Issue 5. Ensure Information Security including Personal Information Protection

Based on management's firm belief that all company-generated information, including new drug development data and clinical trial results, is a key asset for sustainable growth and innovation, Hanmi Pharm is continuously investing in building a safe and efficient information protection system. Through this system, we rigorously safeguard essential data for research, development, and global business operations, while implementing systematic security procedures to prevent leaks of customer personal data and confidential information.
We will continue to maintain a global-standard information security framework, proactively addressing potential risks across our R&D and business activities.

Key Achievements in 2024

Maintained the ISO 27001 certification
(First acquisition in the pharmaceutical industry)

7 consecutive years

No violations of information protection laws occurred

0 cases

Information technology investment, manpower (based on the top 10 pharmaceutical companies in Korea)

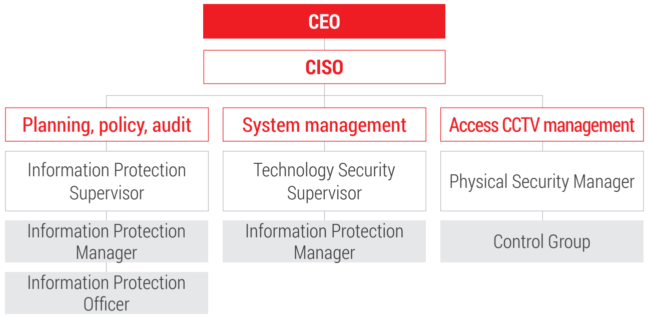
(as of 2023) 1 st place

I. Governance

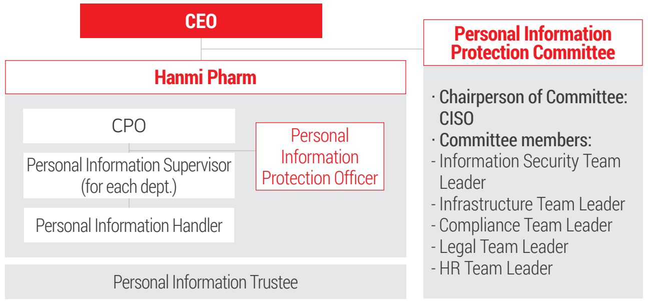
Decision-making Structure

Hanmi Pharm operates an Information Security Committee to carry out our data protection activities systematically and effectively. In addition, the CEO is appointed as the chair of the committee and personally reviews and decides on major issues related to information and personal data protection. Whenever significant matters arise, the committee holds weekly meetings. Due to the recent increase in cybersecurity threats and data breaches targeting the pharmaceutical and biotech industry, the Information Security Committee proactively implements an independent and structured information protection management system. In particular, in order to respond quickly to potential security breaches, we have established reporting mechanisms and penalty regulations, enabling the Committee to respond systematically to any breaches by deliberating and deciding on response measures and the appropriate levels of punishment based on the severity of the violation. However, we have not experienced any personal data leaks or security breaches to date and remain committed to preventing any such incidents.
In order to carry out effective information security and personal information protection activities, we maintain close cooperative relationships with external expert groups to secure specialized information and capabilities, including information security threats and related control measures. Furthermore, we operate an Information Security Operations Committee to deliberate and decide on matters related to the planning, execution, evaluation, and improvement of personal data protection. The Chief Information Security Officer (CISO) and committee members hold weekly security meetings to facilitate communication and cooperation. We plan to conduct regular training programs to further develop the expertise of the executives concerned.

Information Protection Committee


CEO
CISO
Planning, policy, audit
System management
Access CCTV management
Information Protection Supervisor
Information Protection Manager
Information Protection Officer
Technology Security Supervisor
Information Protection Manager
Physical Security Manager
Control Group

Personal Information Protection Operating Organization


CEO
Hanmi Pharm
CPO
Personal Information Supervisor (for each dept.)
Personal Information Handler
Personal Information Protection Officer
Personal Information Trustee
Personal Information Protection Committee
· Chairperson of Committee: CISO
· Committee members:
- Information Security Team Leader
- Infrastructure Team Leader
- Compliance Team Leader
- Legal Team Leader
- HR Team Leader

Operation Method

Method	Management/Operation cycle
Information Security Committee	Deliberation and resolution of major items of agenda related to information security/weekly.
Personal Information Security Committee	When a matter regarding personal information arises for deliberation by the committee.

