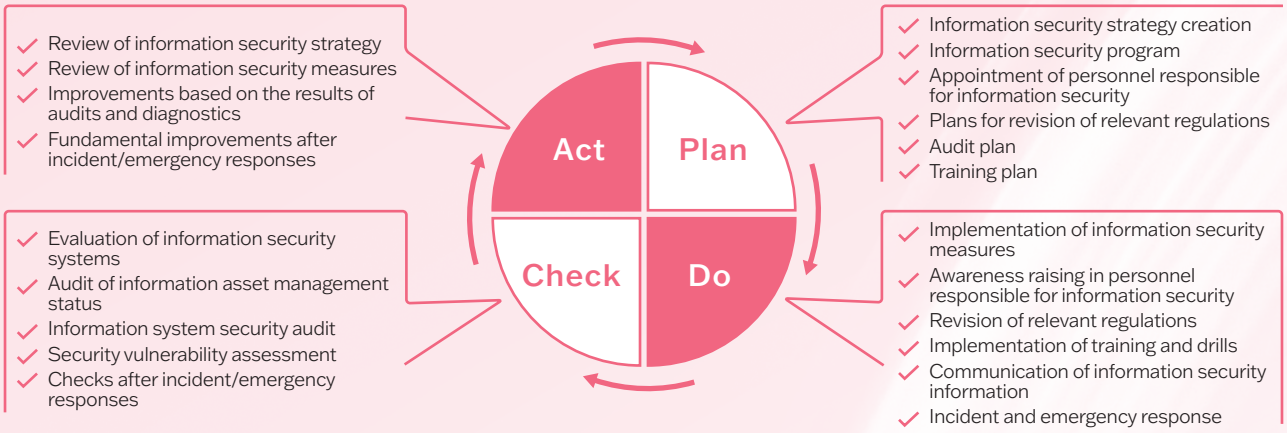
In each regional headquarter, the representative is responsible for managing the handling of information assets and information systems within their jurisdiction. This includes the management of confidential information and information systems, the establishment and operation of regulations, the implementation of security measures, and the execution of education and training. They are responsible for all aspects of information security.

Furthermore, each regional headquarter has designated personnel in charge of information security, who are working in collaboration with Shiseido's headquarters to continuously improve information security activities.

Management at Group Companies

The heads of each department and office within the Shiseido Group companies are responsible for regularly checking the protection and management status of the information assets handled in their departments and offices. They also bear responsibility for employee education and training, as well as responses in the event of an incident.



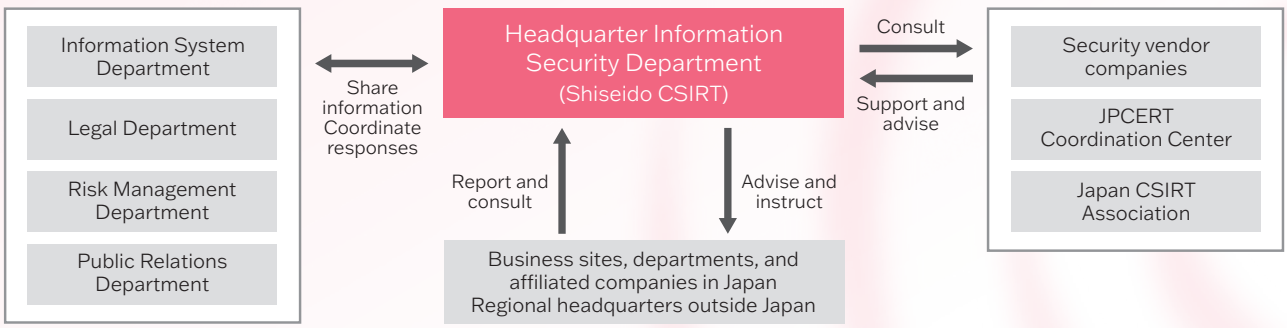


Incident Response Process

In the event of an incident related to information security, the Information Security Department acts as the point of contact, cooperating with the Risk Management Department and Information Systems Department as required by the effect of the incident. When incidents at overseas sites occur, personnel and teams responsible for information security at each regional headquarter act as the point of contact, working with the Information Security Department and other organizations to respond as necessary.

We have also established a Shiseido Computer Security Incident Response Team (Shiseido CSIRT) comprising members of multiple different departments including the Information Security Department, Risk Management Department, and the Information Systems Department, allowing us to respond to security incidents rapidly. In addition to collecting and analyzing incident-related information and information on vulnerabilities and predicting attacks, and the executing the required countermeasures, we have worked with specialist external organizations to implement incidence response training attended by the personnel responsible for security in each region. Shiseido CSIRT is a registered member of the Nippon CSIRT Association and participates in various working groups and yearly multidisciplinary training exercises. Furthermore, we are in close communication with other external specialist information security organizations and the information security departments at other companies.

