UNOFFICIAL TRANSLATION

Readers should be aware that only the original Thai text has legal force and that this English translation is strictly for reference.

Notification of the Office of the Securities and Exchange Commission

No. Sor Thor. 37/2559

Re: Rules in Detail on Establishment of

Information Technology System

By virtue of Clause 5(1) in conjunction with (11) and (12) of the first paragraph under Clause 12 and Clause 14 of the *Notification of the Capital Market Supervisory Board No. Tor Thor. 35/2556 Re: Standard Conduct of Business, Management Arrangement, Operating Systems, and Providing Services to Clients of Securities Companies and Derivatives Intermediaries* dated 6 September 2013, the SEC Office hereby issues this Notification, as follows:

Clause 1 This Notification shall come into force as from 1 September 2017.

Clause 2 In this Notification:

"***Notification of Standard Conduct***" means the *Notification of the Capital Market Supervisory Board No. Tor Thor. 35/2556 Re: Standard Conduct of Business, Management Arrangement, Operating Systems, and Providing Services to Clients of Securities Companies and Derivatives Intermediaries* dated 6 September 2013;

"***software program***" means any calculation system which displays an analysis to give advice on the value or the appropriateness of any investment in securities or derivatives;

"***IT assets***" means:

(1) system assets, i.e., computer network, system software, application software, and information systems;

(2) equipment assets, i.e., computers, equipment, data recorders, and other equipment;

(3) information assets, i.e., information, electronic data, and computer data.

Clause 3 This Notification shall apply to the persons licensed to engage in securities business or derivatives business in the following categories:

(1) securities brokerage, securities trading or securities underwriting;

(2) investment advisory providing investment planning to clients or using ***software programs*** in providing services to clients;

(3) mutual fund management excluding foreign investment funds;

(4) private fund management;

(5) securities borrowing and lending;

(6) financing securities business;

(7) derivatives brokerage;

(8) derivatives advisory providing investment planning to clients or using ***software programs*** in providing services to clients;

(9) derivatives manager;

In the case that an intermediary under the first paragraph is a commercial bank under the law on financial institution business, a life insurance company under the law on life insurance, or a financial institution established under a specific law, the intermediary shall comply with Clause 11 and Clause 23(4) of this Notification only.

Clause 4 The rules in detail under this Notification are prescribed to ensure that intermediaries comply with the ***Notification of Standard Conduct*** in the part concerning the effectiveness and consistency of the information system in the following matters:

(1) governance of enterprise information technology in accordance with Chapter 1;

(2) establishment of policies, measures, and management arrangement concerning information security in accordance with Chapter 2;

(3) management of ***IT assets*** and the access control to data and information system in accordance with Chapter 3;

(4) information communications security via computer network systems and operations security with respect to information systems in accordance with Chapter 4;

(5) additional rules in accordance with Chapter 5.

Chapter 1
Governance of Enterprise Information Technology

Clause 5 An intermediary shall establish a documented policy on the governance of information technology, which shall contain at least the following matters. Such policy shall be approved by the board of directors of the intermediary or a committee assigned by such board of directors;

(1) management of information technology risks which covers identification, assessment, and control of risks within the organization's acceptable level;

(2) allocation and management of information technology resources which covers the allocation of resources to ensure sufficiency for business operation and establishment of guidelines to support incidents where the resources are insufficiently allocated at a specified level;

(3) establishment of policies and measures on information security under Clause 8 and Clause 9.

Clause 6 An intermediary shall have in place information technology governance in accordance with the following criteria in order to implement the information technology governance policy of the intermediary as specified under Clause 5:

(1) policy on the governance of information technology shall be widely communicated to the relevant personnel of the intermediary in an easily accessible manner in order for such personnel to understand and be able to comply with such policy correctly;

(2) processes and procedures shall be established in line with the policy on the governance of information technology;

(3) policy on the governance of information technology shall be reviewed at least once a year. In case of the occurrence of any event which may significantly affect the governance of information technology, the policy on the governance of information technology shall be reviewed without delay, and the processes and procedures shall be improved in line with the policy which has been changed;

(4) report on the conformance of the information technology governance policy shall be provided to the board of directors of the intermediary at least once a year. In case of the occurrence of any event which may significantly affect the conformance of such policy, the board of directors of the intermediary shall be informed without delay;

(5) internal control for the operation shall be established in accordance with the information technology governance policy, which contains at least the following requirements:

(a) conduct internal audit and operation review, systematically;

(b) correct deviation and follow up the result of correction, systematically.