Roles and Authority of the Dedicated Organization

Type	Roles and authority
CEO	Chairman of the Information Security Committee.
CISO (Chief Information Security Officer)	Development of information security strategies, management of risks, response to cyber-attacks, and protection of organizational assets.
CPO (Chief Privacy Officer)	Establishment of privacy policies, supervision of regulatory compliance, and enforcement of transparency and accountability regarding data use.
Personal Information Handler	Executive of the department responsible for handling personal information.
Person in charge of Personal Information Security	Personal information protection.
Technical Security Manager	Technical personal information protection.
Person in charge of Physical Security	Management of entry/exit, CCTV, etc.
Manager of Personal Information in each Department	Executive of the personal information department.
Personal information protection agents	Operation of the personal information processing system or performance of duties as an agent

Issue 5. Ensure Information Security including Personal Information Protection

II. Strategy_Identifying Risks and Opportunities

Hanmi Pharm identifies key risks and opportunities that could have a significant impact on our stakeholders and sustainability concerning information security such as personal information protection based on the results of the IRO (Impacts, Risks, and Opportunities) analysis, and strives continuously to develop effective response strategies based on the findings.

RISK

Disruption of Business Operations, Leading to the Leak of Core R&D Technologies, Exposure of Personal Information, and System Failure

Characteristics of impact	Actual impact
Affected stakeholders	Shareholders and investors
Severity of impact on society/environment	Scale ■■■■□ Scope ■■■■■ Recoverability ■■■■□
Expected financial impact	Possibility of occurrence ■■■□□ Scale ■■■■□
Impact on corporation	- Widespread damage caused by the inoperability of production facilities. - Imposition of fines or penalties for violations of the Personal Information Protection Act.
Corporation's response	- Establishment of an international standard information security management system. -Raising employees' awareness about information security.

OPPORTUNITY

Establishment of an Information Security Management System

Characteristics of impact	Potential impacts
Affected stakeholders	Customers
Severity of impact on society/environment	Scale ■■■□□ Scope ■■■■□
Expected financial impact	Possibility of occurrence ■■■□□ Scale ■■□□□

- Completing the technical preparations for information security, including acquisition of the ISO 27001 certification.
- Preventing information security incidents through systematic security education and campaigns.
- Preventing financial losses due to legal disputes.
- Securing business continuity and industrial competitiveness by eliminating the risk of disruption of business operations.

Issue 5. Ensure Information Security including Personal Information Protection

II. Strategy_Identifying Risks and Opportunities

Establishing an International Standard Information Security Management System

Strengthening Information Protection Regulations/Guidelines and Personal Information Processing Policies

Information protection declaration

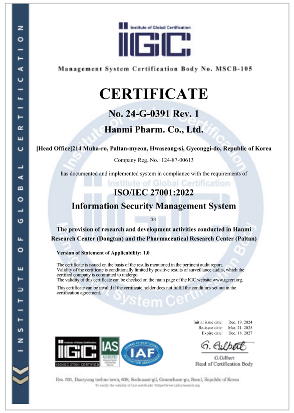
Personal information processing policy

Hanmi Pharm, driven by our leadership's firm commitment to information security, has fully established or revised five security regulations and eight guidelines (as of 2025) in order to ensure the confidentiality, integrity, and availability of all company-generated data. All documents related to information protection, including the relevant regulations and guidelines, personal information processing policy, and personal information internal management plan, reflect the amendments to the Personal Information Protection Act and the internal operating status, and are revised periodically. In particular, recognizing the growing security risks associated with the rapid advancement of AI technology, we introduced guidelines on the use of generative AI in 2024 to provide a secure management framework for AI applications.

Whenever amendments to the Personal Information Protection Act are made or updates of the personal information processing policy become necessary, we regularly revise our policies and publish the details of the changes on our main website so as to ensure easy access for stakeholders. Our personal information processing policy and our declaration on information protection, which contains management's intentions, can be reviewed in the linked webpages.

Renewed the ISO 27001 Certification (International Standard for Information Security Management) for a Seventh Consecutive Year

In 2018, Hanmi Pharm became the first company in the pharmaceutical industry to obtain ISO 27001, a globally recognized international standard for information security management systems (ISMS). Then, in 2024, we renewed the ISO 27001 certification, ver. 2022, thus maintaining our certification for a seventh consecutive year. Furthermore, to objectively assess the security of our information protection management system across all of our new drug and formulation technology research activities, we include external auditors in our internal audit process. We will continue to maintain these international standard certifications, further enhancing our competitiveness as a global pharmaceutical company while advancing a superior and secure information security management system.



