Declaration on Cybersecurity Management

The Concordia Financial Group, Ltd. (hereafter, "CFG") and its group companies (*1) agree with "positively implementing cybersecurity measures from the point of view of both value creation and risk management", which is one of the important issues for management raised by the Japan Business Federation in its "Declaration on Cybersecurity Management", and have adopted the CFG "Declaration on Cybersecurity Management" (hereafter, "this Declaration"). Based on this Declaration, management will take the initiative to further strengthen cybersecurity measures against cyberthreats, which are becoming more serious and more sophisticated.

(Note 1) Group companies covered by this Declaration: The Bank of Yokohama, Ltd., Higashi-Nippon Bank, Ltd., and their consolidated subsidiary companies.

1. Recognition as a Management Issue

Cybersecurity is actively tackled by management as an investment. Managers themselves must not neglect to deepen their understanding of the latest situation regarding cybersecurity. Also, managers themselves directly face up to the risks in the present situation, recognize security as an important management issue, and display leadership as managers by tackling security measures on their own initiative.

In protecting the assets of customers and enabling stable operation of the financial system, which is a part of the critical infrastructure of the nation, cyber risks are treated as one of the top risks for CFG and management takes the lead in continuously promoting countermeasures.

2. Formulation of Management Policy and Declaration of Intention

The CFG has formulated management policy and a Business Continuity Plan (BCP) for rapid recovery from incidents. These not only deal with identification and defense, but also with detection, response, and recovery. Management proactively discloses its decisions to stakeholders inside and outside the company, and endeavors to voluntarily provide various kinds of reports regarding the risks recognized and the actions taken in response.

Specifically, in order to respond to evolving cyber risks, a "Concordia Financial Group CSIRT" (*2) has been established composed of IT personnel and CSIRT members from each group company. This CSIRT carries out periodic training and exercises, develops procedures, rules, etc., during normal times, and also when an incident occurs, it

provides emergency response together with a cooperating specialist company 24 hours a day, 365 days a year. It also discloses initiatives to strengthen security with integrated reports etc.
(Note 2) Computer Security Incident Response Team

3. Construction of the System Inside and Outside the Company and Implementation of Measures

The company provides sufficient budgetary and personnel resources to develop systems within the company and allocates the necessary personnel, technology, and physical measures are allocated. It provides human resource development and education at each level of management and planning, technical, and general staff. It also takes measures for the supply chain, including clients, suppliers, and overseas.

Specifically, a specialized cybersecurity department has been established that proactively implements countermeasures and introduces the latest security technology based on the changing environment, which is marked by increasing utilization of digital technologies and transformations in working methods. A third party uses TLPT (*3), evaluates our cybersecurity posture, etc. in order to continuously audit and check the effectiveness of the countermeasures introduced and to work for improvement.

As personnel measures, periodic training and email drills are carried out to improve cybersecurity literacy for all group executives and employees. Specialist human resources are actively secured and cultivated by recruiting from the outside and by providing security training by specialist organizations to raise group personnel to global standards.

In addition to monitoring within our corporate group, we monitor clients, cloud service suppliers, and other suppliers, and execute measures for the security of our supply chains.

(Note 3) Threat-Led Penetration Testing

4. Dissemination to the Public of Systems and Services with Security Measures Implemented

The CFG incorporates cybersecurity measures into our various business activities, such as the development, design, production, and supply of systems and services.

Specifically, it introduces the latest security solutions so that customers can use our financial services with confidence, and develops an attitude that enables us to proactively respond to the threats posed by cyber risks. The CFG also raises awareness

of safety when customers use our financial services.

5. Contributing to Building a Safe and Secure Ecosystem

The CFG promotes the cultivation of personal networks and information sharing and dialog both in Japan and overseas, based on cooperation among the relevant government departments and agencies, organizations, groups, etc., where each party proactively shares their information. We also contribute to stronger cybersecurity in society as a whole by raising awareness of countermeasures based on various types of information.

Specifically, we make appropriate reports at appropriate times to the Financial Services Agency, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), the Information-Technology Promotion Agency, police and other investigative organizations, etc., and exchange information through Financials ISAC Japan, JPCERT, etc., in order to strengthen cybersecurity measures for society as a whole.

(Enacted April 1, 2022)__