

# INFORMATION SECURITY

## 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 practice one of our Values stated in the Fujitsu Way, to "Contribute to a trusted society using technology."

For further details on information security management, please refer to *Fujitsu Group Information Security Report 2019*: [https://www.fujitsu.com/global/images/gig5/security-2019\\_en.pdf](https://www.fujitsu.com/global/images/gig5/security-2019_en.pdf)

### Information Security Policy

The Fujitsu Group places ICT as its core business. Our corporate vision is to contribute to creating a safe and secure networked society. With this vision, we are working to ensure and further improve the level of information security throughout the Group.

In April 2016, we established the Fujitsu Group Information Security Policy\*1 in order to share this vision and encourage action by each employee. Based on this policy, we are implementing information security measures, along with establishing internal rules related to information management and ICT security at Group companies in Japan and overseas.

\*1 Complete text of the Fujitsu Group Information Security Policy (Global Security Policy): [https://www.fujitsu.com/global/images/gig5/InformationSecurityPolicy\\_en.pdf](https://www.fujitsu.com/global/images/gig5/InformationSecurityPolicy_en.pdf)

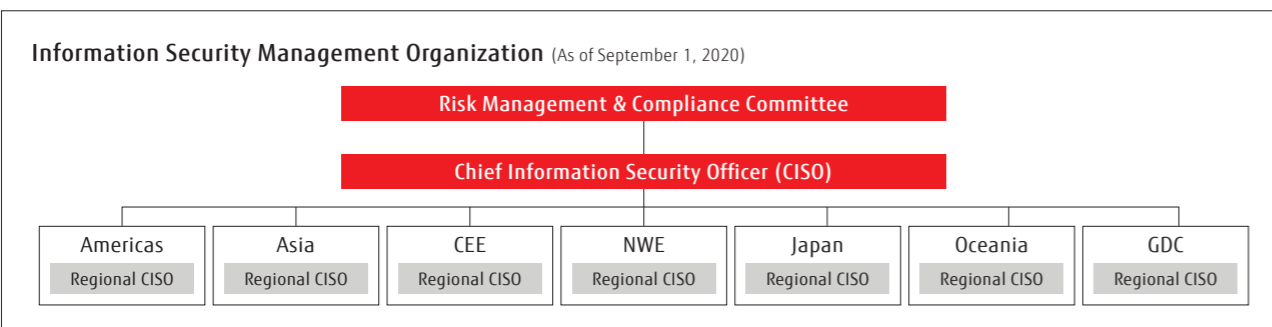
Keidanren, otherwise known as the Japan Business Federation, announced its Declaration of Cyber Security Management\*2 in March 2018. The Fujitsu Group supports Keidanren's declaration as being consistent with the principles set forth in the Fujitsu Declaration on Cybersecurity,\*3 released in November 2016.

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

\*3 The Fujitsu Declaration on Cybersecurity [https://www.fujitsu.com/global/documents/about/csr/security/Cybersecurity\\_declaration.pdf](https://www.fujitsu.com/global/documents/about/csr/security/Cybersecurity_declaration.pdf)

### Structure of Information Security Management

Given the recent increase in cyberattacks, the Fujitsu Group appointed a chief information security officer (CISO) under the authority of the Risk Management & Compliance Committee in order to further strengthen security measures within the Group. Moreover, in aiming to strengthen our global information security management, we have appointed regional CISOs around the world.