In addition, we hold incident response training with the information Security Department at least twice a year and reflect the points that these drills confirm as requiring improvement in the Incident Response Manual as needed to enhance our ability to respond.



Information Security Management at Production Facilities

To allow us to offer a stable supply of Shiseido products to consumers, we are strengthening security measures at production facilities. As part of this initiative, we have been conducting a series of factory security assessments at our factories in Japan and overseas since 2020.

We completed assessments of all production facilities in Japan in fiscal 2023. Monthly meetings between factory groups tasked with information security and the Information Security Department are scheduled for factories in Japan for which assessments have been completed to strengthen security measures after assessment and promote reliable corrective measures. Security incident response training is also held annually to check the response systems and processes used when security incidents occur onsite and improve our ability to handle them.

Information Security in the Supply Chain

We are working to manage and monitor cases where business partners utilize personal or confidential information possessed by the Shiseido Group, or where tasks with a significant effect on the business continuity or quality assurance of the Group are outsourced to business partners, in an effort to ensure that information security is protected appropriately in the execution of the outsourced tasks. The Shiseido Group Supplier Code of Conduct clearly defines the protection of confidential information and personal information. We request that all business partners comply with the Code of Conduct and require that those who are entrusted with tasks involving the handling of important information check their information security systems and put security measures in place as necessary.

Employee Awareness

The Shiseido Group has introduced a globally standard e-learning platform to improve employee awareness of information security and conducts quality-assured training in all regions. The Group has also put systems in place that provide real-time comprehension of the state of training and participation rates in each country.

In addition to e-learning, we have also instituted programs to explain the Group's rules and policies on information security during onboarding training for new career hires as well as onsite training for new employees in the basics of security. Moreover, members of the Information Security Department provide onsite lectures on security to business departments periodically. Based on the latest threat intelligence, Information Security Department members give in-person lectures on threat information that each department should be aware of. At each of these onsite lectures, there is interactive communication that helps improve employee awareness.

Additionally, regional headquarters overseas are also implementing original measures. The Americas regional headquarter is engaged in quarterly e-mail response training, while the EMEA regional headquarter uses gamification and other similar measures to improve employee motivation.

Major e-learning programs on information security

Training on information security basics	Conducted once annually for all employees at headquarter in each region
Training on specific themes based on threat trends	Held as required based on the external environment and threat trends **Examples of implementation** Training on e-mail-related issues such as Business Email Compromise (BEC)

Information Security Operation

Management of Information Assets

The Shiseido Group has established rules for setting appropriate levels of confidentiality based on the importance of information assets, and has put four levels of confidentiality in place: “Public information,” “Internal information,” “Confidential information,” and “Highly confidential information.” By categorizing our information assets appropriately, applying labels, and encrypting as required, we do our utmost to prevent leakage of important information assets.

Additionally, we assign only the minimum rights required to access information assets necessary for each person to carry out their respective roles. We also set rules regarding disposal and data retention periods for information assets and are strengthening our systems for monitoring when uploading information assets to unauthorized public cloud environments.

