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. Nor Por. 3/2559

Re: Guidelines for Establishment of Information Technology System

---

Whereas 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 ("*Notification No. Tor Thor. 35/2556*") and the *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* dated 12 September 2016 ("*Notification No. Sor Thor. 37/2559*") require that intermediaries establish policies, measures and operating systems for governance of technology and information security as well as supervise, monitor and examine compliance with such policies, measures, and operating systems, and review the suitability thereof regularly;

In the interest of meeting the aforesaid requirements by the intermediaries, the SEC Office, by virtue of Clause 5(3) in conjunction with the first paragraph of Clause 12 (11) and (12) and Clause 14 of the *Notification No. Tor Thor. 35/2556*, hereby issues this Notification of Guidelines, as follows:

Clause 1 The Guidelines deal with the following matters:

(1) establishment of policies, measures and operating systems relating to the governance of enterprise information technology and operating systems for information security;

(2) supervision, monitoring and examinaion of compliance with the policies, measures and the operating systems under (1);

(3) review of suitability of (1).

In the case that the intermediaries have fully complied with the Guidelines under the first paragraph, the SEC Office shall consider that the intermediaries have already complied with the *Notification No. Tor Thor. 35/2556* and the *Notification No. Sor Thor. 37/2559*. In case of adopting a different approach from the Guidelines, the intermediaries are required to prove that such approach follows the principles and requirements concerning information technology system prescribed in the *Notification No. Tor Thor. 35/2556* and the *Notification No. SorThor. 37/2559*.

Clause 2 The details of the Guidelines under the first paragraph of Clause 1 are described in the Appendix attached hereto, which contains the following matters:

(1) Chapter 1: Governance of Enterprise IT

(2) Chapter 2: IT Security with the following details:

2.1 Information Security Policy;

2.2 Organization of Information Security;

2.3 Human Resource Security;

2.4 Asset Management;

2.5 Access Control

2.6 Cryptographic Control;

2.7 Physical and Environmental Security;

2.8 Operations Security;

2.9 Communications Security;

2.10 System Acquisition, Development and Maintenance;

2.11 IT Outsourcing;

2.12 Information Security Incident Management;

2.13 Information Security Aspects of Business Continuity Management.

Notified this 12th day of September 2016.

(Mr. Rapee Sucharitakul)

Secretary-General

Office of the Securities and Exchange Commission

Appendix

Definitions

"***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;
"***critical IT assets***"	means	the IT assets that are related to or necessary for carrying out ***critical activities***;
"***critical information systems***"	means	information systems which support the operation of the ***critical activities***, for example, trading systems, back-office systems, and investment management systems, etc;
"***critical activities***"	means	the activities relating to providing services, entering into transactions or other activities of the intermediaries, in which disruption may have significant impact on their clients, undertakings, businesses, reputation, financial condition, and operating performance;
"***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;
"***teleworking***"	means	the operation which accesses the critical information system with indirect connection to the organization's internal network systems;

"***cloud computing***"	means	a type of internet-based computing that provides shared computer processing resources and data on demand according to the definition by the National Institute of Standards and Technology (NIST);
"***outsourcee***"	means	the external parties engaged by the intermediary in the operation on an ongoing basis and must exercise its discretion or make decision in the operation for the intermediary;
"***end user***"	means	the employees of the intermediary and contractors who engage in the operation and has access to the sensitive information or the organization's critical information systems, but excluding the clients;
"***information processing facility***"	means	any equipment, operating systems, or infrastructure that are necessary or facilitate to process data completely, accurately, and effectively, such as IT equipment, applications, computer network systems, procedures, or information processing areas, etc.

Chapter 1: Governance of Enterprise IT

Objective:

Information technology systems are taken on a major role as a business driving force and constitute one of the core operating systems where disruption will have an impact on the operation of intermediaries, investors, and confidence in the capital market. Senior management, therefore, has an important role in managing the implementation of information technology in the business operation and has the duty to convey the goals under the missions, strategies, policies, and operating plan at the enterprise level to the information technology-related goals under the supervision of the board of directors to ensure that the use of information technology in the business operation facilitates the intermediaries in achieving the specified goals with appropriate use of resources and efficient management of risks, in line with the good corporate governance principles.

Provisions in the *Notification No. Sor Thor. 37/2559*

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 ensure that the information technology governance meet the following criteria in order to comply with the governance of information technology of the intermediary established 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.

Additional Guidelines

1. The policy on the management of information technology risk under Clause 5(1) should be in line with the policy and management of enterprise risk and should contain the following matters at a minimum:

(1) identification of IT-related risks;

(2) assessment of risk which covers likelihood or frequency of incidents and significant or potential impacts in order to prioritizing the management of information technology risk;

(3) establishment of tools and measures for managing risk level to be in the enterprise's acceptable range (risk appetite);

(4) establishment of IT risk indicators for risks identified under (1) and arrangement of monitoring and reports of such indicators for appropriate risk management in a timely manner;

(5) assignment of roles and responsibilities of the accountable persons and the responsible persons for the management of information technology risk under Clause 5(1).

2. The policy on the allocation and management of information technology resources under Clause 5(2) should be in line with the corporate strategic plan in order to achieve the goals in accordance with the established mission, strategies, policies and operating plans and such policy should contain the following subject matters at a minimum:

(1) establishment of criteria and factors for prioritizing IT projects, for example, suitability with the corporate strategic plan, impact on business operations, or urgency for use;

(2) preparation and approval of the budget for IT projects, which are in line with the corporate budget plan and the corporate strategic plan;

(3) allocation of sufficient human resources for the information technology function, for example, arrangement or development of personnel skills, employment of external IT personnel;

(4) management of critical risks in the case of being unable to allocate sufficient resources for the operation of the information technology function, for example, resignation of key IT personnel, insufficient budget or demand for resources exceeding the specified level in the capacity plan;

(5) assignment of roles and responsibilities of the accountable persons and the responsible persons for the allocation and management of the information technology resources under Clause 5(2).