INSTITUTE OF GLOBAL CERTIFICATION

Institute of Global Certification IGC

Management System Certification Body No. MSCB-105

CERTIFICATE

No. 24-G-0391 Rev. 1

Hanmi Pharm. Co., Ltd.

[Head Office]214 Muha-ro, Paltan-myeon, Hwaseong-si, Gyeonggi-do, Republic of Korea

Company Reg. No.: 124-87-00613

has documented and implemented system in compliance with the requirements of

ISO/IEC 27001:2022

Information Security Management System

for

The provision of research and development activities conducted in Hanmi Research Center (Dongtan) and the Pharmaceutical Research Center (Paltan)

Version of Statement of Applicability: 1.0

The certificate is issued on the basis of the results mentioned in the pertinent audit report.
Validity of the certificate is conditionally limited by positive results of surveillance audits, which the certified company is committed to undergo.
The validity of this certificate can be checked on the main page of the IGC website www.igcert.org.

This certificate can be invalid if the certificate holder does not fulfill the conditions set out in the certification agreement.

Initial issue date:	Dec. 19. 2024
Re-issue date:	Mar. 21. 2025
Expire date:	Dec. 18. 2027

G. Gilbert

G.Gilbert
Head of Certification Body

IGC ISO/IEC 27001 CERTIFIED IAS ACCREDITED IAF

Rm. 501, Daeryung techno town, 638, Seobusaet-gil, Geumcheon-gu, Seoul, Republic of Korea

To verify the validity of this certificate : https://www.iafcertsearch.org

Developing and Implementing Security Policies in line with the Introduction of M365

Five principles for the safe use of M365 by Hanmi Pharm employees

1. Store your documents in a secure repository.
2. When sharing important documents, grant permissions only to a specific user.
3. Upon receiving a personnel appointment such as a transfer or reassignment, ensure a thorough handover of responsibilities.
4. When working on a shared PC, access M365 via a web browser.
5. Before handing any documents over to external parties, always obtain approval for their release.

After fully introducing Microsoft 365 (M365) throughout the entire company in October 2024, Hanmi Pharm developed security issue-specific scenarios related to potential document leaks and security violations within the system and established a focused monitoring process in order to create a highly secure work environment. As part of this effort, we have devised and implemented plans to automatically detect and eliminate various threat factors, including walking out with documents, illegal intrusions, hacking, abnormal insider behavior, and any suspicious actions by employees who are about to leave the company.
Furthermore, as the introduction of M365 significantly transformed the internal IT environment, it became apparent that there was a need to establish new policies and disciplinary regulations concerning abnormal behaviors. To address this issue, we have completely revised or newly implemented regulations and policies to operate a more advanced security management system.

Efficient and Safe Use of Generative AI

As the adoption of generative AI by corporations and companies continues to increase, Hanmi Pharm has taken proactive measures to ensure its safe usage. First, we blocked all generative AI sites that had not undergone security verification within our internal network; then, we established new user guidelines for generative AI and distributed them across our corporate group and also developed training programs for employees wishing to use generative AI. Only those who complete the training are granted access to designated generative AI sites via shared accounts, ensuring a secure AI usage environment.

Hanmi	생성형 AI 사용 지침	[illegible]	[illegible]
		[illegible]	[illegible]

생성형 AI 사용 지침

한미사이언스㈜
한미약품㈜

[illegible] 생성형 AI 사용 지침

We continuously monitor the development of new generative AI technologies, immediately blocking sites that pose national security risks. We have also established a master plan for strengthening the level of information security and personal information protection management in order to establish internal strategies for responding to the trends of domestic AI policy establishment and legislation, such as the drafting of AI-related laws and the revision of the Personal Information Protection Act and the Act on Promotion of Information and Communications Network Utilization and Information Protection, so as to reflect the growing use of AI. Looking ahead, we remain committed to reviewing generative AI technologies for the safe use of generative AI, educating our employees, and fostering a secure environment for AI-driven improvements of business efficiency.

