

INFORMATION SECURITY MANAGEMENT

Ensuring Information Security

Bearing in mind that ICT constitutes a fundamental part of the Fujitsu Group's business, we maintain Groupwide information security, while proactively striving to secure and improve customers' information security with our products and services. In this way, we contribute to the Fujitsu Way, our corporate philosophy that articulates a desire for "a networked society that is rewarding and secure."

For further details on information security management, please refer to *Fujitsu Group Information Security Report 2018*.

<http://www.fujitsu.com/global/about/resources/reports/securityreport/>

Information Security Policy

With ICT as our core business, the Fujitsu Group's Corporate Vision states that we will "contribute to the creation of a safe, pleasant, networked society." We work to maintain and further improve our information security level throughout the Group.

In April 2016, we formulated the Fujitsu Group Information Security Policy*¹ with the aim of sharing this thinking throughout the Group and having each employee take action. The Japan Business Federation (Keidanren) also announced its Declaration of Cyber Security Management*²

in March 2018. The Fujitsu Group supports Keidanren's declaration, which shares the same principles as those set forth in the Fujitsu Cyber Security Declaration, which was released in November 2016.

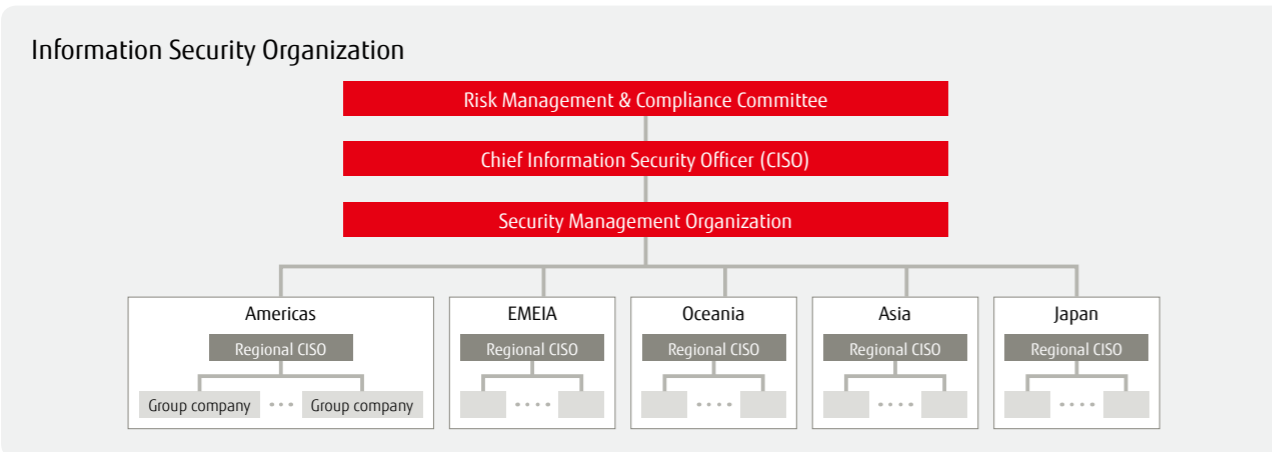
*1 Fujitsu Group Information Security Policy, full text: http://www.fujitsu.com/global/images/gig5/InformationSecurityPolicy_en.pdf

*2 Keidanren's Declaration of Cyber Security Management (Link to Keidanren website): <http://www.keidanren.or.jp/en/policy/2018/018.html>

Structure of Information Security Management

In order to further strengthen its security measures in response to the recent trend of increasing cyberattacks, Fujitsu appointed a chief information security officer (CISO) under the authority of the Risk Management & Compliance Committee.

Moreover, to strengthen the Group's global information security management governance, we have appointed regional CISOs around the world.



Three Priority Measures for Information Security Based on the Concept of "Defense in Depth"

Cyberattacks in recent years, exemplified by "advanced persistent threats (APTs)," have become more sophisticated, diverse, and complex, while conventional single-layer security measures are no longer able to completely defend against them.