Chapter 2
Establishment of Policies, Measures, Management Arrangement on Information Security

Clause 7 In this Chapter:

"***teleworking***" means the operation which accesses the critical information system with indirect connection to the organization's internal network systems;

"***use of mobile device***" means the use of mobile devices in the operation to access the critical information system via direct connection to the organization's internal network systems;

Clause 8 An intermediary shall establish a documented information security policy which addresses at least the following matters:

(1) policy on the use of ***cloud computing*** which covers the methods for selection and evaluation of cloud providers, review of the qualifications of the cloud providers, the terms of services, and inspection of records and evidence;

(2) policy on the use of cryptographic controls and key management for protection of sensitive and critical information;

(3) policy on the transfer of information within organization's networks and with external entity's networks;

(4) policy on access control on information and ***information processing facilities*** in line with IT security requirements;

(5) policy on the use of IT outsourcing which covers selection and evaluation of the ***outsourcee***, review of the ***outsourcee***'s qualifications, and provision associated with the use of services to ensure mitigation of risks from the ***outsourcee***'s access to the organization's ***IT assets***.

For the purpose of (4) in the first paragraph, the term "***information processing facilities***" means any equipment, operating systems, or infrastructure that are necessary or facilitate data processing completely, accurately, and effectively such as IT equipment, applications, computer network systems, procedures, or information processing areas, etc.

Clause 9 An intermediary shall establish information security which contains at least the following measures:

(1) in case of ***teleworking*** or using mobile devices, the security measures shall be properly sufficient for confidential or critical information. In this regard, the mobile devices shall be registered prior to the intended use and such registration shall be reviewed at least once a year and upon any replacement of mobile devices;

(2) measures on the use of ***cloud computing*** under the policy established in Clause 8(1) which covers:

(a) an agreement between the cloud provider and the intermediary which contains at least the following matter:

1. roles and responsibilities of the cloud provider and the liabilities to the intermediary in the case that the cloud provider fails to comply with the agreement;.

2. operating procedures that meet the internationally-accepted information security standards;

3. measures on IT security, access control, and information disclosure;

4. audit of the cloud provider's operation by an independent auditor;

5. conditions in the case that the cloud provider subcontracts to another cloud provider and the provision on liabilities that may arise due to the operation of such cloud provider;

(b) qualifications of the subcontracted cloud provider on information security aspect which are comparable to those of the cloud provider or meet the international standards;

(c) monitoring, evaluation, and review of the services performance of the cloud provider;

(d) procedures for data migration to the new cloud provider in case of any replacement of the cloud provider.

Clause 10 An intermediary shall have in place the management arrangement for the organization of information security in accordance with the following criteria:

(1) define and document information security roles and responsibilities and establish operating guidelines for the personnel of the intermediary;

(2) establish a cross-check for operation of information security to prevent potential risks;

(3) establish communication channels with the SEC Office, the regulatory authority for information technology, and the service provider that supports the operation of the organization's information systems, and update contacts of each channel.

Clause 11 An intermediary shall establish the information security incident management in accordance with the following criteria:

(1) establish procedures and processes to manage information security incidents;

(2) define the person responsible for managing information security incidents;

(3) report any information security events to the responsible person under (2) and the SEC Office without delay;

(4) carry out testing of procedures and processes in the management of information security incidents under (1) at least once a year and the testing shall at least cover the management of cyber security threats (cyber security drills);

(5) review procedures and processes in the management of information security incidents, after the testing under (4) is carried out, at least once a year;

(6) evaluate the results of the testing under (4) and the review under (5) and report such evaluation to the board of directors of the intermediary or its assigned committee at least once a year. Such evaluation shall be carried out by a person who is independent from the responsible person for managing information security incidents under (2);

(7) maintain all documents related to the management of information security incidents at least two years from the date of issue, in a way that such documents are prompt to be called or inspected by the SEC Office without delay.

For the purpose of (4) in the first paragraph, the term "cyber security threat" means a threat that affects or damages or entails risks to the operation of the intermediary which arise from the use of services or applications on computer networks, the Internet, telecommunications networks or satellite services.

