Compliance & Risk Management

We will report on our efforts toward compliance and risk management, which are the foundations that support our corporate activities.

Compliance

Basic Approach to Compliance

In 2004, our 50th anniversary, aiming to be a company that is trusted by society both in name and reality, and one that develops and grows in an enduring manner, we established our “Compliance Declaration,” which expresses the determination of top management to tackle compliance, and the “TACHI-S Code of Ethical Practice,” which provides specific standards of conduct based on corporate ethics.
At the same time, to ensure corporate activities based on the TACHI-S Code of Ethical Practice, we have established “Compliance Management Regulations,” which stipulate the compliance-related management organization and measures to be taken in the event of a violation of the TACHI-S Code of Ethical Practice, and “Internal Reporting System Standards,” which stipulate the operation method of the internal reporting system. These systems were established to ensure that all officers and employees comply with laws and regulations and conduct corporate activities ethically.
Based on the above, our corporate management will enhance its ability to purify ourselves as a company, to promote sincere corporate activities, and to continue to be a company that is trusted by all stakeholders.

Compliance Declaration

Thanks to the efforts of many over the years, the TACHI-S Group has earned a reputation as a sincere and earnest company with technological capabilities and has built its current position through this trust. We will sincerely strive to continue to be a company that is trusted by society, because we recognize that this is an absolute requirement for corporate growth and development. As we celebrate the 50th anniversary of our founding, we have clarified our code of conduct and established it here as the “TACHI-S Code of Ethical Practice.” We will make this Code of Ethical Practice the basis of our actions and strive to practice the following.

1. We will fully consider our impact on the environment, provide products that are useful and safe for society, ensure corporate transparency, and strive to live up to the trust of all our stakeholders.
2. We will comply with all laws and rules, including the spirit of such laws and rules, both in Japan and abroad, and act with social common sense.
3. We will act responsibly and cultivate ethical values as a good corporate citizen, based on the spirit of our company motto, “Cooperation Through Mutual Compromise.”

We hereby pledge to comply with the “TACHI-S Code of Ethical Practice” and to promote compliance-based corporate activities.

Developed April 25, 2004

Compliance Promotion System

To ensure compliance with the TACHI-S Code of Ethical Practice, the following compliance system has been established.

[Ethics Committee]

The committee is chaired by the President and consists of all Directors and relevant Executive Managing Officers as committee members. It plays a role in maintaining and strengthening the compliance system (Secretariat: Management Audit Office, held once a year in principle).

