SHISEIDO

Information Security Report 2026

CEO Message

The Shiseido Group is committed to realizing our mission, “BEAUTY INNOVATIONS FOR A BETTER WORLD,” and strives to remain the most trusted beauty company among consumers worldwide.

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.”

In recent years, the rapid advancement of cutting-edge digital technologies—particularly generative AI—has significantly transformed business practices, working styles, and relationships with customers. Amid this accelerating digitalization, the Shiseido Group has actively expanded its e-commerce initiatives. Since the launch of our membership service “Beauty Key” in 2022, we have welcomed over three million members, delivering an integrated customer experience through our mobile application.

Furthermore, our “Beauty DNA Program,” which combines dermatological research with AI technology, offers personalized skincare analysis based on DNA testing, along with comprehensive lifestyle advice covering diet, sleep, and exercise—enabling deeper and more holistic beauty support.

Within our organization, the adoption of advanced digital technologies, including generative AI, is also transforming the way we work—enhancing operational efficiency, accelerating decision-making, and fostering an environment that supports creative value creation.

As digitalization advances at this rapid pace, we recognize that information security is not merely a system-level issue, but a critical management priority that underpins our business operations. In 2026, the Shiseido Group continues to position information security as one of its top priorities. In recent years, sophisticated ransomware attacks targeting Japanese global enterprises have intensified, posing an unprecedented threat to business continuity. In response, the Shiseido Group is swiftly establishing a robust defense system based on Zero Trust architecture. Furthermore, we are focusing on ensuring rigorous security that enables the safe utilization of generative AI.

The Shiseido Group has set “By connecting with people, we pursue, create, and share new beauty, enriching everyone’s lives.” as new vision 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 outlines the Shiseido Group’s latest initiatives and steadfast commitment to information security. We hope it provides you with valuable insight into our ongoing efforts.

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

Message from the Officer in charge of Information Security

To be recognized as the most trusted beauty company, the Shiseido Group work together to promote information security measures to ensure that our products and services can be used with peace of mind.

Thank you for your interest in the Shiseido Group’s Information Security Report for 2026. I am Makoto Toyoda, in charge of information security and information systems at the Shiseido Group.

As stated in the message from President and CEO 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.

With the emergence of generative AI and autonomous AI agents, technology is evolving at a dramatic pace. The Shiseido Group actively embraces these advances as powerful engines for business growth. Conversely, this technological evolution has also led to more sophisticated cyberattacks. In particular, the intensification of ransomware attacks targeting Japanese global enterprises represents one of our most significant business continuity concerns. In this environment, we proactively gather intelligence on the latest security technologies, focusing heavily on utilizing them to construct an autonomous, advanced security infrastructure.

First, we are accelerating the deployment of solutions based on the "Zero Trust" concept across all global locations, moving away from traditional perimeter defense. This ensures a consistently secure environment of access regardless of location or device, robustly protecting Group assets from external threats such as ransomware.

Second, we are focused on securing a safe operational environment for generative AI and autonomous agents. When rapidly adopting transformative technologies, it is vital to guarantee security without compromising convenience. We are establishing a framework for highly secure identity and access management that extends beyond human users to "non-human" accounts, such as AI agents. This guarantees a consistent level of security across a complex, hybrid environment of people, devices, and AI.

Furthermore, technological solutions must be accompanied by heightened awareness among the people who use them. To build robust security governance, we continuously foster a group-wide security culture through regular training for all employees worldwide and strategic information sharing among regional leadership.

There is no "completion" or final goal when it comes to information security. We will always stay ahead of evolving threats, utilizing the latest technology as our shield to steadfastly protect our customers' precious data and our business.

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 sincerely hope this report provides you with a deeper understanding of our evolving information security initiatives.

