RISK MANAGEMENT/COMPLIANCE

The OKI Group is working to reinforce risk management under the Risk Management Committee. In accordance with our “Compliance Commitment” and, in order to perform corporate activities fairly, we are focusing on the enhancement of training, and we have established consultation and reporting contacts.

Risk Management Initiatives

OKI has established the Risk Management Committee (with the President as Committee Chairman, and outside directors and Audit & Supervisory Board members as advisors) in order to manage risks related to the Group’s business activities certainly. While it deliberates and decides on basic policies for risk management, the Committee identifies risks to be managed based on the basic policies, and deliberates and decides on policies to prevent the manifestation of such risks, as well as policies concerning scenarios in the event of a crisis.

Risks to be managed are determined by assessing the risks accompanied with the whole Group’s business activities, from the perspective of responding to stakeholder requests, as well as the compliance risks (risks associated with violations of laws, regulations, and internal rules). Of these risks, common risks (risks requiring common management across the Group) are registered by the control division and manifestation preventive measures are deployed within the Group. By doing so a management cycle in which the Compliance Committee (see next section) regularly checks the implementation status has been put into place.

Initiatives to Promote Compliance

The OKI Group has established the Compliance Committee (with the Chief Compliance Officer as Committee Chairman) in accordance with the top management’s Compliance Commitment thereby striving to ensure rigorous compliance. On a quarterly basis the Committee monitors the management progress of the common risks identified by the Risk Management Committee. The Committee also deliberates and decides on compliance training plans and oversees their implementation. Moreover, we implement fixed-point observations on conduct and awareness relating to compliance of executives and employees, and to make the most of such measures, we implement compliance awareness surveys on an ongoing basis.

In order to discover and rectify improper activities at an early stage, we have established consultation and reporting channels to enable anonymous reports, as well as reports to outside directors and Audit & Supervisory Board members at every Group company, and stipulated whistle-blowing regulations such as those about the protection of whistle-blowers. In fiscal year 2018, 66 reports and consultations were received at the OKI Group in Japan. Furthermore, the system which includes an external contact point and Group-wide contact point newly established in the previous fiscal year was made known to all employees again this year with a 93% awareness of the whistle-blowing system resulting from the awareness survey (up 9% from the previous fiscal year).

Ongoing Compliance Training

The OKI Group implements training sessions for compliance managers at seven sites in Japan for employees at senior manager level as regular training. Participants learn in these sessions, and roll out the gained knowledge in their business units. The deployment of such knowledge is checked through an e-learning program for all executive officers and employees of the Group. We have tools in place to promote learning and retention of program content such as sharing specific examples through the booklet called “Case Examples of Compliance” on the intranet.

Since fiscal year 2018, some overseas Group companies have started a unified e-learning compliance training program, the scope of which will be further expanded in fiscal year 2019.

Main Compliance Training Programs (for the OKI Group in Japan) in FY2018

Training Overview	Participation Rate
Training sessions for compliance managers (implemented in July-August 2018) Main themes: The importance of compliance, financial reporting laws, contract management, EU General Data Protection Regulation (GDPR)	100%
The e-learning program about on-the-job compliance (implemented in December 2018 to January 2019)	99.9%
Anti-monopoly Act training for marketing & sales sections (implemented in November 2018 to May 2019)	100%

Thorough Compliance with Anti-monopoly Act

In February 2017, the Japan Fair Trade Commission issued a cease and desist order in accordance with the Anti-Monopoly Act and ordered OKI to pay fines with regard to trade related to digital wireless communication systems for firefighting and emergency use. We are working on prevention measures to ensure this never happens again.

A system based on our regulations for compliance with the Anti-monopoly Act has been implemented and operated for recording contact with competitors. With respect to training, the Anti-monopoly Act is repeatedly taken up to ensure that all rules are strictly adhered to. In fiscal year 2018, sales training was provided by an external instructor from the Japan Fair Trade Institute.

In addition to continually monitoring the implementation of Anti-Monopoly Act-related rules and improving the effectiveness of our framework, we will strive to generate a sense of compliance awareness by continuing to send out compliance messages from top management.

Approaches to Anti-Corruption

Anti-corruption is Principle 10 raised in the United Nations Global Compact, and is a global social issue. We are promoting anti-corruption initiatives based on the "OKI Group Anti-Corruption and Anti-Bribery Policy" that we put into practice in fiscal year 2013.

