

KIRIN

キリンホールディングス株式会社
Kirin Holdings Company, Limited



INFORMATION SECURITY REPORT

For information security that goes from “supporting the company” to “leading the business”

We are leading the Group’s information strategies through information system governance, by integrating the information system functions (people, goods, and money) of the entire group and being involved in the entire IT lifecycle from IT strategy development to implementation of projects.

Information Security Basic Policy

Under this Policy, rules are established regarding information security and information is managed appropriately.

Rules are also revised as and when appropriate in accordance with changes in the internal and external environment, to maintain our security standards without security operations becoming outdated.

As businesses have become increasingly dependent on IT and IT-related incidents are becoming risks that threaten the very existence of those businesses, as a company, we believe that it is important, for the development of our businesses, to explain the actions we are taking against such risks through our Information Security Report.

We hope that, by proactively releasing this Information Security Report, we will gain the trust of our customers, which will lead to the healthy development of the industry as a whole.

Structure of Information Security Regulations

- Establishment, implementation, and sustainable improvement of the information security management system
- Implementation of education
- Business sustainability management
- Compliance with laws and regulations, rules, and contractual requirements

■ Privacy Policy

<http://www.kirinbs.co.jp/privacy2.html>

*Some of our group companies have established their own separate Privacy Policies.

■ Website

<https://www.kirinholdings.co.jp/>

■ Period Covered by this Report

This report covers actions and initiatives related to information security between January and December 2019.

■ Companies Covered by this Report

This report covers all Group companies, but not all of the actions and initiatives described in the report were taken at all companies.

CONTENT

Information Security Governance	6
Information Security Framework	8
Framework for Responding to Information Security Incidents	10
Information Security Risks	11
Information Security Measures	15
Information Security-related Human Resources Development	19
Information Security Track Records	24



This booklet is a compilation of the information security reports of the entire Kirin Group, with reference to the Information Security Report Model issued by the Ministry of Economy, Trade and Industry.



Our aim is to raise awareness among employees by establishing our own rules for Kirin Group businesses.

INFORMATION SECURITY GOVERNANCE

The Kirin Group aims to raise awareness among our employees by establishing the Kirin Group businesses' own rules, based on the policy and regulations, as well as general information security rules.

