Information Security Risk Management

Information assets are one of the most important management resources and pose risks that may undermine the foundation of corporate management. The Group, therefore, appropriately maintains and manages all information assets it holds.

Information Security Responsibilities

SuMi TRUST Holdings clearly states, in the Information Security Management Rules under the Risk Management Rules on which directors have the authority to amend and approve, that the head of overall information security risk management is the officer in charge of the IT & Business Process Planning Department, and that the supervising department conducting overall information security risk management is the IT & Business Process Planning Department.

Security Audit

For the Group's overall systems, self-evaluations are carried out every year using the System Risk Evaluation Table of the System Risk Management Guidelines established in line with the Center for Financial Industry Information Systems' (FISC) security measures, and the results are reported to the officer in charge. Furthermore, with regard to cyber security, third-party assessments are regularly made by the Deloitte Tohmatsu Group in Japan and overseas.

Client Information Management

The Group regards client protection as a top management priority, and has established an appropriate client protection management framework that reflects the business attributes of each Group company. In particular, regarding client information management, the Group has published its Declaration for the Protection of Personal Information which is a policy to securely protect the personal information, and specific personal information, of its clients and shareholders (see page 95 for details).

Response to Threat of Cyberattack

The threat of cyberattacks and the damage they can inflict are growing both in Japan and overseas. Under such circumstances, SuMi TRUST Holdings is engaged in the following activities to protect the precious assets of its clients from the attacks.

* See page 119 for the framework towards international financial regulations, including cyber security

Improvement of Internal Response Systems in Preparation for Cyberattacks

The Group has formulated its Cyber Security Management Declaration against cyberattacks, working to strengthen security measures led by management.

* For details of the Cyber Security Management Declaration please see: https://www.smth.jp/en/about_us/management/risk/pdf/CSMD.pdf

To respond to cyberattacks, SuMi TRUST Holdings monitors computer systems of SuMi TRUST Bank around the clock. In addition, SuMi TRUST Holdings has established SuMiTRUST-CSIRT as an internal organization for gathering information, conducting analysis, and implementing measures relating to cyberattacks, and coordinates with outside expert organizations to strengthen its management system.

Enhancement of Internet Banking Transaction Security

In terms of internet banking, SuMi TRUST Bank offers "Rapport," a type of security software specifically for internet banking, free of charge to help shield clients' precious deposits and other assets from fraudulent transactions.

Furthermore, the Bank has introduced a telephone authentication service*. It is strongly recommended that all internet banking clients register for telephone authentication in order to prevent any unauthorized payments.

SuMi TRUST Holdings will continue to keep abreast of other companies' moves and new technologies and implement thoroughgoing security measures so that clients' transactions remain safe. The measures include the early detection and prevention of unauthorized remittances.

* An authentication service using a client's mobile phone, smart phone, or home phone number in addition to the Sumitomo Mitsui Trust Direct card's confirmation number when making first transfer to a new account

Employee Training

The Group conducts the following training every year to educate and raise awareness of information security risk management across the whole Group.

e-learning	Information security training (once every six months)
	Countermeasures training on e-mail cyberattacks (targeted attacks) (twice a year)
Training	Response to suspicious e-mails that simulate targeted e-mail attacks on random people (monthly)

* Training is available not only for full-time employees but also for some employees of outsourcing contractors.