Fujitsu Group Initiatives for Sound Protection of Customers’ Information Assets

The organizations and Group companies in the Fujitsu Group that provide system integration service are called upon to maintain an even higher level of information management than the rest of the Fujitsu Group because they have many more opportunities to handle customer information assets and personal data. That is why Fujitsu’s Information Security Council Secretariat (Council Secretariat) provides its information security management system based on a security management framework to all related organizations and Group companies. Related organizations and Group companies apply the framework and promote policies.

Our Approach to Establishing an Organization to Promote Information Security

Cyber-attack threats have become sophisticated and diversified, resulting in global debate about various types of business regulations. Consequently, Fujitsu launched the Security Steering Committee in 2013 to share information on cyber security and discuss our business policies.

The Security Steering Committee is comprised of directors overseeing the various businesses undertaken by the System Integration Service Business; directors in charge of Japanese sales, marketing, and overseas sales divisions; and outside experts called upon to ensure impartiality.

Fujitsu abides by the principles of the “Fujitsu Technology and Service Vision.” Reliability of information is important for a “Human Centric Intelligent Society,” so it is vital to create a system where information utilization can continue on the assumption that accidents happen. The committee discusses and approves policies for projects requiring a global-level response, starting with countermeasures to the threat of cyber-attacks and observance of laws governing international cloud centers, as well as handling personal information.

The Security Steering Committee promotes activities to enhance the security quality of Fujitsu’s system integration and services. The committee is a substructure of the Information Security Council (Council), which decides on the direction of the Fujitsu Group’s security activities and is one of the Information Security Policy participating organizations (participating organizations).

In addition, the committee promotes security personnel training for system integration and services for the entire Fujitsu Group.

Development and Execution of Security Governance

Targeted attacks on specific corporations and groups, website attacks, and personal information leaks have been increasing even further in recent years. This has created the need to implement risk management from a corporate management perspective. To this end, Fujitsu is pressing ahead with security initiatives under information security governance.

The System Integration Service Provider Organization and Group companies take part in the Council. Participating organizations formulate security plans, introduce security measures, promote information security activities and conduct internal audits based on the Security Management Framework (SMF; See the next page for details). They also strive to improve the management framework and security measures by confirming and evaluating the status of daily information security activities and security incidents and accidents.

Information Security Council Structure

Security Steering Committee Structure

Organization (each unit)
- Information security promotion division
  - Information Security Manager
  - Information Security Auditor
- Group companies
  - 47 companies

Participating organizations

Council Secretariat
- Information Security Council
- 64 units
- Council Secretariat
- Committee member
- Committee member
- Committee member
- Outside experts
- Top executives
- Chairperson/Vice chairperson

Each SI Service Provider Organization
- Each SI Service Provider Organization
- Each SI Service Provider Organization

* SI: System Integration
Information Security Management Promotion System

Participating organizations have established the “Information Security Council Activities Guidelines” with the goal of sound protection of customer and internal information to better handle information including customer information assets and confidential information. Based on these guidelines, participating organizations maintain and promote information security. Quarterly promotion meetings are held for information security managers and information security auditors from participating organizations to exchange information and opinions on security policies. The head of the participating organizations shall be the person responsible for promoting information security.

Furthermore, the Council Secretariat provides participating organizations with various assistance, as necessary, including support for effective measures and advice on enhancement initiatives needed to promote information security activities. This promotes the continuation of information security activities among participating organizations.

Conversely, each participating organization promotes the information security activities stipulated by the Council and maintains information security standards.

SMF (Security Management Framework)

The Council Secretariat provides participating organizations with the SMF as a template to implement information security management. The SMF incorporates the ISO/IEC 27000 family, the Ministry of Economy, Trade and Industry (METI) Information Security Audit Standards, and other Japanese and international standards, in addition to the Fujitsu Group’s rules. The SMF consists of documents on the information security management system and the information security audit system. When carrying out their operations, participating organizations must follow the customers’ industry guidelines and fulfill the security requirements such as items regarding management in their contract with the customer. Each participating organization uses the SMF template to prepare its own information security-related documents and subsequent operations.

The SMF takes steps to respond to recently increasing cyber-attack risks and information leak risks from unauthorized internal activity by following the latest security countermeasure standards and extending their scope. The SMF draws on all manner of rules and guidelines related to information security controls that have been announced around the world, based on the regulations of the Fujitsu Group, thereby maintaining a consistent level while promulgating them through all participating organizations.

As an example, in handling the Social Security and Tax Number System that was officially implemented from 2016, Fujitsu Group has prepared its own guidelines and check sheet to enable participating organizations to formulate detailed rules for meeting the requirements for handling the system.

The relationships between the SMF, Fujitsu Group’s rules, international standards, industry guidelines, and so forth are shown in the following diagram.