Clause 12 An intermediary shall establish information security of the business continuity management in accordance with the following criteria:

(1) determine requirements for information security and the continuity of information security management in adverse situations;

(2) establish procedures, processes and controls to ensure the required level of continuity for information security;

(3) define the recovery time objective (RTO) for information system and its priority to be recovered based on its criticality and potential impact;

(4) consider redundant information systems, if needed, to ensure availability as required under (3).

Clause 13 An intermediary shall create an awareness of IT policy and related procedures among its employees and contractors who are engaged in the operation by accessing the organization's information or internal information system, and arrange for such personnel to perform their functions in accordance with the established policy and procedures by meeting the following criteria:

(1) educate all employees and contractors on IT security policy relevant to their job function;

(2) communicate to the employees and contractors that they should exercise precaution and refrain from using the organization's information systems which may likely damage the intermediary or the capital market or have an impact on the national security, and that they are required to report violations or any significant abnormality to the person responsible for the information security incident management without delay;

(3) put in place a disciplinary process to take action against any employee who has committed an IT security breach.

Chapter 3
Management of IT Assets and Access Control

Clause 14 In managing ***IT assets*** and assess control of data and information systems, an intermediary shall comply with the following criteria:

(1) management of ***IT assets*** under Clause 15 to Clause 17;

(2) physical and environmental security measures of ***IT assets*** under Clause 18;

(3) physical and environmental security measures of equipment assets under Clause 19;

(4) assess control of operating systems and information under Clause 20.

Clause 15 An intermediary shall ensure that the IT asset management meets the following criteria:

(1) identify persons or units responsible for each type of ***IT assets*** over the whole asset lifecycle;

(2) establish the terms for acceptable use of ***IT assets***;

(3) in case of any change to the responsible person or unit, protection roles and responsibilities to relevant ***IT assets*** should be reviewed.

Clause 16 ***IT assets*** associated with systems assets or equipment assets shall be identified and inventory of these assets should be drawn up an maintained. Such inventory shall be reviewed at least once a year or upon any material change.

Clause 17 Information shall be classified in terms of sensitivity and other ***IT assets*** (i.e., systems asset and equipment asset) shall be classified in terms of criticality in order that such ***IT assets*** are given an appropriate level of protection in accordance with their sensitivity and criticality to the intermediary. In case of information, the intermediary shall establish the procedures for preventing against unauthorized disclosure, modification, removal or destruction of sensitive information stored on media.

Clause 18 An intermediary shall establish physical and environmental security measures to protect ***IT assets*** in accordance with the following criteria:

(1) assess security requirement of ***IT assets*** based on their results of a risk assessment and criticality;

(2) define the secure areas and the siting of the critical ***IT assets*** to ensure security and prevent unauthorized physical access.

Clause 19 In addition to the physical and environmental security measures under Clause 18, an intermediary shall prevent loss, damage, theft or compromising of equipment assets, and interruption to the organization’s operation.

Clause 20 An intermediary shall implement access control of information and information systems in accordance with the following criteria:

(1) there shall be a user management in place to limit access for authorized users only, as follows:

(a) a formal user registration process to enable assignment of assess rights; (b) the allocation and use of privileged access rights should be restricted and controlled;

(c) the allocation of passwords should be controlled through a formal management process;

(d) monitor and review the users' access rights at a regular interval.

(2) there shall be requirements in place for users to comply with the organization's practices in the use of passwords;

(3) there shall be controls of unauthorized access to information systems and applications, as follows:

(a) control access of users and system administrators to information and application system functions in accordance with the defined access rights;

(b) control access to information systems and applications by a secured log-on procedure;

(c) establish password management systems to ensure security of passwords;

(d) tightly restrict and control the use of utility programs and limit access to program source code.

Chapter 4
Information Communications Security via Computer Network Systems and Operations Security with respect to Information Systems

---

Clause 21 An intermediary shall establish measures on communications security and operations security in respect of the following matters:

(1) communications security via computer network systems under Clause 22;

(2) operating procedures relating to information systems under Clause 23.

Clause 22 An intermediary shall establish measures for communications security in accordance with the following criteria:

(1) manage and control computer network systems in a secure way to ensure prevention of any action that may cause a risk to information in networks;

(2) arrange network services agreements (including service levels, management requirements, and security mechanisms of all network services) with vendors;

(3) segregate network domains properly, define the perimeter of each domain clearly, and control the access to each domain in a secure way;

(4) put in place procedures to protect information transfer through computer network systems;

(5) arrange for the personnel of the intermediary or an outsourcee (if any) to have in place confidentiality or a non-disclosure agreement.

