7-3 Risk Management

Basic Policy

In order to ensure the continuation of operations based on safety and reliability, our Group has established a company-wide risk management system that correctly identifies risk factors related to our Group's business activities, and continuously examines and implements measures to reduce the likelihood of occurrence of such risks and to minimize losses in the event of occurrence of such risks.

Promotional Structure

Asahi Intecc's Board of Directors has established various rules and regulation such as crisis management rules and rules for managing related parties, etc., in order to prevent risks that could significantly impact our Group's operations and to manage losses that have occurred, and it has also established a risk management system that spans across the entire Group.

Regular risk management concerning our Group's day-to-day operations are carried out appropriately within the scope granted to each department in accordance with the regulations on administrative authority. In addition, each department in the Administration Division verifies and confirms the risk management status of each division of our Group based on their expertise and knowledge of each business process. Each department is supposed to report any problems to the Board of Directors.

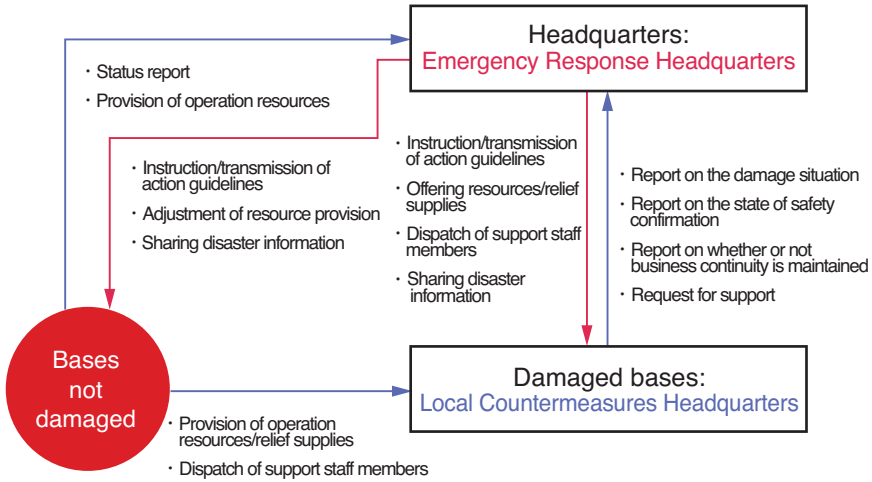
Response to Large-Scale Disasters

Basic Thinking

Our Group aims to rapidly become an international company by developing and stably supplying products that consistently exceed the expectations and the needs of the market by establishing the highest levels of reliability and safety and by contributing to medical care around the world.

In normal times, our Group will plan and implement countermeasures against risks such as large-scale disasters and pandemics. In the event of an emergency, the highest priority will be given to ensuring human lives and safety, and we will continue to provide relief and support in the affected areas and supply products stably.

■ Roles of Emergency Response Headquarters



Emergency Response Headquarters

In the event of an emergency, such as a disaster, in our Group, the emergency response headquarters headed by the President & CEO shall be responsible for crisis management in accordance with the crisis management rules, in order to ensure quick and appropriate response. By establishing a centralized information communication system, etc., we will protect the safety of the employees and the local community while endeavoring to stably supply products.

7-3 Risk Management

BCP (Business Continuity Plan)

Our Group is proceeding with formulating the Asahi Intecc Group BCP (Business Continuity Planning) with the aim of continuity/early restoration of our business activities and the system of delivery of our products to our customers in case of emergency. We define tasks to realize continuity/early restoration of priority operations and essential tasks for corporate operations for each group, and take measures in the case of emergency based on this planning.

BCP Basic Policy

1. Give top priority to securing the safety of each person.
2. Assess the damage situation and strive for early restoration to normal operation activities of the corporation to minimize the effects on our customers.

BCP (Business Continuity Plan) for Production Bases

As part of our Group's BCP (Business Continuity Plan), production diversification is underway at the Thailand Factory, the Hanoi Factory, and the Cebu Factory.
In addition to moving forward with the production transfer from the Thailand Factory to the Hanoi Factory, production transfer is also underway from the Hanoi Factory to the Cebu Factory. Concerning the transfer, manufacturing facilities, equipment, and jigs designed and manufactured at the Thailand Factory and the Hanoi Factory will be introduced to the Cebu Factory, establishing a stable production line.

Our Group is required to build a system for stable delivery of our products under any circumstances as a duty of a medical device manufacturer, which brings products involved in the lives of patients to society.

Disaster Prevention Handbook

7-3 Risk Management

Information Security Basic Policy

(1) Basic Policy

In order to deal with the information security risks that are becoming increasingly serious day by day, in addition to complying with laws and regulations, guidelines, and other societal norms concerning information security, we have implemented information security measures necessary to protect Asahi Intecc's clients and business operation based on the perspectives outlined below.

