(Translation)

Readers should be aware that only the original Thai text has legal force and that this English translation is strictly for reference. The SEC, Thailand cannot undertake any responsibility for its accuracy, nor be held liable for any loss or damages arising from or related to its use.

Notification of the Office of Securities and Exchange Commission
No. OrThor/Nor. 5/2547
Re: Operational Control and Security of the Information Technology of Securities Company

---

For the purpose of rendering the securities companies to efficiently comply with the Notification of the Office of Securities and Exchange Commission No. SorThor/Nor. 34/2547 Operational Control and Security of the Information Technology of Securities Company with the same level of standard. The Office has issued a Guideline for Operational Control and Security of the Information Technology of a Securities Company whereas this Guideline compose of mandatory[M] and accredit [A] and if the company had already complied with the mandatory[M] completely, it shall be deem that the company had complied with this Notification. Providing that if the company had already complied with the accredit [A], it shall render the company is capable of efficiently preventing risk in information technology and it attain an assessment the risk in information technology in the better level. In Nevertheless, the securities company may complies with other guideline, if the securities company demonstrate to the Office that such other guideline is capable of efficiently preventing risk in information technology of the securities company with an acceptable standard for Operational Control and Security of the information technology of a securities company. The essential of this guideline is compose of:

1. Policy of Security of the Information Technology of a Securities Company.
2. Segregation of Duties.
3. Physical Security.
4. Information and Network Security.
5. Change Management.
6. Backup and IT Contingency Plan.
7. Computer Operation.
8. IT Outsourcing.

Policy of Security of the Information Technology.

Objective

Providing a policy of security of the information technology has an objective for the user and the concerned person realise the essential of security of the information technology thoroughly had known the duties and responsibilities and guideline on controlling the various risk which have a content covering the policy making, detail of policy and compliment of policy.

Compliance Guideline

1. Policy Preparing

- Preparing a written policy of security of information technology and the executives, computer staff and user of various division have to participate in preparing a policy with approval by the Board of company at least. In case where the securities company is the affiliated company of other financial institution, the securities company may comply with the policy of security of the information technology of such financial institution. **[M]**
- Reviewing and modify updatable by having a risk assessment once a year at least the policy and indicated the concerned risks, arrangement the importance of information and computer system, specify the acceptable level of risk and specify measure or practice for risk controlling **[M]**
- Keeping a written policy of security in the place where the user and the concerned person can simply reach **[M]**

2. Detail of Policy

- Identifying clearly the purpose and scope and having a content cover the following matter **[M]**
  - Security of the Information Technology of a Securities Company.
  - Segregation of Duties.
  - Physical Security.
  - Information and Network Security.
  - Change Management.
  - Backup and IT Contingency Plan.
  - Computer Operation.
  - IT Outsourcing.

3. Compliance of policy.

- Announcing and communicating to concerned person thoroughly for the purpose of compliance such as training etc. **[M]**
- Providing an oversee system the operation of officer under the policy strictly **[M]**

- providing an inspection and assessment of the sufficiency of policy and internal control information technology system by independent unit once a year at least by an internal unit of the securities company or by an outsider inspector **[M]**
- notifying to the Office without delay in case appeared that have significant case effect to the security of the information technology [1] **[M]**
- proving a method or compliance guideline support to compliance with the prescribed policy **[M]**
- determining clearly duties and responsibilities for users and concerned person such as duties of user in case where appeared that the computer affect virus , duties and responsibilities for staff of network system securities duties and responsibilities for interim employment etc.**[M]**

[1] significant case effect to the security of the information technology mean an effect causing the securities company operate business inconsistent namely trading securities system was damaged and unable to operate in the normal condition etc. or an effect causing harm to the customer's information or customer's asset such as customer's information or information of investment units incorrect because of computer system assessment or modification by the unauthorised person"etc.

Segregation of Duties.

Objective

Segregation of Duties have an objective for a cross-check system among the personnel in computer division which reduce the infrastructure risk.

Compliance Guideline

- Segregating l the developer from the system administrator that perform in the production environment.

- Providing a written job description which identified clearly duties and responsibilities of each type of work and responsibilities of the personnel in the computer division.

- Providing a reserve personnel for the importance work for performing instead in of necessary case such as system administrator computer operator etc..

Physical Security.

