Information Security Policy

Information Security Policy Document

Principal Capital Public Company Limited (the Company) is an organization that has adopted the information technology to support and enhance the efficiency of performance. Failure of information system service or any causes of error in service might lead to the information technology system interruption and unsafe which could affect the Company's reputation or confidentiality. All users must collaborate to prevent the damage of the information technology and computer networks or minimize the probability of its damage. Hence, the Company agrees to formulate the information technology system security policy.

Article 1

Definitions and Terms

"Computer asset" refers to all assets involved computer system usages such as hardware, software and data etc.

"Network system" refers to computer network system owned by the Company.

"Server" refers to a computer in network system, which is used as the central functioning such as repository of data or software service for other computers or network control.

"Remote access" refers to the ability of a computer or a network system to get access to other computers or network system via communication devices or transmission media such as Modem, VPN

"Access control" refers to the mechanisms that control the access or usage of computer asset with the authorized rights.

"Computer" refers to the devices that process data electronically followed by the software instructions to give a required outcome such as server, personal computer and notebook computer.

"Computer device" refers to the computer and the electronic devices that are attached to computer to support the computer's operation toward its requirement.

"Transmission media" refers to any medias that connect computer devices together such as copper, fiber-optic, wireless

"Hardware" refers to the computer device.

“Software” refers to a set of instructions that command computer to operate as required.

“System software” refers to the software that controls and works with computer hardware such as operating system, etc.

“Application software” refers to the software designed for specific tasks such as word processing software, accounting application software.

“Information technology system” refers to the system of an organization encompassing information technology, computer systems and networking to process information utilized in planning, service, service support, communication developing and controlling in an organization. It is consisted of computer hardware, networking, programs, systems and information.

“Information” refers to the numeric or graphic data that is processed and organized to be user-friendly and utilized in the management, planning, decision making, etc.

“System” refers to the information technology system applied in tasks to achieve the goals such as filing storage system, accounting system.

“Operating system” refers to the software that controls a computer’s operation and allocates resources which is memory unit allocation, input devices controlling (keyboard, mouse) and output device (monitor, printer).

“Firewall” refers to the security system that consists of a set of computer devices and software preventing the access by unauthorized external users and restricting the usage of internal users in accordance with the company policy.

“Data” refers to character string, instruction, instruction sets or related one that is created, transmitted, received, stored or processed in the computer system by computer hardware electronically including the electronic data in accordance with the electronic transactions law.

“File” refers to a set of data records that are kept together and defined in a unit with a specific name such as in-use software and other document files created, named, recorded in the media.

“User” refers to the company personnel or other third parties who are entitled to use information technology system of the Company.

“Network administrator” refers to a person who is responsible for network monitoring and maintenance.

“Host/Server administrator” refers to a person who is responsible for server monitoring and maintenance.

“Firewall administrator” refers to a person who is responsible for firewall monitoring maintenance.

“User account” refers to the account that the user uses to access and activate information technology system in accordance with an agreement of users and information technology service providers.

“Administrator account” refers to the account that the administrator uses for server management.

“Configuration document” refers to the document that identifies and defines the information technology system’s functional and physical characteristics to be practicable usage as required.

“Risk” refers to the probability of violating the asset security.

“Incident” refers to any events that impact on the security of information technology system.

“Company personnel” refers to an employee of the Company.

“Division” refers to a department of organization structure.

“Data owner” refers to one or more than one company personnel whom is assigned to be responsible for data.

“Malicious Software” refers to hardware or software that intently input to the system without the permission by a malicious person to respond the purpose of computers or information technology system or other instruction set damage, adaptation or adding.

“External organization” refers to the organization that gets permission to access, use data or information technology system of the Company, which being entitled according to types of application and must be responsible for non-disclosure confidentiality of the company without permission.

Article 2
Security Policy

The objective is to provide management direction and support for information security in accordance or correspondent with relevant laws and regulations.

After the enforcement of this notification, the information technology division is responsible for formulating the regulations that are necessary for information technology system and network security of the Company with the approval by the CEO and the CEO supports the policy, budgeting, resources and others that are necessary for improving information technology system and network security continually.

The information technology system and network security policy shall be published and communicated to all employees, external service provider and relevant parties to be acknowledged and conducted.

The information technology system and network security policy shall be reviewed and assessed at least one time per year, or when there are major changes which affect the security of the Company's information technology and computer networks.

Article 3
Organization of Information Security

3.1 Organization of information security within internal organization

The objective is to manage information technology system and network security within the Company.

CEO is in charge of appointing representatives or working groups from different divisions of the Company to coordinate or cooperate in the creation of information technology system and computer network's security, in which those representatives or working groups shall be clearly assigned their responsibilities on the security of the Company's information technology system and computer network.

The representatives or working groups appointed by the CEO shall be responsible for managing and controlling information technology system and computer network's security of the Company including reviewing the information technology security policy, preparing procedures and guidance on information technology and computer network security as well as and any documents relevant to the information technology system and computer network's security.