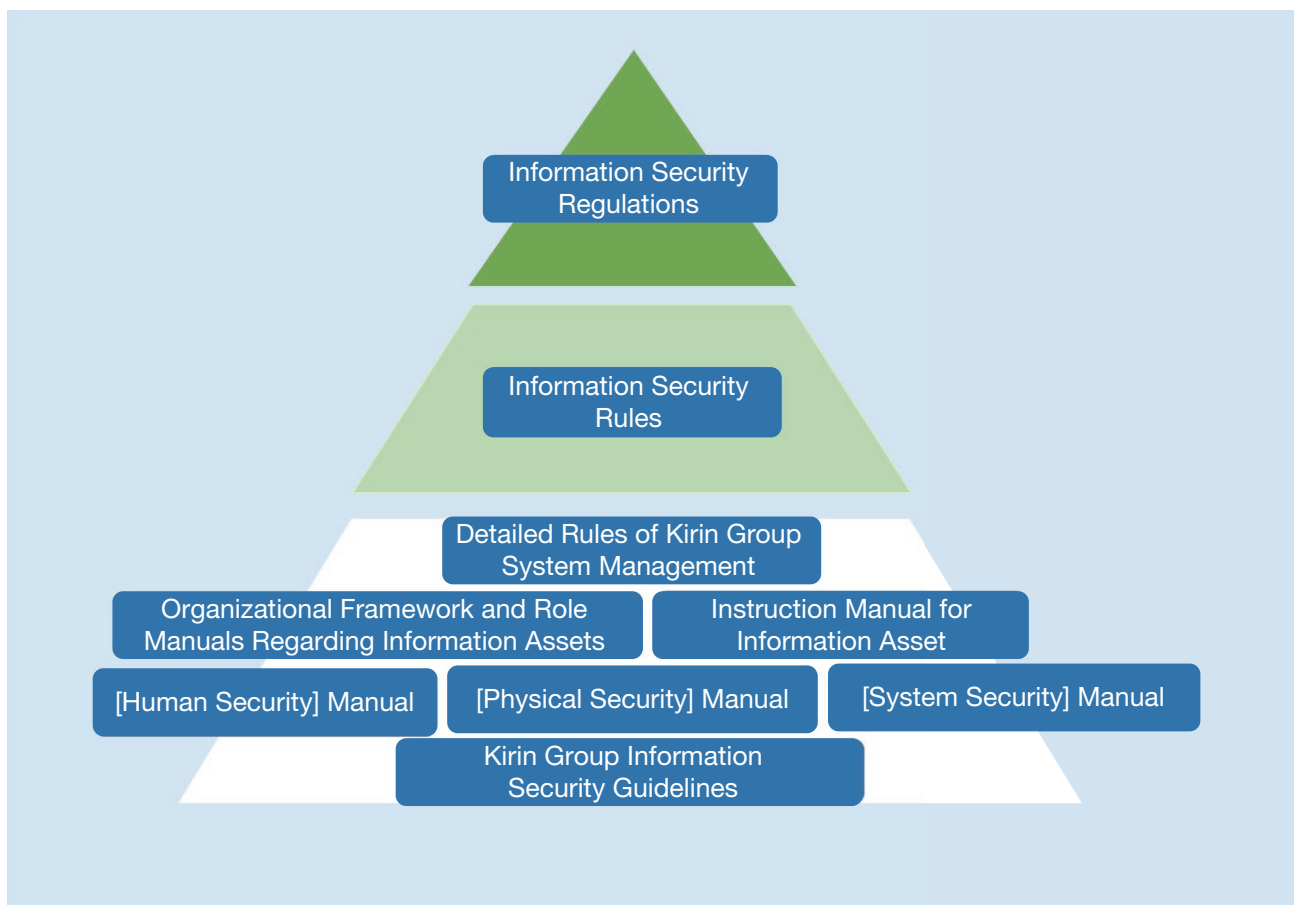
Information Security Guidelines

We endeavor to provide guidelines that will suit the circumstances of each group company, by preparing a range of manuals for employees based on the Information Security Regulations.

Instruction Manuals

The Kirin Group has prepared these manuals on the basis of our policy and regulations and in accordance with the Kirin Group businesses' original rules. They are updated as necessary, based on reviews by an independent consulting company and feedback regarding problems with e-learning programs, to ensure that common viewpoints are incorporated.

Structure of Information Security Regulations





We oversee and advise Group companies for the improvement of the information security of the Kirin Group.

Covering the Entire Kirin Group

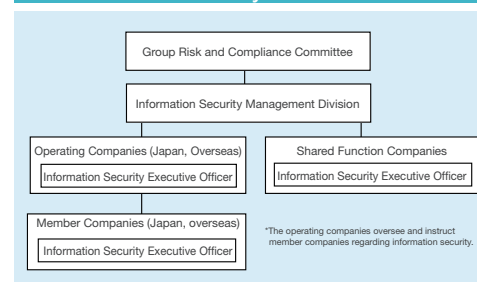
Established in accordance with international standards, the Kirin Group Information Security Regulations stipulate basic approaches, measures, and management methods related to information security across the entire Kirin Group.

Simultaneously, Information Security Guidelines have also been established for overseas Group companies, and the various Group companies overseas are making efforts to raise their employees' awareness of information management and improve their relevant skills through e-learning and other regular training programs for all employees of overseas Group companies.

As a new initiative, we are also working progressively on the strengthening of individual authentication and entry/exit controls.

It is with initiatives such as these that the Kirin Group is pursuing the reinforcement of information security.

Information Security Framework Chart

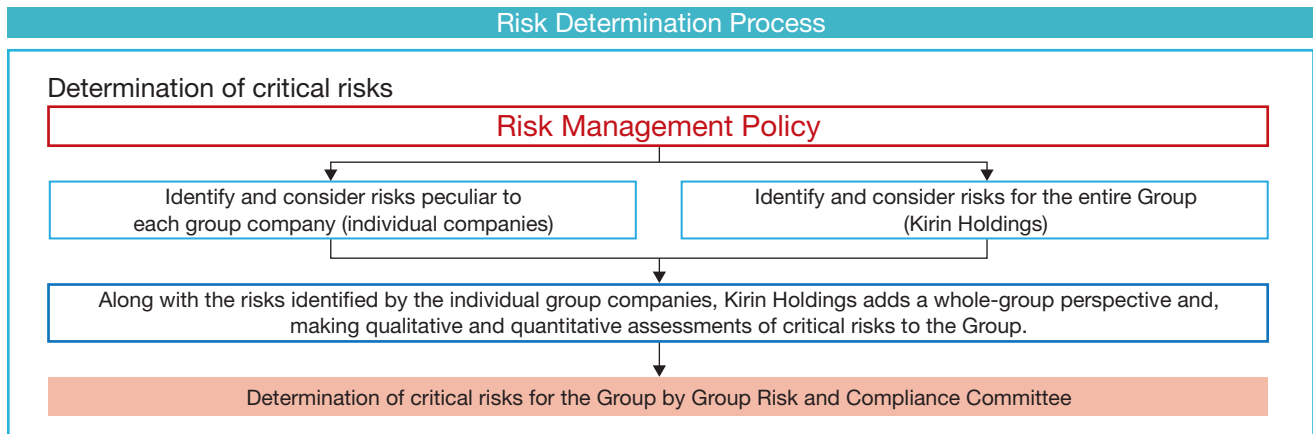


INFORMATION SECURITY FRAMEWORK

In the Kirin Group, Kirin Business System Company, a shared function company in the area of IT, has been positioned as the division for the oversight and promotion of information security improvements for the entire Group. This company supervises and advises Group companies to improve information security in the Kirin Group.