Objective

. Physical Security have an objective for preventing unauthorised person access risk, integrity risk or make available risk. In case of damage prevention, it has an objective for preventing information and computer system from available risk according to a content cover the guideline for entering the computer centre and damage prevention system which the securities company should provide for the computer centre.

Compliance Guideline

1. Computer Centre Controlling

- Storing the importance computer devices such as server device network device etc. in the computer centre or prohibited zone and identifying right for computer centre.**[M]**
- In case of unauthorised person may have a necessary to in the computer centre sometime, it shall control strictly namely determine the computer centre officer monitor the compliance all the time. **[M]**
- Providing record system for entering the computer centre and such record shall compose of personal detail, time of entering and there should be inspected that record consistently. **[M]**
- Arranging the computer centre separately such as network zone, server zone and printer zone etc. for the purpose of compliance convenience and render efficiently controlling for accessing the importance computer devices. Moreover, it should be separate the zone that officer from various division can reach from the computer centre such as a zone where used for keeping the report that the computer division publish for other agency and a zone where stored the tape recorder of the comment's marketing officer **[A]**

2. Damage Prevention

2.1 Fire Prevention system

- Providing an alarm device such as smoke detector, heat detector etc. in order to prevent or suppress fire immediately. **[M]**
- The computer centre shall have automatic fire suppression system. For the preserved computer centre, it shall have an fire extinguisher tank at least for preliminary fire suppression. **[M]**

2.2 Electricity Prevention system

- Providing a prevention a computer system form damage of inconsistent electricity. **[M]**

- Providing a preserved electricity system for the important computer system for the purpose of contingency operation**.[M]**

2.3 Temperature and humidity controlling system

- Controlling the environment condition which have temperature and humidity appropriately according to settle the temperature of the air conditioner and humidity level suitable for specification of the computer system, whereas the computer system may fail to function under unsuitable temperature and humidity condition. **[M]**

2.4 Water leak-detecting system.

- In a case where level of floor or computer centre has lifted for the purpose of instalment the air conditioner system, including instalment electric system and network system below, it shall install water leak sensor in the place where has installed a water pipe in order to suppress leak water instantly. Moreover, in case of the computer centre located in the place having risk for water leak, there should notice consistently that have a water leak or not. **[M]**

Information and Network Security.

Objective

. Information and network security have an objective for controlling unauthorised person for access risk, integrity risk of information or the compliance of computer. For the preventing of trespass via the system have an objective for preventing person, virus other malicious code unable to access risk or availability risk of information or the computer compliance which have a content covering the securities of information, computer system, server device and network zone.

Compliance Guideline

1. Information management

- Determining the level of secret, compliance guideline for keeping the category of the level of secret and compliance guideline for controlling access the information in each category of the level of secret, both direct access and indirect access, including the destroy method for information in each category of the level of secret. **[M]**

- Transmission of importance information via the public network, it shall receive an international standard encryption such as SSL,VPN etc. **[M]**
- Providing a measure on controlling the correct of information that storage, input, operate and output. In case of distributed database or storage the concerned database, it shall control the database correctly and completely. **[M]**
- Providing a measure on securities of information in case of take the computer out of the company such as deliver to repair or destroy the information which stored in media recorder the etc.. **[A]**

2. Controlling the users privilege[2]

- Determining the privilege for use the information and computer system such as application system, internet accessing privilege etc. to the user as a manner of duties and responsibilities. It shall determining the privilege only in the case of compliance with the written approval by the authorised person, including consistently reviewing such privilege. [**M]**
- For the necessary case that employ the privilege user,[3] there shall be control strictly that employment. **[M]**

  For the consideration that if controlling the privilege user adequate strictly, the Office shall take the following factor for consideration in generally:
  - Given approval by the authorised person;

[2] User means information owner, system administrator, computer operator, system developer and other officer using the computer system.
[3] privilege user means Root or other user having the most highest right.

- Controlling the privilege user strictly, such as controlling the compliance such user in a manner of dual control which imposing two officer possess half of password or keeping the password in the safe etc. and restriction for the necessary case only
- Specifying the compliance period and instantly when that period had lapse.
- Change the password strictly in case of the compliance finished or in the necessary case for compliance in the long period, it should change password in every three months etc.

