Information Security

Basic Concept

While advancements in digital technologies create new value, there is a growing risk of information leaks and shutdowns due to cyberattacks. These attacks become more sophisticated every day and could interfere with business continuity. Risk management related to information security has become one of the most important issues for corporate entities. In response, Hitachi, which aims to be a global leader through our Social Innovation Business, emphasizes cyber security measures from the perspectives of value creation and risk management.

Topic	Overview
Information Security	Based on our information security policy, Hitachi pursues an optimal security structure under the supervision of our chief information security officer (CISO), confirming our sense of unity and agility as One Hitachi. Specifically, we work to prevent information leaks, conduct in-house information security education, and perform internal audits related to information security.
Cybersecurity	To address risks associated with the diversification of cyberattack methods, we expanded the scope of security risk management and strive to reduce business risks in the development and verification environment for creating products and services, production and manufacturing environments, supply chains, and product and service development processes.
Data Protection	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.

Information Security

Approach to Information Security

Approach

The progress of digitization has brought new opportunities for creating value, but this progress also amplifies the risks that businesses face, including information leaks and operational disruptions caused by increasingly sophisticated cyberattacks that impede business continuity. To minimize these risks, risk management related to information security has become one of the most crucial challenges for companies. Against this backdrop, Hitachi, aiming to be a global leader in the Social Innovation Business, is engaged actively in information security initiatives. We recognize cybersecurity measures as a crucial management challenge that addresses both value creation and risk management. Since Hitachi consists of numerous companies, we are pursuing our businesses as a unified group, *One Hitachi*. In line with this business policy, we address information security as One Hitachi, as well, striving to establish optimal security measures and ensure a sense of unity and agility. To this end, we accelerate the security measures based on common initiatives in accordance with the overall Hitachi policy.

Information Security Report
https://www.hitachi.com/sustainability/download/pdf/Infomation_Security_Report_2022_EN.pdf

Information Security Policy

Policy GRI 2-23

Hitachi created an information security policy to protect information assets, including information entrusted to us by our customers, the systems that store that information, and the information systems that provide social infrastructure services. We established various rules and implementation systems based on this policy, and we address the challenges of information security management on an active basis.

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

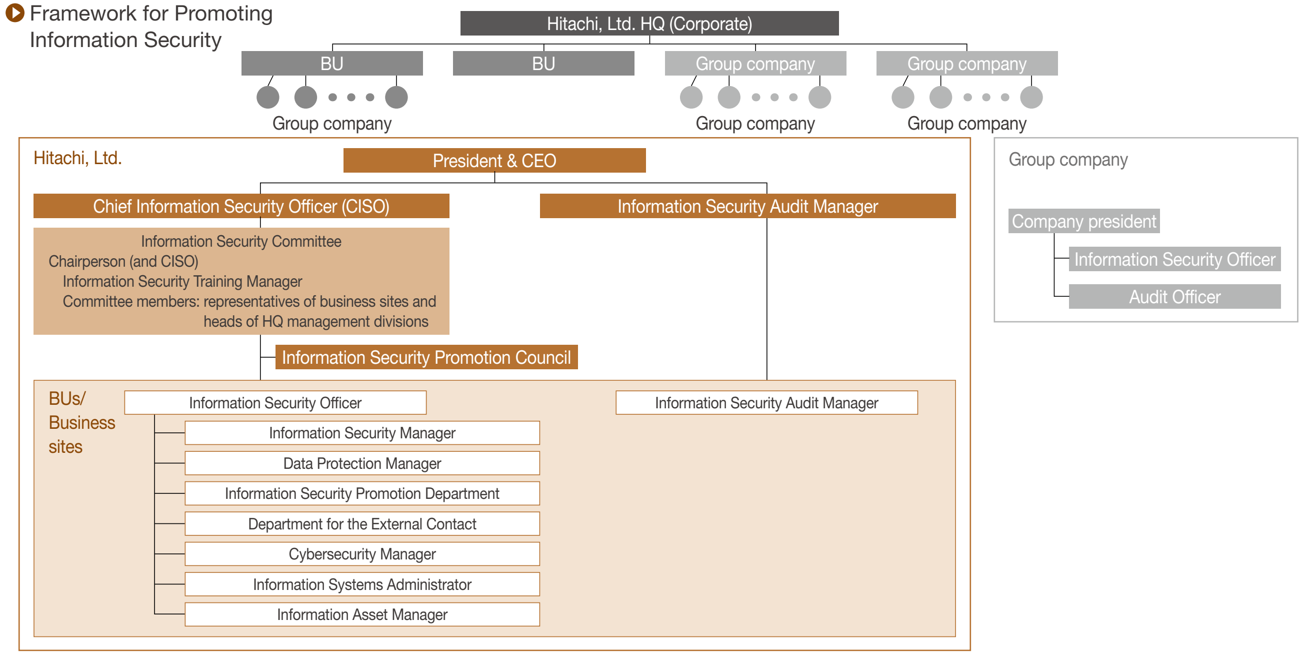
Framework for Promoting Information Security

Structure GRI 2-13/2-24/3-3

The Chief Information Security Officer (CISO) has overall responsibility and authority for implementing and operating information security and personal information protection, and oversees information security for all Hitachi products, services, and internal facilities.