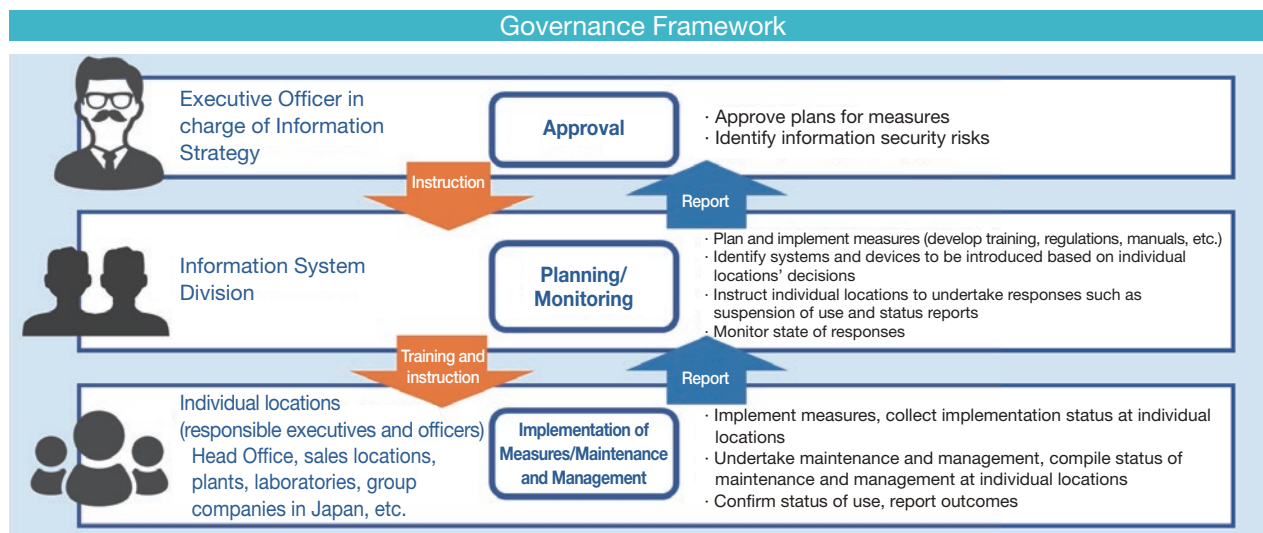
Important Risk Determination Framework

Individual Group companies identify and consider risks that are peculiar to their respective businesses from both qualitative and quantitative aspects, based on the Kirin Group’s Risk Management Policy. The Group Risk and Compliance Committee secretariat (Corporate Planning Department of Kirin Holdings Company) collects and scrutinizes these risks. The Group Risk and Compliance Committee then examines those risks that would have a large impact or a high probability of incidence or that are common to the entire Group and determines them to be critical risks for the Group.



Information Security Governance Framework

In addition to clarifying the frameworks for initiatives regarding information security measures and reducing the risks of leaks of information assets, we will respond to external threats against information security and enhance effectiveness of information security measures.



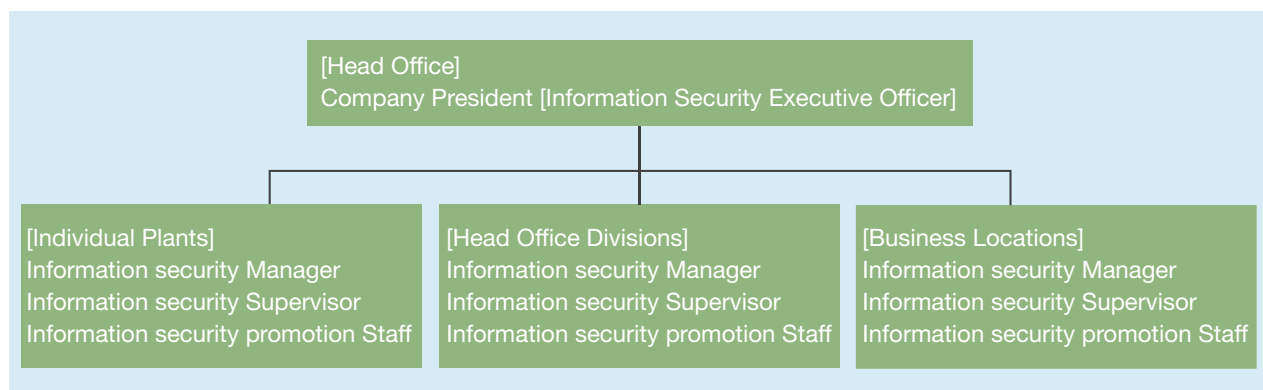
Information Security Promotion Framework

Information security promotion staff will play the central role in the promotion of information security.

Appointment of Information Security Executive Officer

- The Information Security Executive Officer, who has been given authority by the President, will have responsibility for the building and maintenance of frameworks in each company and the appropriate handling and management of information assets.
- Selection of information security Managers/Officers/promotion Staff
- Information security Managers, etc., will be appointed at each plant, business location, and Head Office division. (However, depending on the size of the business, these roles may be held concurrently with other positions.)

