Unofficial Translation

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

Appendix 3

[Attached to the SEC Office Notification No. Sor Thor. 38/2565]

Information Technology Security

Scope of Operation

1. Low-risk, medium-risk or high-risk business operators shall comply with the provisions specified hereunder.

2. Small-scale business operators shall maintain fundamental IT security at least in the following matters:

2.1 Part 2: Personnel and third-party management Clause 2.2 third parties

2.2 Part 5: Data and IT system access control Clause 5.3 Stipulating measures for controlling, limiting and monitoring privileged users (privileged user management)

2.3 Part 8: IT operations security, as follows:

Clause 8.1 System configuration management

Clause 8.4 Server and Endpoint Security

Clause 8.5 Stipulation of Bring Your Own Device (BYOD) Security Policy and Measures

Clause 8.9 Technical Vulnerability Assessment

Clause 8.10 Penetration Test

Clause 8.11 Patch management

2.4 Part 11: IT Incident Management, Clause 11.3 Reporting IT incidents, personal data violations, and events causing damage to assets users due to IT system security incidents.

Operation related to Information Technology Security

Part 1: Organization of Information Technology Security

A business operator shall ensure there is such organization which shall at least contain the following features:

1.1 Establishing an organizational structure for IT operations with details of duties and

responsibilities of the personnel in writing; and

1.2 Establishing a cross-check for IT operations to prevent potential risks;

Part 2 Personnel and Third-Party Management

Personnel or Third Party	Management
2.1 Related personnel or those who use IT systems to perform their work	A business operator shall conduct personnel management under Clause 2.1 appropriately by at least undertaking the following acts: (1) having a process for personnel selection as follows; (1.1) considering knowledge, competence, and adequacy in the operation; (1.2) checking background of personnel prior to employment sufficiently and in line with the risk of the position and duties and responsibilities thereof. (2) requiring the personnel to understand, acknowledge and affix their signature for acknowledgement of the following matters: (2.1) the roles and responsibilities of such personnel in relation to IT security; and (2.2) non-disclosure agreement (3) raising awareness of IT risk among personnel who can access data or application systems within the organization so the personnel could use the application systems safely; (4) requiring personnel to refrain from using the IT systems in such a manner that will cause damage to the capital market or that is illegal, or violates requirements or code of conduct established by the business operator (if any); (5) establishing disciplinary action policy for responding to personnel violating or failing to comply with IT security policies and measures; and

Personnel or Third Party	Management
	(6) establishing a procedure to be undertaken upon the end of employment or change in the position in order to prevent potential breach or damage to IT assets.
2.2 Third parties are subject to management if the business operator undertakes any of the following acts: 2.2.1 using IT services from third parties; 2.2.2 connecting its IT system to third parties; or 2.2.3 allowing third parties to access business operator's sensitive data or client data.	A business operator shall manage third parties under Clause 2.2.1, 2.2.2 or 2.2.3 in the following manners: (1) assessing the risks from the use of services, connection or access of data by third parties, including their subcontractors (if any); (2) establishing procedures and criteria for selection of third parties; (3) specifying the roles and responsibilities of the business operator and the third parties clearly in writing; (4) In case of a third party being a significant IT service provider according to the results of the risk assessment in Clause 2.2 (1), a service agreement or contract shall specify the right for the business operator, the SEC Office, and external auditors appointed by the business operator or the SEC Office to audit the operation and internal control of such third party. If there is a necessary ground preventing the business operator from specifying the right to audit pursuant to the first paragraph above in the agreement or contract, the business operator shall have assessment or monitoring measures that are prudent, adequate and in line with the risk and significance of the use of services, connection or data access; (5) having a non-disclosure agreement for third parties or their subcontractors if such persons can access the business operator's sensitive data or client data; (6) supervising, monitoring, and managing risks from the use of services, connection, or access to data from third parties which

Personnel or Third Party	Management
	shall be consistent with the risk level and the level of significance of such third parties; (7) maintaining IT security from the use of services, connection, or access to data from a third party to be in line with the business operator's IT security standards; and (8) making preparations for responding to any potential IT incidents with significant impacts to ensure continuity of services or business operation.

Part 3: IT Asset Management

A business operator shall establish an IT asset management to ensure that IT security operations is appropriate, complete and up-to-date, as follows:

3.1 developing an IT asset inventory of hardware and software including the licenses thereof;

3.2 designating a person or unit to be responsible for each item of IT assets; and

3.3 providing regular maintenance of IT assets.

Part 4: Data Security

A business operator shall appropriately maintain data security to ensure its confidentiality, integrity and availability, as follows:

4.1 designation of a person or unit as a data owner;

4.2 data classification and guidelines on security that are in line with the data classification, covering the following data:

4.2.1 data at endpoint

4.2.2 data in transit

4.2.3 data at rest

4.3 establishment of guidelines for secure data input, data processing and data disposal;

4.4 preparation of a complete and up-to-date data inventory.