<table>
<thead>
<tr>
<th>Relationship between the SMF and Fujitsu Group’s Rules, International Standards, Industry Guidelines, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Excerpt</strong></td>
</tr>
<tr>
<td><strong>Implement information security management using templates</strong></td>
</tr>
<tr>
<td><strong>Customize</strong></td>
</tr>
<tr>
<td><strong>Participating organizations</strong></td>
</tr>
<tr>
<td><strong>Fujitsu Group’s rules</strong></td>
</tr>
<tr>
<td><strong>METI Information Security Audit Standards</strong></td>
</tr>
<tr>
<td><strong>ISO/IEC 27000 Family</strong></td>
</tr>
<tr>
<td><strong>Industry guidelines</strong></td>
</tr>
<tr>
<td><strong>Management items accompanying contracts with customers</strong></td>
</tr>
</tbody>
</table>

Security Improvement Efforts

Human Resources Development

Information Security Manager Training is provided to information security managers and information security promoters for promoting and managing information security at participating organizations. Since fiscal 2012 the Council Secretariat operated an e-learning program that was also offered to encourage information security managers to continuously hone their own skills. For members of participating organizations, there is also an Information Security Course. This comprises a basic version and individual-theme versions set each year, to meet the demand from participating organizations.

Furthermore, in response to demand for developing internal auditors, the Council Secretariat has also launched Information Security Auditor Training.

The Council actively encourages information security auditors to acquire auditor qualifications certified by the Japan Information Security Audit Association (JASA) to increase the quality of information security audits within the Fujitsu Group and move them along their career path. As of fiscal 2015, 142 employees had acquired auditor qualifications and were actively engaged in internal audits and committee audits.

<table>
<thead>
<tr>
<th>Number of people in training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training course name</td>
</tr>
<tr>
<td>Information Security Manager Training (Group)</td>
</tr>
<tr>
<td>Information Security Manager Training (e-learning)</td>
</tr>
<tr>
<td>Information Security Auditor Training</td>
</tr>
</tbody>
</table>
Periodic Security Checks

On “Security Check Days” implemented by the Fujitsu Group each month, personnel confirm the security settings of PCs and smart devices, as well as the administration of removable media devices. At the Council, the information security measure diagnostic tool (IT Policy N@vi) is installed in all PCs to diagnose the security measures and operational status of each PC. When a PC is started, diagnostic items* are automatically checked, with the results displayed on the PC monitor. Furthermore, by having the information security managers of each organization easily confirm the results of all PCs, Fujitsu has effectively increased the penetration of security measures.

The Council provides a security check sheet for smart devices that conforms to the Company-wide policy. The check sheet is used by various participating organizations to ensure smart device security.

* Diagnostic items: 26 items including OS, viruses, passwords, encryption, and prohibited configuration items

Information Security Audits

The Council defines two types of information security audits: internal audits conducted by the participating organizations themselves and external audits of the participating organizations conducted by the Council Secretariat from an independent perspective.

By having regular internal and external audits of the participating organizations, we confirm the penetration and entrenchment of information security management practices and the operational status and entrenchment of information security measures, which provides guidance for making improvements.

External audits are conducted yearly under themes stipulated by the Council Secretariat and audit plans are proposed. The Council Secretariat takes the lead in forming an audit team comprised of members who hold JASA auditor qualifications. This plays a role in the career track of the security auditors described above, and helps to improve the quality of internal audits at each organization. The audit team confirms the promotion of information security management, identifies any deficiencies, and proposes improvements, among other activities, to maintain and improve security across all participating organizations. Outstanding measures in audited organizations will be introduced as examples at the Council and utilized to raise the level of security across all participating organizations.

In other activities, experts from the Council Secretariat implement special audits of specific projects, as well as participating organizations. This is to set themes individually to address individual requests from participating organizations and to meet operational requirements.

Social Media Training

SNS* has become quite popular as a communication tool in our daily life. With the increase in the number of users of SNS, for business or private purposes, the question of where corporate responsibility lies when problems occur has emerged.

In the face of these situations, Fujitsu has published the guidelines, Rules and Manners for Participating in Social Media. Based on these guidelines, the Council Secretariat has prepared an educational program titled “Information Security Course for Social Media” and delivers this to members.

The course explains the risks in using SNS and gives examples that guide learners on proper uses of the media.

* SNS: Social Networking Service

Security Audits for Systems Delivered to Customers

The Fujitsu Group formulates security standards that should be satisfied in Internet-connected systems delivered to customers. A pre-delivery security audit where specialized security departments objectively verify whether these systems meet guidelines is obligatory as part of quality inspections.

Security Audits for Systems Delivered to Customers

Fujitsu Standards.

Security audits for systems delivered to customers comprise two parts: an “infrastructure pre-delivery security audit” for the infrastructure (OS/middleware) and a “web application security audit” for web applications. Regarding web application security audits in particular, security assessments are performed at the systems design stage to rapidly extract and resolve any security problems related to web applications.

This ensures that the systems delivered to customers have been confirmed to meet a consistent security level established by the Fujitsu Group, while helping to prevent security incidents caused by unauthorized access from outside. Following the inception of security audits for systems delivered to customers, Fujitsu has confirmed a sharp decline in incidents caused by insufficient security configuration in the systems integration process.