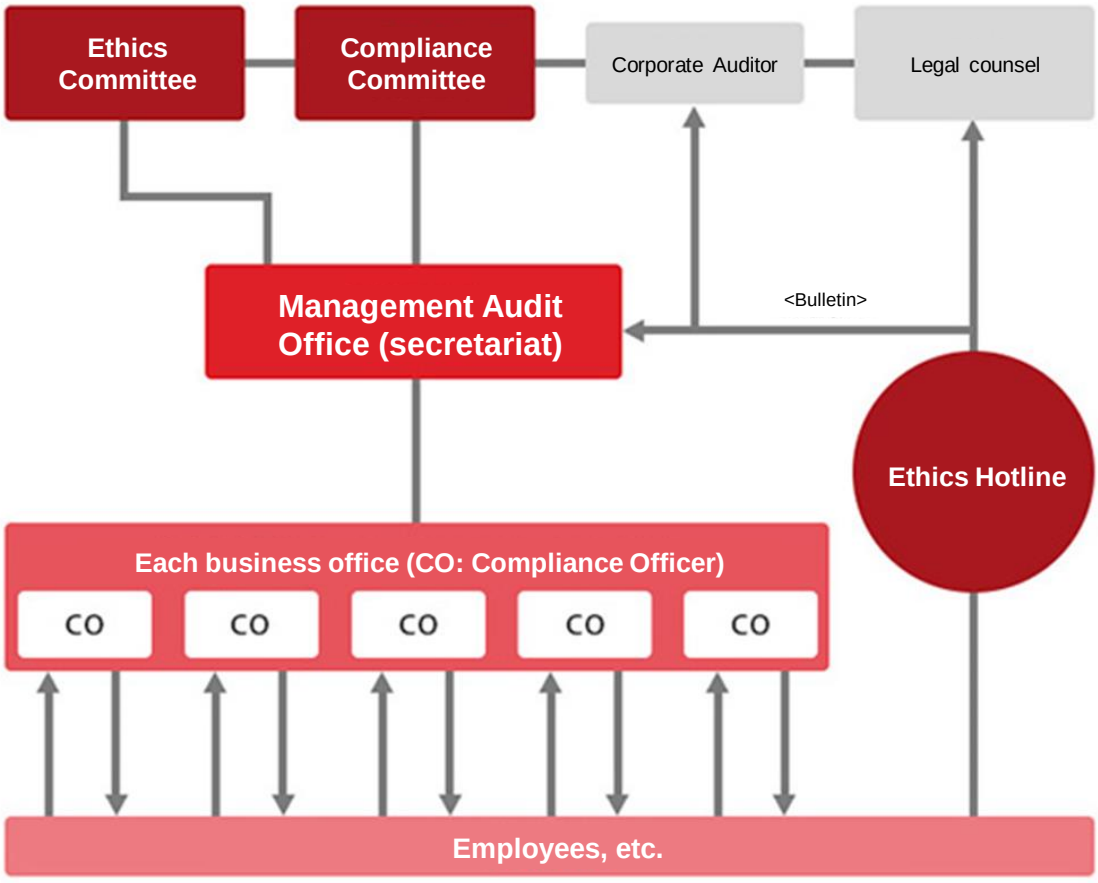
[Compliance Committee]

The committee is chaired by a Compliance Officer and consists of Outside Directors, Corporate Auditors, and legal counsel as committee members, and is responsible for directing investigations into the facts of cases involving violations of ethics or laws and regulations, and for making recommendations on such violations (Secretariat: Management Audit Office, convened by the committee chair as necessary).

[Compliance Officer]

A corporate ethics officer assigned to each business site regarding compliance,
and is responsible for providing advice on consultation from employees and supporting the operation of the compliance system.

Compliance System



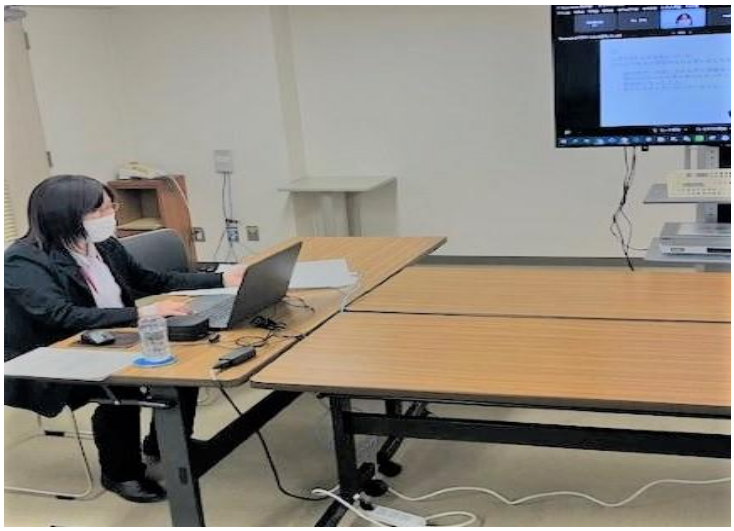
Raising Awareness of Compliance

We formulate compliance action plans every year with the theme of “Each and every employee should view compliance as a matter of familiarity and practice it in their daily work,” and we conduct the following educational activities.