Part 5: IT Access Control

A business operator shall ensure there is efficient access control to prevent the access and revision to systems or data by ineligible or unauthorized persons, as follows:

5.1 establishing guidelines on management of user accounts and access rights and reviewing the rights appropriately and regularly in line with the duties and responsibilities, including having a process for removal of the rights when such rights are no longer needed;

5.2 establishing an authentication process that is suitable for the risk and prevents repudiation; and

5.3 stipulating measures for controlling, limiting, and monitoring privileged users (privileged user management), as follows:

5.3.1 requiring MFA when logging in and changing passwords for the operating systems and the database systems that are related to the critical IT system;

5.3.2 if a business operator has restrictions on MFA, it may use another equivalent method instead and shall conduct a risk assessment and consider adequate risk control measures before applying for exception approval;

5.3.3 implementing strict control and monitoring the use of privileged user accounts.

Part 6: Cryptographic Control

A business operator shall ensure there is cryptographic control that is reliable and in line with international standards by stipulating a secure method for encryption and key management to ensure that the confidentiality, integrity and authenticity of data are appropriate and efficient, as follows:

6.1 stipulating secure encryption method;

6.2 establishing cryptographic key management by stipulating control measures for generating, installing, storing, backing up, revoking and destroying cryptographic keys;

6.3 stipulating measures on control of the cryptographic keys provided by a third party which shall be examined to ensure that the generated cryptographic keys are not shared with other users; and

6.4 stipulating an incident response process in the case of leakage of the cryptographic

key.

Part 7: Physical and Environmental Security

A business operator shall put in place physical and environmental security for IT assets, as well as the protection system, and maintenance processes for hardware and facilities related to IT in order to prevent damage to IT assets stored at the primary site, backup site, and the third-party colocation data center.

Part 8: IT Operations Security

A business operator shall put in place IT operations security measures to ensure that operations related to data processing will be correct and secure. Such measures shall address at least management of the following matters.

8.1 System configuration management by establishing processes for controlling system configurations and regularly reviewing the system configurations to ensure that they are correct and secure;

8.2 Sufficient and secure change management to ensure that changes will correctly and completely meet the specified objectives and that an unauthorized change is prevented;

8.3 Measures and procedures shall be in place for managing capacity, monitoring system efficiency, and forecasting the use of IT resources in order to ensure that the current business operations are supported and the resource are allocated efficiently for future usage;

8.4 Server and endpoint security is aimed at protecting such devices from being used as a channel for data leaks or unauthorized access to the IT systems;

8.5 Stipulation of teleworking, mobile device, and bring your own device (BYOD) security policy and measures by taking into account the related risks and putting in place appropriate control measures;

8.6 Sensitive data should be backed up using an appropriate method and frequency to ensure the availability of data consistent with the goal of restoring the IT system where the IT system and primary data were interrupted or damaged. Backup copies of data and the data recovery process shall be tested at least once a year;

8.7 IT system logs shall be produced and stored completely and adequately for use as evidence of electronic transactions. They may also be used for monitoring and reviewing accesses to and uses of data and the IT system as required by law;

8.8 Security monitoring involves using a process or tool to prevent and detect IT incidents, malware, or cyber threats which may affect the security of critical IT systems.

8.9 Technical vulnerability assessment of the IT systems shall be conducted in accordance with the risk level to identify vulnerabilities and rectify them to prevent potential cyber threats in a timely manner. The technical vulnerability assessment of the critical IT systems and all internet-facing IT systems shall be conducted at least once a year and upon every significant change to such systems, such as changes to the IT infrastructure or addition of critical functions, etc.

8.10 Penetration test

8.10.1 A business operator shall conduct a penetration test, as follows:

Application Systems	Penetration Test
(1) Application systems and internet-facing network systems	(1.1) At least once a year; and (1.2) Upon every significant change to such systems.
(2) Systems other than those in (1)	An assessment of intrusion risk through the internal network shall be conducted to specify the scope and the penetration test as deemed appropriate.

8.10.2 The penetration tests above shall be carried out by in-house or external experts who are independent from the system owner;

8.10.3 In the event that any vulnerabilities are identified, a business operator shall take steps to rectify them and prevent potential cyber threats in a timely manner to eliminate any risk from such vulnerabilities;

8.10.4 A business operator shall retain reports of operations under Clause 8.10 for a minimum of two years from the date of creation, in such a way that such documents are readily available upon request for inspection by the SEC Office;

8.10.5 A business operator shall submit the report on penetration test results without delay upon notification by the SEC Office.

8.11 11 There shall be patch management by putting in place a process to control the installation of patches on systems and devices to reduce the risk of potential attacks.

Part 9: Communication System Security

A business operator shall have appropriate communication system security to ensure that the communication system and data transmitted through the communication system will be safe and secure and can prevent potential cyber intrusions or threats as well as being able to provide continuous services.