Makoto Toyoda
Chief Officer
Chief Information Technology Officer
Shiseido Company, Limited

Contents

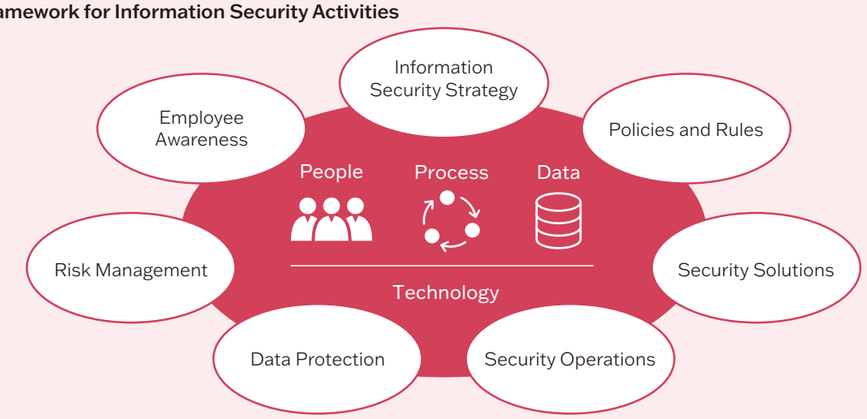
Publication

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
As of June 2026
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

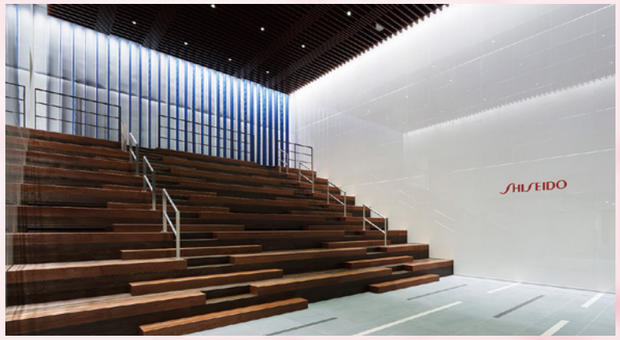


Information Security Governance

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.



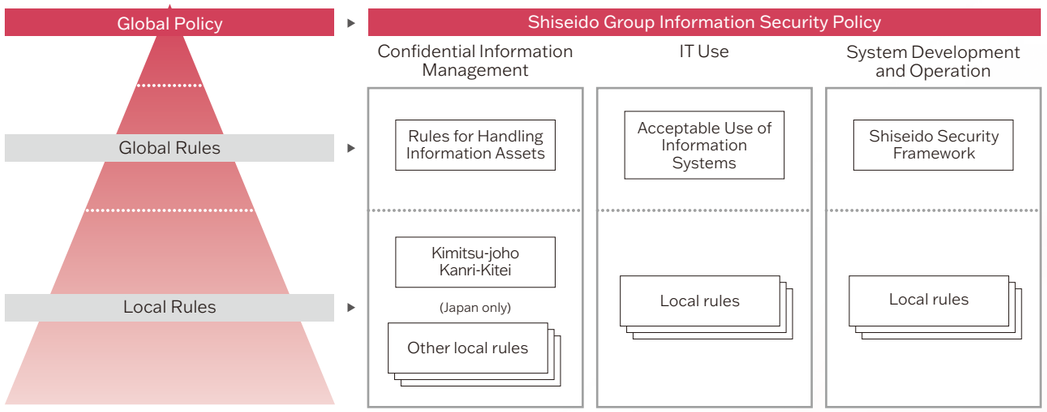
Policies and Rules

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 headquarters 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 Executive Officer (CEO), the representative executive officer, is ultimately responsible for information security.

Additionally, we have established an Information Security Department within Shiseido headquarters. 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. In recognition of our efforts to strengthen group-wide security management, the Shiseido Group was awarded the Excellence Prize in the “Security Measures and Operations” category at the Japan Security Awards, hosted by the Security Division of the Japan Digital Transformation Promotion Association in October 2024.
URL / Link: https://security-awards.jp/winners.html *Japanese only