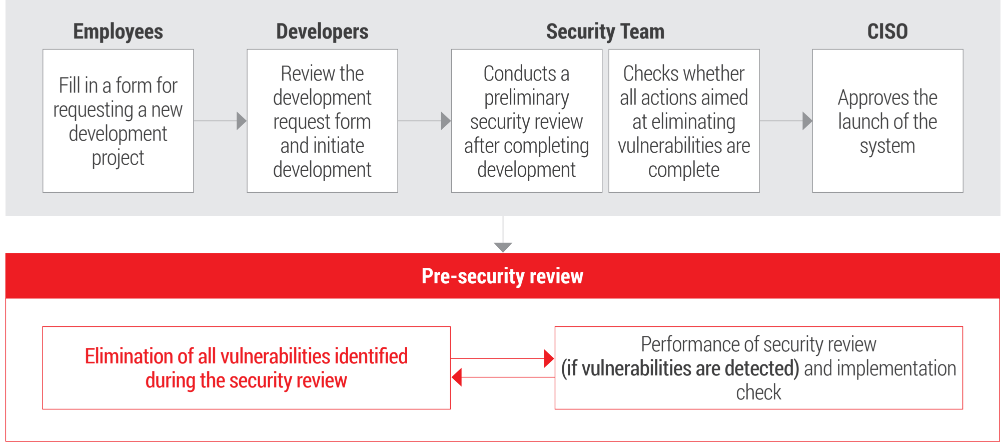
Issue 5. Ensure Information Security including Personal Information Protection

II. Strategy_Identifying Risks and Opportunities

Establishing an Information Security Audit and Inspection Process

Introducing a Pre-security Review Process

Hanmi Pharm conducts thorough security assessments before launching any external systems and services to ensure information protection and personal data security, thereby eliminating potential risks in advance. These security assessments include infrastructure vulnerability diagnostics, simulated system hacking tests, and compliance checks for personal data protection. A system can only be launched after confirming that all vulnerabilities have been addressed and receiving approval from the Chief Information Security Officer (CISO). Furthermore, we continuously review the latest laws and key compliance issues to refine our security audit criteria. As of the first quarter of 2025, we have conducted pre-launch reviews of ten systems, successfully addressing thirty-two vulnerabilities before making them operational. We strictly enforce the principle that systems cannot be launched unless all vulnerabilities have been fully resolved.
All of the services provided by us undergo a rigorous security review process to eliminate potential weaknesses and data risks before being made available to users.

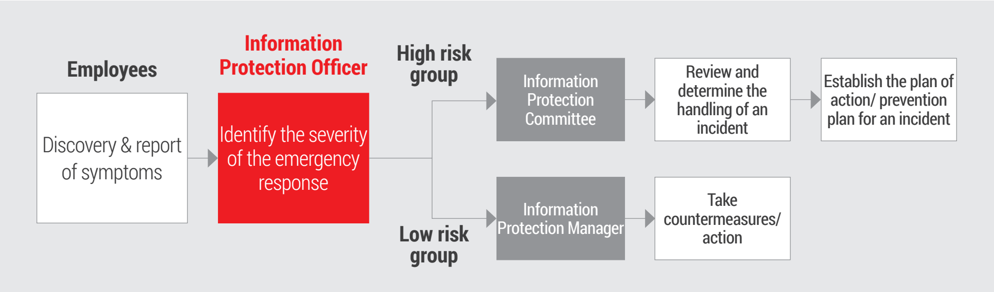

Employees
Fill in a form for requesting a new development project
Developers
Review the development request form and initiate development
Security Team
Conducts a preliminary security review after completing development
Checks whether all actions aimed at eliminating vulnerabilities are complete
CISO
Approves the launch of the system
Pre-security review
Elimination of all vulnerabilities identified during the security review
Performance of security review (if vulnerabilities are detected) and implementation check

Conducting IT System Vulnerability Checks and Mock Hacking Attacks

Hanmi Pharm conducts infrastructure vulnerability checks and mock web hacking attacks during the annual ISO 27001 certification audit process in order to maintain a security framework that meets global standards. We also evaluate all internal information systems to ensure proper measures are in place for personal data security, reinforcing systematic management for data protection. Beyond our own operations, we aim to actively enhance information security across our entire corporate group. This includes such initiatives as infrastructure vulnerability diagnostics, penetration testing, and assessments of personal data processing systems.

Process of Reporting/Responding to Personal Information Cyber Security Incidents

Hanmi Pharm implements rigorous preemptive and follow-up measures to protect personal data, and carries out various activities to ensure data security. We have established regulations and guidelines to mitigate the risk of customer data leaks and have also developed a rapid response system for handling any incidents. Furthermore, we have taken out personal data protection liability insurance to prepare for additional risks. To prevent the spread of damage and ensure swift recovery in the event of a data breach, we have developed the “Manual for Responding to Personal Data Leaks”. This manual outlines the procedures for promptly identifying the cause of an incident, implementing measures to prevent further leaks, notifying affected individuals, and reporting the facts pertaining to an incident to the relevant authorities. In particular, the privacy manager reports incidents directly to the CEO and organizes a rapid response team to systematically address breaches, while simultaneously devising victim assistance and recurrence prevention strategies. Furthermore, we collaborate with the Personal Information Protection Commission to assess the severity of incidents, determine appropriate response measures and penalty levels, and implement regular security training and internal management plans to prevent security breaches.