Activities to raising awareness of compliance

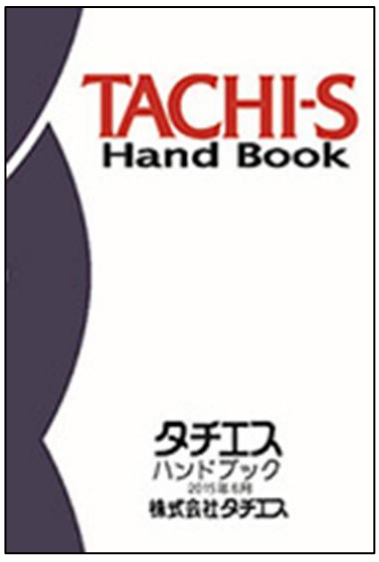
・Conducting compliance education for all employees at certain times after joining the company (e.g., new employee or new manager education), and at different levels.
・A corporate ethics workshop is conducted each year as part of Corporate Ethics Reinforcement Month by an outside lecturer for Directors, Managers, and representatives of domestic subsidiaries.
・Regularly publishing the “Compliance Letter,” which communicates familiar compliance cases in an easy-to-understand, four-panel cartoon format, and the “Compliance Mail Magazine,” which contains news of public interest and mini-tests.

Corporate Ethics Workshop (November 2022)



In addition, the “Compliance Declaration,” “Compliance Management Regulations,” “Internal Reporting System Standards,” and “TACHI-S Code of Ethical Practice” are compiled into a compact handbook that is easy to carry, and which is distributed to all employees to promote compliance awareness.

The “TACHI-S Handbook” used to raise awareness



Internal Monitoring

To comply with laws and regulations and engage in ethical corporate activities, we believe it is important to develop and operate an “internal monitoring system” to serve as a foundation for preventing injustice and unethical behavior, and for identifying problems at an early stage should they occur. An “internal reporting system” has been established at all Group companies to handle consultations and reports on fraudulent, illegal, or unethical activities by organizations or individuals, as well as violations of our own Code of Ethical Practice and internal rules.
In addition, we regularly conduct “business audits” to confirm appropriateness, compliance, and effectiveness of operations in departments that execute business. During these audits, we also check the status of ethics and legal compliance.
Furthermore, we conduct annual compliance awareness surveys of our employees to ascertain their level of understanding and awareness of compliance, and we use this information in educational activities.