3. The information security policy under the provision of Clause 5(3) should contain the subject matters prescribed in Clause 1, Chapter 2 of the additional practice guidelines relating to the information security policies and measures at a minimum;

4. The intermediary should assign senior management as the accountable person in complying with Clause 6(2).

Provisions in the *Notification No. Sor Thor. 37/2559*

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:

(4) Reporting 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.

Additional Guidelines

5. In complying with Clause 6(4), the intermediary should undertake the following acts:

(1) establish the procedures for the preparation, monitoring and supervision of reporting to ensure that reporting is complete, accurate and timely;

(2) require that reporting must cover the following subject matters in accordance with appropriate periods:

(a) activities relating to the approach of risk management or allocation and management of IT resources, for example, a summary of the risk management or allocation of IT resources in a year, etc.;

(b) any progress of the IT project (if any);

(c) any compliance with the regulations, rules or agreement made with external parties and internal parties, for example, submission of incident reports to the SEC Office upon an occurrence of an event that affects the IT systems or monitoring of the service provider to ensure that its operation is in accordance with the terms specified in the service level agreement;

(d) effectiveness for adopting new IT system in business operation. For example, monitoring of the operating time after the technology is applied to improve operating procedures and the accordance of the adopted IT system with the business objectives;

(e) issues and obstacles.

6. The intermediary should assign senior management as the accountable person in complying with Clause 6(4).

Provisions in the *Notification No. Sor Thor. 37/2559*

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 specified under Clause 5:

(5) internal control for the operation 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.

Additional Guidelines

7. In complying with Clause 6 (5), the intermediary should ensure that the internal control system is monitored and evaluated and deviation of established internal control is rectified as follows:

(1) monitor, inspect and evaluate the effectiveness of the operating procedures of the work unit responsible for the following functions by an independent auditor:

(a) operation associated with the policy in Clause 5 (1) (2) and (3);

(b) reporting on compliance in Clause 6 (4).

(2) conduct control self-assessment to measure the effectiveness of the operating procedures;

(3) engage an independent auditor to process and report the results of the actions under (1) and (2) and any deviation detected and the results of correction to the board of directors or the audit committee and senior management in accordance with periods of assessment, periods of monitoring of correcting deviation or without delay when significant deviation is detected.

Chapter 2: IT Security

1. Additional Guidelines relating to Information Security Policy

Provisions in the *Notification No. Sor Thor. 37/2559*

Clause 5 An intermediary shall establish a documented policy on the governance of information technology, which contains 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: (3) establishment of policies and measures on information security under Clause 8 and Clause 9.

Additional Guidelines

1. The information security policy under Clause 5(3) of Chapter 1 should cover the following matters at a minimum:

1. Security of ***IT assets***;

- access control [Referring to Item 5];
- physical and environmental security [Referring to Item 7].

2. Information management and confidentiality:
   - asset classification [Referring to Item 4.2];
   - backup [Reference to Item 8.3];
   - cryptographic control [Referring to Item 6].

3. Supervision of the operating personnel:
   - ***end user*** controls, for example:
   - protection of unattended user equipment [Referring to Item 7.2];
   - mobile devices and ***teleworking*** [Referring to Item 2.2];
   - installation of software on operating systems [Referring to Item 8.5];
   - IT outsourcing [Referring to Item 11].

4. Management of the computer network systems and information transfer:
   - communications security [Referring to Item 9]
   - information transfer [Referring to Item 9.2]

5. Protection against threats to information systems:
   - protection from malware [Referring to Item 8.2].
   - technical vulnerability management [Referring to Item 8.6].

6. System acquisition, development and maintenance [Referring to Item 10]

2. Organization of Information Security

2.1 Internal Organization

Objective:

To establish measures to control the operation of information security within the organization to ensure compliance with the information security policy.

Provisions in the *Notification No. Sor Thor. 37/2559*

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.

Additional Guidelines

1. The intermediary should assign a senior executive to be the accountable person in complying with Clause10 (1) and (2);

2. In complying with Clause 10 (2), the intermediary should clearly segregate duties of operations relating to information security within the organization in order that operation cross-check is performed for prevention of potential risks, for example, segregation of personnel who operate in the developmental function ("developer") from the personnel who operate in the system administration ("system administrator") in the production environment. In the case that duties cannot be segregated due to the size of the business, the intermediary should establish a process for monitoring and inspecting closely and regularly the operation of the relevant personnel to mitigate potential risks.

2.2 Mobile Devices and Teleworking

Objective:

To establish the security measures for ***teleworking*** and using of mobile devices to access the organization's internal information systems.

Provisions in the *Notification No. Sor Thor. 37/2559*

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.

