Information Security

Approach

The IHI Group has established the IHI Group Information Security Policy to ensure the protection of confidential information of customers and business partners as well as corporate management and technical information. The Group strives to properly manage information while maintaining and improving information security.

Policy

IHI Group Information Security Policy

The IHI Group hereby sets the following IHI Group Information Security Policy for the purpose of ensuring the security of information assets in its possession and thereby further solidifying its trust-based relationship with customers, users and society.

(Basic Activities)

1. The IHI Group will take appropriate measures with technology, organization and employees, in order to protect information assets against any leakage, theft, loss, destruction, illegal access, and disaster. In the event of any security problem regarding this information, the IHI Group will locate the cause as quickly as possible, and exert every possible effort to minimize the damage incurred.

(Information Assets)

2. "Information assets" refer to the information the IHI Group handles in the course of business activities, regardless of the type of media, and the equipment, facilities and services necessary for handling such information.

(Scope)

3. This Information Security Policy applies to all those using the information assets of the IHI Group, including but not limited to officers and employees of the IHI Group companies and temporary staff.

(Compliance with Laws, Regulations, etc.)

4. The IHI Group will strictly observe the laws, regulations and codes pertaining to the protection of information assets, and the requirements and obligations regarding information security provided for in the agreements with the customers.

(Training)

5. The IHI Group companies will provide all those using the information assets of the IHI Group with the necessary education on information security to enhance and maintain their awareness thereof.

(Management of Information Security)

6. The IHI Group companies will establish a mechanism of implementing and managing information security by taking measures such as establishing rules concerning information security and appointing persons in charge of information management, thereby conducting, maintaining and improving information security activities on a continual basis.

(Responsibilities of Senior Management)

7. The Senior Management of the IHI Group will set the example of enforcing this Information Security Policy. In the event of any infringement of this Policy, senior management will address the situation properly by defining their authorities and responsibilities, and do their utmost to resolve the problems, diagnose their causes, and prevent their recurrence.

(Punishment)

8. Any action in violation of the rules of information security will incur punishment according to the employment regulations of IHI Group companies.

(Announcement)

9. This Information Security Policy will be announced and notified to all those using the information assets of the IHI Group as well as being announced to the public.

Information Security

Governance

The IHI Group has established an Information Security Promotion Framework, chaired by the Officer in charge of Group DX as its Chief Information Security Officer. The Information Security Subcommittee operates within the DX Promotion Committee as an organization in charge of promoting the company's information security activities overall. An Information Security General Manager is appointed at each IHI corporate division, Business area, Business Unit, and affiliated company to accelerate activities under this framework. Matters of particular importance regarding operation and management are discussed by the Board of Directors.

●Information Security Activity Promotion Framework

●Information Security Subcommittee

Chairperson	General Manager of Intelligent Information Management Division
Subcommittee members	Business areas, Business Units, and corporate divisions
Secretariat	Information Security Department
Number of meetings convened in FY2023	3

Risk Management

Information Security Management System

The IHI Group convenes the Information Security Subcommittee three times a year to plan, implement, and evaluate information security measures within its corporate divisions, Business areas, and Business Units in an annual cycle. Each fiscal year the Group sets priority measures based on the internal and external conditions, such as increasing of remote work and growing threat of cyber attacks.
In fiscal 2019, the Group built a three-stage auditing framework for information security consisting of three types of audits by its own organizations, Business areas, and corporate divisions from different auditors to strengthen checks ("C") in the PDCA cycle. Each organization (IHI divisions and affiliated companies) conducts its own internal audit, the corporate division executes documentation audits, and each Business area, as the responsible division, implements on-site audits. From fiscal 2021 onwards, each Business area has conducted audits of information security measures at all of the Business Units and affiliated companies under its supervision and has worked to improve any issues discovered.
Divisions and affiliated companies involved in highly sensitive national projects in the IHI Group must undergo annual reviews by an external specialized agency to renew the ISO 27001 international information security certification for maintaining a high level of security.

Measures to Prevent Information Leakage During Remote Work

Remote work throughout the IHI Group as a measure to prevent the spread of the COVID-19 virus has gained traction as one of many work styles. However, remote work increases information security risks such as improper use, loss, or theft of information devices due to the higher number of information devices taken outside of the office.
To prevent the improper use of information devices, the IHI Group works to raise employee awareness through e-learning and internal newsletters covering security compliance rules for work done outside the office. These rules specifically prohibit personal use of company computers and prohibit business data from being stored on personal IT devices of the individual and/or family.
In addition, as a general rule when performing work outside of the company, the Group has implemented measures to make use of computers that do not store business data, reducing information leakage upon loss or theft of these devices.

Establishing the SOC and CSIRT

In order to respond to the growing threat of cyber attacks, the IHI Group has set up a SOC (Security Operation Center) and conducts security monitoring of PCs, servers, and network equipment. Additionally, the Group has established a CSIRT (Computer Security Incident Response Team) and put a framework into place for quickly responding to incidents detected through security monitoring. The Group has also prepared a response procedure manual for ensuring its ability to appropriately respond to cyber security incidents, outlining response procedures such as identifying the scope of breach and taking containment measures.

Information Security

Initiatives

Information Security Measures

The IHI Group takes steps to address information security risks from three perspectives: rules, tools, and education. The rules include the IHI Group Information Security Policy, IHI Group Information Security Measure Standards, and Information System User Rules. The Group has adopted antivirus software and other security tools, which are always kept up to date.

Evaluation of Information Security Measures

The IHI Group assesses the information security measures of the entire Group quantitatively every year based on the benchmark for information security measures implemented by companies offered by the Information Technology Promotion Agency, Japan (IPA).
The level of information security measures in fiscal 2023 was 3.8 out of 5. The Group will strive to achieve a score of 4, and further continue to improve our level of information security in fiscal 2024.

●Evaluation of Information Security Measures

(Unit: Score, Scope: IHI and consolidated subsidiaries)

Item	FY2020	FY2021	FY2022	FY2023
Evaluation of information security measures (out of 5)	3.4	3.7	3.7	3.8

Education/Awareness Building

Employee Education

The IHI Group provides e-learning on a yearly basis, targeting all employees to deepen their understanding of information security rules and tools, and to maintain and raise employee information security awareness.

●Rate of Participation in e-Learning

(Unit: %, Scope: IHI)

Item	FY2020	FY2021	FY2022	FY2023
Rate of participation in e-learning	96.0	96.8	96.9	98.9