Cyber Security Management Declaration

Sumitomo Mitsui Trust Holdings, Inc. (the "Company") and its group companies (*1) recognize the necessity of "working proactively to ensure cybersecurity from the two perspectives of value creation and risk management" as stated in the Japan Business Federation's (Keidanren) Declaration of Cyber Security Management, and has enacted its own Cyber Security Management Declaration.

As Japan's sole financial group specialized in trust banking, the Company will further strengthen management-led cyber security measures to protect customers' precious assets against the threat of cyber attacks.

1. Recognition as a management issue

Managers will work energetically to deepen their understanding of the current situation and proactively manage the positioning of and investment in cyber security. Managers will also squarely confront risk, recognizing serious management issues and exhibiting leadership as they take responsibility for the implementation of responses.

Specifically, the Company defines risk associated with cyber attacks as a top-priority risk source. Based on discussions and investigations led by management, the Company will promote risk countermeasures at the management level.

2. Decision of management policy and declaration of intent

The Company will decide management policy and BCPs (business continuity plans) for the earliest possible recovery from incidents with an emphasis on detection, response and recovery, as well as identification and defense. Managers will take the initiative to declare their intent to internal and external stakeholders, and will make efforts in disclosure, autonomously reporting recognized risks and response initiatives in various reporting documents.

Specifically, based on its management plan, the Company will work to respond to cyber attacks as follows:

- Improving manuals, etc. for measures in times of normality and emergencies
- Strengthening its ability to respond to incidents through periodic training and drills
- Improving contingency plans
- Disclosing initiatives to strengthen security through disclosure materials, etc.

3. Implementation of internal and external structures and countermeasures

In addition to securing a sufficient budget, personnel and other resources, the Company will improve its internal structure and take necessary measures in personnel, technology, logistics, and other areas, and train and educate employees at each level, including management, project management, engineers, and general staff. It will also make efforts for measures in the supply chain, including overseas, and with customers and service providers.

Specifically, it will place SuMiTRUST-CSIRT as its internal organization that proceeds with collection and analysis of information and measures, etc. related to cyber attacks and ensure necessary staffing, as well as strengthen human resources continuously utilizing a security training program, etc., and work to enhance the management system while collaborating with external specialized agencies.

The Company will also strive to implement security measures that leverage advanced technologies, and implement supply chain measures through status monitoring of cyber security measures, including cloud service providers and overseas entities.

4. Dissemination to society of the products, systems and services for which countermeasures have been taken

The Company will strive to engage in cybersecurity countermeasure business activities including development, design, production and delivery.

In order to protect customers' precious assets, we will implement various security measures such as installation of antivirus software on customers' terminals, advanced authentication, and encryption of communication data for services such as Internet banking.

Through our website, etc., we also call for countermeasures to use our services safely by calling attention to abuse of passwords and virus infection, etc.

5. Contribution to building of safe and secure ecosystems

Based on collaboration with related government departments, organizations, groups and others, we aim to share information by proactively providing their information and build personal dialogue networks in Japan and overseas. Furthermore, by drawing attention to the range of countermeasures for different types of information, we aim to contribute to a strengthening of cybersecurity nationwide.

Specifically, through appropriate and timely collaboration with related government and other bodies such as the Financial Service Agency, National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Information-technology Promotion Agency, the police and others, while also sharing information with security intelligence agencies including Financial ISAC (*2), FS-ISAC (*2) and JPCERT/CC (*3), we aim to contribute to the enhancement of the cybersecurity of society as a whole on a global basis.

(*1) Each group company subject to this declaration

Sumitomo Mitsui Trust Bank, Limited, Sumitomo Mitsui Trust Club Co., Ltd, Sumitomo Mitsui Trust Card Co., Ltd., Sumitomo Mitsui Trust Loan & Finance Co., Ltd. and Sumitomo Mitsui Trust Asset Management Co., Ltd.

(*2) Financials ISAC Japan, FS-ISAC

An organization that provides cyber-security-related information and analysis to financial institution members. Financials ISAC Japan is aimed at financial institutions doing business in Japan, while FS-ISAC is targeted at financial institutions in the U.S.

(*3) JPCERT/CC

JPCERT/CC is an organization that accepts reports on the sites in Japan, provides support for response, grasps the occurrence situation, analyzes the method, and considers and gives advice on measures to prevent recurrence from a technical standpoint with regard to computer security incidents such as intrusion and denial of service caused via the Internet.