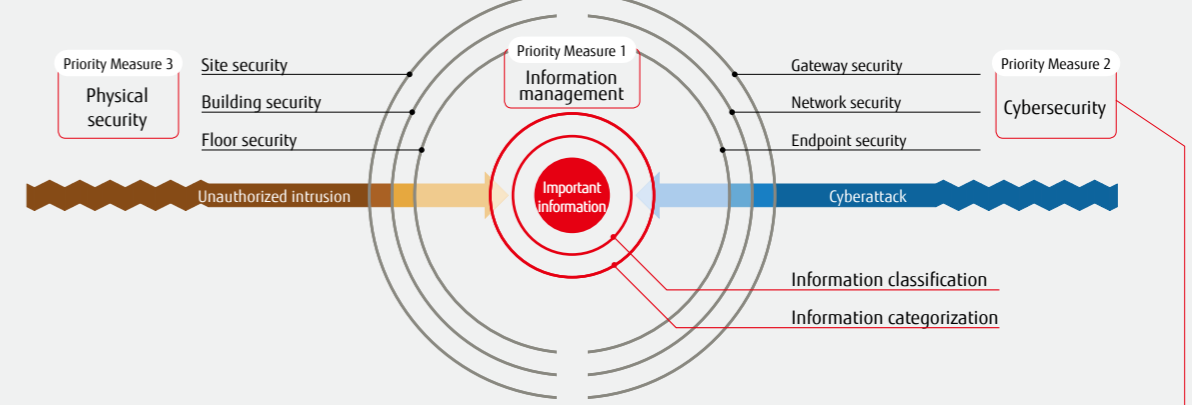
The Fujitsu Group has adopted the concept of "defense in depth" as its basic concept for information security, which utilizes a multilayer defense mechanism with several different defense measures instead of one. "Defense in depth" has three goals: preventing attacks by setting multiple defensive barriers, rapidly detecting attacks by establishing multiple detection functions, and minimizing damage after infiltration.

With such a multilayered approach to defense, we can prevent attacks and minimize damage.

The Group has adopted three priority security measures to protect internal information: "information management,"

which aims to protect information; "cybersecurity," which is centered on measures that protect systems against cyberattacks; and "physical security," which prevents unauthorized access to offices, factories, and other facilities.

"Defense in Depth" Conceptual Image



Cybersecurity

To prepare for cyberattacks, the Fujitsu Group implements separate measures at multiple layers based on network characteristics. We are working to protect against increasingly sophisticated, diverse, and complex cyberattacks via our "defense in depth" security.

This combines gateway security measures including firewalls and APT measures, network security measures such as unauthorized access detection, and endpoint security measures including malware measures as well as security patch management.

Protection of Personal Information

Fujitsu acquired the "PrivacyMark"^{*3} in August 2007, and has continuously worked to strengthen its personal information protection framework, which includes handling personal information involving annual training and audits. Fujitsu Group companies in Japan also acquire the PrivacyMark when necessary, and work to ensure personal information management. Overseas Group companies post on their websites the privacy policies designed to meet the laws and social requirements of respective countries.



*3 Fujitsu received PrivacyMark certification from JIPDEC. The PrivacyMark is granted to business operators that appropriately handle personal information under personal information protection management systems conforming to JIS Q 15001:2006.

Response to the GDPR*⁴

We have established a global system for handling personal data subject to the General Data Protection Regulation

(GDPR) and are reinforcing our protection of personal data. Under the guidance of the CISO organization and legal department, we have developed internal rules such as guidelines related to the protection of individual rights in response to the GDPR. Collaborating with EMEIA and other regions around the world, we provide check sheets for the formulation, design, and initial setting of systems and/or services. We have also updated the operation process to deal with internal rules and have held employee training sessions.

In response to regulations on the transfer of personal data outside of the EU, we applied to the Dutch Data Protection Authority in December 2017 for our Binding Corporate Rules for Processors, which are common rules established across the Fujitsu Group related to the handling of personal data that customers have entrusted to the Fujitsu Group for processing.

*4 The GDPR (EU regulations requiring companies, organizations, and groups to protect personal data) was enacted on May 25, 2018. It includes regulations on transferring personal data out of the European Economic Area and the obligation to report personal data breach within 72 hours.