Employees
Discovery & report of symptoms
Information Protection Officer
Identify the severity of the emergency response
High risk group
Information Protection Committee
Review and determine the handling of an incident
Establish the plan of action/ prevention plan for an incident
Low risk group
Information Protection Manager
Take countermeasures/ action

Implementation of the TSS (Team Security Score) System

As the Personal Information Protection Act continues to be strengthened, shifting penalties from individuals to financial sanctions against corporations, Hanmi Pharm has intensified our information security efforts. To enhance security awareness among our employees, we have implemented the Team Security Score (TSS) program, which evaluates each team’s security levels and applies incentives and penalties accordingly. Under this program, employees who report spam emails or potential data leaks receive reward points, while those who fall victim to simulated phishing attacks or violate the security regulations face losing points. Since the program’s announcement in July 2024, security violations have decreased by approximately 70% compared to the first half of the year and by around 64% compared to the second half of the previous year, demonstrating a significant increase in employee vigilance regarding security risks.
We will continue to strengthen the security awareness of our employees. In particular, we plan to introduce additional TSS reward and penalty criteria in 2025 to reinforce secure practices in the use of Microsoft Teams. Through these initiatives, we are committed to establishing a more robust information protection system and further enhancing our security standards.

Issue 5. Ensure Information Security including Personal Information Protection

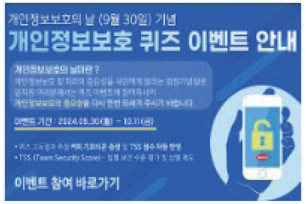
II. Strategy_Identifying Risks and Opportunities

Raising Employees' Awareness about Information Security

Launching an Interactive Campaign to Enhance Employees' Awareness of Information Security

Hanmi Pharm actively conducts various interactive campaigns to raise employees' awareness of information security and establish a security-focused culture in our daily operations. In particular, the two "Information Security Quiz" events held in 2024 were designed based on real-world security scenarios, practical cases, and examples of legal violations and penalties. These events effectively heightened employees' awareness of the legal risks related to information security.

Through this employee participation campaign, Hanmi Pharm assists our employees in recognizing information security as an integral part of their daily work and seamlessly incorporating security practices into their work tasks. Hanmi Pharm plans to continuously develop an information security culture centered on employees' participation so that they can familiarize themselves fully with information security issues and perform their work with a high level of security awareness.



개인정보보호의 날 (9월 30일) 기념

개인정보보호 퀴즈 이벤트 안내

개인정보보호의 날이란?

이벤트 기간 : 2024.09.30(월) ~ 10.11(금)

이벤트 참여 바로가기

7월 10일

정보보호의 날 이벤트 안내

제13회 정보보호의 날을 맞아 퀴즈 참여를 통해 우리 회사의 정보보호 규정을 다시 한 번 상기해 보시고, 회사 정보 자산 보호에 힘써주시기 바랍니다.

기간 : 2024.07.08(월) ~ 07.12(금)

참여 바로가기

Information Security Training

Hanmi Pharm continuously provides both online and offline information security training for new employees, while developing customized education programs tailored to the latest technological trends and company developments. This effort ensures that all employees strengthen their security competencies.

In particular, in 2024, Hanmi Pharm conducted security training related to the adoption of Microsoft 365, helping employees to manage information securely in the new work environment. Additionally, with the company-wide implementation of generative AI, specialized security training was provided to ensure the safe use of AI.

By consistently developing and implementing timely, tailored education programs alongside fundamental security training, Hanmi Pharm remains committed to enhancing our employees' security awareness and practical capabilities in an ever-changing digital environment.

Information security training distributed by Hanmi Pharm

1. Personal information protection and personal information leak prevention training (Mar. 2025).
2. M365 security training (Mar. 2025).
3. Generative AI security training (since Jun. 2024).
4. Legal mandatory training on personal information protection (annual).
5. Online information security training for new employees (ongoing).
6. Training for employees who click on malicious emails (ongoing).