Additional Guidelines

1. In the operation with the ***use of mobile devices*** to access the organization's internal operating system, excluding the mail service system, the intermediary should establish a measure for protection of critical information under Clause 9(1) by taking the following guidelines into consideration:

(1) prior to the use of the mobile devices, register the mobile devices, for example, brand, model, operating system, serial number, and MAC address, etc., and review the registration at least once a year. Upon any replacement of mobile devices, review the registration and deregister the old devices to ensure that the ***use of mobile devices*** complies with the information security policy. The intermediary may use other registration technology instead if considered appropriate;

(2) establish a measure for protection of confidential or sensitive data in case of loss of mobile devices, for example, entering passwords prior to using a mobile device (lock screen) or remote wipe-out, etc.;

(3) determine the types of application services that allow using via mobile devices. Establish a measure for control of access to such application services by taking into consideration network connection security, for example, limiting access to certain application services if connecting to external networks, etc.;

(4) encrypt critical data stored on mobile devices and transmitted via computer network systems;

(5) communicate protection measures with the users and arrange for the users to sign for acknowledgement and awareness of usage risks and the guidelines to control such risks;

(6) ensure that only copyrighted software and appropriate software patches are installed and establish measures for protection against malware intrusion or damage to confidential or critical data stored on mobile devices;

(7) arrange for actions to mitigate impact when an information security incident occurs, for example, immediate disconnection upon being aware of an incident, etc.

In the case that the mobile devices are the property of the employees, the intermediary should consider adopting the guidelines in Items (1) - (5) at a minimum, and establish control measures that are comparable to or as a substitute for the guidelines in Items (6) - (7), for example, conduct regular inspection of mobile devices, or if an employee violates the rules, impose a penalty or remove the access right to application service.

2. In case of teleworking, the intermediary should establish prudent and sufficient security measures for the information that is accessed, processed, and stored in the operating areas under Clause 9(1) by taking into consideration:

(1) establishment of appropriate physical information security measures which are prudently sufficient to the scope of operation in the ***teleworking*** site;

(2) sufficient control of the user rights to access sensitive or critical information;

(3) communication security of organization's critical operating systems and computer network systems for connection or transmission of sensitive or critical information via remote access, for example, firewall requirements, malware protection, user access rights and data or network encryption;

(4) prevention of information leakage in case of using virtual desktop technology;

(5) prevention of unauthorized access to information by other persons using the accommodation, e.g., family and friends;

(6) inspection of the access right of the employees authorized to operate in the ***teleworking*** site;

(7) protection against malware.

Provisions in the *Notification No. Sor Thor. 37/2559*

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.

Clause 9 An intermediary shall establish the information security which addresses at least the following matters:

(2) the 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 matters:

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. the 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 other 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.

Additional Guidelines

3. In the case that the ***cloud computing*** was employed to carry out ***critical activities***, the intermediary shall ensure that at least the following matters is in place:

3.1 establish the policy on the use of ***cloud computing*** under Clause 8(1) which contains at least the following matters:

(1) assess risks relating to the use of ***cloud computing*** services;

(2) define areas or function the ***cloud computing*** shall be employed for carrying out ***critical activities***;

(3) define the eligible types of services such as Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS);

(4) establish the selection criteria and a due diligence process by taking into account the confidentiality of critical information, the integrity of data and the information systems and availability of the IT services provided to serve clients or to support ***critical activities***;

(5) require periodic reviews of the cloud provider such as the financial condition or the capacity planning, to ensure that the cloud provider is sufficiently prepared to provide services on demands;

(6) disseminate and communicate the ***cloud computing*** policy with the relevant employees and procure their signature for acknowledgement to create awareness of the IT security in the use of the cloud computing;

(7) define clear roles and responsibilities of the cloud provider such as the data backup, the helpdesk services, the procedures and processes to resolve the issues, and lists of contact persons and the communication channels, etc.;

(8) define the level of security for each type of data to be used in the cloud service by classifying information according to organization's classification scheme and establish the operating procedures for each level of classified information;

(9) define information security requirements appropriate to each type of cloud service employed for preventing threats and unauthorized access;

(10) adopt the multi-factor user authentication for the administrator log-in page to the critical information systems;

(11) inspect records and evidence to detect potential issues arisen from the use of cloud service.

3.2. establish the service agreement between the cloud provider and the intermediary under Clause 9(2)(a) as follows:

(1) specify that the intermediary is the owner of the information;

(2) determine the type of ***cloud computing*** services;

(3) determine the network security requirements such as the encryption of information transmitted through computer network system, the prevention of distributed denial of service (DDoS) attack, the intrusion from malware, the protection against threats advanced persistent threat (APT), the network segregation, the application-to-application encryption, defense-in-depth and the network hardening;

(4) define a clear set of controls including access control, monitoring and reporting of defect, efficiency and overall conditions of cloud service;

(5) define clear roles and responsibilities of the cloud provider on the data backup, defect resolution process, service level agreement, recovery time objectives (RTO) and recovery point objectives (RPO);

(6) set forth the liability if the cloud provider is unable to provide services in accordance with the service agreement;

(7) require that the relevant provision or documents relating to the service agreement contains policy on prevention of information leakage which may occurs from the cloud provider;

(8) the cloud provider should not be allowed to access and disclose the intermediary's information without consent, unless the intermediary is informed and gives a consent to do so, or such access and disclosure are made in accordance with the governing law of the cloud server hosting country or the law governing security of the origin country of the cloud provider;

(9) the cloud provider shall update operating processes to be in accordance with the current internationally-accepted information security standard without delay in case of any update to such standard;

(10) require that the cloud provider is audited by an independent auditor at least once a year;

(11) define the provision upon termination of services (exit plan) such as the provision on information retention and removal is in place to ensure that the intermediary's information cannot be recovered;

(12) a clear term for subcontract of the ***cloud computing*** service should be in place. The term should provide, at a minimum, that such subcontracting is a part of the cloud provider's service and that the cloud provider should be responsible for any damages arising from any act or operation of other cloud providers.

