Under the corporate governance system, the Fujitsu Group promotes appropriate information management and information usage according to Group rules, as part of risk management.

Corporate Governance and Risk Management

Corporate Governance

The main emphasis of Fujitsu’s corporate governance is on having the non-executive directors provide oversight and advice to executive directors in their management execution role within the Board of Directors, while adopting the Audit & Supervisory Board system.

Specifically, while assuming mutual supervision between directors and oversight of directors by the Board of Directors, Fujitsu makes a clear distinction between the management execution role and the management oversight role on the Board of Directors and, moreover, makes sure that there are at least as many non-executive directors responsible for management oversight as there are executive directors responsible for management execution.

In addition, in selecting candidates for non-executive directors, consideration is given to the candidate’s backgrounds and insight into Fujitsu’s business so that effective advice that reflects a diversity of viewpoints can be obtained.

Furthermore, Audit & Supervisory Board members provide audits and oversight from the outside of the Board of Directors, and Fujitsu has established the Executive Nomination Committee, the Compensation Committee, and the Independent Officers Council of its own accord, thereby augmenting the Board of Directors. The overall approach is designed to raise corporate value through effective corporate governance.

Risk Management

Through its global activities in the ICT industry, the Fujitsu Group continuously seeks to increase its corporate value, and to contribute to its customers, local communities and all other stakeholders. Management places a high priority on properly assessing and dealing with risks that threaten the achievement of our objectives, taking steps to prevent the occurrence of these risk events, and establishing measures to minimize the impact of such events if they do occur, and prevent their reoccurrence. Moreover, we have built a risk management and compliance system for the entire Group and we are committed to continuously implementing and improving it.

Corporate Governance Structure

With the aim of integrating and strengthening its global risk management and compliance structures, the Fujitsu Group has established a Risk Management and Compliance Committee as an internal control committee that reports to top management. The Risk Management & Compliance Committee appoints a Chief Risk Compliance Officer for each department and company throughout the Group, and encourages them to cooperate together both to guard against potential risks and to mitigate risks that materialize, thereby forming a risk management and compliance structure for the entire Group.

Risk Management & Compliance Structure
Promotion of Information Security

Ensuring Information Security

Bearing in mind that ICT constitutes a fundamental part of the Fujitsu Group’s business, the Fujitsu Group maintains information security throughout the Group and also proactively strives to maintain and improve its customers’ information security through Fujitsu’s products and services, and thereby contributes to the Corporate Philosophy that articulates our desire for “a network society that is rewarding and secure.”

Fujitsu Group Information Security Policy (Excerpt) (Global Security Policy)

I. Purpose
The purpose of this Fujitsu Group Information Security Policy (this “Basic Policy”) is to set forth basic matters, such as measures and frameworks, regarding Fujitsu Group’s information security in accordance with the “Cybersecurity Management Guidelines” formulated by the Ministry of Economy, Trade and Industry of Japan, as well as to declare, both internally and externally, that the Fujitsu Group will not only maintain the information security throughout the Group but also proactively strive to maintain and improve our customers’ information security bearing in mind that ICT constitutes a fundamental part of Fujitsu Group’s business, and thereby implements the Corporate Philosophy set forth in FUJITSU Way.

Information Security Organization

In order to further strengthen its security measures in response to the recent trend of increasingly numerous and sophisticated cyber attacks, Fujitsu has appointed a Chief Information Security Officer (CISO) under the Risk Management and Compliance Committee and has reviewed its security organization structure, thereby ensuring the establishment and implementation of information security measures.

Varied Measures to Ensure Information Security

In accordance with the Fujitsu Group Information Security Policy, Fujitsu not only establishes internal policies and procedures and conducts employee training, but also proactively takes advantage of ICT in order to maintain and improve its information security globally.

In addition, Fujitsu has expert teams to appropriately respond to information security incidents.

Information Security Organization

Risk Management & Compliance Committee

Chief Information Security Officer (CISO)

Security Management Division, Corporate Affairs and Risk Management Unit

Establishment of Internal Policies and Procedures

Each Fujitsu Group company establishes its internal policies and procedures regarding information management and ICT security based on the ‘Fujitsu Group Information Security Policy’ and implements information security measures accordingly.