Risk Management

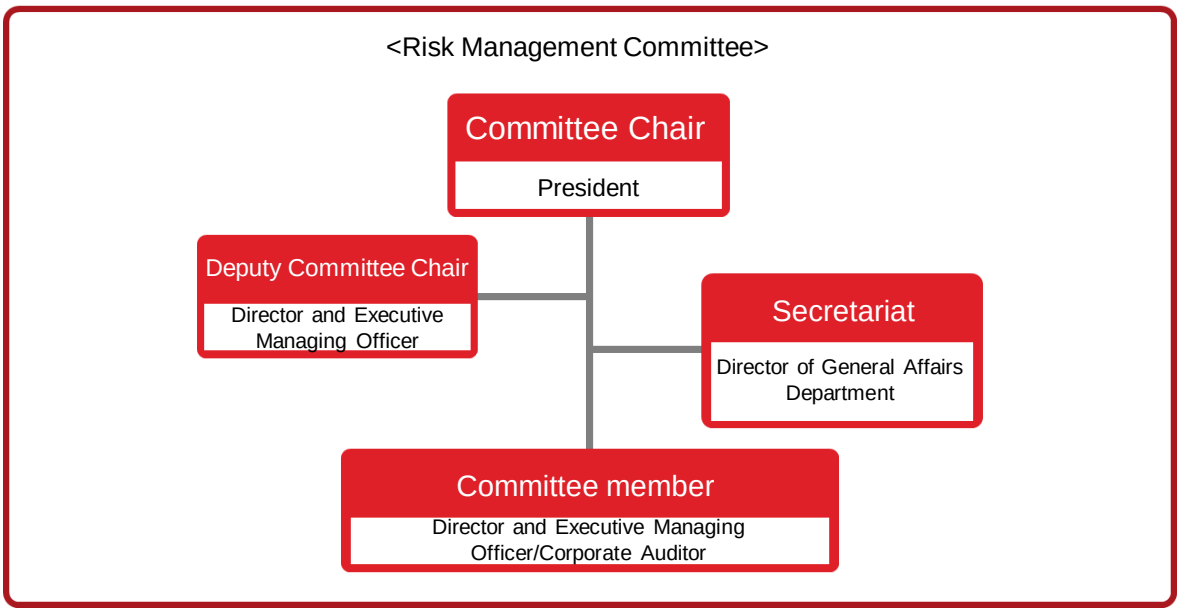
Basic Approach

As the environment surrounding companies changes drastically, and risks become ever more diverse, we conduct risk management activities to identify risks and take prompt and appropriate countermeasures.

Risk Management System

We have established a Risk Management Committee chaired by the President that consists of other Directors and Executive Managing Officers as committee members, and with the participation of Corporate Auditors and the General Affairs Department Director. The General Affairs Department serves as the secretariat for risk management-related deliberations and decisions.