3.3 in the monitoring, evaluation and review of the cloud provider's services in compliance with Clause 9(2)(c), the intermediary should take additional steps as follows:|

(1) monitor the service performance and IT security of the cloud provider to verify adherence to the service agreement;

(2) assess the capacity planning of the cloud provider regularly;

(3) review the terms of service in case of any changes to ensure that the provision of service is in line with the use of service by the intermediary and is in compliance with the security policy of the intermediary;

(4) periodically review the qualifications of the cloud provider, such as the financial condition, the operating procedures and service performance, etc.

3. Human Resources Security

Objective:
To ensure that employees and contractors who engage in the operation by accessing organization's information or internal information system are aware of and fulfill their information security responsibilities.

Provisions in the *Notification No. Sor Thor. 37/2559*

Clause 13 An intermediary shall create an awareness of IT security 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 that 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.

Additional Guidelines

1. The examples of using the organization's information systems in such a way that damages the intermediary or the capital market or has an impact on the national security under Clause 13(2) are: defamation, extortion, impersonation, delivery of chain e-mail, and disclosure of the organization's sensitive information.

4. IT Asset Management

4.1. Responsibility for Assets

Objective:

To ensure that the ***critical IT assets*** are appropriately protected, the intermediary shall identify organizational ***IT assets*** and define proper protection roles and responsibilities.

Provisions in the *Notification No. Sor Thor. 37/2559*

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 and maintained. Such inventory shall be reviewed at least once a year or upon any material change.

Additional Guidelines

- None -

4.2. Asset Classification and Media Handling

Objective:

To ensure that the ***critical IT assets*** are protected at an appropriate level and to prevent unauthorized disclosure, modification, removal or destruction of sensitive information stored on media.

Provisions in the *Notification No. Sor Thor. 37/2559*

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.

Additional Guidelines

1. The intermediary should ensure an appropriate protection of the ***IT assets*** according to their classification in terms of sensitivity and criticality such as the access control, encrypting sensitive information or information required a high level of accuracy;

2. In handling media under Clause 17, the intermediary shall take additional steps as follows:

2.1 put in place, if no longer required, a removal process of information stored on media to prevent information leakage;

2.2 define media disposal procedures when no longer required;

2.3 consider risks of media degrading while stored information is still needed and methods on how to handle such risks in case of prolonged storage;

2.4 keep all media in a safe and secured environment in accordance with the manufacturer's instructions (if any);

2.5 establish security procedures for physical media transfer from the operating areas.

5. Access Control

5.1 Business Requirements of Access Control

Objective:
To limit access to information and the ***information processing facilities***.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

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

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.

Additional Guidelines

1. The intermediary should establish the documented policy under Clause 8(4) which address the following subject matters at a minimum and review the policy regularly:

(1) define access right to information and information system appropriate to users' roles and responsibilities. There shall be a periodic review of the user access rights and an immediate removal of access rights for any person whose access is no longer necessary;

(2) segregate access control roles, e.g., access request, access authorization, and access administration;

(3) at a minimum, identify the networks and network services which are allowed to be accessed and authorized persons, procedures to control and prevent access to networks and network services, the means used to access securely, user authentication requirements, and monitoring the authorized uses of network services;

(4) verify the identity of users in networks, in particular, if the dynamic IP address is used.

5.2 User Access Management

Objective:
To ensure authorized user access and to prevent unauthorized access to systems and services.

Provisions in the *Notification No. Sor Thor. 37/2559*

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 access 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.

Additional Practical Guidelines

-None-

5.3. User Responsibilities

Objective:

To prevent the unauthorized access to information systems.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

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

Additional Guidelines

1. In order to comply with Clause 20(2), the intermediary should require that users be accountable for safeguarding their user IDs, passwords, and any personal information that may be potentially used to request a change of the user IDs and passwords.

5.4. System and Application Access Control

Objective:|

To prevent unauthorized access to information systems and applications.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

(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.

Additional Guidelines

1. The examples of the control of access to information systems and applications under Clause 20(3)(b) are the protection against brute force log-on attempts and the retention and examination of log-in attempt log regularly, etc.

2. In order to comply with Clause 20(3)(c), the intermediary should consider putting in place the relevant procedures as follows:

(1) require the use of individual user IDs and passwords to maintain accountability;

(2) allow users to select and change their own passwords and include a confirmation procedure to verify input errors;

(3) require users to create strong passwords such as the password length shall be at least 6 - 8 characters and may include special characters (such as “#”);

(4) require users to change their passwords at the first log-on and enforce password

changes at least once every six months;

(5) prevent previously used passwords;

(6) not display passwords on the screen while being entered;

(7) store password files in encrypted form and keep them separately from application system data;

(8) limit the number of entering wrong passwords. In practice, there should not be more than 10 unsuccessful attempts;

(9) transmit passwords to users securely such as in sealed envelopes.

6. Cryptographic Control

Objective:
To ensure appropriate and effective use of cryptography to prevent the confidentiality and/or integrity of sensitive and critical information.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

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

Additional Guidelines

1. The policy under Clause 8(2) should address the type, strength and quality of the encryption algorithm based on a result of risk assessment and the required level of protection on sensitive and critical information. Also, such policy should identify persons responsible for implementing policy on the use of cryptographic controls and key management;

2. The policy on key management under Clause 1 should include requirements for managing cryptographic keys through their whole lifecycle. There should be an established guideline on cryptographic algorithm, key length, usage practices and secure process for key management.

The intermediary should monitor key management related activities at a regular interval to ensure compliance with the established policy and guideline.

7. Physical and Environmental Security

7.1 Secure Areas

Objective:
To prevent unauthorized physical access to the secure areas such as the data center, the backup site, and network equipment employed areas (i.e., floor switches or routers) that might cause damages to the organization's information and ***information processing facilities***.

