Basic Policy on Fujitsu Group Information Security
(Global Security Policy)

I. Purpose

The purpose of this Basic Policy on Information Security (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.

II. Basic Principles

(1) The Fujitsu Group shall, in carrying out its business, appropriately handle information provided by our individual or organizational customers and suppliers, and thereby protect the rights and interests of such individuals and organizations.

(2) The Fujitsu Group shall, in carrying out its business, appropriately handle trade secrets, technological information and any other information of value, and thereby protect the rights and interests of the Fujitsu Group.

(3) The Fujitsu Group shall exercise endeavors on research and development as well as development of human resources in order to provide products and services that contribute to maintaining and enhancing our customers' information security, and thereby promote sustainable development of our customers and thus society at large.

III. Definition of Information Security

In this Basic Policy, the following terms shall have the following meanings.

(1) "**Information**" means any information stipulated in relevant internal policy (ies), if any, as the information that the Fujitsu Group handles during the course of business regardless of its form of distribution, including public information, confidential information, and personal information.

(2) **"Information security"** means the preservation of confidentiality, integrity and availability of information, which shall include information management, physical security, and cybersecurity.

(3) **"Cybersecurity"** means a state where necessary measures are taken and properly maintained (i) to prevent leakage, loss or damage of data, or otherwise manage the security of such data, and (ii) to ensure the safety and reliability of IT systems and networks.

IV. Information Security Structure

Based on the "Basic Policy on the Establishment of Internal Control System", the Fujitsu Group shall acknowledge various factors threatening the Fujitsu Group's information security as risks inherent in its business, and therefore, establishes the following structure.

(1) The Risk Management & Compliance Committee, which reports directly to the Board of Directors and consists of the President & Representative Director, Executive Directors and the Risk Management Officer, shall exercise management of such risks globally.

(2) The Risk Management & Compliance Committee shall appoint a Chief Information Security Officer (CISO) and delegate responsibility and authority with respect to the execution of global information security measures within the Fujitsu Group. The CISO shall be appointed from its executive officer who is in charge of any of the Global

Corporate Functions such as IT security division and/or Legal division.

(3) The CISO shall report on the execution status of its duties to the Risk Management & Compliance Committee, periodically as well as when necessity arises.

(4) The Risk Management & Compliance Committee shall establish the Cybersecurity Committee as its subcommittee, which shall discuss overall cybersecurity strategies of the Fujitsu Group from an expert point of view.

V. Information Security Measures

1. Establishment of Framework for Information Security Measures

(1) The Fujitsu Group shall identify the assets it shall protect within the Fujitsu Group, understand the whereabouts and contents thereof, analyze information security risks bearing in mind the architecture of systems and networks, and implement global information security measures proportionate to such risks.

(2) The Fujitsu Group shall establish a plan to implement global information security measures in a sound manner, and implement processes (PDCA cycles) in order to monitor and continuously improve the execution thereof.

2. Establishment of Related Policies and Compliance with Laws

(1) The Fujitsu Group shall establish relevant internal policies globally in order to appropriately implement information security measures, and cause its executive officers and employees to be aware of and comply with such internal policies.

(2) The Fujitsu Group shall strictly respond to any violation of laws or internal policies related to information security.

3. Dedication of Resources

(1) The Fujitsu Group shall secure and allocate management resources necessary to globally implement appropriate information security measures.

(2) The Fujitsu Group shall develop and secure highly skilled security personnel in a planned and consistent manner.

(3) The Fujitsu Group shall train and raise awareness of its executive officers and employees on information security, and cause them to become aware of its importance and take action.

(4) The Fujitsu Group shall proactively participate in external information sharing activities and reflect such activities into its information security measures.

4. Information Security within the Supply Chain and Outsourcing Partners

The Fujitsu Group shall inform its suppliers in the supply chain and IT management outsourcing companies of its policies on information security and require them to maintain appropriate information security in accordance with such policies.

5. Disclosure

The Fujitsu Group shall disclose its efforts on information security through publications such as the "Information Security Report" to the extent that such disclosure does not hamper its ability to ensure information security.

VI. Information Security of the Customer

(1) The Fujitsu Group shall proactively endeavor to maintain and improve its customers' information security through information security products and services.

(2) The Fujitsu Group shall endeavor to assure security quality during the development of its products and services.

(3) The Fujitsu Group shall proactively conduct research and development on information security and continuously endeavor to update its technology and know-how.

VII. Information Security Incident Response

The Fujitsu Group shall establish the following structures and policies in case of occurrence of information security risks ("information security incidents").

(1) The Fujitsu Group shall establish reporting structures and initial response manuals, ensure that relevant persons are aware thereof, and conduct periodic and practical training.

(2) The Fujitsu Group shall establish expert teams (such as CERT: Computer Emergency Response Team / CSIRT: Computer Security Incident Response Team) under the supervision of the CISO in order to respond to information security incidents.

(3) The CISO shall report to the Risk Management & Compliance Committee in the event of a significant information security incident.

(4) The Risk Management & Compliance Committee shall determine its policy on how to respond to such information security risks, instruct the prevention of recurrence, and, as necessary, report to the Board of Directors.

(5) The Fujitsu Group shall, depending on the situation, give notice to government authorities and relevant persons of information security incidents.

VIII. Amendments and Abolishment of This Basie Policy

Amendments or abolishment of this Basic Policy shall be determined by the resolution of the Risk Management & Compliance Committee.

Notwithstanding the foregoing, minor amendments may be effectuated at the discretion of the CISO.

Last updated: 31 January 2019