Monitoring Activities

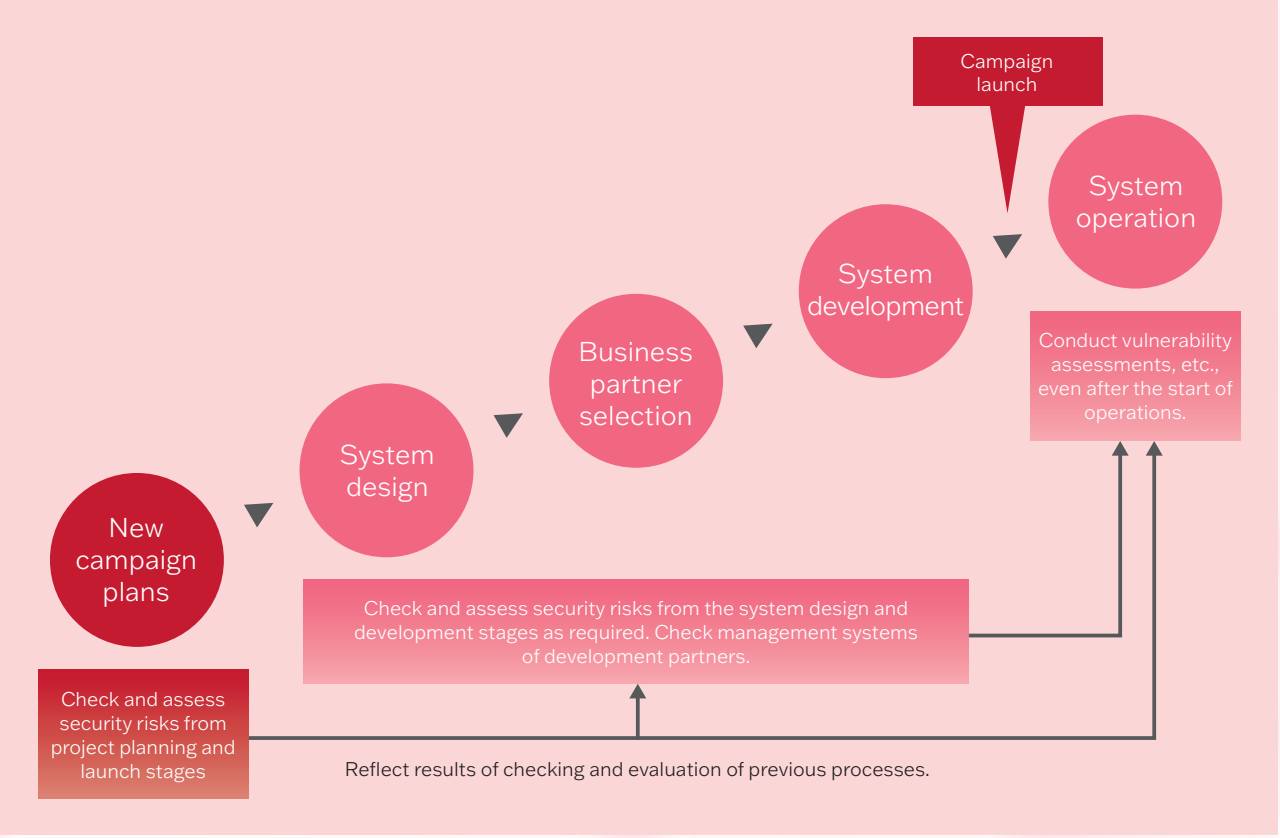
The Shiseido Group evaluates information systems and associated operational processes and works to improve any corrective measures found by assessment.

Additionally, we conduct regular checks of information system platforms and applications for vulnerabilities and implement measures to address any that are detected. Moreover, in addition to constant monitoring using threat intelligence, we utilize external specialists to conduct third-party evaluations of systems and measures related to information security and reflect suggestions for improvements and enhancements identified in these evaluations in the development of our information security strategy. We have established security monitoring systems that cover all regional headquarters around the world, and are working daily to improve the accuracy of our monitoring.

Security & Privacy by Design

Shiseido has processes in place to allow relevant departments to apply to the Information Security Department in advance for the construction of new systems, use of unauthorized cloud services, and implementation of new campaigns through mediums such as social networking services. After application, the Information Security Department checks and evaluates risks from the standpoint of information security, with each project only moving forward when these personnel determine that these risks have been mitigated to below a certain level. Members from the Information Security Department participate from the start and planning stages of projects and take time to assess and evaluate risks, allowing new initiatives to be launched safely without the need for rework.

In September 2022 we installed workflow systems with a view to improving operational efficiency within the Information Security Department. These will enhance information retrieval and allow centralized management of inquiries and requests for assistance from various Shiseido departments.