Chaired by the CISO, the Information Security Committee determines all policies and measures for information security and personal information protection. These policies and measures are announced to all Business Units (BUs) and Group companies through channels such as the Information Security

Framework for Promoting Information Security


Hitachi, Ltd. HQ (Corporate)
BU
BU
Group company
Group company
Group company
Group company
Group company
Hitachi, Ltd.
President & CEO
Chief Information Security Officer (CISO)
Information Security Audit Manager
Information Security Committee
Chairperson (and CISO)
Information Security Training Manager
Committee members: representatives of business sites and heads of HQ management divisions
Information Security Promotion Council
BUs/ Business sites
Information Security Officer
Information Security Manager
Data Protection Manager
Information Security Promotion Department
Department for the External Contact
Cybersecurity Manager
Information Systems Administrator
Information Asset Manager
Information Security Audit Manager
Group company
Company president
Information Security Officer
Audit Officer

Promotion Council. BU and Business sites operate their own information security divisions, with the head of the BU or business site serving as information security officers. These divisions 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.

Information Security Management

Activities

Hitachi established a framework for information security management based on the ISO/IEC 27001 international standard. We enhance information security by ensuring information security response measures comply with the United States government standard SP800-171. The Information Security Rules and the Personal Information Protection Rules including *Information Security Standards* are communicated globally by Hitachi, Ltd. and Group companies headquarters. Hitachi also makes use of shared security services and related information security support provided by regional headquarters in the Americas, Europe, Southeast Asia, China, and India.

Preventing Information Leaks

Hitachi engages in a number of IT-related measures such as device encryption, secure PC use, electronic document access control and expiration processing software, ID management and access control via authentication infrastructure, e-mail and website filtering, etc. to prevent information leaks. In response to the recent proliferation of targeted e-mail attacks and other cyberattacks, we not only participate in an initiative to share information between the private sector and the government, but also strengthen various IT measures that include defense-in-depth strategy.

To prevent leaks from procurement partners, we review their information security measures based on Hitachi's own standards before allowing them to 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.

Education on Information Security

Hitachi holds annual e-learning programs on information security and personal information protection for all executive officers and employees. The participation rate in Hitachi, Ltd. in fiscal 2022 was 100% (excluding those who could not attend due to personal leave, etc.). Besides, Hitachi offers a variety of programs depending on the target and aims, such as those for new employees, new managers, and lectures for information system administrators. Hitachi also implements simulation training to educate employees about phishing attacks and other cyberattacks. Employees receive deceptive e-mails as phishing simulations to heighten their awareness of security through direct experience.

Training programs in Hitachi, Ltd. are shared with the Group companies in order to actively implement training on information security and personal information protection in the entire group.

Information Security Management Evaluation and Monitoring

Hitachi implements information security and privacy protection initiatives based on the PDCA cycle of the information security management systems stipulated by Hitachi, Ltd. We conduct regular audits and inspections to monitor and evaluate whether management and measures for information security and data protection are implemented properly in each department.

All divisions of Hitachi, Ltd. and Group companies in Japan conduct annual internal audits of personal information protection and information security. Internal audits at Hitachi, Ltd. are conducted independently by audit managers appointed by the President and CEO. They are not allowed to audit their own units, which underlines our commitment to fairness and objectivity in auditing. The Group companies in Japan conduct internal audits equivalent to Hitachi, Ltd., and all audit results are confirmed by Hitachi, Ltd.

Hitachi requires Group companies outside Japan to use a common global self-check approach to ensure groupwide inspections. All departments in Hitachi, Ltd. perform self-directed personal information protection and information security operation checks annually. In addition, departments involved in operations that handle important personal information (739*[1] related operations identified as of March 2023) perform personal information protection operation checks every month. Through these measures, we check operational status regarding personal information regularly.

Hitachi is also engaged in groupwide security risk reduction activities through regular on-site assessments of the status of information security measures. A team of in-house security specialists is responsible for identifying any deviations arising from self-checks. Further, Hitachi, Ltd. and Group companies in Japan contract with an external organization to conduct quarterly external vulnerability assessments of servers open to the public and other external vulnerabilities.

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

Cyber-Security Initiatives

Activities

To address the risks posed by the increasing diversification of cyber-attack methods, origins, and impacts, Hitachi is expanding the scope of our security risk management. Traditionally, we focused risk management on response measures for internal IT environments. To reduce business risks going forward, we will include the development and verification environments used to create products and services, production and manufacturing environments, and the supply chain and product/service development process.

Cyber-Security Management

Hitachi established standards for internal IT environment-related vulnerability response measures and network security. We also require BUs/Group companies to conduct regular status assessments of these measures and perform corrective actions. As a companywide measure, we launched an initiative to monitor vulnerability mitigation for each device and follow up with users/administrators to expand the application of such measures.