(2) Information Security Risk Management System

Our Group has appointed a Chief Security Officer to promote an information security system, manage risks concerning information security, and ensure the organization-wide implementation of various measures, and the entire company works towards information security.

Initiatives to Strengthen Information Security

Implementation of Information Security Measures

Our Group has established its Information Security Regulations and implements human, organizational, and technical measures to reduce the risk of information asset leakage, alteration, loss, and information system outages due to cyber-attacks, damage to facilities, and communication problems. To respond to increasingly sophisticated and diverse information security risks in recent years, we periodically review our measures, appropriately prioritize the risks that could occur, and continue to implement security measures.

Information Security Training

As part of information security training, our Group provides group training when employees join the Company and distributes regular security education content utilizing E-learning, with the purpose of fostering a sense of ethics and security awareness. Furthermore, we aim to maintain and improve security awareness by implementing targeted attack email training and regularly disseminating information about incidents that have occurred either inside or outside of the Company that could serve as lessons, as well as the latest trends in suspicious emails and viruses that are mainstream in the public domain. Going forward, we will continuously add security training content and expand types and frequencies of training to enhance the content of the information security training that our Group has provided to date.

Incident Response

In addition to introducing a mechanism to monitor and block the occurrence of cyber-attacks, ransomware, information leaks, etc., we have developed the necessary systems for incident response (CSIRT) in advance, such as the reception of incident occurrence, support for response, and consideration of measures to prevent recurrences. In order to limit the spread of damage and the occurrence of secondary damage, our Group continually reviews the necessary systems and procedures to enable prompt and effective incident response, and continuously enhances its ability to respond to incidents.

Internal Audit

Internal audits are conducted regularly to ensure information security. We specifically emphasize audit results concerning the handling of personal and confidential information, and we have a system in place to follow up on the completion of improvement measures when improvement is deemed necessary.

Human measures

- **Establish a system for responding to information security incidents (accidents)**
  Establish a CSIRT (Computer Security Incident Response Team) system to collect and analyze vulnerability information, respond to incidents, and share information and collaborate with internal and external organizations
- **Implementation of information security training**
  Implement company-wide targeted attack email training and training in anticipation of incidents

Technical measures

- **Enhancing PC/server security**
  - Measures against computer viruses: Introduce a mechanism to constantly monitor all servers and PCs for suspicious activities and immediately shut them down if detected
  - Development of backup environment: Establish an environment to recover data for important servers in the event that data is erased or encrypted
- **Enhancing internet security**
  - Web filtering: Develop a mechanism to block access to suspicious and malicious websites such as fraudulent websites
  - E-mail countermeasures: Develop a mechanism to detect and reject suspicious and fraudulent e-mails
- **Enhancing network security**
  Develop a mechanism to restrict access to the internal network

7-3 Risk Management

Reference: Risk Model

Examples of Possible Risks

The chart to the right shows a wide range of risks, including risks that could impact investor decisions. Statements about the future in the text are based on the judgments made by our Group as of the end of FYE June 2024 and can be associated with the seven key issues of sustainability.

		Key issues
①Medical Field	Legal Regulations	Supplying safe and secure products
	Health Care Reforms	Supplying safe and secure products
	Quality Control System	Supplying safe and secure products
	Dependence on Specific Products	On-site problem-solving through innovation
	Dependence on Sales in Specific Regions	Strengthening risk management
	Response to Technological Innovation	On-site problem-solving through innovation
	Purchase from Specific Suppliers	Supply chain management
②Industrial Field	Customer Specification	
	Competitive Landscape	On-site problem-solving through innovation
③Common Issues in Each Field	Overseas Business Development	Strengthening risk management
	Dependence on Overseas Production	Supply chain management
	Price Increase in Raw Materials	Supply chain management
	Intellectual Property Rights	On-site problem-solving through innovation
	Natural Disasters and Large-Scale Disasters	Strengthening risk management
	Impact of Epidemics and Infectious Diseases	Strengthening risk management
	Risks due to Climate Change	Measures to reduce environmental burden
④Company-Wide Matters	Foreign Exchange Risks	
	Equity Risks	Strengthening corporate governance
	Acquisition Risks	Strengthening corporate governance
	Impairment and Valuation Loss Risks	Strengthening corporate governance
	Information Security	Strengthening risk management
	Industrial Safety and Product Safety Risks	Supplying safe and secure products
	Securing Global Human Resources	Strengthening global human resources
	Human Rights Risks	Supply chain management
	Corruption Prevention	Supply chain management