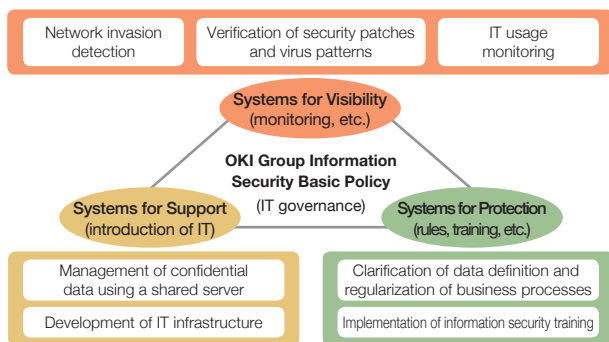


Based on the OKI Group Security Policy, the OKI Group has established a system to ensure information security under the leadership of the Information Security Committee. We properly manage and protect company and customer information, including personal information, through various activities such as reviews of efforts for information security (biannual), and information security audits.

Three Perspectives of Information Security System

As a company which provides products and services designed for information security, in order to boost its own information security, OKI Group uses the 3 perspectives shown in the diagram below to advance its security measures.



In fiscal 2013, as part of "Systems for Support," OKI's own cloud services for smartphones called EXaaS Mobile Desk Service, of which introduction was initiated in the previous fiscal year, was applied to all internally-connected smartphones, putting in place an environment that allows safe and easy access to in-house information.

Major activities in fiscal 2013

Systems for Visibility	• Further enhancement of monitoring for cyber attacks
Systems for Support	• Full implementation of safe use of smartphones
Systems for Protection	<ul style="list-style-type: none"> • Collective training for staff members responsible for promoting the introduction of information security measures in all divisions of OKI and the Group members (June) • E-learning sessions on "Personal Information Protection and Information Security" for all employees (August) • "Information Security Simultaneous Inspection" covering all the employees (October)

"Visualization" of Action Implementation Level at the Supplier Side

Aiming at an improved information security level across the supply chain, OKI continuously verifies how the information security measures are implemented at the suppliers to which we provide critical confidential information. Specifically, we ask our suppliers to carry out self-evaluations based on the check list prepared by OKI. The results are converted into points using our unique method, to allow sharing of their activities and issues. In fiscal 2013, OKI used these self-evaluations to share the issues with the suppliers whose previous survey had rendered a relatively low evaluation, with the intention of solving the problems. As a result, all the targeted suppliers achieved "high evaluation" against the OKI's criteria.

OKI-CSIRT for Prompt Response to Security Accidents

OKI has established an organization specializing in security incident responses called OKI-CSIRT^{*1}, which collaborates with

In order to enhance our preventive measures against threats to computer security and improve our capacity to respond to them, we established OKI-CRIST^{*1} as an organization specializing in responding to security accidents. It also coordinates our Group with outside organizations; Nippon CSIRT Association (NCA), other company CSIRTs, related ministries and agencies, etc.

In fiscal 2013, in order to address the increasing targeted email^{*2} attacks, OKI further strengthened the anti-virus measures and the exit controls for blocking the information leakage routes from infected PCs and servers. In addition, it informed its employees in a timely and appropriate manner through Intranet and company news to raise their awareness.

^{*1} CSIRT: Computer Security Incident Response Team

^{*2} Targeted email: Email sent to a specific organization or individual, as a cyberattack to steal information

Enhanced Actions at Overseas Sites

Since fiscal 2008, the OKI Group has promoted the implementation of information security measures at Chinese site. As we have worked to apply anti-virus software suited for viruses observed in China, set up the local help-desk system, and implemented measures for information leakage via mobile PCs, the implementation level has almost been reduced to the level of the Group companies in Japan.

In fiscal 2013, enhancement of security measures was also launched in the other Asian sites as well as Oceania sites, by establishing the Information Security Guidelines for 9 sites and designating security managers at each site.

Promotion of Acquiring ISMS Certification

The OKI Group is working to acquire the ISMS^{*} certification for divisions involved in building and operating internal information systems, and for divisions engaged in general system design construction and related services. As of June 2014, five companies and seven business units of the OKI Group are ISMS-certified organizations, and are currently proceeding with the review of provisions that are applicable to the standard revisions for fiscal 2013.

^{*} ISMS: Information Security Management System

Enhancing the Protection of Personal Information

The OKI Group has 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 at the corporate level, and in business units and group companies.

The OKI Group has also promoted its group companies' acquisition of the PrivacyMark certification, so they can take appropriate measures to protect personal information. OKI and seven group companies have acquired the PrivacyMark certification as of June 2014.