In the development/test and production/manufacturing environments, we established standards and guidelines for infrastructure construction and operations to ensure security compliance in each environment, and we pursue measures based on these guidelines within the Hitachi Group. We also share information security requirement standards established by Hitachi with our procurement partners, working cooperatively to enhance security.

We established management guidelines to address and maintain the security of products and services, and we follow measures based on these guidelines within the Hitachi Group.

Cyber-Security Monitoring

The Hitachi Security Operation Center (SOC) monitors security on an around-the-clock basis to ensure global-scale cyberattacks are detected and response measures initiated immediately. The Incident Response Team (IRT) collects and develops threat information and manages our response to any security incidents.

Cyber-attack methods are becoming more sophisticated every year, with an increasing number slipping past detection systems. More often, these attacks tend to go undetected for long periods, resulting in increased damage. In this context, Hitachi strengthens cyber surveillance through Endpoint Detection and Response (EDR)*[1] to monitor device behavior and perform authentication protection. We continue to improve and strengthen our cyber monitoring environment using the latest technology.

*1 Systems to monitor suspicious behavior and respond quickly to attacks on endpoint devices such as computers.

Data Protection Initiatives

Activities GRI 418-1

As digital technology continues to advance, the global trend toward leveraging data only accelerates. This situation has led to heightened interest in the protection of personal information and cross-border data exchange. In such an environment, Hitachi places significant importance on personal information protection initiatives to ensure the secure management of personal information received from customers and personal information involved in business operations. As a member of the global community, Hitachi is committed to protecting personal information in accordance with our vision for personal information protection, which is to provide safety and trustworthiness, and to value individual rights.

Personal Information Protection

Hitachi, Ltd. established the Personal Information Protection Policy which is announced to all executive officers and employees, and is also publicly available. Hitachi created a personal information protection management system based on this policy. This system ensures the protection of personal information by such means as appropriate management of personal information, educational programs for all employees, and periodic audits. We do not share personal information with third parties without data subject's prior consent. Even in cases where prior consent is obtained, Hitachi requires the third party to whom the data is provided to comply with Hitachi's Personal Information Protection Policy.

Hitachi also strives to safeguard personal information globally based on each company's personal information protection policy, and we ensure that these companies comply with all applicable laws and regulations in each country and region, as well as to the expectations of society at large.

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

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

Governance

Corporate Governance
Business Ethics and Compliance
Risk Management
Information Security
Executive Summary
Information Security
Governance Data

PrivacyMark Certification

Hitachi, Ltd. obtained PrivacyMark[1] certification, which is a third-party certification of personal information protection. The entire Hitachi Group is committed to personal information protection, and 37 Hitachi Group companies in Japan have been granted the PrivacyMark as of the end of July 2023.

[1] PrivacyMark: A third-party certification 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 (invested by Japan Information Processing Development Corporation).

Privacy Protection Initiatives

In response to social demands for privacy protection measures, Hitachi, Ltd. aims to provide more appropriate and high-quality services and products, and foster trust with consumers and other stakeholders, by balancing privacy protection and the use of personal data.

In 2014, we established the position of personal data officer to oversee personal data handling in Digital Systems & Services, which drives our digital business. We also established the Privacy Protection Advisory Committee to consolidate our knowledge on privacy protection, support risk assessments, and consider response measures.

Further, we began companywide effort by adopting the Hitachi Privacy Impact Assessment (PIA) in 2023.

Through these initiatives, we structure measures to prevent issues related to privacy, implementing privacy impact assessments for operations that involve personal data handled by employees.

Responding to Personal Data Protection Laws Around the World

With the increasing risk of privacy violations, 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 complies with the Amended Act on the Protection of Personal Information, and in the event that a leak may result in a situation that would harm the rights and interests of individuals, Hitachi promptly report said leak to the Personal Information Protection Commission and notify the affected individuals. We recorded one case of personal information leakage at Hitachi, Ltd. during fiscal 2022. We identified the scope of the impact related to this incident and took appropriate action.

Hitachi also formulated a groupwide internal code of conduct concerning the protection of privacy, which takes into consideration international legal frameworks such as the European General Data Protection Regulation (GDPR). This code of conduct became effective as of April 2022. Moreover, individuals responsible for personal data protection are appointed in each Group company, and support functions for regional group companies have been established within each regional headquarters. In this way, we ensure consistent personal information protection on a global scale.

Third-Party Evaluations and Certifications

Activities

Hitachi encourages the acquisition of third-party evaluations and certifications for information security management. Our data centers and other divisions obtain certification from the ISMS Accreditation Center (ISMS-AC) in accordance with the ISO/IEC 27001 Information Security Management System international standard. Eight divisions have received this certification at Hitachi, Ltd., and 28 divisions representing 23 Group companies[1] have also received this certification.

[1] As of the end of June 2023