Provisions in the *Notification No. Sor Thor. 37/2559*

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.

Additional Guidelines

1. The intermediary should design the secure areas by considering physical protection against natural and man-made disasters. Perimeters of building or site should be physically solid and should not expose any information related secured areas to the public;

2. The intermediary should grant access right to enter the secure areas for only relevant persons, establish physical entry control to ensure that only authorized personnel are allowed to access, and conduct a periodic review on the access rights granted;

3. The intermediary should establish the security systems for data center such as CCTV, fire alarm systems, fire extinguisher or automatic fire suppressing system, uninterrupted power

supply, temperature and humidity control systems as well as maintain such security systems in a good condition on a regular basis;

4. The intermediary should closely monitor and control external party support service personnel working in the secure areas;

5. The intermediary should isolate the delivery and loading areas where unauthorized persons could enter the premises from data center;

6. The intermediary should site the ***information processing facilities*** such as the server and network equipment safely in the secure areas.

7.2 Equipment Asset

Objective: To prevent loss, damage, theft, or compromising of equipment assets, and interruption to the organization's operation.

Provisions in the *Notification No. Sor Thor. 37/2559*

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.

Additional Guidelines

1. The intermediary should protect equipment assets from disruptions caused by failures in supporting utilities (e.g., electricity, telecommunications, ventilation and air conditioning);

2. The intermediary should have measures relating to cabling security for protections of power and telecommunications line in the ***information processing facilities*** and put in place a periodic maintenance to prevent damages;

3. The intermediary should correctly maintain equipment assets to ensure their continued availability and integrity;

4. The intermediary should have controls on unauthorized removal of equipment assets out of areas. Also, there should be records of equipment assets being removed off-site and procedures to ensure security of equipment assets off-premises, by taking into account the different risks of working outside the organization's areas;

5. All items of network equipment such as switch, firewall and router should be verified to ensure that any critical information relevant to configuration has been completely removed or restored to factory setting by using techniques to make the original information non-retrievable;

6. The intermediary should ensure that unattended user equipment has appropriate protection, and should adopt a clear desk policy to ensure that sensitive or critical information on papers or storage media shall be locked away when not required as well as a clear screen policy such as session time-out or automatic lock screen, to ensure that sensitive or critical information shall not be appeared on the computer screen when unattended or not in use.

8. Operations security

8.1 Operational procedures and responsibilities

Objective:
To ensure correct and secure operation relating to the information systems.

Provisions in the *Notification No. Sor Thor. 37/2559*

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;

Additional Guidelines

1. The intermediary should document operating procedures associate with the information systems for users to correctly operate in compliance with the IT security policy such as computer start-up and close-down procedures, processing of information, monitoring of systems performance, and operating schedule. The operating procedures should be reviewed and updated regularly and made available to relevant users;

2. The intermediary should establish operation controls in particular if there is any changes to the structure of operating systems, operating procedures and operating systems that affect information security. Such controls may include the followings:

- define written operating procedures in case of significant changes;
- require planning and testing of changes;
- assess potential impacts of changes;
- establish a formal approval process for proposed changes;
- establish a verification to ensure requirements of IT security policy have been met;
- communicate change details to all relevant persons to ensure correct operations;
- establish fall-back procedures from unsuccessful changes.

3. The intermediary should monitor the functions of information systems and equipment assets to ensure continuity and efficiency. In addition, the evaluation should be made to project the future capacity requirements based on current use of resources for ensuring the required system performance;

4. The intermediary should separate development and production environments and allow to access by only authorized personnel for each environment. Such separation may be in the form of using different computers or separating areas in the same computer.

8.2 Protection against Malware

Objective:
To ensure that information systems are protected against malware.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

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

Additional Guidelines

1. The intermediary shall establish measures under Clause 23(2), at a minimum, as follows:

(1) a policy prohibiting the use of unauthorized software;

(2) preventive and detective controls of the use of unauthorized software and known or suspected malicious websites;

(3) installation and regular update of malware detection software, as well as defining responsible personnel to report and deal with malware threats;

(4) regular reviews of the software and data content of systems supporting ***critical activities***. The presence of any unapproved software or changes should be investigated;

(5) procedures to monitor and verify threat intelligence to make all relevant users become aware of threats.

8.3 Backup

Objective:

To protect against loss of data.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

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

Additional Guidelines

1. The intermediary should establish a backup policy for critical business information, computer operating systems, application software and program source code to ensure continuity of operations. The followings, at the minimum, shall be taken into account:

(1) define backup procedures which shall contain the followings at a minimum:

(a) data to be backed up;

(b) frequency of backups;

(c) type of media storage;

(d) copies of data to be backed up;

(e) comprehensive backup procedures;

(f) location and storage of backup media;

(g) recovery procedures in case of data loss.

(2) store backup media and copies of backup procedures in a remote location to escape any damage from a disaster at the main site, which should be given an appropriate level of protection as described in the section of Physical and Environmental Security;

(3) define a recovery point objective (RPO) such as the type of data required and the point in time in the past of data that should be recovered from backup media;

(4) in the case that a prolonged period of backup retention is required, consideration shall be taken for the method of data restoration in the future, for example, if the data is kept in a particular form of media, equipment and software relevant to restore such data should also be stored.

8.4 Logging and Monitoring

Objective:

To completely record events and sufficiently generate evidence on the use of information systems for inspection of a conflict 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. It should also be required to monitor and analyze such recorded evidence.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

(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***.