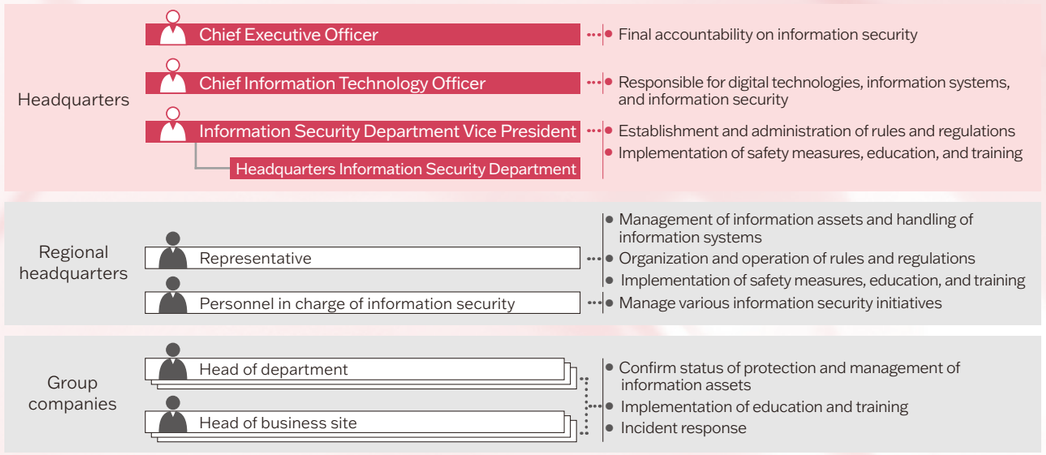
Management at Regional Headquarters

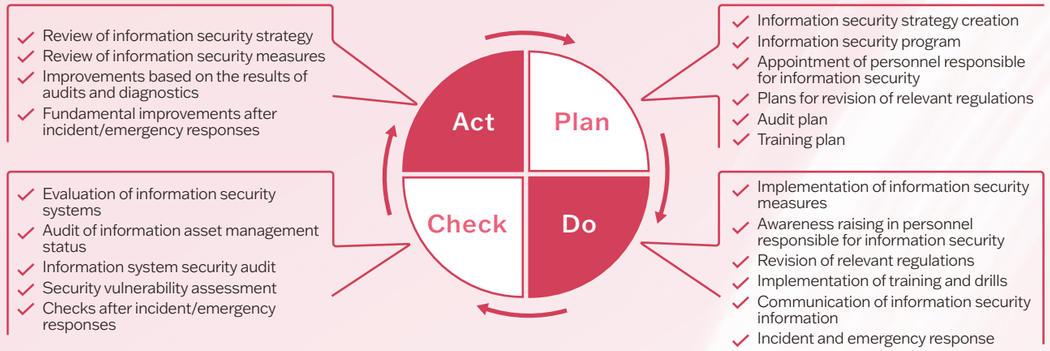
In each regional headquarters, the representative is responsible for managing the handling of information assets and information systems within their jurisdiction. This includes the management of confidential information and information systems, the establishment and operation of regulations, the implementation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

Furthermore, each regional headquarters 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.





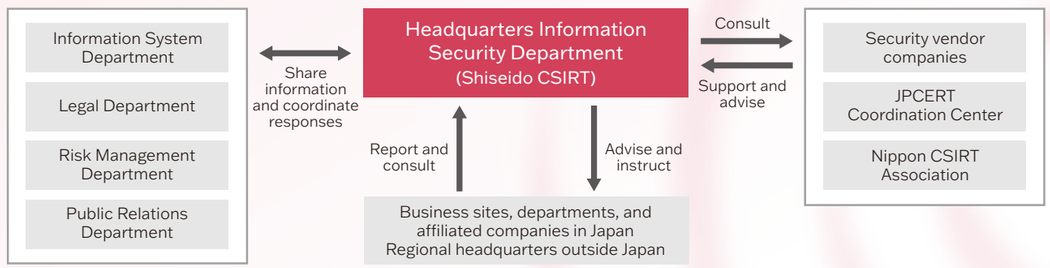
Incident Response Process

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 headquarters 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. Furthermore, we are accelerating our transition to a Zero Trust architecture through the deployment of advanced, integrated security solutions, aiming to prevent incidents and minimize their impact should they occur.