Information Security Organization Framework Covering All Employees



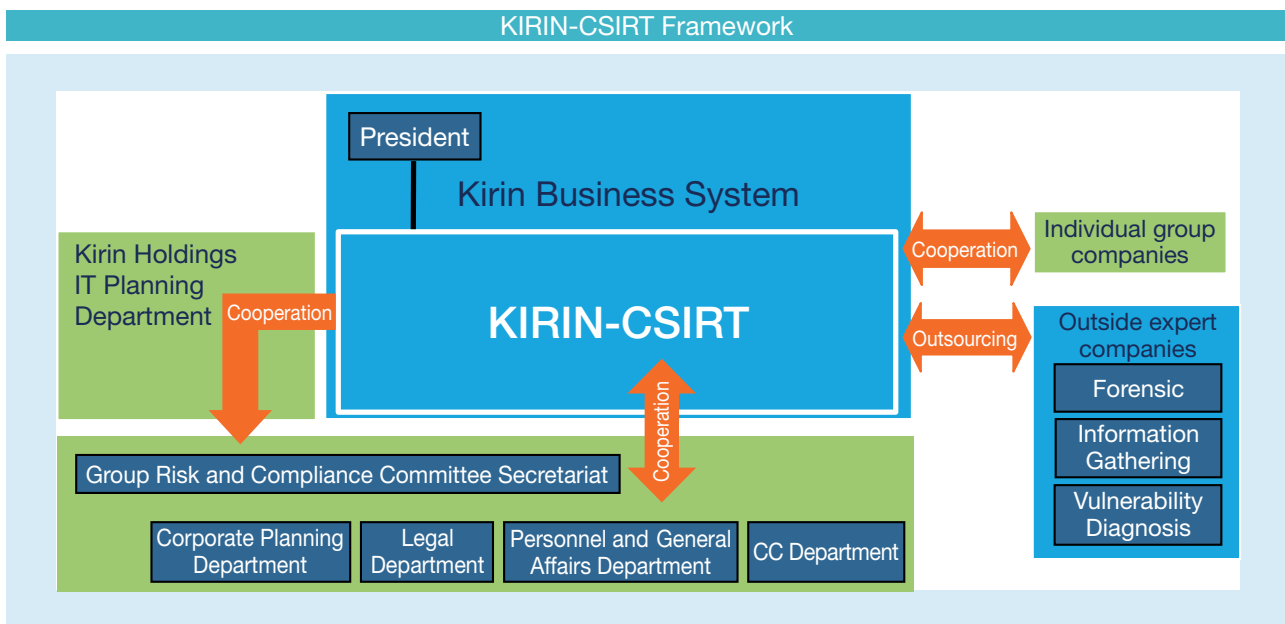
Framework for Responding to Information Security Incidents

The Kirin Group is addressing information security measures, which is a critical risk in the Group, through the establishment of KIRIN-CSIRT (Computer Security Incident Response Team), to respond to accelerating threats of cyber-attacks.

KIRIN-CSIRT

KIRIN-CSIRT strives to bolster responses against threats of cyber-attacks, such as viruses and unauthorized access from outside, through the establishment of security response frameworks in the Group and the implementation of human, physical, and technical measures.

Objective	Cooperation with Relevant Sections
<p>This initiative is effective in allowing the Group to implement speedy, structured responses in the event of a security incident. KIRIN-CSIRT is establishing frameworks for responding to security risks.</p>	<p>KIRIN-CSIRT has been established with the cooperation of the Group Risk and Compliance Committee secretariat, IR Office, CSV Strategy Department, Legal Department, and CC Department.</p>



What is CSIRT (Computer Security Incident Response Team)?

CSIRT is a collective term for the organizations that take action when a (predominantly security-related) problem occurs on computers or networks (particularly the Internet).

Information Security Risks

- If a person uses an information asset without understanding the scope of disclosure and degree of importance of the information, there is no guarantee that the user will not divulge information to others to whom it must not be disclosed.
- The Kirin Group implements appropriate management regarding the following information.

Information Management

Companies possess a range of important information, including management information, sales information, technology information, and personal information. Information assets are divided into categories based on the composition of the assets and managed appropriately.

Information Management Based on Confidentiality Category

- Particularly important information assets that only extremely limited personnel within the company may know
- Information assets that only limited personnel within the company may know
- Information assets that any personnel within the company (limited group companies in certain circumstances) may know
- Public information that any personnel within the company or external party may know

Destruction

Rules for destruction of data are established and managed in accordance with the medium of the data.

Destruction/Deletion	Method
Printed materials [paper]	- Printed materials [paper] are destroyed by methods such as shredding and dissolving - Caution is exercised in management until the materials are dissolved. - Caution is exercised in management and storage of security boxes, storage boxes, etc.
External recording media	- External recording media such as floppy disks, CDs, and DVDs are physically destroyed.
Electronic data	- All electronic data subject to destruction, including backup data, is deleted
Personal computers	- All data stored on hard disk must be thoroughly deleted, using specialist data erasure software. Alternatively, the recording device (hard disk) itself is physically destroyed.