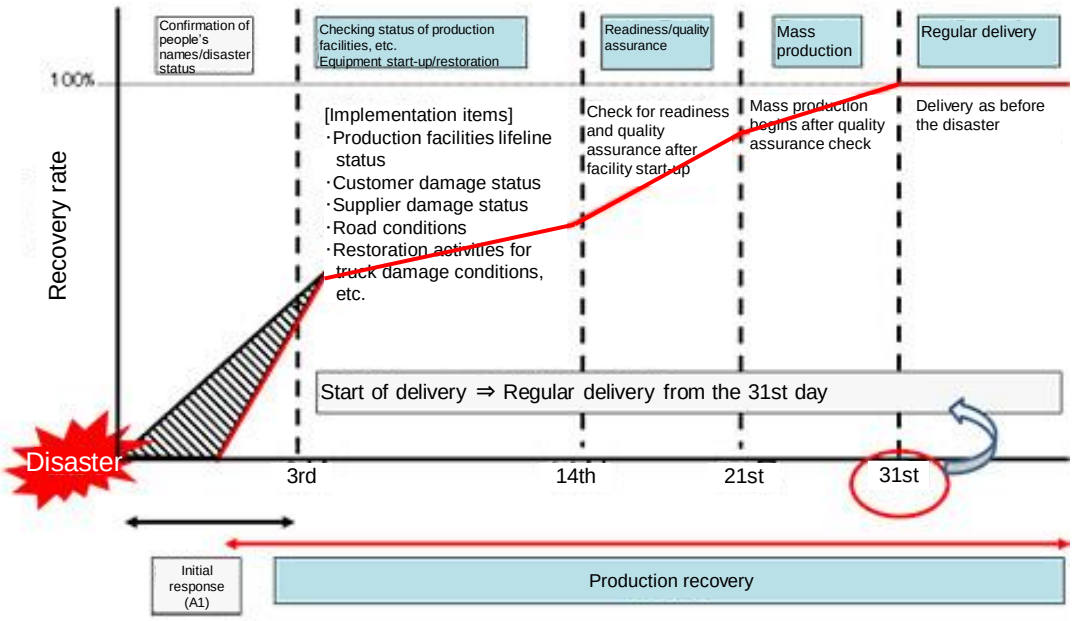
Risk Management System



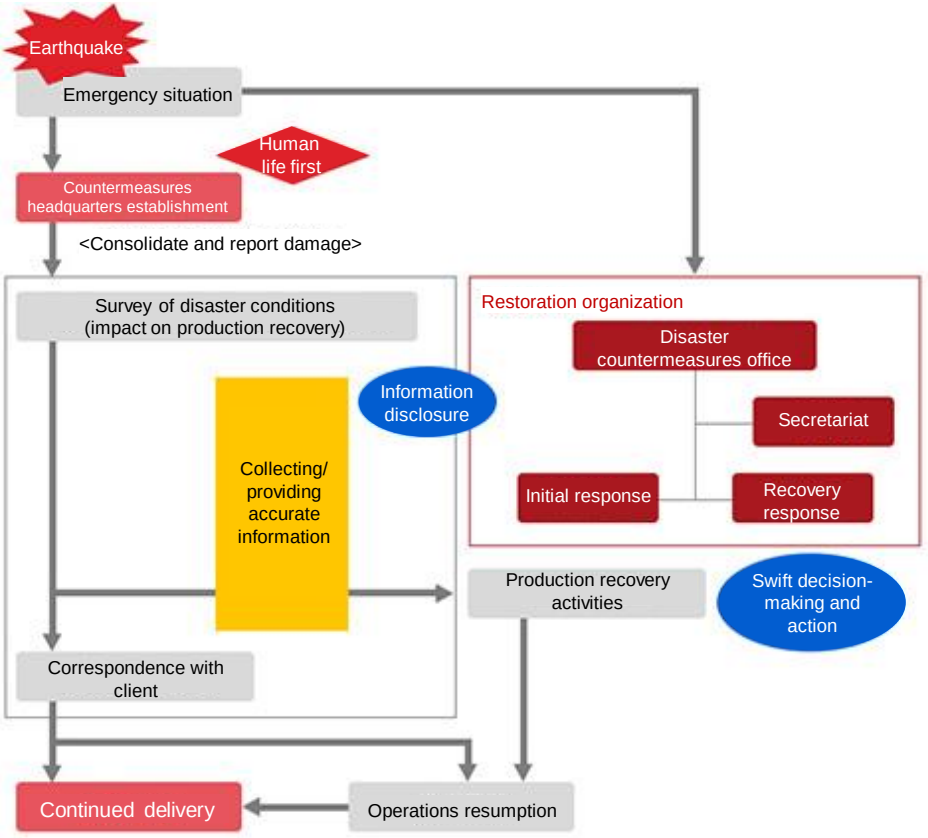
Business Continuity Plan (BCP)

We have formulated a Business Continuity Plan (BCP) to minimize damage and swiftly restore operations in the event of a major disaster or accident occurrence. Specifically, assuming the occurrence of a major earthquake, the scope of production restoration and the flow to restore production are defined to restore production activities as soon as possible.