- In case of non compliance in front of computer's screen, it shall have a measure on preventing unauthorised person from such as determining the user log out in the time that not perform in front of computer's screen.**[M]**
- In the necessary case that the user who is the information owner give other user the right to reach or modify his information such as share file etc., it shall give the right for specific person or specific group only and cancel such right when there is no more necessity, and the information owner shall have the evidence of giving such right and specified the compliance period and cancel such right when that period had lapse.**[M]**

3. Controlling the compliance of user account and password.

- Providing the identification and authentication measure prior to access to the computer system strictly such as impose hardly password for presumption etc. and determining that each user has his own user account. **[M]**

  Providing that the consideration that determine hardly password for presumption and control using of password strictly or not, the Office shall take the following factors for consideration in generally:
  - determining the password that having properly length, For a international standard requires for six characters of minimum lengtht.
  - using a special letter such as : ; < > etc..
  - the general user should change the password every six months at least. For the privilege user such as system administrator and default user etc. should change the password in every three months at least.
  - For each time of changing password, it should not determine new password similar to the latest password.
  - do not determine the password in the typical form such as "abcdef" "aaaaaa" "123456" etc..
  - determining the password related to name , surname, date moth or year of birth, address etc..
  - determining the password in a manner of the word in the dictionary.
  - determining the times that accept the user for entering incorrect password. For the general practice, it is not exceed three times.

- providing a method for deliver the password to the user strictly and safety such as put in a sealed envelop.
- The user who receiving the default password or receiving a new password should change the password instantly.
- The user should keep the password secret. In case of accessing the password by other person, the user should change the password instantly.

- Having an encryption the file that keeping the password for the purpose accessing or modifying. **[M]**
- Inspecting consistently a name list of user for the importance operational system[4] and inspecting a name list account of unauthorized user such as the name list account of resigned officer, default user etc. and cease the operation instantly when encounter it such as disable, delete out from the system or change the password etc.. **[M]**

4. Security of the computer server.

- Having method or compliance guideline for inspect the security of the computer server. In a case appeared that having operate or alter abnormally the parameter, it shall be improve and report instantly. **[M]**
- Providing a service[5] as necessary. In case of necessary service cause a risk to the security system, it shall provide additional preventing measure. **[M]**
- Installing a necessary path of the importance operational system in order to fill consistently a loophole of program of system software such as DBMS operational system and web server etc..**[M]**
- Testing the system software related to the security and operation effectiveness prior to installment and after altering or maintenance.**[M]**
- Providing compliance guideline for operate the software such as personal firewall, password cracker etc. and consistently inspect the operation of software utility. **[M]**
- Determining clearly the person to responsible for specifying, altering or changing the other value of parameter of the program system. **[M]**

5. Management and inspection of network

- Segregating the network separately for operation such as internal network, external network, DMZ etc.. **[M]**
- Providing the trespass preventing system such as firewall etc. between the internal network and external network **[M]**
- Providing the trespass monitoring system and abnormally operating system via the network system whereas it shall monitor consistently the following matter at least **[M]**
  - Attempt to trespass via the network **;**
  - abnormal operation**;**
  - compliance and alteration a network by unauthorized person.

[4] the importance operational system means securities trading system, securities operational system, securities trading system via internet and network system.
[5] Service means various services of the server device such as telnet, ftp, ping etc..

- Preparing a network diagram which having a detail related to scope of internal network and external network and other devices and modify up to date. **[M]**
- Inspect the securities of devices prior to connect to network system such as virus scanning, value specifying inspection related to security etc.. and cancel absolutely connection of physical disconnect and disable port that unnecessary to connect to network system out of the network system. **[M]**
- In case of accession to the network system as remote access or connect to external network by using modem (dial out), it shall given an approval by the authorized person and controlling strictly such as using a call back system, open-close modem controlling, authentication, operational detail record and in case of dial out, it shall cancel the computer connecting from the internal network system etc., including cancellation of connectionon when out of work. **[M]**
- Determining clearly the person to responsible for specifying, altering or changing the other value of parameter of network system. And devices connecting to the network and reviewing for determine of value of parameter once a year at least. Moreover, for the determination, modification or alteration a value of parameter, it shall notify to concerned person each time. **[M]**
- For the using other tools to inspect the network system, it shall given an approval by the authorized person and limit the operation for the necessary case only. **[M]**

6. Configuration management

- Prior to configure the system and computer device, it should assess related affect and record such alteration up to date, including communicate to the concerned person for acknowledgement. **[M]**
- It should install software as necessary for operation and legal copyright. **[M]**

7. Capacity planning.

- Providing an assessment the importance computer system in advance for compliance support in the future. **[M]**