Management at times of employment, resignation, and employment changes

The following matters concerning confidentiality are included in a written pledge or the employment agreement.

- Important information that employees could have gained knowledge of in the course of their duties is specified and the employees are asked to confirm their duty of confidentiality at the time of their resignation or dismissal.
- Information that employees could have gained knowledge of during their employment must not be disclosed to competitor companies.
- Information that employees could have gained knowledge of in the course of their duties at a company or an organization where they previously worked must not be disclosed or used without obtaining the approval from such company or organization.



We manage and use important information such as personal information appropriately.

Personal Information

In accordance with the Kirin Group Personal Information Protection Regulations, Policy, and Matters for Disclosure, for the appropriate protection and use of personal information that has been accumulated by individual companies in the Kirin Group, the scope of its handling is divided into categories and specific handling is established in accordance with the life cycle of the information.

Categories of Personal Information


All personal information handled by the Kirin Group is managed based on the following categories.

- Personal information obtained from customers
- Personal information obtained from suppliers
- Personal information handled in operations contracted from the party outsourcing the operations (contracted information)
- Personal information of employees
- Personal information of recruitment applicants and departed employees

Personal Information Handling Manual

Handling of personal information is managed in accordance with the Personal Information Handling Manual.

Checklist	Description
Obtain/Produce	Identify the purpose of use of the information as clearly as possible and use it to the extent that it is necessary to achieve that purpose.
Use or provision/outsourcing of operations	Use the information within the scope of purpose of use for which the consent of the information's owner has been obtained. If it is necessary to disclose or provide personal information to a third party, always obtain the consent of the information's owner.
Transfer or transmission	When handing over information, always obtain internal approval and keep records of such handovers.
Storage	Storage methods will be based on the information category.
Disposal	Information will be disposed of immediately and appropriately to reduce the possibility of information leakage.



Handling of personal information is managed in accordance with the Personal Information Handling Manual.

Management in Areas

If the inside and outside of information facilities are not divided into areas by the level of importance, it could potentially lead to unauthorized physical infiltration of the premises and facilities of Group companies.

The physical environment of business locations also has a major effect on information security, so if controlling that environment is difficult, we respond through other means such as operational rules.

Talk and Behavior

From various perspectives, including the potential for “loose talk,” “viewing materials in situations where others could see it,” “leaving materials behind after a meeting,” and “responding to external inquiries (including fraudulent ones),” rules have been established for the handling of information assets outside the workplace.

Taking Information Out

A lack of caution when taking information assets outside may result in its loss or theft. The inability to confirm receipt and a high risk of the information asset being lost during shipment and receipt with certain delivery methods have been taken into consideration in the establishment of these rules.

Management of Sub-contractors

If a sub-contractor causes an incident such as a leak of information, the Kirin Group, as the outsourcing party, will be held responsible. Sub-contractors perform operations that the outsourcing party would normally perform on behalf of the outsourcing party. As the outsourcing party, the Kirin Group has an obligation to manage and supervise its subcontractors to ensure that they do not cause such incidents.

Use of the Internet

Use of the company’s information devices for non-work purposes is prohibited.

These devices are equipped with security devices to control communications.

Browsing the Internet

Use of the Internet for non-work purposes is prohibited. Downloading files from web pages is permitted only if it is for work purposes.

Use of Social Media

When posting information on the internet in a private capacity, our employees have an obligation to ensure that the content posted does not infringe on compliance and moral considerations.

Use of Information System

Logs are kept that record the activity of users of the system, exception processing, and information security events. These logs are stored for certain periods to supplement future investigations and monitoring of access control.


Use of Smart Devices

If it is possible to save operational information through access to the internal system and e-mail, information leaks may occur unless appropriate security functions are put in place.

Security functions required for company-supplied smart devices may differ according to the rules of use and security measures for those devices, so appropriate functions will be decided and installed.

Measures against Information Security Incidents

If information security incidents or any events that could potentially cause an information security incident are not reported and acted on appropriately, there is a possibility that an incident may actually occur or that the damage may be exacerbated. Rules have been established in which immediate notice is to be given to pre-designated contact points in cases where actual or suspected security incidents are discovered.



Rules have been established in which immediate notice is to be given to pre-designated contact points in cases where actual or suspected security incidents are discovered.

Active and Proactive Detection

Monitoring Structure

If a human-related or machine-related security incident or suspected incident is discovered, it must be reported to the security incidents report contact immediately.

If the security incidents report contact is unknown, the informant will check with the security manager, who will then start monitoring the situation.

Response Slogan

If an actual or suspected security incident is detected, immediately report to the pre-designated contact point

Stand-alone shutdown of communication from employee's terminal

Individual employee prevents secondary damage

A system has been installed that allows individual employees to instinctively shut down communication when they feel suspicious about Internet communication, e-mail, or an individual employee and report it to information system staff.