Logging descriptions

Category of logs	Minimum Logging Details	Minimum Period of Retention
Physical Access Logs	Name of access persons, Dates, Times and Access Attempts (if any)	At least 3 months
Authentication Logs for Database and Network Access	User IDs, Dates, Times and Access Attempts	At least 3 months

Category of logs	Minimum Logging Details	Minimum Period of Retention
Application Logs	User IDs, IP Addresses, Dates and Times. In case of the securities trading system, the details shall include: Securities Symbol, Broker Numbers (4-digit), SET Order IDs, Account IDs, Dates & Times of transactions (yyyy/mm/dd - hh:mm:ss:sss), Source Public and Local IP Addresses, Destination IP Addresses, Full URL, Terminal Type (if any, such as iPad, iPhone). The intermediary must be able to identify user identities and Local IP addresses at the time of use (not applicable to the use via employees' personal devices).	At least 1 year for the intermediary undertaking securities business in the brokerage, dealing or underwriting of any securities, which is not limited to debt securities or investment unit, and derivatives agent. At least 6 months for the intermediary undertaking securities business in the area not covered above.
Internet Access Logs	User IDs, IP addresses, Organization IP addresses, Date, Times and Full URL of destination website. The intermediary must be able to identify user identities and IP addresses at the time of use.	
Audit Logs[1]	User IDs, Dates, Times and records of reading & editing on data.	At least 6 months.
Event Logs of Operating Systems and Network Firewall	Dates, Times, Event Services for OS such as service status and Event Services for Network Firewall such as rules modification of network firewall.	As necessary and sufficient for inspection, based on risk assessment of the organization.
Network Firewall Logs	Dates, Times, Source and Destination IP addresses, Firewall Actions and Port Connections.	
Database Logs	User IDs, Dates and Times.	
Electronic Messaging Logs[2]	User IDs, Dates, Times and Messages (including attached files) throughout entire conversations.	At least 6 months.

[1] Applicable only to access persons of the intermediary undertaking any type of securities business.
[2] Applicable only to access persons of the intermediary undertaking securities business in the brokerage, dealing or underwriting of any securities, which is not limited to debt securities or investment unit, derivatives agent, and management of mutual fund or private fund.

Note: The definition of "access person" (person allowed to access the organization's insider information) shall be in accordance with the *Notification of Guidelines on Policies, Measures and Processes* relating to any action which may cause a conflict of interest with clients.

Additional Guidelines

1. The intermediary should have log information and logging facilities (including system administrator logs and system operator logs) protected against tampering, damage or unauthorized access and reviewed at least once a year or upon a material change;

2. The intermediary who is a member of the Stock Exchange of Thailand ("SET") should synchronize the clocks of all equipment and information systems relevant to securities trading and clearing to a reference time source of SET's trading system to ensure correct and effective inspection of inappropriate transactions;

3. In the case that the intermediary shares the use of ***critical information systems*** with its overseas affiliated company, the intermediary may require such affiliated company to monitor and analyze logs, and keep results of log analysis.

8.5 Installation of Software on Operational Systems

Objective:
To ensure the integrity of operational systems.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

Additional Guidelines

- None -

8.6 Technical Vulnerability Management

Objective:

To prevent exploitation of technical vulnerabilities.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

(6) establish an effective management process for technical vulnerabilities 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;

Additional Guidelines

1. The intermediary should keep monitoring intelligence relating to technical vulnerabilities that may pose risks to information systems and should carry out vulnerability assessments, patching of vulnerable findings, and planning of incident response in case that identified vulnerabilities are exploited. Such procedures should address the followings:

(1) define and establish roles and responsibilities associated with technical vulnerability management, including vulnerability risk assessment on relevant ***IT assets*** (in particular ***IT assets*** at high risk), patching, and any coordination responsibilities required;

(2) install patches to vulnerable systems without delay after such patches are tested and evaluated to ensure they are effective and do not result in any side effects. In the case that patches are unavailable, the intermediary should follow vendor's instructions;

(3) establish effective technical vulnerability management process aligned with incident management activities to ensure preparedness of incident response function when an incident occur. This should include situations where a vulnerability is identified but there is no proper countermeasure;

(4) keep a log for all procedures undertaken relevant to technical vulnerability management. In the case that automatic patching is used for any equipment or systems after ensuring that such patching will not cause any damages, the intermediary may consider to not keep a log for procedures undertaken to such equipment or systems.

8.7 Information Systems Audit

Objective:
To ensure an adequate and appropriate planning of information systems audit whereby such audit activities should cause the least effect to the operational systems.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

(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.

Additional Guidelines

-None -

9. Communications Security

9.1 Network Security Management

Objective:
To ensure the protection of information in networks and its supporting ***information processing facilities***.

Provions in the *Notification No. Sor Thor. 37/2559*

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 actions 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.

Additional Guidelines

1. The minimum actions that should be taken for network security management under Clause 22(1) are as follows:

(1) separate operational responsibilities between network administrator and computer administrator. Responsibilities and procedures for the management of computer network system and network equipment should be clearly defined;

(2) restrict systems connection to the network such as a connection restriction on port outlet;

(3) allow connection of service port as necessary, and there should be a mechanism to

authenticate connected devices such as the IP address and type of devices connected;

(4) establish controls to safeguard the confidentiality and integrity of data passing over public networks and wireless networks, as well as to protect connected systems and applications. Such controls may include network encryption or network segregation. Moreover, there should be a special control to maintain the availability of network services such as an arrangement of network load balance;

(5) apply logging and monitoring of activities associated with ***critical information systems*** in networks to enable recording and detection of actions that may affect, or are relevant to, network security. In case of internet access activities, internet access log should contain minimum details as described in the Item 8.4: Logging and Monitoring.