8. Virus prevention and malicious code.

- Providing a virus prevention measure efficiently and up to date for the server computer and user's computer connecting to the network system such as install a virus preventing software etc. **[M]**
- The computer division should prepare the manual for virus prevention in order to be a compliance guideline, including consistently notify and educate the user for a new virus. **[M]**
- Controlling the user disable a virus preventing system installed and notify concern person instantly in case appeared that found virus. **[M]**

9. Audit log.

- Providing a record of functional of server and network computer system, application log record, information of trespass prevention system such as login-logout logs, login attempts, command line and firewall log etc. for the purpose of inspection and it shall keep such record for three months at least. **[M]**
- Providing consistently an inspection of operational recording of user**.** **[A]**
- Providing a preventing measure for alteration of other record and limitation of right for only concerned person to access to the record. **[M]**

Change Management.

Objective

. Change Management have an objective for rendering the developed or altered computer system having the correct and complete integrity which satisfies the need of the user, and reducing the integrity risk by the content covering the development procedure or alteration from the beginning such as request including take the developed operation system or altered for operate in the true condition.

Compliance Guideline

1. operational procedure determining

- Providing a written procedure or compliance guideline for operational system development or alteration which having the regulation related to requested procedure, development or alter procedure, examining procedure and transfer operational system procedure. **[A]**
- Providing a procedure or compliance guideline for emergency change and having record the reason of necessity and given an approval by the authorised person each time. **[A]**
- It shall communicate the detail of such procedure to concerned person for acknowledge and control to comply**. [A]**

2. Controlling the development or alteration the operational system

2.1 Request.

- A request for development or alteration the operational computer system shall prepare in writing (electronic transaction like e-mail) with an approval by the authorised person such as chief of Section requested, chief of computer division requested etc.. **[M]**
- Providing an assessment of importance effect in witting for the operation security and functionality. **[A]**
- Reviewing related governmental regulation because the various alteration may effect to compliance with the governmental regulation. **[A]**

2.2 Development environment functionality

- Segregating the computer for development environment from production environment and controlling the access for concerned person for each Section only. Providing that such segregation may done by arrange computer one by one or arrange the zone within the same computer. **[M]**
- Requestor and concerned user should have participation in development procedure or alteration in order to develop the operational system satisfy the desire. **[A]**
- Concern to security and availability of operational system at the beginning of development or alteration. **[A]**

2.3 Examination

- Requestor and computer division include other concerned user shall participate in examination in order to ensure that operational computer system, which developed or altered, having an effectiveness and correct integrity and satisfies the need prior to transfer for operating in real condition. **[M]**
- In the importance operation, there shall be an agency or independent team for examining that have compliance under system development and examine prior to transfer for operating in real condition. **[A]**

2.4 Transfer for operating in real condition

- Inspect the transfer of operation system correct and completely. **[M]**

2.5 Document and detail preparation for operational development system and keeping a version of developed operational development system.

- Providing a storage of information ,related to program using currently**,** which having a detail of development or alteration in the past.**[M]**
- Revising up to date the document of operational system after the development or alteration such as information structure document, operational manual, name list account of user, functional program and program specification etc. and keep such document in the safe place and simply use. **[M]**
- Keeping a program of prior to developed version for use in case of present version is out of work. **[M]**

2.6 Post-implementation test

- Determining a test of developed or altered operational system after operate for a period in order to assure that a functionality having an efficiency, the assessment system is correct and complete and satisfies the need of user. **[A]**

2.7 Communication of alteration

- Providing communication of alteration to concerned user in order to be able operate correctly. **[M]**

Backup and IT Contingency Plan.

Objective

Backup and IT Contingency Plan have an objective for prepare information and computer system for operate consistently, efficiently and availability risk which having content cover the guideline for information and computer system backup, including examination and storage and IT Contingency Plan.