Framework of Information Security Rules

Fujitsu Group Information Security Policy

<table>
<thead>
<tr>
<th>Information Management</th>
<th>ICT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Information Management Rules</td>
<td></td>
</tr>
<tr>
<td>• Other Company Confidential Information Management Rules</td>
<td></td>
</tr>
<tr>
<td>• Personal Information Management Rules</td>
<td></td>
</tr>
<tr>
<td>• Rules for Information System Security</td>
<td></td>
</tr>
<tr>
<td>• Rules for the Use of Fujitsu PKI*</td>
<td></td>
</tr>
</tbody>
</table>

Implementation Procedures

Japanese Group Companies

Information Systems Security Policy, etc.
Preparation of rules and policies for each company

Overseas Group Companies

* PKI (Public Key Infrastructure): Rules relating to the use of systems for personal identification and encoding.
Training and Raising Awareness Regarding
Information Security
Since FY 2008, the Fujitsu Group has promoted a common slogan “Declaration for thorough information management! Information management is the lifeline of the Fujitsu Group.”

Fujitsu Limited and its domestic group companies have been working to increase information security awareness at the individual employee level by displaying posters at respective offices and affixing information security awareness stickers to all business PCs used by employees. Furthermore, e-Learning courses are held for all our employees, including executives, every year in order to further establish information security awareness.

Similarly, measures such as employee training are continuously conducted at overseas group companies in order to raise employee awareness regarding information security.

Enhancing Security with ICT
Fujitsu has also taken steps to enhance security by utilizing ICT. For example, Fujitsu has introduced a tool called “ShieldMailChecker,” developed by Fujitsu Social Science Laboratory Limited, to all domestic group companies in order to prevent information leakage caused by erroneous email transmission to external parties.

Activities by Information Security Promoting Organizations at the Business Group Level
Business units and group companies that provide system integration services within the Fujitsu Group have established information security promoting organizations, which implement a higher level of information management and enhanced security.

Many of these organizations have actively obtained ISMS (Information Security Management System) certification*1 (43 organizations certified as of June 2016), and promote secure management of confidential information such as customer data.

Responding to Cyber Attacks
In order to maintain the security of the Fujitsu Group’s globally integrated intranet, Fujitsu monitors its network 24 hours a day, 365 days a year, through its GSOC (Global Security Operation Center), which is comprised of security teams at main offices around the world. Information security incidents, such as malware infection, will be reported promptly to the administrator located at the source of the incident with instructions regarding risk elimination, and appropriate countermeasures will be planned. Furthermore, Fujitsu coordinates with external organizations such as government ministries and agencies in order to work together on early detection and resolution.

In addition, newly developed systems will undergo prior review by our security control division in accordance with relevant information security policies to ensure that adequate measures are taken against cyber attacks and any issues are resolved.

Information Security Presentation for Business Partners
As a result of dramatic changes in the ICT environment in recent years, the risk of information leaks has never been higher. In response, the Fujitsu Group has held information security presentations not only for Group employees but also for domestic business partners to which we outsource software development and services, and has worked to share information on challenges and to thoroughly implement prevention measures.

Example of presentations held in FY 2015

Personal Data Protection Initiatives
Fujitsu has established the “Personal Data Protection Policy” and “Rules for Management of Personal Data.” Based on these rules, we give training on how private information should be handled and carry out surveys in an ongoing effort to strengthen the protection given. In August 2007, we acquired company-wide PrivacyMark*2 certification and have since renewed this certification every two years. Domestic Group companies are also acquiring PrivacyMark certification individually as necessary and are promoting thorough management of personal data. Overseas Group companies are also publishing privacy policies that meet their various national legal and social requirements on their main public websites.

*1 ISMS (Information Security Management System) certification: A system for verifying compliance with the ISO/IEC 27001 international standard for information risk management.

*2 PrivacyMark: A certification system relating to the handling of private information. The system is operated by the Japan Institute for Promotion of Digital Economy and Community.