The "OKI Group Anti-Corruption and Anti-Bribery Policy" complies with anti-corruption laws and regulations that apply in each country and region where the OKI Group operates, such as the Japanese Unfair Competition Prevention Act, the US Foreign Corrupt Practices Act, and the UK Bribery Act. The policy defines the basic requirements for complying with laws and regulations and conducting business appropriately. As company bylaws, we established specific rules for recording the exchange of the gifts and receiving/offering entertainment, and compliance with these rules at each Group company is monitored annually by OKI's control division.

Emergency and Disaster Response

The OKI Group has established Safety Countermeasure Committees at its domestic and overseas sites, as well as at subsidiaries, in order to ensure "protect people's lives," "prevent secondary accidents," "contribute to local communities and foster good relationships with them," and "continuity of business operations" in the event of disasters. For "continuity of business operations," each business and corporate (headquarter) division develops Business Continuity Management (BCM) and a Business Continuity Plan (BCP), based on BCM Development Guidelines. The contents of each BCP are reviewed annually to improve its effectiveness. In fiscal year 2018, earthquake drills took place across four departments from initial response to implementing the BCP.

INFORMATION SECURITY

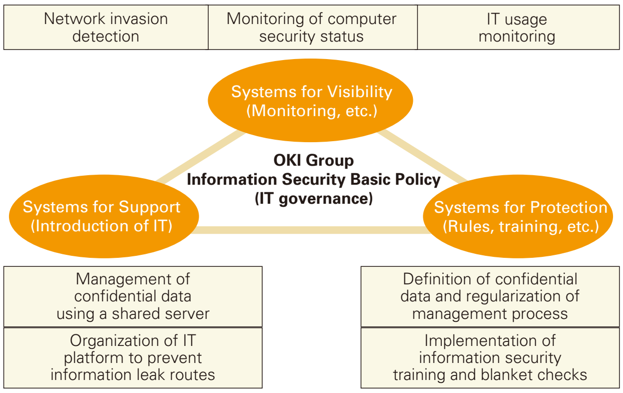
Based on the OKI Group Security Basic Policy, the OKI Group has established a system to ensure information security and works to properly manage and protect company and customer information.

Three Systems of Information Security

The OKI Group is working on IT improvements to support business growth with the aim of reinforcing earning capacity. Among these improvements, measures to strengthen information security from the viewpoint of minimizing management risk are being developed. In the OKI Group, we use the three systems shown in the diagram to broadly promote information security measures for computers, networks and information systems. We have established an organization specializing in security incident response called OKI-CSIRT*, which collaborates with external organizations, in order to enhance our prevention against threats to computer security in the Group and improve our capacity to respond to them.

In fiscal year 2018, in line with the revisions to the Cybersecurity Management Guidelines, points relating to recovery from a cyber attack were included in the incident response manual and security inspections on contractors were carried out.

*CSIRT: Computer Security Incident Response Team


Network invasion detection
Monitoring of computer security status
IT usage monitoring
Systems for Visibility (Monitoring, etc.)
OKI Group Information Security Basic Policy (IT governance)
Systems for Support (Introduction of IT)
Systems for Protection (Rules, training, etc.)
Management of confidential data using a shared server
Organization of IT platform to prevent information leak routes
Definition of confidential data and regularization of management process
Implementation of information security training and blanket checks

Enhanced Actions at Overseas Sites

The OKI Group has promoted information security measures at overseas sites, including such actions as laying down information security guidelines in each country and region, appointing security managers at each site, and adopting control tools.

In fiscal year 2018, training on the attachment-style targeted e-mail attacks which had been carried out up until the previous fiscal year was changed to a phishing e-mail format which has been more prevalent in recent years. This training has been conducted not only at sites in Japan, but also in Europe, the United States, China, and Asia.

Enhancing Protection of Personal Information

We in the OKI Group have enhanced protection of personal information, based on the Privacy Policy. We have committed to the protection of personal information under the leadership of our Chief Privacy Officer. Privacy managers have been appointed in all divisions and subsidiaries. In May 2018, the Group's response to the EU General Data Protection Regulation (GDPR) was compiled as a policy document, and measures have been taken based on this.

OKI and seven Group companies have acquired PrivacyMark certification in Japan as of June 2019.

Protecting your PRIVACY
10300032