Clause 23 An intermediary shall establish measures for operations security relating to information systems in accordance with the following criteria:

(1) define operating procedures relating to the information systems to ensure correct and secure operations;

(2) establish measures for prevention against, and detection of, malware and measures for recovering information systems from malware attacks;

(3) back up copies of critical business information, computer operating systems and application software, as well as take and test program source code at least once a year;

(4) completely and sufficiently store and record logs for inspection of conflicts of interest in the organization, use of information and information systems in compliance with assigned roles and responsibilities, unauthorized access, abnormal and/or illegal use of information systems and user identification of Internet trade clients, as defined in the table attached hereto. It should be required to monitor and analyze, based on the risk assessment of the organization, logs recorded from the use of ***critical information*** systems.

(5) implement procedures to control the installation of software on the operating systems and establish measures to restrict the installation of software by users to ensure the integrity of the operating systems;

(6) establish an effective management process for technical vulnerability as follows:

(a) carry out penetration testing with ***critical information systems*** connected to untrusted networks by a person who is independent from units and responsible for information technology in accordance with the results of risk assessment and the business impact analysis as follows:

1. in case of highly ***critical information systems,*** penetration testing shall be carried out at least once every three years and upon any material change to such systems;

2. for ***critical information systems*** apart from those mentioned above, penetration testing shall be carried out at least once every six years.

(b) carry out vulnerability assessments with all ***critical information systems*** at least once a year and upon any material change to such systems, and report the results to the compliance unit or the internal audit unit without delay.

(7) perform an audit of information systems as follows:

(a) draw up an audit plan on information systems in accordance with the results of risk assessment;

(b) define the scope of technical audit on information systems to cover key assessed risks, provided that such audit shall not affect any operations;

(c) perform an audit of information systems outside business hours if such audit could affect system availability.

Chapter 5
Additional Criteria

Clause 24 An intermediary shall ensure that system acquisition, development, and maintenance of the information systems meet the following criteria:

(1) establish information security related requirements in the requirements for new information systems or enhancements to the existing information systems;

(2) maintain information security for information involved in application services;

(3) establish controls of development or changes to the existing information systems in compliance with the established change control procedures;

(4) carry out testing of information system developed or changed to ensure that such information systems are able to function efficiently, process accurately, and meet the requirements of the users;

(5) ensure that appropriate changes are made to the business continuity plan when information systems are developed or changed;

(6) control people, processes, and technology associated with the development of information systems to ensure information security across the entire development lifecycle

(7) supervise, monitor, and control the activities of outsourced information system development to ensure consistency with the terms of services;

(8) carry out testing of the developed information systems by users or independent testers.

Clause 25 In the case that an intermediary appoints an outsourcee to engage in its information systems function, the intermediary shall comply with the following criteria:

(1) establish conditions and controls relating to information security in an agreement signed by both parties;

(2) monitor, evaluate, review and audit service delivery of the outsourcee regularly;

(3) re-assess and manage risks in case of changes to the processes and procedures and controls associated with information security, or changes of the outsourcee;

(4) establish measures for supervising the outsourcee to comply with the operating criteria prescribed by the SEC, the Capital Market Supervisory Board, or the SEC Office, with respect to the outsourced function, as well as the protocol established by the intermediary in order to comply with such criteria. Such measures shall at least control that the outsourcee shall not process any characteristics whereby there is a reason to believe that there are weaknesses or inappropriateness for control and good operating practice;

(5) arrange an incident response policy in case of any occurrence of a security incident to the information systems;

(6) define the right of the intermediary to inspect the operation of the outsourcee to ensure compliance with the agreed term. With the exception where the outsourcee has a restriction to do so, the intermediary should establish another measure to ensure that the operation of the outsourcee remains in compliance with the agreed term;

(7) establish the term for the outsourcee to agree upon to allow the SEC Office to call and inspect the relevant documents or to enter and inspect the operation of the outsourcee.

Notified this 12th day of September 2016.

(Mr. Rapee Sucharitakul)
Secretary-General
Office of the Securities and Exchange Commission