Production recovery scope



Production recovery flow in the event of an earthquake

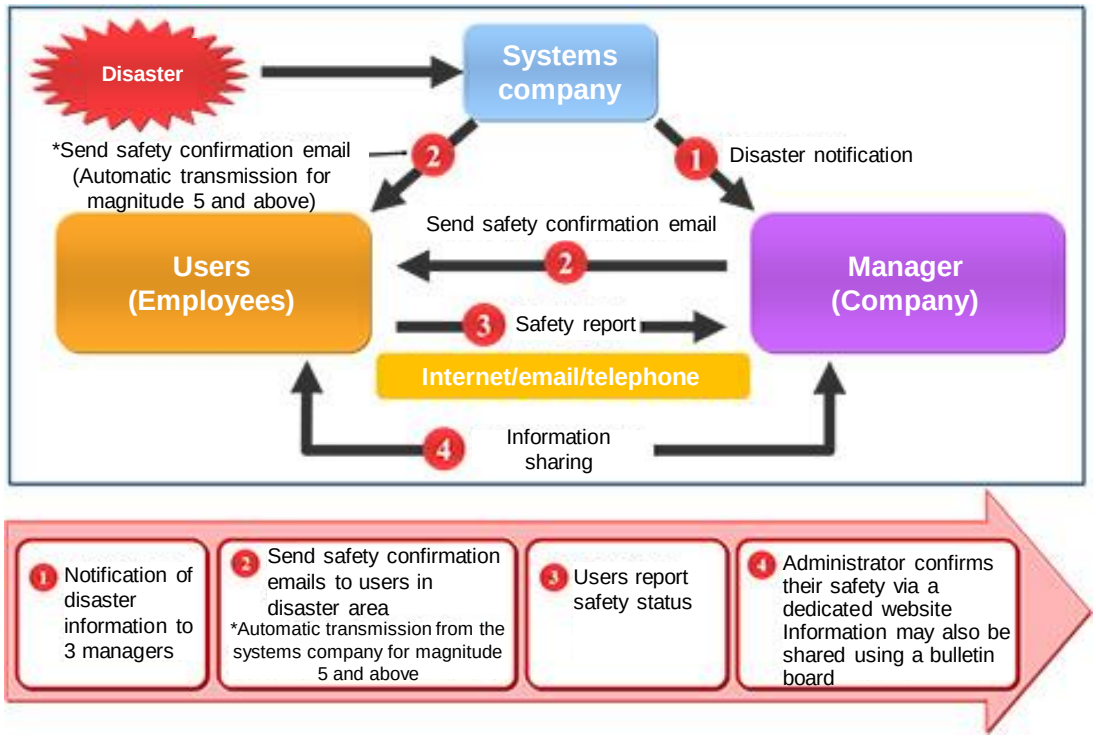


BCP training

Implementing a System to Confirm Employee Safety

In the event of a disaster, it is imperative that employee safety be confirmed, means of communication secured, and information shared. Based on the necessity to introduce an efficient and reliable system, we introduced a safety confirmation system from a systems company as a means of confirming and communicating the safety of our employees in the event of a disaster or other emergency as part of our disaster prevention system. In addition, regular training is conducted to ensure that employees are proficient in system operation and that the system is operating normally.

Overview of the safety confirmation system



Internal Reporting System

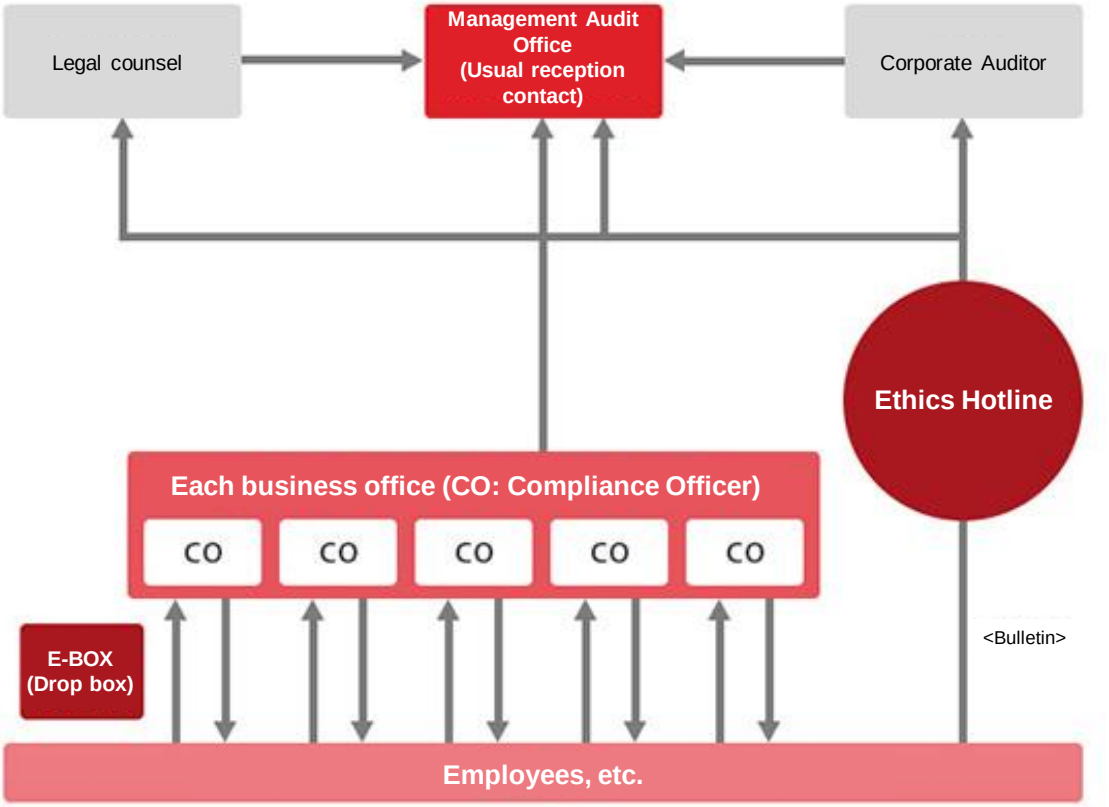
The Purpose of Introducing the Internal Reporting System