9.2 Information Transfer

Objective:
To maintain the security of information transferred within an organization and with any external entity.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

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

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

(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.

Additional Guidelines

1. The following actions should be taken by the intermediary in light of Clause 8(3) and Clause 22(4):

(1) put in place formal policies and procedures for protection of information transferred through the use of all types of communication facilities. Such policies and procedures shall address at least the followings:

(a) acceptable procedures for the transfer of information through various electronic channels;

(b) procedures designed to protect transferred information from mis-routing, interception, modification, destruction and transmission of malware;

(c) procedures for protecting transferred sensitive or critical information in the form of attachment and automatically forwarded email to an external entity;

(d) use of cryptographic techniques to protect sensitive or critical information transferred through certain communication channels that require a high-level of security such as cloud computing;

(2) The intermediary should put in place protection for information involved in electronic messaging. There shall be measures that prevent any tampering, damage or unauthorized access of information, require a stronger level of authentication controlling access from publicly accessible networks and maintain reliability and availability of the service. In addition, the use of electronic messaging provided by external public services such as instant messaging, social networking or file sharing should be properly controlled such as obtaining an approval prior to the use, and should be used in compliance with relevant law and regulations.

2. The confidentiality or non-disclosure agreements under Clause 22(5) should address the followings at a minimum:

(1) ownership of information, intellectual property and how to protect such information;

(2) responsibilities and actions of signatories to avoid unauthorized information disclosure;

(3) procedures for request of information access and rights of the signatory to use information;

(4) the right to audit and monitor activities that involve sensitive or critical information;

(5) process for notification and reporting to relevant persons of unauthorized disclosure or information leakage;

(6) expected actions to be taken in case of breach or termination of agreements, including terms for information to be returned or destroyed at agreement cessation.

10. Systems Acquisition, Development and Maintenance

10.1 Security Requirements of Information systems

Objective:

To ensure that information security is an integral part of the organization's information systems, including services provided over public networks, across the entire lifecycle (i.e., acquisition, development, operation, and maintenance).

Provisions in the *Notification No. Sor Thor. 37/2559*

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.

Additional Guidelines

-None-

10.2 Security in Development and Support Process

Objective:
To ensure complete and correct information processing after system development or modification and in accordance with the user requirements, as well as to ensure that information security is designed and implemented within the development lifecycle of information systems.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

(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.

Additional Guidelines

1. The controls of development or changes to existing information systems under Clause 24(3) should address at least the followings:

(1) conduct a risk assessment of the impacts of changes;

(2) establish procedures to ensure that system changes or development are submitted and approved by authorized personnel. There should be controls of impacts after changes, acceptance of changes or development by authorized personnel prior to implementations, and maintenance of documents of all change requests;

(3) establish procedures for emergency change request and document a reason for such change. Emergency change request should always be approved from authorized personnel;

(4) update the system documentation set on the completion of each change such as details of data structure, operating documentation, list of authorized personnel and user procedures. The system documentation set should be kept in a safe and accessible area;

(5) maintain version controls for all software updates or fall-back procedures in case of system malfunction or failure;

(6) communicate information associated with system changes to relevant persons for their acknowledgement to ensure correct operation;

(7) maintain an audit trail of all change requests;

2. In order to comply with Clause 24(5), the intermediary should carry out testing of information systems developed or changed to ensure correct functionality and accordance with user requirements. In addition, the business continuity plans should be updated in concurrence with such changes.

3. The followings should be taken into account for the purpose of compliance with Clause 24(6):

(1) security controls for sensitive data to be processed, stored and transmitted by the system. Moreover, movement of data from and to the development environment should be controlled;

(2) controls of access to the development environment;

(3) monitoring of change to the development environment;

(4) backups are stored at secured offsite locations.

4. For testing of developed information system by a user or independent tester under Clause 24(8) to ensure correct functionality and accordance with user requirements and IT security policy, the intermediary should establish controls to prevent leakage of the tested data.

11. IT Outsourcing

11.1 Information security in IT outsourcing

Objective:

To ensure protection of the organization's ***IT assets*** accessible by an ***outsourcee***.

Provisions in the *Notification No. Sor Thor. 37/2559*

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

(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***;

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;

(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 possess any characteristics for which 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 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***.

Additional Guidelines

1. The policy for outsourcing the IT services of the intermediary under Clause 8(5) should address at least the following matters:

(1) the selection and evaluation of ***outsourcee*** (due diligence), with an emphasis given to the confidentiality of sensitive information, the integrity of information and information systems and the availability of information systems. For example, the ***outsourcee*** should prepare the incident response plan in case of any incident that may affect IT security of information systems by taking into account the intermediary's business continuity plan, and the recovery procedures to resume normal operation as prescribed in the agreed terms to ensure the availability of information and information processing at all times;

(2) a periodic review of the ***outsourcee*** such as its financial condition and adequacy of service capacity to ensure ongoing services of the ***outsourcee***;

(3) a written agreement on information security requirements and associated controls signed by both parties. The intermediary should ensure that the ***outsourcee*** is obligated to maintain information security for the outsourced operation of the intermediary;

(4) roles and responsibilities of the ***outsourcee***;

(5) type of information access that the ***outsourcee*** will be allowed in order for the intermediary to prepare appropriate controls and monitoring of information access based on a need-to-know basis;

(6) processes and procedures for monitoring of information accessed by the ***outsourcee***;

(7) information security upon transition of information;

(8) accuracy and completeness controls to ensure integrity of the information or information processing provided by the ***outsourcee***;

(9) a standardized process for monitoring of the ***outsourcee***'s operation.