Part 10: IT Project Management and System Acquisition, Development and Maintenance

A business operator shall have IT project management and IT system acquisition, development and maintenance to ensure security throughout the entire life cycle of its IT systems, as follows:

Operations	Details
10.1 IT Project Management	Establishing a project management framework to ensure efficient management of significant IT project, ensuring they are delivered accurately and completely as planned and the specified goals are achieved.
10.2 IT System Acquisition	Criteria for acquisition of IT systems and service providers shall be established to ensure that the acquired systems meet the business requirements and IT security requirements. The criteria shall take into account the flexibility of changing service providers, technological changes, and changes that are significantly related to business operations.
10.3 IT System Development	Control measures in relation to IT system development including designing, developing, system testing, and system deployment shall be established to ensure that the system is accurate, secure, reliable, ready for use, and adequately flexible to accommodate usage and aligned with the business plan, by undertaking at least the following acts:

Operations	Details
	(1) establishing detailed requirements of the system and technical specifications of the developed system, as follows: (1.1) security; (1.2) availability; and (1.3) capacity. (2) segregating the roles and responsibilities of persons involved in system development to ensure that the system will be reviewed before deploying into production; (3) segregating the environments of the application systems used for development and testing from production; (4) putting in place a process or tool to ensure secure source code development; (5) conducting testing on the IT system that has been developed, revised or changed to ensure that such system will be able to accurately and comprehensively process data and meet the needs of users; (6) having measures for ensuring the integrity of data conversion; (7) having measures for maintaining the security and confidentiality of sensitive data used in testing; (8) conducting a performance test of the systems related to electronic services or electronic transactions upon significant development or change of the systems, to ensure that such systems are able to support the number of concurrent users and transactions in line with business requirements;

Operations	Details
	(9) in the case that a third party is assigned to develop or change IT systems, a business operator shall monitor and ensure that their operations comply with the assignment agreement; and (10)) having a process for application for approval from the management or the committee assigned by the business operator before system deployment.
10.4 IT System Change	(1) Conducting impact assessments and prioritization of changes; (2) Establishing a process for requesting change approval, which must be granted in writing by the system owner unit to ensure the necessity for the change has been appropriately considered; (3) Conducting tests before configuring or deploying changes to production to reduce potential risks or impacts; (4) Having a process for approving the release of changes to production from the management or the committee assigned by the business operator; (5) Implementing a process or tool that controls source code version changes and supports fallback; and (6) Updating supporting documents of application systems that have been changed.

Part 11: IT Incident Management

A business operator shall manage IT incidents in an appropriate and timely manner, as follows:

11.1 providing a point of contact for reporting of IT incidents by personnel, clients, and relevant parties;

11.2 establishing a plan or process for management of IT incidents;

11.3 reporting IT incidents, personal data breaches, and IT system security incidents that cause damage to a client's assets to the responsible person and the SEC Office without delay upon discovery of such incidents;

11.4 conducting a root cause analysis of any IT incident to establish guidelines on solutions and prevention of future recurrence of such incident;

11.5 recording data related to IT incident management and storing such data for a minimum of two years from the date of such incident, in a way that such data are readily available upon request for inspection by the SEC Office; and

11.6 testing and reviewing IT incident management processes or plans at least once a year. The testing shall cover the management of cyber security drills. The results of these testing and review shall be reported to the board of directors or the committee assigned by the board of director.

Part 12: IT Contingency Plan

A business operator shall establish an IT contingency plan to address IT incidents that impede normal service or continuous business operations. The business operator shall have the capability to restore the system to its normal state within a reasonable time frame, as follows:

12.1 appointing a task force or a unit responsible for preparation of an IT contingency plan;

12.2 establishing a process for preparation of an IT contingency plan, which shall cover the following acts:

12.2.1 conducting a risk assessment to identify risk scenarios that may disrupt the IT processes and systems, thereby causing the business operator to be unable to provide normal services or operate business continuously;

12.2.2 conducting a business impact analysis on the risk scenarios under 12.2.1 to prescribe an appropriate recovery time objective (RTO), a recovery point objective (RPO), and a maximum tolerable downtime (MTD); and

12.2.3 preparing a written IT contingency plan approved by the board of directors or the committee assigned by the board of directors;

12.3 providing a backup IT system and necessary resources to enable system recovery according to the established recovery time objective;

12.4 communicating the IT contingency plan to relevant personnel to ensure they understand and are able to comply with the IT contingency plan appropriately;

12.5 reviewing and testing the IT contingency plan at least once a year and upon occurrence of any necessary ground for such review and test. The results of the testing and review shall be reported to the board of directors or the committee assigned by the board of directors;

12.6 stipulating processes for handling incidents of IT resources overusing or exceeding the capacity of the specified indicators such as limiting services through certain channels or disconnecting from a service provider or third party that affects the IT system; and

12.7 providing the following contact information to enable efficient coordination of reporting IT incidents or requesting assistance from relevant external agencies, and such information shall be regularly updated:

12.7.1 a list of regulators and third parties that provide services or are connected to the IT systems of the business operator; and

12.7.2 contact channels and a list of relevant persons of the regulators or the third parties under Clause 12.7.1.