Declaration of Cyber Security Management of the SBI Shinsei Bank Group

SBI Shinsei Bank and SBI Shinsei Bank Group member companies[*1] (hereinafter, "the Group") respect and follow the purpose of the Declaration of Cyber Security Management by the Japan Business Federation ("Keidanren"). Therefore, the Group formulated and announced the Declaration of Cyber Security Management of the Group. Based on the Declaration, the Group will further enhance, under the leadership of its management, the cybersecurity measures against cyber threats that have become more serious and sophisticated.

1. Recognize Cybersecurity as a Management Issue

The Group will enhance its own understanding of the latest cybersecurity circumstances and actively engage in management by considering cybersecurity measures as an investment. The Group will take responsibility for cybersecurity measures while recognizing that cybersecurity is a critical management issue, confronting realities, addressing risks, and exercising leadership.

Having positioned cyber-attacks as one of the material management risks, the Group will promote countermeasures on cyber-attack based on the discussions and examinations at management meetings and Board of Directors' meetings to enable its customers to use safe and secure financial services and to perform its social responsibilities.

2. Develop Management Policies and Declare Intentions

The Group will develop management policies and business continuity plans aimed at prompt recovery from security incidents while prioritizing detection, response, and recovery in addition to identifying and protecting against risks. The Group will take the lead in declaring companies' intentions to internal and external stakeholders and make every effort to voluntarily disclose the risks that the Group has identified, and measures to deal with the risks in its corporate reporting.

Acknowledging that building cybersecurity structures is one of the Group's important managerial challenges, it will develop strategies related to system security responding to the changes in the external environment and threats, in order to constantly enhance its structure to defend itself .

3. Build Internal and External Systems and Implement Security Measures

The Group will ensure sufficient budgets and human resources, establish internal systems, and take necessary initiatives including personnel, technical and physical measures.
The Group will develop human resources and conduct training programs required for those at every level, including the management, corporate planning staff, technical specialists, and other employees. It will manage cybersecurity throughout domestic and international supply chains, including business partners and outsourcing contractors.

The Group has established C-SIRT[*2], a dedicated function to cyber security in the Group Headquarters, to enhance its organizational capability by securing necessary budgets and human resources. SBI Shinsei Bank Group's C-SIRT will a) organize cyber security-related rules, b) gather information about the latest attacks and system vulnerability, c) implement cyber-attack countermeasures to its networks, servers and PCs and regularly check the countermeasures, d) monitor fraud remittances and e) conduct drills and training for employees.

4. Contribute to Widespread Use of Cybersafe Systems, and Services

The Group will manage cybersecurity across the full spectrum of corporate activity, including development, design, production, and supply of systems, and services.

It will enhance security checks for system development to enable our customers to use safe and secure financial services and to perform our social responsibilities. For transactions through the internet, the Group will enhance security measures such as authentication methods and fraud detection systems. It has also implemented phishing site closure service as a countermeasure against increased phishing.

5. Contribute to Building Safe and Secure Ecosystems

The Group will collaborate with relevant government agencies, organizations, industry associations, and other bodies to actively share information, engage in dialogue, and build human networks, both in Japan and internationally. It will contribute to reinforcement of cybersecurity throughout society by raising awareness of measures taken on the basis of such information.

Specifically, the Group will contribute to the realization of a safe and secure cyber environment for the entire society through proactive coordination with information institutions such as Financial ISAC[*3], FS-ISAC[*4] and JPCERT[*5], as well as providing timely and appropriate reports to government offices such as the FSA, National center of Incident readiness and Strategy for Cybersecurity (NISC), the Information-technology Promotion Agency (IPA), Japan and other investigative institutions.

*1 APLUS, Shinsei Financial and Showa Leasing, Group member companies that are target for the Declaration
*2 Computer Security Incident Response Team
*3 Financials ISAC Japan
*4 Financial Services Information Sharing and Analysis Center. Established in the U.S. in 1999, the organization shares information among its members exceeding 5,000.
*5 JPCERT Coordination Center, a general incorporated association. Gathers computer security information to support responses to security incidents and releases computer security-related information.

End