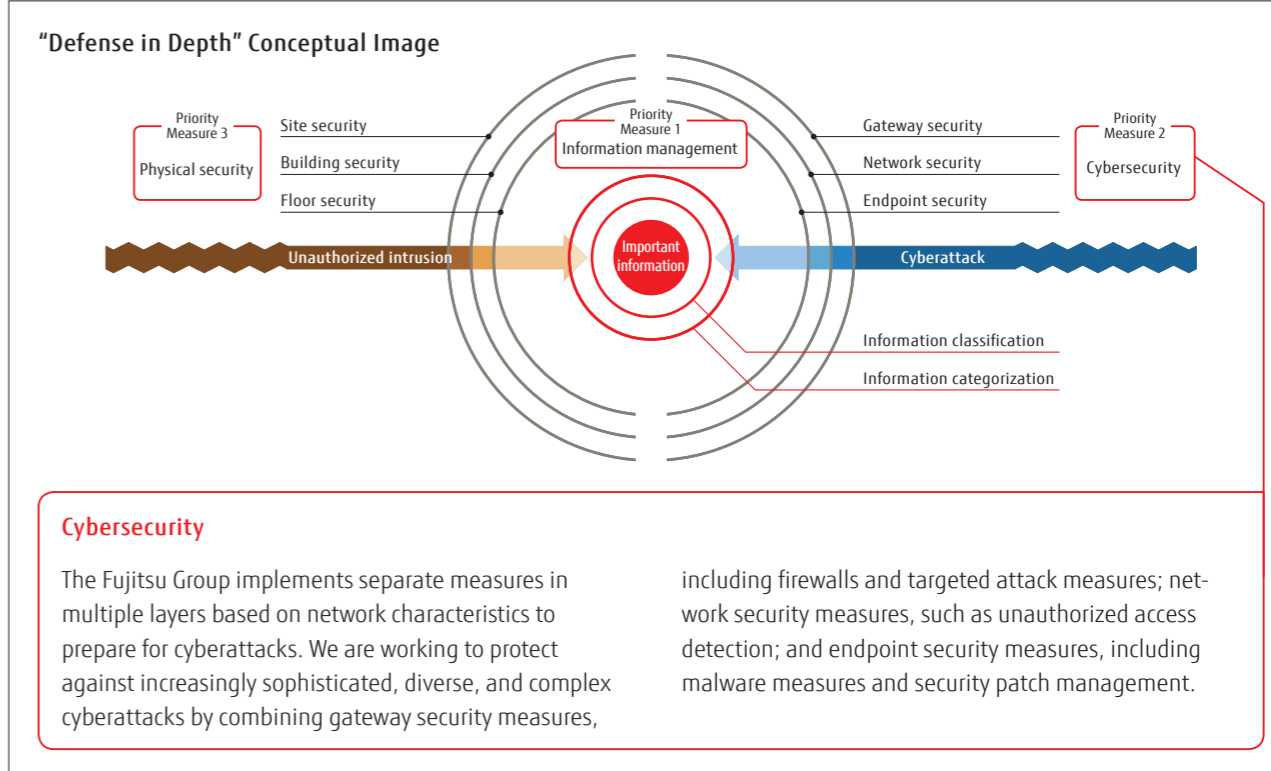
### Three Priority Measures for Information Security Based on the Concept of "Defense in Depth"

The cyberattacks in recent years are prime examples of targeted attacks. These attacks have an unprecedented level of sophistication, diversity, and complexity. It is no longer possible to achieve comprehensive protection by using conventional security measures.

The basic concept of information security measures at the Fujitsu Group incorporates "defense in depth." This refers to multilayer protection via multiple measures, instead of seeking protection through a single measure. Defense in depth has three objectives: 1) to prevent attacks by establishing a

multilayered wall; 2) to discover attacks at an early stage by establishing a multilayer detection function; and 3) to minimize damage in the event of infiltration. Appropriate implementation of these defense measures makes it possible to prevent attacks and minimize damage.

The Fujitsu Group implements the following three priority internal information security measures: 1) information management for protecting information; 2) cybersecurity that focuses on measures for protecting systems against cyberattacks; and 3) physical security that prevents unauthorized access to facilities such as offices and plants.



### Cybersecurity

The Fujitsu Group implements separate measures in multiple layers based on network characteristics to prepare for cyberattacks. We are working to protect against increasingly sophisticated, diverse, and complex cyberattacks by combining gateway security measures,

including firewalls and targeted attack measures; network security measures, such as unauthorized access detection; and endpoint security measures, including malware measures and security patch management.

### Protection of Personal Information

As part of our efforts to protect personal information, Fujitsu acquired the PrivacyMark\*4 from JIPDEC in August 2007. We are also working to continually enhance our personal information protection, including annual training and audits on personal information handling.

Domestic Group companies also acquire the PrivacyMark as needed and implement thorough personal information management. Privacy policies based on the laws and social demands of each country are posted on the websites of overseas Group companies.



\*4 The PrivacyMark is granted to business operators that appropriately handle personal information under personal information management systems that conform to JIS Q 15001:2017.

### Response to the GDPR\*5

Fujitsu has developed a global personal information protection scheme and is working to further strengthen the protection of personal data. Under the guidance of the CISO organization and legal business units, we cooperate with overseas regions and others to develop various internal rules and guidelines related to the protection of individual rights in response to the GDPR. We have also made check sheets for our design and initial setting. Furthermore, we have updated the operation process in accordance with such internal rules and guidelines 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 Group for processing.

In January 2019, the European Commission and the Japanese government mutually recognized each other's data protection laws as providing an adequate level of protection. Based on this recognition, Fujitsu established internal rules related to the handling of personal information transferred between regions, and ensured awareness of these rules throughout the Group.

\*5 The GDPR (EU regulations requiring companies, organizations, and groups to protect personal data) was enacted in May 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.