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 policies and rules on information security during monthly onboarding training for career employees 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.

Furthermore, recognizing the recent surge in ransomware attacks that have severely impacted business operations, we also plan to conduct a dedicated training program for executive management in 2026, simulating major incident scenarios.

Additionally, regional headquarters overseas are also implementing original measures. The Americas regional headquarters is engaged in quarterly phishing drills. Meanwhile, the EMEA regional headquarters provides employee education programs focused on mitigating risks associated with generative AI-driven deepfakes.

Major e-learning programs on information security

Training on information security basics	Conducted annually for all employees at headquarters 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)

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.

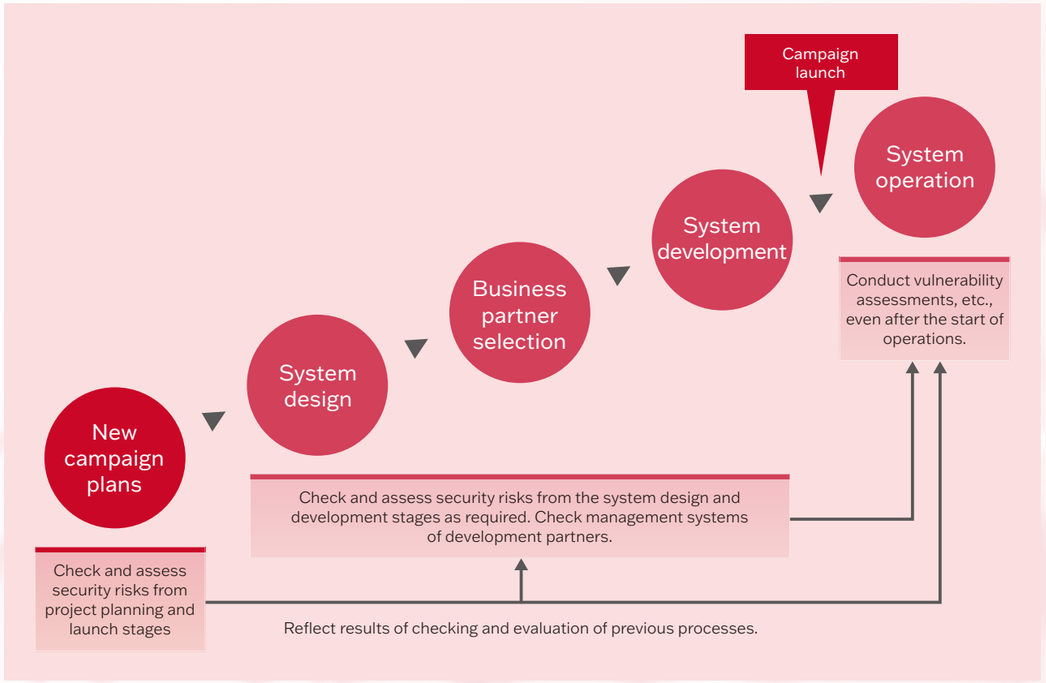
Additionally, we conduct regular checks of information system platforms and applications for vulnerabilities and implement measures to address any that are detected. Moreover, in addition to constant monitoring using threat intelligence, we utilize external specialists to conduct third-party evaluations 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 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.

Beyond new systems, we are progressively deploying multi-factor authentication (MFA) across our existing e-commerce sites in the Japan region to prevent unauthorized access from cyberattacks.

In 2025, the Shiseido Group established a dedicated risk assessment process to address emerging risks associated with the business use of generative AI. As part of this initiative, we require that key generative AI tools be configured with model training disabled by default, thereby reducing the risk of information leakage. Moreover, to adapt swiftly to the rapid evolution of generative AI and autonomous AI Agent, and to ensure their continuous, safe utilization, we are advancing the formulation of a more comprehensive policy and accompanying guidelines in 2026.