2. The information security agreement under Clause 25(1) shall, at a minimum, address the following issues:

(1) description of information to be provided or accessed by the ***outsourcee***, and method of accessing such information;

(2) classification of information according to the organization's IT security policy;

(3) measures to ensure that sensitive or critical information, intellectual property rights and copyright are protected as required by law and regulation;

(4) obligation of the ***outsourcee*** to operate under an agreed set of controls including access control, monitoring the ***outsourcee***'s operation to be in compliance with the agreed provisions, reporting upon the intermediary's requests, defined resolution processes, and actions to be taken in compliance with the IT security policy of the intermediary;

(5) rules for acceptable use of information;

(6) resolution processes in case of operational errors from the ***outsourcee***'s action;

(7) explicit list of contact persons or relevant partners, particularly persons or partners for information security issues;

(8) additional information security requirements for sub-contracting.

11.2 Supplier Service Delivery Management

Objective:
To ensure service delivery of the ***outsourcee*** in compliance with IT outsourcing agreements.

Provisions in the *Notification No. Sor Thor. 37/2559*

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: (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***.

Additional Guidelines

1. In order to comply with Clause 25(2), the intermediary should consider, in conjunction with one another, the ***outsourcee***'s financial condition, operating procedures and service performance levels.

12. Information Security Incident Management

Objective:
To ensure a consistent and effective approach to the management of information security incidents.

Provisions in the *Notification No. Sor Thor. 37/2559*

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.

Additional Guidelines

1. To establish procedures and processes and define the competent person responsible for managing information security incidents under Clause 11(1) and (2), the intermediary should, at a minimum, determine the procedures and processes as follows:

(1) planning and preparation of incident response;

(2) assessment of information security events or weaknesses and decision on information security events whether they are to be classified as information security incident;

(3) assignment of the responsible person or unit to be a point of contact for security incidents' detection and reporting to the management or the relevant person for their acknowledgement and further action to be taken (escalation of incident);

(4) procedures for an efficient response to resolve security incidents or resume normal operations;

(5) collection of evidence upon occurrence of significant information security incidents without delay such as damage to the client's information or assets, taking into account the key issues such as safety of evidence, rules and responsibilities of personnel involved, selection of competent person on collection and documentation of evidence for analysis and presentation of executive summary to the responsible person. Collection and presentation of evidence should be in accordance with the applicable law;

(6) logging of incident management activities as necessary;

(7) reporting of the information security incidents to the SEC Office and the results of incident handling;

(8) detecting, monitoring, analyzing and reporting of information security incidents. This shall include a post-incident analysis to identify the cause of such incident and the result of analysis should be used in preparation for future incidents.

2. In the reporting of information security incidents to the person or unit assigned to be a point of contact under Clause 11(3), the intermediary should take the following actions:

(1) prepare information security event reporting forms to support the reporting action and to help the reporting person to understand all necessary actions to be taken upon occurrence of an information security event. The content of the report should, at a minimum, contain date and time, description of event, potential impact, action taken, result of action taken, length of time to resolve, cause of event and preventive measures;

(2) report to the management upon becoming aware of information security incidents, such as the discovery of ineffective security control, an occurrence of incident which may affect the confidentiality, integrity and availability of information systems, human error, breaches of physical security arrangements, non-compliance with policies or guidelines, uncontrolled system changes, malfunctions of software or hardware, and access violations;

(3) report to the SEC Office upon occurrence of information security incidents, as follows:

(a) system disruption;

(b) intrusion, unauthorized access or unauthorized use of system;

(c) an incident which poses harm to the intermediary's reputation such as website defacement. The reporting shall be done in any of the following manners:

- report without delay upon becoming aware of any information security incident. The content should contain date and time, type of incident, description of incident and potential impact. The reporting may be done verbally or through the electronic messaging system, as deemed appropriate;
- report in writing on the next business day after the occurrence of an information security incident. The content should cover date and time, type of incident, description of the incident and realized impact, actions taken and progress on resolving the incident;
- report in writing upon the end or the resolving of the incident. The content should contain date and time, type of incident, description of the incident and realized impact, actions taken, results of action, length of time to resolve, cause of incident and preventive measures.

(4) if the incident affects the relevant person such as a client, the intermediary should inform such person without delay;

(5) there should be a periodic report on the progress of incident management, and

another report upon the incident having been resolved.

3. In the compliance with Clause 11(4), (5) and (7), the intermediary should take the following actions:

(1) prepare a risk scenario for testing the readiness of management of information security incidents. Such risk scenario should:

(a) relate to the nature, extent and complexity of business of the intermediary;

(b) pose a significant risk to information systems upon occurrence;

(c) contribute a measurable result and be able to make use of such result to review procedures and processes for managing information security incidents;

(d) be reasonable and able to put into action without conflict;

(e) be probable and appropriate to the current situation.

(2) keep and update all documents relating to the test, as follows:

(a) risk scenario conducted in the test;

(b) summary of the test result, the result of evaluation, and the result on the review of the incident response plan.

13. Information Security Aspects of Business Continuity Management

Objective:
To ensure that information security continuity is embedded in the intermediary's business continuity management.

Provisions in the *Notification No. Sor Thor. 37/2559*

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).

Additional Guidelines

1. Establishment of procedures, processes and controls of information security under Clause 12(2) should contain at least the following actions:

(1) prepare the incident response process in accordance with the policy on management of information security incidents;

(2) establish a clear and comprehensive response procedure to each incident and nominate incident response personnel;

(3) prepare details of necessary equipment used during adverse situation for each information system such as the PC model, minimum specification, configuration and network equipment;

(4) define a clear description of the alternative data center (if applicable) such as locations, maps, etc.