We introduced an internal reporting system to promptly discover fraudulent, illegal, or unethical acts by organizations or individuals, or acts that violate the TACHI-S Code of Ethical Practice or the Code of Conduct, to minimize risk to the company caused by violations of the Code of Ethical Practice, and to promote compliance.

Internal Reporting System Structure

The name of our internal reporting system is the “Ethics Hotline.” All TACHI-S employees, including officers and all others who have an employment relationship with TACHI-S (temporary employees, etc.), are eligible to use this system and are informed about it. In addition, in accordance with the “Whistleblower Protection Act,” the contact point for reporting may be selected from among legal counsel, corporate auditors, or the Management Audit Office, and reporting may be done anonymously. We accept reports and consultations via dedicated telephone line, dedicated mail, E-boxes (suggestion boxes) set up at each office, email, telephone, in writing, and in person.

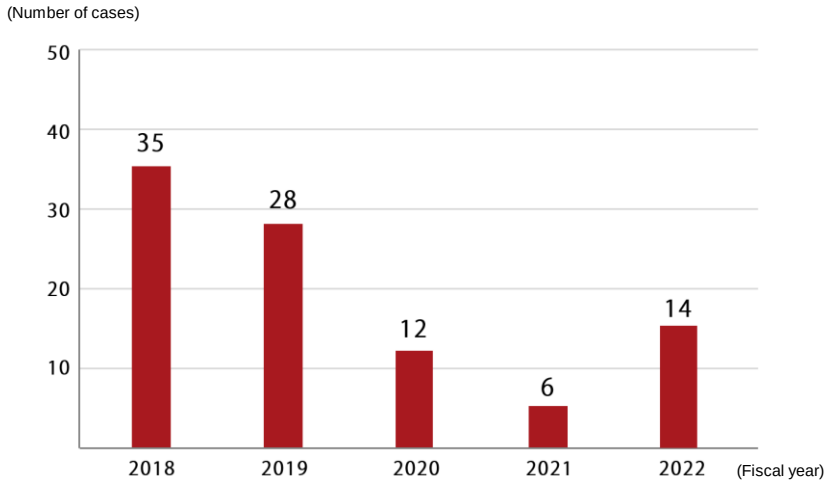
Ethics Hotline consultation and reporting flow



Occurrence of Internal Reporting

The number of cases reported to the Ethics Hotline is as follows.

