Information Security

GRI 103-2

Why

— Why it matters —

Even as the development of IoT creates new value, cyberattacks are growing increasingly sophisticated and widening in focus from traditional IT to encompass the IoT/OT field as well. The risks for corporations include leaks of information, operational stoppages, and even direct disruption to business, making information security one of the most critical issues companies face. Hitachi, in expanding its Social Innovation Business worldwide, has highlighted the importance of working to ensure cybersecurity as a key management issue and is engaged in information security governance efforts.

Also, amid rapidly expanding data use with the development of digital technologies, privacy risks are increasing as well. In working to provide a safe and secure social infrastructure system, Hitachi is prioritizing personal information protection efforts in order to realize the secure management of personal information entrusted to us by our customers, personal information related to business operations, and more.

Information Security

Personal Information Protection

What

— What we are doing —

- Disseminating Information Security Policy
- Strengthening information security management
- Implementing security monitoring
- Preventing information leaks
- Providing education programs on information security
- Conducting thorough personal information protection/information security audits and inspections
- Responding to personal data protection laws around the world
- Acquiring PrivacyMark certification
- Managing customer information
- Promoting privacy protection efforts by digital business divisions

How

— How we are doing it —

Policy and promotion structure

Hitachi has established Information Security Policy to foster cybersecurity risk management. The Information Security Committee is chaired by the Chief Information Security Officer (CISO), who is the C-level executive with ultimate authority and responsibility regarding the handling of information security and personal privacy issues. The committee determines relevant policies and measures, while the information security heads at each Hitachi business unit and Group company promote workplace awareness and oversee the implementation of measures.

	Achievements in FY 2021
Strengthening information security management	Advanced the strengthening of information security governance worldwide, based on our rules for information security, established in compliance with the ISO/IEC 27001 standard, and furthermore enhanced with NIST SP 800-171 U.S. government standard. Implemented IT countermeasures and activities to raise security awareness among employees in conjunction with promoting telecommuting Implemented measures to reduce security risks during deals/post-merger integration in conjunction with acquisitions and sales of companies
Security monitoring	Enhanced cyber monitoring by using endpoint detection and response to monitor equipment operation, implemented authentication, and strengthened cyber monitoring
Education on information security	Held e-learning programs on information security and personal information protection for all executive officers and employees (Hitachi, Ltd. attendance rate: 100%)
Thorough personal information protection/information security audits and inspections	Conducted personal information protection/information security internal audits at all Group companies and divisions (Annually)
Responding to personal data protection laws around the world	Formulated and put into effect from April 2022 a Group-wide internal code of conduct concerning protection of personal information, which takes into consideration international legal frameworks, such as the European General Data Protection Regulation (GDPR)
Acquiring third-party certification related to personal information protection	Acquired PrivacyMark certification for 37 Hitachi Group companies in Japan
Personal information leaks	Personal information leaks: 0

Information Security

Information Security Policy

Policy

Hitachi considers one of its top management priorities to be information security governance to minimize the risk of business disruption such as leaks of information or operational stoppages due to cyberattacks.

As a global company, Hitachi regards cyber security risk as one of our management risks. Accordingly, we have formulated Information Security Policy in line with our corporate management policies and based on our cyber security risk management.

We have our data centers and other divisions certified by the ISMS Accreditation Center in accordance with the ISO/IEC 27001 Information Security Management System international standard. This certification has been received by seven divisions of Hitachi, Ltd. and 27 divisions of 23 Group companies.*1

*1 As of September 30, 2021.