Compliance Guideline

1. information and computer system backup

1.1 Backup

- Backup the importance business information include operating system, application system and mandate system completely on order to be able to operate consistently**. [M]**
- Providing a procedure or guideline of information backup as an operator's compliance guideline which having the following detail at least. **[A]**
  - Backup Information and frequency of preservation
  - Media
  - copy
  - Procedure and method in detailed
  - Place and method of media storage

- Providing a log book of information preservation that the officer using for examining the correct and completion and providing an inspection of such log book consistently. **[A]**

1.2 Examination

- Providing a test once a year for assure that information and preserved program system correctly, completely and functionally. **[M]**
- Providing a procedure or practice for examining and taking information from media to operate. **[A]**

1.3 Storage

- Providing a storage of preserved information media and duplicate the procedure or compliance guideline in other place for security in case of he operational place damaged and providing the entrance controlling and damage prevention for such place as prescribed in topic of Physical Security. **[M]**
- In necessary case for keeping information in a long period, it should concern the method for bring the information to operate in the future such as keeping information in what type, it shall keep device and software related to read that type of media. **[M]**
- Labelling clearly at the preserved information media for rapidly search and preventing of malfunction. **[A]**
- Asking permission for use preserved information media, it shall be done by given approval by the authorised person and preparing a register of receiving and sending of preserved information media which having a

detail of receiver, sender, authorised person, type of information and time. **[A]**

- Providing a destroy method of information and media which out of use, including various importance information in hard disc remained in the recycle bin. **[A]**

2. IT Contingency Plan.

- having emergency plan for backup the computer system or provide computer system to replace without delay and cause a least damage. The emergency plan shall have a following detail **[M]** :
    - arrange the importance of operational system. Relationship of operational system and time for backup each operational system;
    - determine the event or priority of violent of problem ;
    - determine for solving the problem in detail;
    - determine the responsible officer and authorize person and having name list and telephone number of all concerned person;
    - having a detail of necessary device that using in the emergency case of each functionality such as computer version , specification, configuration and network device etc.
    - n case of the company having a preserved computer center, it shall identify clearly a detail of the preserved computer center such as location, map etc..
    - modifying the IT contingency plan up to date and keep a the IT contingency plan outdoor.

- Testing an operation under the IT contingency plan once a year at least by testing in a manner of duplicate a real situation in order to assure that able to operate in practice and having a record of such test. **[M]**
- Communicating the IT contingency plan to necessity concerned person to acknowledge. **[A]**
- In case of having an emergency event, it should record the detail of event, cause of problem, and dissolution method. **[A]**

Computer Operation.

Objective

Computer operation have an objective for operate the computer system correct, consistent and efficiently that having content cover guideline for computer operation such as oversee of operational computer system, problem management, and controlling the report preparing that rendering to reduce the risk on integrity risk and availability risk.

Compliance Guideline

1. Computer Operation.

- Providing a written procedure or compliance guideline for various importance permanent operation as a guideline for the computer operation such as procedure for open-close system, procedure for assessment, procedure for monitoring the operation system effectiveness and compliance schedule etc. and modify procedure or compliance guideline up to date. **[M]**
- Determining a computer operation comply via menu and limit the operation by using command line as necessary. **[A]**
- Determining a log book a detail of various permanent operation and such log book should have a following detail: **[A]**
  - Operator
  - Operational time
  - Operational Detail
  - Occurred problem and solution
  - Position of system
  - Supervisor

2. monitoring

- Monitoring the importance operation system effectiveness to consistently and efficiently functions such as transmission system for securities trading, connection between company and Securities exchange business, hard disc operation, CPU operation etc. in order to use an information for capacity system assessment . **[M]**

- Providing maintenance computer system and other device in a good condition and ready for operation. **[A]**

3. Dissolution

- Determining clearly name list duties and responsibilities for dissolution such as determining the person responsible for dissolve a problem of trading securities etc. including telephone number of concerned person for connecting when the problem occurred .**[M]**
- Providing a problem and abnormal record system any d report to the commander consistently and singing when receiving the report for the purpose

for gathering problems and inspect the cause, including study as a guideline to dissolve and prevent problem. **[A]**

4. report preparing control

- Asking for publish other report, it should given an approval by the authorized person. **[A]**
- Providing a register controlling of publishing and deliver a report, keeping the report published strictly and determining have a signature when received a report. Moreover, it should destroy a report which out of use. **[A]**

IT Outsourcing

Objective

IT outsourcing may cause a risk to the securities company in various means different from carry out a business cause of the securities company such as access risk integrity risk that escalate because of the operation of the outsourcing. Therefore, IT outsourcing have an objective for rendering the securities company get service of information technology from other provider efficiently, acceptable and able to control a risk and having a content cover guideline for selection and controlling a outsourcing operation.