Number of consultations and reports to the Ethics Hotline (TACHI-S and affiliates)

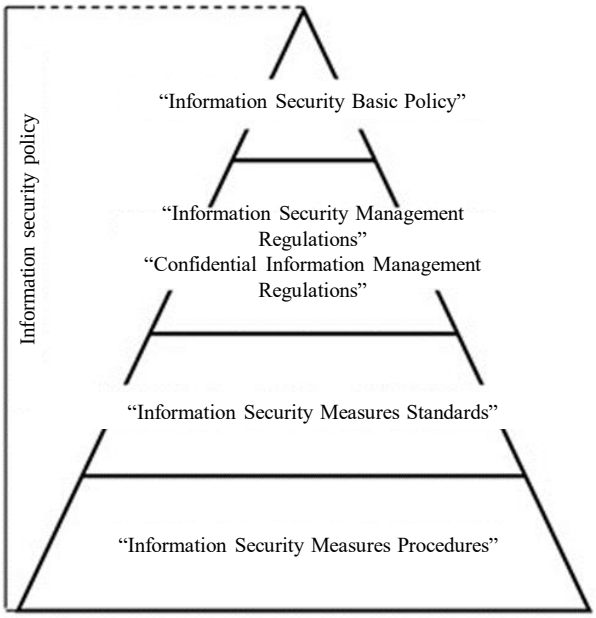


Information Security

Basic Policy on Information Security

To protect our information assets, we have established a basic policy on information security. Based on this policy, we will work on continuous information security measures to prevent information leaks and other problems from occurring and maintain the trust of our customers. Our Information Security Policy is a clear statement of the policies and standards set to protect the information assets of the organization and consists of the following.

Information security policy system



Information Security Policy

1. Subject of Information

Information assets are not limited to hardware, software, networks, and files. They also include documents necessary for business, information obtained in the course of business, knowledge, and knowhow.

2. Proactive Measures for Information Assets

Our information assets will be used as effectively as possible and appropriate information security measures will be implemented in accordance with the given asset's level of importance.

3. Incident Response Measures

In the unlikely event of a breach, the cause of the breach will be swiftly identified and action will be taken to minimize damage.

4. Promotion System

With the understanding and support of Directors, the Information Security Committee shall be responsible for the development and operation of a company-wide information security system.

5. Education

Awareness and education activities regarding information security will be continuously conducted for all employees, including Directors and contract employees.

6. Employee Obligations

All employees, including Directors and contract employees, shall understand the Basic Policy on Information Security and act in accordance with the relevant regulations.

7. Penalties

Strict measures will be taken against those who violate the Basic Policy on Information Security and related regulations.

Developed March 27, 2007

Initiatives to Strengthen Information Security

To raise employee awareness of the necessity and importance of information security, in February and March, which is the government's "Cyber Security Month," we conduct employee education using our internal portal to check the level of understanding. In addition, to promptly inform employees of information security threats and prevent information leaks, an internal portal for "security incident alerts" and an information security contact point have been set up, and we are always working with employees to respond to problems.
The security system is divided into entry, exit, and individual countermeasures, which are periodically evaluated. Entry countermeasures prevent viruses from entering the company through email, web browsing, or external attacks. Exit countermeasures prevent information leakage outside the company in the event that an internal computer is infected with a virus. Individual countermeasures include software to monitor computer behavior and controls that block the use of USBs to prevent direct introduction of viruses. Security systems are already installed for both entry, exit, and individual measures. In addition, these systems are monitored 24/7/365 to ensure protection from viruses.
To respond to information security risks that continuously occur, we are strengthening our countermeasures and monitoring on a regular basis. We also take comprehensive information security countermeasures to ensure that our employees can use our IT environment safely.

Countermeasures against information security risks in IT usage environments

Ongoing enhancements focused on countermeasures against increasingly sophisticated cyber attacks

(1) External/internal communication restrictions (communication restrictions and record keeping)
(2) Incoming email virus and spam prevention
(3) Public server attack prevention
(4) Remote connection security enhancement (authentication)
(5) Measures against information leaks when sending mail
(6) Control of dangerous internet browsing
(7) Virus infection from internet browsing and unauthorized communication countermeasures
(8) PC information leakage countermeasures (device encryption)
(9) Unauthorized external media connection restrictions (operation record retention)
(10) PC and server virus protection and monitoring