Information Security Policy

1. Formulating administrative rules for information security and ensuring their continual improvement
2. Protection and ongoing management of information assets
3. Legal and regulatory compliance
4. Education and training
5. Preventing incidents and taking action when they occur
6. Ensuring business processes are optimized within the corporate group

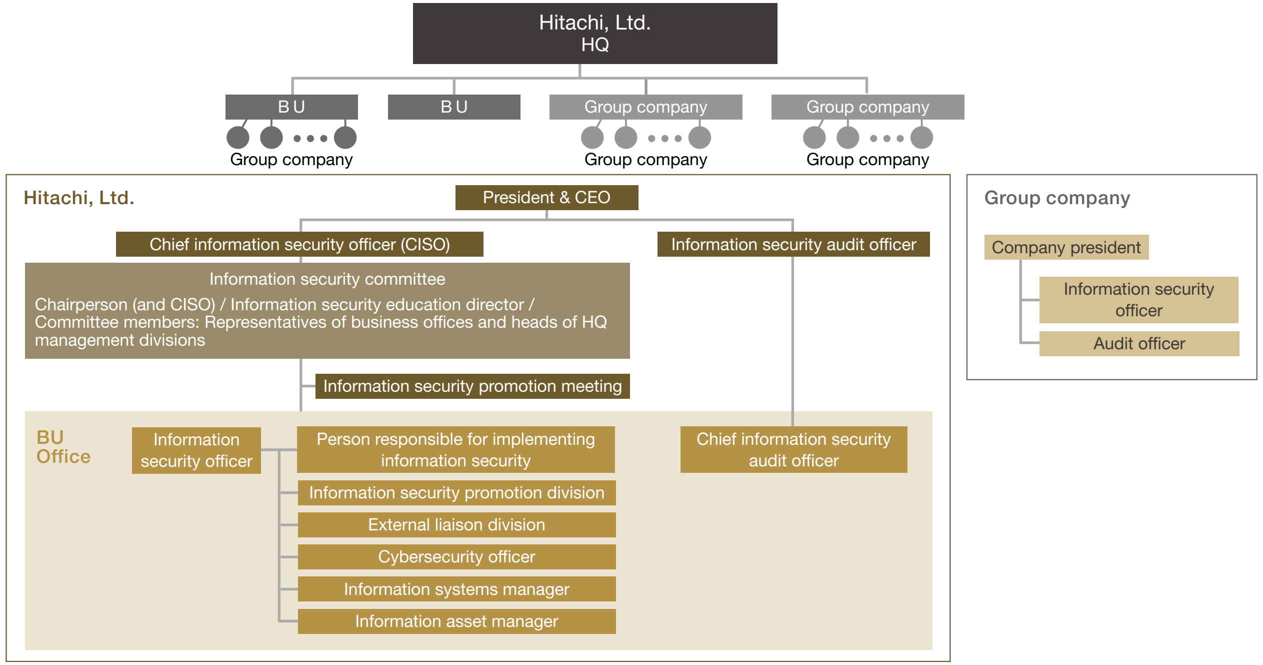
Framework for Promoting Information Security

Structure

At Hitachi, Ltd., the Chief Information Security Officer (CISO), who is the C-level executive with ultimate authority and responsibility regarding the handling of information security and personal privacy issues, oversees the promotion of information security for all Hitachi products, services, and internal facilities.

Chaired by the CISO, the Information Security Committee determines all policies and procedures for information security and personal information protection. Business Units (BU) and business sites establish information security promotion divisions, with the heads of the units and sites serving as information security officers. These divisions work to implement information security management in each workplace and provide relevant education to employees. This framework is also implemented at Group companies to promote information security across the Group through mutual cooperation.

Framework for Promoting Information Security


Hitachi, Ltd.
HQ
BU
BU
Group company
Group company
Group company
Group company
Group company
Hitachi, Ltd.
President & CEO
Chief information security officer (CISO)
Information security audit officer
Information security committee
Chairperson (and CISO) / Information security education director / Committee members: Representatives of business offices and heads of HQ management divisions
Information security promotion meeting
BU Office
Information security officer
Person responsible for implementing information security
Information security promotion division
External liaison division
Cybersecurity officer
Information systems manager
Information asset manager
Chief information security audit officer
Group company
Company president
Information security officer
Audit officer

Information Security Management

Activities

Hitachi has established information security management based on ISO/IEC 27001 and has been working to strengthen information security by reviewing regulations with the U.S. government standards SP800-171 due to the intensifying cyberattacks in recent years. These rules are globally distributed by Hitachi, Ltd. and its Group companies. Other measures include actively promoting the use of shared security services and related support for information security provided by regional headquarters in the Americas, Europe, Southeast Asia, China, and India.