We rank first among the Top 10 pharmaceutical companies in terms of IT investment and personnel

As a research-driven company, Hanmi Pharm prioritizes risk management and information protection, considering our handling of both core pipelines and sensitive medical data provided by patients and hospitals. To strengthen our security framework, we continue to invest heavily in information technology and specialized personnel. Per our mandatory 2024 Information Security Disclosure (KISA), we invested a total of KRW 27.5 billion in IT, a figure approximately 2.5 times higher than the average investment of the top 10 pharmaceutical companies, thereby solidifying our position as an industry leader in security investment. In addition, we have an average of 43.3 professional personnel working in the field of information technology, the largest number of IT personnel among the top 10 pharmaceutical companies, demonstrating outstanding competitiveness in information technology and security capabilities. Our information security investment and personnel operation status are transparently disclosed through the public disclosure portal link, allowing public access to the relevant data.

Type	2022		2023	
	Investment amount (KRW)	Information technology personnel (persons)	Investment amount (KRW)	Information technology personnel (persons)
Hanmi Pharm	276.5	47.6	274.9	43.3
Company A	94.5	37.6	146	40.3
Company B	100.8	25	101.8	26.2
Company C	106.1	34	100.5	43
Company D	83.2	14.7	97.2	18.3
Company E	82.8	13.2	90.6	13.5
Company F	85.1	30.2	84.3	31.2
Company G	92.8	21.8	84.2	22
Company H	46.4	12.1	56.4	14.5
Company I	10.3	6.3	11.5	6.8
Average	96.5	24.3	104.7	25.9

* Source: Consumernews (Jul. 04, 2024).
Hanmi Pharm ranks first among the top 10 pharmaceutical companies in terms of IT investment and personnel.

Issue 5. Ensure Information Security including Personal Information Protection

III. Risk Management

Monitoring risk and opportunity	Monitoring period	Monitoring target	Monitoring method	Management and supervision
Establishment of security procedures in line with the introduction of new systems (Teams)	Periodically	Employees	· Establishment of security procedures for the new system - Advance guidance and training (guide). - Identification of problems and strengthening of security by responding to issues, questions, and inquiries that arise during actual use.	Information Team
Prevention of personal information leaks caused by the use of generative AI	Periodically	Employees	· Publication of internal guidelines (implementation) - Prohibition of the use of personal accounts. - (If necessary) Accounts should be issued only to teams and personnel who have completed the relevant security training. - Establishment of a continuous management plan for safe use.	Information Team
Pre-security review process	Periodically	Employees/Partners	· Introduction of a pre-security review process - Development completed → Establish a vulnerability diagnosis plan →Perform a diagnosis →Establish a vulnerability action plan and take actions → Check implementation → Launch service	Information Team
Monitoring of and response to changes in the law	Periodically	-	· Revision and implementation, taking into consideration the internal regulations/guidelines and business impact.	Information Team
Prevention of personal information leaks	Periodically	Employees	· Promotion of campaigns aimed at raising employees' security awareness; performance of internal security reviews to prevent security incidents.	Information Team

Issue 5. Ensure Information Security including Personal Information Protection

IV. Indicators and Goals

Key indicator	2024 target	2024 performance	Achievement status	2025 target	Mid-to-long term (2030) plan
Establishment of an international standard information security management system	Maintain the ISO 27001 certification.	· Passed the ISO 27001:2022 renewal audit.	Achieved	· Pass the ISO 27001 surveillance audit.	· Renew ISO 27001 certification. · Obtain ISO 27701 certification (international standard for information security management).
	Complete the establishment of the pre-security review process system.	· Completed measures against vulnerabilities before introducing the new system. - Measures were taken against 32 vulnerabilities in 10 systems (as of Q1 2025). * New systems: Carrying-out system for Teams, HMP community, etc.	Achieved	· Conduct a pre-security review before introducing new systems and approve system launch after taking measures to ensure personal information safety.	· Conduct a system security review of all affiliated companies.
Raising employees' awareness about information security	Raise the level of maturity of employees' awareness of information security issues.	· Defined the level of maturity of employees' information security awareness and established measurement criteria to spread the information security culture.	Achieved	· Distribute training programs throughout the company - personal information protection training, M365 security training, and generative AI security training.	· Design information security training tailored to the role and position of each employee.
Prevention of (personal) information leaks	Achieve zero incidents related to personal information leaks or security breaches.	· Recorded zero cases of personal information leaks or security breaches.	Achieved	· Achieve zero incidents related to personal information leaks or security breaches.	· Achieve zero incidents related to personal information leaks or security breaches.