All company personnel shall not disclose the Company's confidentiality, except obtaining permission from the Company.

The Company shall set procedures to examine the operational management and other operations relevant to information technology system and computer network by an independent examiner at planned intervals, or when significant changes occur.

3.2 Organization of information security relevant to clients or external parties

The objective is to maintain the security of the Company's information and information processing facilities that are accessed, processed, communicated to clients or external parties.

The risks to the Company's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting the access.

All identified information security requirements shall be addressed before giving external parties access to the Company's information or assets.

Agreements with third parties involving accessing the Company's information or information processing facilities must be governed before giving external parties access to the Company's information or information processing facilities.

Article 4
Asset Management

4.1 Responsibility for asset

The objective is to achieve and maintain appropriate protection of the Company's assets from any potential damages.

Inventory of all key information assets must be created and maintained regularly including ownership of this inventory must be formally established.

Rules for the acceptable use of information and assets associated with information processing facilities must be formally identified and documented to protect those assets from damage occurred by lacking of carefulness and maintaining.

All key assets must be maintained in the appropriate storage orderly.

The authorization to use computer assets shall be as follows:

- Relevant information technology system and information processing facilities provided by the Company are to be used in the Company's mission. The personal use must be limited and reasonable nature depended on the appropriateness and not interferes to the duty performance.
- The Company's personnel as well as other personnel and/or juristic person hired by the Company are responsible for ensuring the protection of assigned assets and examining these assets including data and information of the Company to be safe and correct.
- Users must use the Company's assets and devices with extreme caution and protect as though your own.
- All clients, laptops, and servers of the Company must be protected with the operating system password for every access and must be secured with a password-protected screensaver with the automatic activation feature set a moment or must be lock the screen or log off when the device is unattended.
- While off-site working, users must be in aware and responsible of the assigned assets.
- Users must not connect the personal owned computer to the Company's network including not install any software in the Company's computers without permission from information technology department.
- Laptops storing the confidential information must be protected as same as the in-use computers in the Company such as anti-virus software, anti-spyware software, and updating security patches software regularly.

- The Company's computer assets must not be modified or installed any facilities without the permission by the relevant management of division and the company personnel must not permit unauthorized person to install any hardware or software in the computer without exception.

The authorization to use software shall be as follows:

- The company personnel must not install or publish the pirated software in the Company's computer system.
- Both in-house developed and commercial software computing and storing the confidential and important information must be examined, controlled and approved appropriately by the data or system owner before installing in the Company's information technology system.
- All information technology system used by the general users must be provided with sufficient supported documents in order that general users could be understood and workable.
- Lists of software and information technology system installed in the user's computers must be prepared in the official document approved by the CEO to ensure that such software is copyrighted and installed for the Company's objectives.

The acceptable use of internet shall be as follows:

- The company provides internet to support operation and facilitate employees seeking knowledge and communicating to external personnel in order to enhance the Company's work and service efficiency.
- Users must use internet carefully and this usage must not cause spoiling the Company's and related personnel's reputation or not involve in illegal conduct. Anyhow, internet misuse is breach of discipline and might be legal prosecution.
- Internet usage must access through the authorized gateway or provided workstations for specific propose only. Anyhow, the Company reserves the rights to inspect users' internet usage to detect the internet misuse.
- Users are prohibited to click the pop-up advertising window or access any websites advertised by spam because there might be malware in these websites or hack the users' computer without permission and acknowledge.
- Users are prohibited to visit, download or copy pornography or inappropriate or illegal media.

- The Company do not support personal opinions expressed in electronic format (such as web board or blog). Anyhow, damage caused by the personal views is in the responsibility of such employee.

The authorization to use e-mail shall be as follows:

- All e-mail users within the Company must have their own e-mail account.
- E-mail account must be secured with a password-protected to prevent violation and

e-mail misuse.

- E-mail account with a specific purpose such as itsupports@principalcapital.co.th may be created as a group e-mail and/or to share among more than one user. There must be an employee assigned to be an owner of that e-mail account.
- All e-mail accounts and e-mails (including personal e-mail) created and stored on computer system or network are considered as the Company's assets.
- Users must use only the authorized software to access and/or communicate in e-mail system of the Company.
- E-mail's storage size on the central server (mailbox size) is limited. When mailbox size is used reaching at designated storage space, users shall be notified by warning message from the system. When mailbox size exceeds the storage space, users shall not be able to send or receive E-mail from then.
- Email and attachment size are limited. In case of exceeding size, such e-mail will be returned to the users with the message notified that unable to send.
- Users must delete unnecessary e-mail from their own mailbox regularly to maintain mailbox size according to the Company's requirement. In this regard, users must keep only e-mail relevant to woks and the ones stipulated by the law.
- Do not use an e-mail account of the Company in any illegal conducts such as tobacco, liquor, smuggled goods, pirated software publishing.
- Do not use an e-mail account of the Company for announcing any information in electronic communities, such as web board, blog, bulletin board except such announcing is for the Company's businesses.