The Information Security Promotion Council and other bodies convey policies and procedures for information security and personal information protection determined by the Information Security Committee internally and to other companies in the Hitachi Group. Information security officers at business sites and Group companies ensure that these decisions are implemented in the workplace.

Details of our information security initiatives are contained in our Information Security Report.

Information Security Report
https://sustainability.hitachi.com/wp-content/uploads/2022/03/Information_Security_Report_2021_EN.pdf

Achievements in Fiscal 2021

As Hitachi promotes new workstyles based on telecommuting, the vulnerability posed by employees' security awareness becomes a risk. Considering this threat, we are working to raise security awareness among our employees with an employee-centered approach alongside IT-based security measures. Also, given the vigorous acquisition and sale of companies in recent years, we keep an eye on the security conditions during deals/post-merger integration, and take measures to reduce security risks.

Security Monitoring

In Hitachi, the Security Operation Center (SOC) monitors security on an around-the-clock basis so global-scale cyberattacks can be detected and countermeasures initiated right away. The Incident Response Team (IRT) collects and develops threat intelligence*[1] and manages the response to any security incidents.

Cyberattacks become more sophisticated each year, with damage tending to increase as attacks slip past conventional detection and go undiscovered for longer periods. To counter this risk, we are working to enhance cyber monitoring by using endpoint detection and response to monitor equipment operation, as well as implementing authentication. We continue improving and strengthening our cyber monitoring environment using the latest technology.

*[1] Threat intelligence: An approach to countering cyberattacks using knowledge of new threats gathered from multiple sources of information on cyber security.

Preventing Information Leaks

Activities

Hitachi takes the following IT steps to prevent information leaks: encrypting devices; using thin clients;*[1] employing electronic document access control and expiration processing software; maintaining ID management and access control by building an authentication infrastructure; and filtering e-mails and websites. In response to the recent spate of targeted e-mail attacks and other cyberattacks, we are participating in an initiative to share information between the private sector and the government. We are also enhancing various IT measures such as a defense in depth strategy.

To prevent leaks from our procurement partners, we review their information security measures based on Hitachi's own standards before allowing them access to confidential information. We also provide tools to procurement partners for security education and for checking business information on computers. In addition, we require procurement partners to check and remove business information from personal computers.

*[1] Thin client: A terminal with the minimum necessary software. Thin client computing significantly enhances cyber security by storing applications and data on the server.

Note: Hitachi normally refers to its suppliers (including vendors or providers) as "procurement partners" who build business together on an equal footing.

Education on Information Security

Training

Hitachi holds annual e-learning programs on information security and personal information protection for all executive officers and employees. Approximately 35,000 employees at Hitachi, Ltd. take these programs, and the percentage of employees completing these programs reaches 100% every year (excluding those who cannot attend for reasons such as being on leave). The company offers a variety of courses that have different goals and are tailored to different target audiences, including new employees, new managers, and information system administrators. Hitachi, Ltd. also implement simulation training to educate employees about phishing attacks and other cyberattacks. Employees are sent deceptive e-mails as phishing simulations to heighten their awareness of security through direct experiences.

Educational programs from Hitachi, Ltd. are shared within the Group to provide Group-wide education on information security and personal information protection.

Thorough Personal Information Protection/ Information Security Audits and Inspections

Activities

The Hitachi has developed its approach to security based on the PDCA (plan-do-check-act) cycle for its information security management system that Hitachi, Ltd established. Hitachi conducts annual internal audits of personal information protection and information security at all Group companies and BUs.

The President & CEO of Hitachi, Ltd. appoints officers to conduct internal audits. These officers are not allowed to audit their own units, underlining our commitment to fairness and objectivity in auditing.

There are 169 Hitachi Group companies*[1] in Japan that conduct internal audits in the same way as Hitachi, Ltd., and all results are subject to confirmation by Hitachi, Ltd. Hitachi requires Group companies outside Japan to use a common global self-check approach to ensure Group-wide auditing and inspections. All BUs conduct annual self-inspections for Confirmation of Personal Information Protection and Information Security Management, and monthly inspections for operations that involve processing important personal information (740 registered operations as of March 2022). This regular control mechanism ensures ample safety management and implementation.