Raising awareness of this action widely will prevent secondary damage caused by suspect devices and support healthy business activity.

Incident Response Policy and Process

Incident Level

Incident levels are defined according to a five-grade scale, based on the size of the incident's impact.

The Kirin Business System Interim Risk Committee will make suspension decisions based on the incident response level. Relevant sections will participate in the meetings to make those decisions.

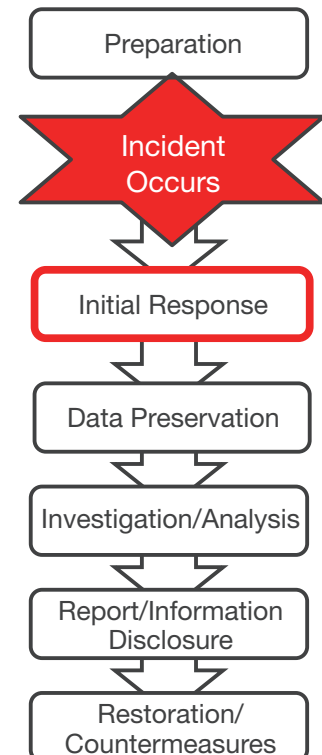
Further, depending on the situation, decisions will be made by the executive officer in charge or the Group Risk and Compliance Committee.

Basic Policy at Time of Response

Order of Priority

1. Secure human life (health and safety)
2. Comply with laws and regulations
3. Prevent leaking of customers' personal information, minimize damage
4. Prevent Kirin from providing an environment for cyber-attacks due to virus infection, resulting in involvement or support of a cyber attack
5. Continue with operations

Response Process





Preparing education
resources development



HRD for Information Security

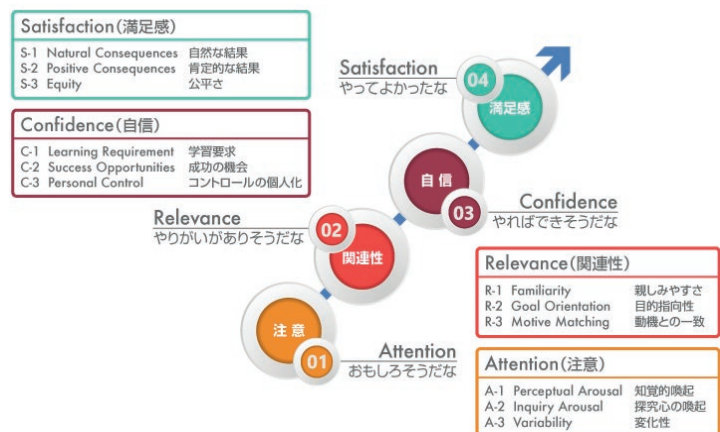
To make employees aware that what they are learning directly concerns them and to encourage them to grow, we have prepared education curricula and conduct human resources development that is centered on the ARCS Model, based on analysis of educational motivation.

HRD Centered on the ARCS Model

To make employees aware that what they are learning directly concerns them and to encourage them to grow, we have prepared education curricula and conduct human resources development that is centered on the ARCS Model, based on analysis of educational motivation.

ARCS Model

ARCS Model: Four Factors



To make information security education effective, it is important that the trainees feel convinced.

Incidents can be prevented proactively by making use of learnings and detecting the forewarnings of security incidents appropriately. Through information security education, we are improving our ability to detect security events by raising the risk sensitivity of all employees of the Kirin Group.

Information Security Personnel

Employees are able to accumulate knowledge about information security by exercising empathy, interest, and recognition, and to take action and put their new knowledge into practice with understanding, agreement, and practicality. Under this policy, we define security personnel as “Recognizers” and “Understanders” at the acquisition stage

Work-based Goals

The image of the aimed-for personnel will vary depending on the nature of the work. Goals are set for each type of work and duty and efforts are made to achieve them.

Definition of information security personnel covering all employees

Definition	Ability
Recognizer (May be multiple stages)	- Personnel with information security <u>knowledge</u> - Understands necessity of Kirin Group’s information security regulations
Understander (Security master)	- Personnel who can take actions with knowledge as a recognizer - Has specific understanding of purposes, policies, and necessary actions of information security - Able to act as a contact when information security incidents occur - Possesses knowledge and can put it to use in actual operations

Knowledge and Behavior of Employees

Personnel	Knowledge Aspect			Action Aspect
	General Knowledge	Peculiar to Kirin	Person concerned	Person concerned and others
Recognizer	○	○	△	—
Understander	○	○	○	△ (Responsible location)