Compliance Guideline

1. Service provider selection

- Determine regulation for selection a service provider and select the provider which have a operational procedure careful, concise and reliable. **[M]**
- Making a contract identified clearly a data confidentiality and scope of work and service level agreement. **[A]**

2. Service provider controlling

- In case of get a service on operational development, it shall determine a service provider able to access to the part of develop environment only. Nevertheless, in a necessary case to access to the part of production environment, it shall control or monitor a service providing strictly in order to assure that satisfied the prescribed scope, such as providing the company officer control strictly the service provider's operation in case of onsite service and providing the company officer control strictly the service provider's operation in case of providing service in a manner of remote access and close immediately a modem when a service finished. etc. **[M]**
- Determining a service provider prepare a compliance manual and related document and modify it up to date. **[M]**
- Determining a service provider provide report the functionality, other problem and resolutions.**[M]**
- Determining a procedure of inspect the work of service provider. **[M]**

Notified this 14th Day of March 2006.

Thirachai Phuvanatnaranubala
(Mr. Thirachai Phuvanatnaranubala)
Secretary-General
Office of the Securities and Exchange Commission

(Translation)

Original proposed guideline		Comment/question	From company	The SEC Office's comment
Backup and IT Contingency Plan.				
Preparing readiness in emergency case	○ There must have a detail of device that using in emergency case o the system's work	Peopose to Modify to "specification"	IT Club	Approve with the comment of the company.
	○ It should communicate emergency plan to concerned person acknowleged as necessary and preventing unauthortized person acknowleged	Propose to delete "preventing unauthortized person acknowleged"	IT Club	Approve with the comment of the company.

Summary of proposition and comment of hearing of regulation and compliance guideline information technology.				
Original proposed guideline		**Comment/question**	**From company**	**The SEC Office's comment**
	Come into force after the expiration of six month as from the notified date.	Propose to enforce after the expiration of one year as from the notified date	- Aberdine Securiities Public Company Limited - Premavest Securiities Public Company Limited - Thanachart Securiities Public Company Limited	The period of six month adequate fro preparing a readiness, it shall come into force after the expiration of six month as from the notified date.

Original proposed guideline		Comment/question	From company	The SEC Office's comment
Policy of Security of Information Technology.				
Preparing policy	○ Preparing a written policy of security of information technology and the executives, computer staff and user of various division have to participate in preparing a policy with approval by the Board of company at least.	Could comply with the policy of the parent company?	- Aberdine Securiities Public Company Limited	Add content of compliance guideline " In case where the securities company is the affiliated company of other financial institution, the securities company may comply with the policy of security of the information technology of such financial institution."

Original proposed guideline		Comment/question	From company	The SEC Office's comment
Preparing policy	providing an inspection and assessment of the sufficiency of policy and internal control information technology system by independent unit once a year at least by an internal unit of the securities company or by an outsider inspector	Propose to modify from "mandatory" to "accredit"	- Aberdine Securities Public Company Limited	Add content of compliance guideline " In case where the securities company is the affiliated company of other financial institution, the securities company may comply with the policy of security of the information technology of such financial institution."
	notifying to the Office without delay in case appeared that have significant case effect to the security of the information technology	Propose to expand the meaning of "significant effect"	Thai Military Securities Public Company Limited	For the purpose of exactly understanding, the Office has expand the meaning of "significant case effect to the security of the information technology" as "an effect causing the securities company operate business inconsistent namely trading securities system was damaged and unable to operate in the normal condition etc. or an effect causing harm to the customer's information or customer's asset such as customer's information or information of investment units incorrect because of computer system assessment or modification by the unauthorised person"etc.
		Propose to delete the following content "significant effect" because hard to interpret or modify to have to "notify to the executive acknowledge"	IT Club	

Original proposed guideline		Comment/question	From company	The SEC Office's comment
Physical Security.				
Damage_prevention	○ In a case where level of floor or computer centre has lifted for the purpose of instalment the air conditioner system, including instalment electric system and network system below, it shall install water leak sensor in the place where has installed a water pipe in order to suppress leak water instantly. Moreover, in case of the computer centre located in the place having risk for water leak, there should notice consistently that have a water leak or not.	Propose to modify from "mandatory" to "accredit"	IT Club	Approve with the comment of the company.
Security of the information, computer system and network system				
Information management	○ Transmission of importance information via the public network, it shall receive an international standard encryption such as SSL,VPN etc. **[**	Propose the option for determining a password before transmit information instead of encryption.	IT Club	encryption for transmission of information via the public network is convert the information for prevent information form accessed by unauthorised person in transmission line whereas determine a password before transmit information is only a specification of person who sent the information, it is unable to prevent such case.. So, it

				was approved that still use the post guideline.