A dedicated internal security team at Hitachi, Ltd. conducts regular on-site assessments of the state of information security measures, and investigates external vulnerabilities in public-facing servers once every fourth quarter. In this way, Hitachi, Ltd. is working to reduce security risks by identifying discrepancisses with self-checks.

*1 Including partner companies that have submitted voluntarily

Personal Information Protection

Personal Information Protection Policy

Policy | Structure | Activities

Hitachi places great importance on protecting personal information that is entrusted to us by customers or related to our business operations. As a member of the global community, Hitachi commits to protecting personal information in accordance with a vision for personal information protection summarized as providing safety and trustworthiness, and recognizing the importance of individuals' rights.

Hitachi, Ltd.'s Personal Information Protection Policy sets out its corporate philosophy and principles on personal information protection. The policy is disseminated to all executive officers and employees as well as being publicly available.

Hitachi has also established a personal information protection management system based on this policy. Through the rollout of the system, Hitachi is ensuring protection of personal information by such means as safe handling of personal information, educational programs for all employees, and periodic audits.

Personal Information Protection Policy of Hitachi, Ltd.
https://www.hitachi.com/privacy-e/

Responding to Personal Data Protection Laws Around the World

Approach

With the increasing risk of privacy violations in recent years due to the advent of the digital age following advances in IT and the globalization of socio-economic activities, lawmakers are actively seeking to create and modify relevant laws and legislation in countries and regions around the world. Hitachi ensures thorough global compliance with legal frameworks, continues to monitor related legal frameworks and social trends, and implements appropriate measures.

In Japan, Hitachi will report any leakage of personal information and notify affected individuals, as required by the Amended Act on the Protection of Personal Information. In the event that a leak could result in a situation that would harm the rights and interests of individuals, we will promptly report it to the Personal Information Protection Commission and notify the affected individual(s).

Hitachi, Ltd. has also formulated a Group-wide internal code of conduct concerning the protection of personal information, which takes into consideration international legal frameworks such as the European General Data Protection Regulation (GDPR), and put this code of conduct into effect from April 2022. Furthermore, each Group company is strengthening its system for protection of personal information, and is working to ensure thorough and appropriate protection of personal information on a global scale.

PrivacyMark Certification

Activities | GRI 418-1

Hitachi, Ltd. has received PrivacyMark[*1] certification. The entire Hitachi Group is committed to personal information protection; 37 Hitachi Group companies in Japan have been granted the PrivacyMark as of March 31, 2022.

Hitachi also strives to safeguard personal information globally at Group companies outside Japan, based on each company's personal information protection policy, and ensures that they comply with all applicable laws and regulations in each country and region as well as they respond the expectations of society at large. In addition, there were no cases of personal information leakage by Hitachi, Ltd. during fiscal 2021.

[*1] PrivacyMark: A third-party certification established in April 1998 that is granted by the assessment body the Japan Information Processing Development Corporation to businesses that have taken appropriate security management and protection measures related to personal information.

Management of Customer Information

Activities

Hitachi has deployed customer relations management (CRM) systems, which allow us to collect and accurately manage customer and transaction information, in addition to use as a marketing tool. The data collected in these CRM systems enable us to formulate more effective sales strategies and offer collaborative solutions through cooperation by multiple business sites.

Privacy Protection Initiatives by Hitachi's Digital Business Division

Approach | Activities

Under the Digital Systems & Services Sector, which drives our digital business, we have assigned a personal data manager to unify our handing of personal data, and established a privacy protection advisory committee to support risk assessments and develop countermeasures based on its knowledge and expertise of privacy protection. In accordance with the policies set by the committee, our employees implement privacy impact assessments for processes where personal data will be handled and take measures to prevent privacy violations.

Hitachi Privacy Protection Initiatives for the Utilization of Personal Data (In Japanese only)

https://www.hitachi.co.jp/products/it/bigdata/bigdata_ai/personaldata_privacy/index.html

P187 Thorough Personal Information Protection/Information Security Audits and Inspections