Learnings for the entire Kirin Group

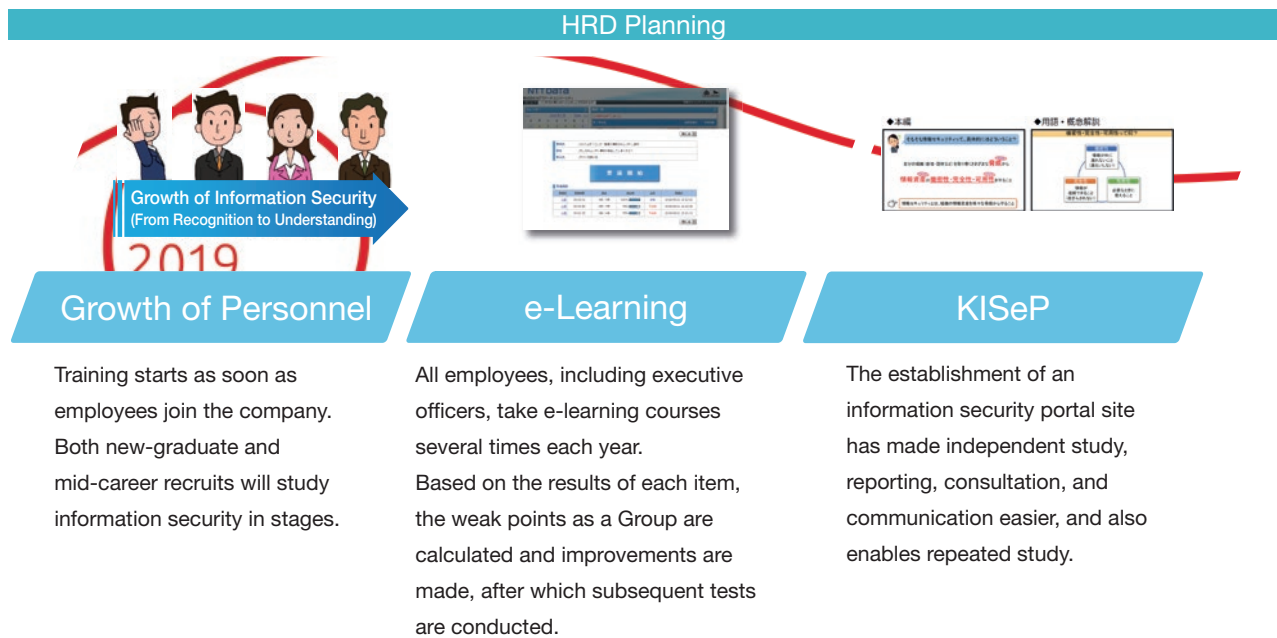
The Kirin Group has a range of curricula with which it strives to enhance individual Group companies’ awareness of information security. Kirin-original education content has been produced, with updates added as necessary every year. Trends are analyzed from actual outcomes and countermeasures are taken.

Updating of Information Security Content



Action for All Employees

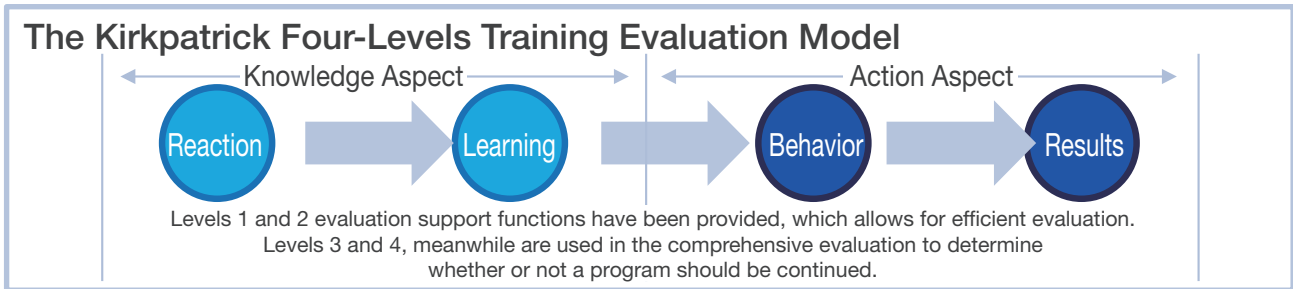
Cultivating human resources will contribute to raising the standard of security responses.



Cultivating human resources contributes to raising the standard of the Kirin Group's security responses

Evaluation of Action

Each action will be evaluated according to a Four-Levels Training Evaluation Model to confirm the validity of policies and strategies and appropriately assess the degree of priority of additional policies and strategies. These evaluations are then put to use in subsequent actions.



Action towards 2020

Employees in grades that have opportunities to come into contact with IT or grades they require decisions regarding managerial risks will obtain knowledge of the Kirin Group for information security.

Employees in grades with fewer opportunities to come into contact with IT will keep cultivating knowledge and awareness of information security steadily over two years in 2020.