Insider Threat Mitigation

At Shiseido, we regard the prevention of insider threats as equally critical as countermeasures against external cyberattacks in strengthening our information security posture. To prevent unauthorized leakage and exfiltration of personal and confidential data handled within the company, relevant departments — including Risk Management Department, Human Resources Department, Legal Department, and Information Systems Department — collaborate to implement countermeasures from organizational, human, and technological perspectives.

Specifically, we have reinforced our rule by revising employment regulations and confidentiality agreements, and we conduct regular training programs focused on insider threat topics for all employees. In addition, we have technically prohibited the use of external storage media such as USB devices to prevent unauthorized data transfers.

Furthermore, we have introduced automated detection mechanisms to identify suspicious data exfiltration via email, USB, or cloud services. In the event of a potential incident, a coordinated response framework involving relevant departments ensures swift and appropriate action. Concurrently, to actively prevent rather than merely detect unauthorized actions, we developed a system in 2025 to block data exfiltration, initiating its operation for targeted employees.

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.

Privileged Account Management

At Shiseido, we enforce strict management of privileged accounts used to servers that store customers' personal information. Given the elevated access rights associated with these accounts, any misuse could result in serious data breaches or operational disruptions.

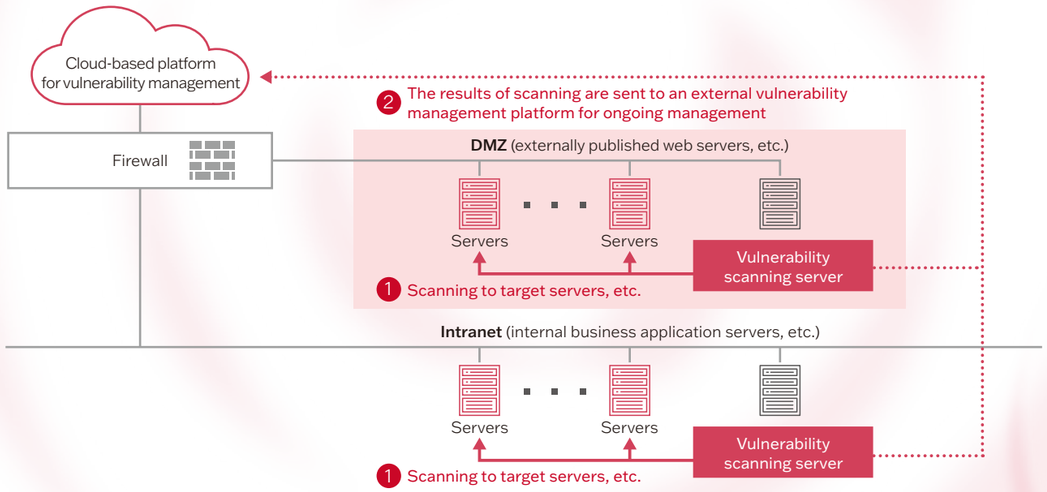
To mitigate such risks, we have implemented a privileged account management solution for servers handling personal data. This system centrally manages the processes of application, approval, execution, and auditing related to privileged account usage. In particular, when external service providers require access, we grant only the minimum necessary privileges on a temporary basis and automatically record and store access logs to ensure transparency and traceability.

Additionally, we conduct regular reviews of privileged account usage, removing unnecessary accounts and reassessing access rights. Through these efforts, we continuously strengthen information security and maintain internal controls, while safeguarding personal information and ensuring trust.

Management of IT Infrastructure Vulnerabilities

Even though IT infrastructure may have been secure when it was constructed, vulnerabilities and other problems are frequently identified over time, requiring rapid responses when serious weaknesses 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.

Shiseido Company Group Security Rating (as of June 2026)

Threat Monitoring by the Shiseido Global Security Operation 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 Operation 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.

In 2025, we expanded our services to establish a global framework that enables 24/7 incident response. By collaborating with external expert teams capable of conducting initial threat analysis and containment 24/7, we have strengthened our capabilities beyond alert monitoring and detection — ensuring that incidents can be addressed promptly and effectively at any time, across all regions.

Shiseido Information Security Report 2026
Editing Team
September 2026

Global Information Security Department,
Global Digital Division, Shiseido Company,
Limited

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