Information Security Risk Management

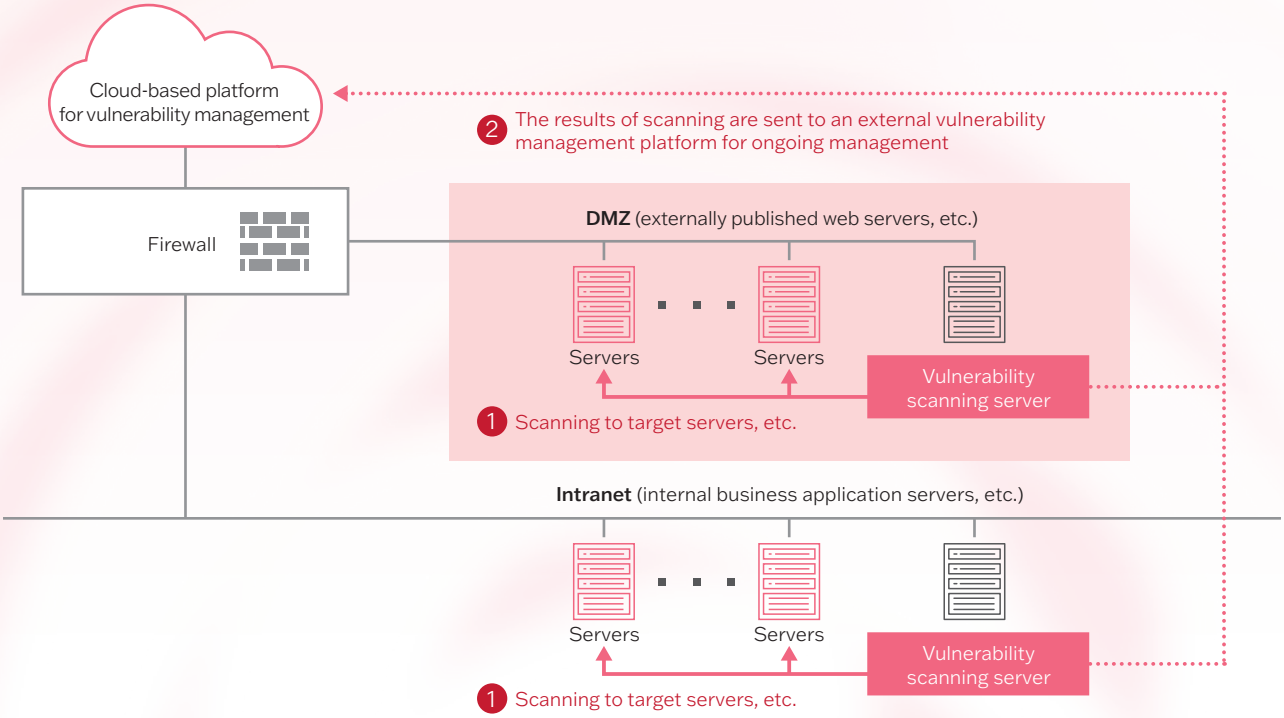
Managing risks related to information security in an appropriate manner requires personnel to maintain specialist knowledge and to keep up with information on the new threats that emerge daily, as well as possess a broad range of practical experience. Conversely, it is not easy to recruit and retain security personnel of this caliber with the required knowledge and experience in-house. Moreover, managerial decisions regarding investment in information security requires accurate evaluation of both threat trends in the external environment and the status of currently implemented countermeasures, and a quantitative grasp of the risk level.

The Shiseido Group defines priority items for monitoring of risks related to information security and has introduced a unique system of monthly evaluations of each item based on set standards, without relying on the experience of individual people. This evaluation also utilizes multiple external sources of threat intelligence to provide a more accurate, multifaceted system of evaluation, allowing timely assessment of temporal changes in risk levels and the need for additional countermeasures. Moreover, external experts also conduct reviews, with the goal of enhancing and improving evaluations.

Management of IT Infrastructure Vulnerabilities

Even though IT infrastructure may have been secure when it was constructed, rapid responses are required when critical vulnerabilities are identified. However, the nature of vulnerabilities disclosed varies widely, as does their impact, making it impractical to address all of them.

Accordingly, the Shiseido Group has deployed tools that assign priorities to vulnerabilities and is constructing operational processes and rules to address vulnerabilities in order, beginning with the most critical ones. It has also set clear criteria (such as “within two weeks” or “within one month”) for the time required to implement responses to vulnerabilities depending on their level of severity and requires system administrators to take corrective action.



Analysis of Website Vulnerabilities

Each brand and business department operates numerous unique e-commerce websites and customer relationship management websites.

Before launching a new site, it is mandatory to perform checks for vulnerabilities. Furthermore, considering that there may be additions or modifications to functions after the start of operation, or changes in the cloud environment, we regularly conduct vulnerability diagnoses. When a serious problem is discovered, the operating department promptly takes corrective action.

Management of Externally Disclosed Assets

Shiseido Group recognizes the importance of comprehensively identifying all externally facing assets, such as servers published on the internet, and implementing necessary security measures to minimize the risk of attacks from malicious actors.

We have introduced a service that allows us to diagnose security risks via the internet and score our security posture. We continuously perform quantitative assessments of our security posture both regionally and globally. Based on these assessments, our Information Security Department communicates with security representatives in each region to steadily promote corrective actions. We also regularly compare our scores with those of other companies in the same industry to ensure that we maintain a level above a certain standard.

Furthermore, we have established new tools and operational processes to discover new externally facing assets, and when assets are found to be unintentionally exposed to the public, we take swift corrective action.

Establishment of the Shiseido Global Security Operations Center

While Shiseido has placed security members in each region to strengthen information security, we aimed for further sophistication and standardization of our measures. In December 2023, we commenced operations of the "Shiseido Global Security Operations Center," which monitors system operations around the clock.

In this initiative, we have built an infrastructure for collecting and analyzing logs under a set of common rules for all regions, utilizing managed services provided by external security vendors. Additionally, with an eye towards the future automation of security operations, we are also developing playbooks with predefined actions to be taken.

Shiseido Information Security Report 2024
Editing Team
July 2024

Information Security Department, Shiseido Company, Limited

Shiseido Creative Company, Limited

Shiseido Company, Limited
6-2, Higashi-shimbashi 1-chome, Minato-ku,
Tokyo 105-8310, Japan
https://corp.shiseido.com/en/