Approaches to Anti-Corruption

Anti-corruption is principle 10 raised in the United Nations Global Compact, and is a global social issue. We put into practice in fiscal 2013 the "OKI Group Anti-Corruption and Anti-Bribery Policy" in the subsidiaries in and outside of Japan, and are enhancing our approach to anti-corruption.

The "OKI Group Anti-Corruption and Anti-Bribery Policy" sets out fundamental points for carrying out operations properly while complying with the related regulations applicable to each country and region in which the OKI Group operates. As company bylaws, we established specific rules governing the exchange of gifts and receiving/offering entertainment, and we have put into place and administer a system in each company of the Group.

Regarding Cease-and-Desist and Surcharge Orders by JFTC

OKI was subject to an onsite inspection by the JFTC on November 18, 2014 on suspicion of violating the Anti-Monopoly Act concerning products and services relating to digital wireless communication systems for firefighting and emergency use, and was fully cooperative with the inspection. On February 2, 2017, OKI received cease-and-desist and surcharge orders from the JFTC based on the Anti-Monopoly Act, and accepted the orders it received with sincerity and seriousness. OKI is working to further bolster compliance and to do its utmost to adopt comprehensive measures to prevent reoccurrence.

ESG SUPPORTS CORPORATE VALUE

INFORMATION SECURITY

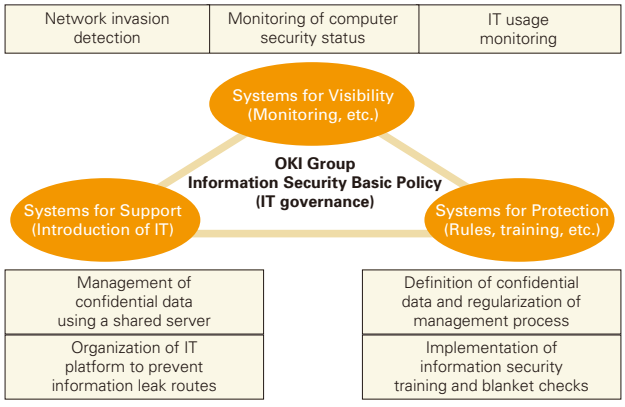
Based on the OKI Group Security Basic Policy, the OKI Group has established a system to ensure information security under the leadership of the Information Security Committee and we work to properly manage and protect company and customer information.

Three Systems of Information Security

In the OKI Group, we use the three systems shown in the diagram below 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 preventive measures against threats to computer security in the Group and improve our capacity to respond to them.

In fiscal year 2016, we disseminated pseudo e-mails to all domestic e-mail users to precisely calibrate their responses to targeted e-mail attacks, which are growing ever more sophisticated, and we are implementing training to confirm and correct their responses.

*CSIRT: Computer Security Incident Response Team



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 2016, along with confirming the adoption and compliance status of guidelines, OKI took steps to introduce restrictions over computer operations at all sites to bolster countermeasures against information leaks in China.

Enhancing Protection of Personal Information

We in the OKI Group have enhanced the 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 in Group companies. OKI and seven Group companies have acquired PrivacyMark certification as of June 2017.

To respond to the amended Act on the Protection of Personal Information, OKI updated and revised its related rules in June 2017.

Protecting your PRIVACY
10300032