Roadmap: From 2019 to 2020

Key Points
 Employees in grades with many chances to come into contact with IT and grades asked to make decisions about managerial risks will **grow** to **L2 Recognizers** in 2020.
 (① Management grade, ② staff, and ③ KBS)

Employees in grades with fewer opportunities to come into contact with IT will remain at **L1 Recognizer** level in 2020, but will **steadily maintain** their **cultivation** of information security awareness. (④ End user grades)

Grade	Current Status	End of 2019	End of 2020	End of 2021	Target
① Management grade	Don't know Not interested	L1 Recognizer	L2 Recognizer		Encourage smooth promotion of security measures at own location
② Staff	Don't know Not interested	L1 Recognizer	L2 Recognizer	Understander	Actually move to roll out smooth promotion of security measures at own location
③ KBS	Don't know Not interested	L1 Recognizer	L2 Recognizer	Understander	Actually move to implement security measures in own systems and users
④ End user grades	Don't know Not interested	L1 Recognizer	L1 Recognizer	L3 Recognizer	Act so as not to cause incidents that would lead to security risks

Action in 2020 and Beyond

Each section will have personnel allocated to promote information security, information security will be maintained, and various initiatives will be pursued, such as contact points for reporting incidents.

In this way, we will develop even stronger information security frameworks.

Roadmap: From 2020 to 2021

Key Points
 Develop **Understanders** with a three-year plan ending in 2021.
 (② Staff and ③ KBS)
 Grades that promote information security will, as **Understanders**, maintain information security in their own location and serve a role as contact points for reporting incidents, etc.
 See "Definition of Personnel" below for detailed definition of "Understander."

Grade	Current Status	End of 2019	End of 2020	End of 2021	Target
① Management grade	Don't know Not interested	L1 Recognizer	L2 Recognizer		Encourage smooth promotion of security measures at own location
② Staff	Don't know Not interested	L1 Recognizer	L2 Recognizer	Understander	Actually move to roll out smooth promotion of security measures at own location
③ KBS	Don't know Not interested	L1 Recognizer	L2 Recognizer	Understander	Actually move to implement security measures in own systems and users
④ End user grades	Don't know Not interested	L1 Recognizer	L2 Recognizer		Act so as not to cause incidents that would lead to security risks

Management Review

In addition to reporting to the top management executives in charge of information strategy when incidents occur, regular briefings are held several times a year. For the purposes of promoting security, these briefings aim to consolidate awareness in the Information System Division. Another aim is to exchange information between top management and the Information System Division regarding what is currently happening and what is being done to mutually check the behavior of all personnel.

Regular Status Surveys at Individual Group Locations in Japan

With the launch of status surveys of operating companies in Japan and overseas based on the Kirin Group's Information Security Roadmap and the establishment of Standards for Use and Management, the status of information security is being surveyed on a regular basis.

During the period covered by this report, surveys were conducted at several locations in Japan and overseas. Monitoring of locations that have had issues of concern is also ongoing.

Reinforcement of Overseas Locations

Matters subject to monitoring have been established for overseas operating companies and evaluations are performed based on status reports provided by the individual companies.

(Started in 2010)

Detection of Incidents

Numerous incidents, including malicious attacks, have been detected, but they have been successfully defended before anything happened.

Status monitoring is conducted on a monthly basis and, if there are any abnormal figures that differ from past social trends or in-house tendencies, the causes are investigated, and responses are planned and implemented.

Response to Attacks on Credit Card Details Entry Screen on EC Websites

Due to the revision of the Installment Sales Act, business operators without certification for handling credit card numbers are now prohibited from storing credit card data on EC websites.

Action has been taken based on this revision of the legislation.



Feedback



Problems, Reflections, and Ideas for Improvement by Employees

Various opinions expressed by employees after information security training conducted in 2019 are being reflected in future initiatives.

Feedback from Information Security Training

Favorable opinions that we want to maintain (extract)

- As long as we are using smartphones and personal computers, issues such as information leaks and virus infection are unavoidable. I realized that I need to check the websites I view and the e-mails I receive more carefully.
- I could not help feeling that the people who say they understand are the ones who understand the least. I am conveying what I learnt to my team members and I will strive for preemptive prevention by reminding them regularly in our daily work.
- I get the feeling that we will see more risks that could lead to work-related information leaks in the future. I hope that the company will hold regular in-house training and provide opportunities to exchange information, to help prevent information leaks both inside and outside the company.
- I have been given opportunities to take information security courses in various workplaces but attending this training has made me realize anew that I need to be careful.
- Holding this kind of training regularly will further increase my own awareness and knowledge.
- This kind of training can be used as an opportunity to gain relatively new information, so I hope it will be continued into the future.

Suggestions for Subsequent Sessions (Extract)

- This kind of session is very effective. However, while I kept what I learned fully in mind immediately after the training, as time has gone on, my attention has tended to wander, so I hope this training will be held regularly.
- The terminology related to information security was difficult and I do not have much knowledge, so I found having to perform information-related operations a challenge. Another problem I had was that I do not know anyone around me from whom I can easily seek advice.

“One KIRIN” Values

キリングループの一員として大切に考える方、気持ち



よろこびがつなぐ世界へ Joy brings us together

Note: Service and product names included in this report are registered trademarks or trademarks of Kirin Holdings or each company.

Kirin Holdings Company, Limited
KIRIN BUSINESS SYSTEM COMPANY, LIMITED

NAKANO CENTRAL PARK SOUTH
10-2, Nakano 4-chome, Nakano-ku, Tokyo 164-0001, Japan