Original proposed guideline		Comment/question	From company	The SEC Office's comment
User account and password**.**	o Providing the identification and authentication measure prior to access to the computer system strictly such as impose hardly password for presumption etc. and determining that each user has his own user account. Providing that the consideration that determine hardly password for presumption and control using of password strictly or not, the Office shall take the following factors for consideration in generally	The system has limitation that unable to impose a password in accordance with the Office's guideline, there shall additional identify that it must impose a password in accordance with the Office's guideline for the Clause that the system capable to support.	Thai Military Securities Public Company Limited	The Office consider that the efficient imposition a password hard to presume. It should impose by the system. However, if the system has a limitation which unable to impose a password in accordance with all of Clause of the guideline prescribed by the Office. The company may impose as an additional policy a control a user to comply with strictly. Proving that the consideration for imposition a password careful and sufficient strictly or not, the Office shall consider in generally that are not consider in each Clause. So, it was approved that still use the post guideline.
		The system has limitation that unable to impose a password in accordance with the Office's guideline, propose to impose as a policy of the Office and asking a cooperation from the user.	- Aberdine Securities Public Company Limited	
		Propose guideline on imposition a password is only an example.	IT Club	

Original proposed guideline		Comment/question	From company	The SEC Office's comment
	- Determining the password that having properly length, For a international standard requires for six characters of minimum lengtht	Propose to impose the minimum length composing only of four characters	Ayudhaya Securities Company Limited	The imposition a minimum length of password is six characters in according with international standard, it was approved that still use the post guideline.
	- For each time of changing password, it should not determine new password similar to the latest password.	Propose to impose a password is not similar to the ex-password for one time.	IT Club	Approve with the comment of the company.
	- determining the times that accept the user for entering incorrect password. For the general practice, it is not exceed three times**.**	Propose the times that accept the user for entering incorrect password not exceeding 5 times**.**	Ayudhaya Securities Company Limited, IT Club	Approve with the comment of the company.
Security of computer server system	○ Install a patch of program of system software such as such as DBMS operational system and web server etc. in order to fill consistently a loophole of program of system software .	Propose to install patch only in case that effect to the operational system.	Thai Military Securities Public Company Limited	Approve with the comment of the company.

Original proposed guideline		Comment/question	From company	The SEC Office's comment
Management and network inspection	○ Providing the trespass monitoring system and abnormally operating system via the network system whereas it shall monitor consistently the following matter at least	Propose to modify from "mandatory" to "accredit"	IT Club	An inspection a trespass via the network is a materiality forpreventing a riks as am access risk, it was approved that still remain "mandatory".
Virus Prevention and malicious code	○ All of server computer and user's computer connecting to the network system have to install a efficiently virus prevention and modify it up to date.	Propose to modify to "providing a measure for virus prevention" because of installment a virus prevention software is not the only mean for preventing virus.	Thai Military Securities Public Company Limited, IT Club	Approve with the comment of the company.

Original proposed guideline		Comment/question	From company	The SEC Office's comment
Audit log	○ Providing a record of functional of server and network computer system, application log record, information of trespass prevention system such as login-logout logs, login attempts, command line and firewall log etc. for the purpose of inspection and it shall keep such record for three months at least.	Propose to keep a log of front office for 5 days.	Ayudhaya Securities Company Limited,	For a purpose of the Office for supervising and reducing a burden of the company, it was approved that the company should keep a functional record of server and network computer system, application log record and record of information of trespass prevention for 3 months at least.
		Propose to keep a log of back office for 30 days.	Ayudhaya Securities Company Limited	
		Propose to keep a system log for 30 days.	Ayudhaya Securities Company Limited	
		Propose to keep all log for 1 month t least.	IT Club	
		Propose to add the inspection of log consistently.	Thai Military Securities Public Company Limited	Approve with the comment of the company by imposing as accredit..

Original proposed guideline		Comment/question	From company	The SEC Office's comment
	○ Providing a prevention measure for alteration of other record and limitation of right for only concerned person to access to the record.	Propose to modify from "system" to "method"	IT Club	Approve with the comment of the company .
		Propose to modify from "mandatory" to "accredit"	IT Club	A prevention measure for alteration of other record **is** materiality of overseeing and inspecting a functionality, it was approved that still remain as mandatory.