- Software for using E-mail must be set up to send all e-mail with the signature of senders by default. The signature is composed of the senders' first name, last name, position, division, company name and telephone number.
- File attached e-mail must be in the standardized format which the receivers could open with basic software in any operating systems such as PDF, DOC, TXT, CSV, XLS, JPG, GIF, PPT and HTML.
- E-mail sent from the Company to external will automatically have a disclaimer sentence attached to them.
- Users are prohibited to copy messages or the confidential attached file in other e-mail users without permission of the item owner.
- Users must compose e-mail carefully with the consideration of sending on behalf of the Company.
- Users are strictly prohibited to modified content, header, and signature in e-mail or other e-mail accounts.
- Users must not consent others to send by their own e-mail account strictly; regardless of a superior, secretary, assistant or any other persons.
- Users must not send the undesirable email to recipients; for example, junk mail or spam mail.
- Users are strictly prohibited to compose or involved in sending e-mail hoaxes or chain letters
- Users are strictly prohibited to send or forward e-mail within the scope of disparagement, defamation, caste discrimination, threats, defamation, obscenity, pornography or containing material that is sensitive to cultural, religion and national stability or royal institution.
- Users are prohibited to send any attached materials related to gambling, obscenity or non-work related that have a negative influence on the Company.
- Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- If users receive a virus warning via the antivirus software application, users must terminate sending that e-mail immediately until computers are fixed and restored to be prompt in use.

The authorization to use telephones, facsimile machines, printers and copying machine

Shall be as follows:

- If users receive a mistaken fax document such as sending to a wrong number or a wrong division, users must inform the sender and destroy that document.
- Users are prohibited to print out the confidential information by a public printer except that it is collected from the printer immediately by an authorized person.
- Users are strictly prohibited to record or leave messages containing confidential information on answering machines or voicemail systems.
- Users are prohibited to disclose confidential information by using speakerphones or any electronic media such as Voice over IP or teleconference except that all participants are identified to be qualified and have a right for acknowledgment in the teleconference.
- Responsible persons must inspect the nearby area in order to ensure that unauthorized persons could not get any confidential information in the dialogue.
- Teleconference is arranged in safe area such as the meeting room with soundproof wall and door.
- Users must talk on phone call with extreme caution to protect eavesdropping by unauthorized persons.
- In case of disclosure on any confidential information on phone call, informants must verify the authorization to acknowledge the information of speakers before disclosure.
- Users must be permitted by data owner to copy or scan the documents any containing confidential information.

4.2 Data and information asset classification

The objective is to ensure that information receives an appropriate level of protection.

Classification guidelines must classify information in terms of confidential level and criticality in order to be safe with appropriate method.

Entire or partial copy must be classified at the same confidential level of the original digital information.

A set of procedures for information involved information technology management labeling and handling must be developed.

Data in hardcopy format must be controlled and secured appropriately from printing, labeling, handling, duplicating, distributing until destructing and formulating the implementation guidelines for officers to ensure that data is under control and security including confidential information must not be disclosed except for working purpose only.

Users must be aware of information secured in users' computers especially computers shared by more than one user. The confidential information must be protected by password login or any appropriate methods of operating system or information system.

Users should store confidential document and media containing confidential information in cabinet that can be locked when not in use, especially during outside office hours or when leaving such document or media on the desk when users are not available.

Confidential information must be cleared off immediately from computing devices such as printers, facsimile machines, copying machines.

Officers must not disclose the Company's confidential information to external parties except that such disclosure is under non-disclosure agreement.

Officers must not talk about or use confidential information of the Company in public places such as lifts, restaurants.

Media repository or mobile devices (ex: PDA, Thumb-Drive, CD-Rom) containing confidential information of the Company must be handled and used with extreme caution.

All key information involving the Company's performance; both stored in users' computers and servers in the responsible of users, must be backed up regularly to restore data in case of any troubles such as virus infection, broken hard disk.

Article 5

Human Resources Security

5.1 Human resources security prior to employment

The objective is to define and recruit personnel prior to employment to reduce the risk of error, theft, fraud and misuse of information system and other information asset of the Company operated by officers.

External outsourcing contractors must strictly follow information technology and computer network's security measure according to the Company's security policy and guideline.

All candidates must be checked background verification before being filled in executives, temporary workers, or trainees with no prior criminal behavior in trespassing, modifying, destructing or hacking data in information technology system of any organizations previously.

5.2 Human resources security during Employment

The objective is to ensure that the company personnel is aware of information operation threats including the provision of training to employees to be able to protect threats.

Employees or users have duty to understand information security procedures established by the Company in order to implement for securing their own assets or assets under their responsibilities.

There must be training about security awareness and procedures to build security equipped with information technology system including communicate to acknowledge security policies and any changes of information technology.

All employees and new staffs must receive training of security policies and procedures, as relevant to their job function before or within 30 days after starting at work. They should attend orientation, sign and also be recorded their training attendance in personnel files.

There must be a disciplinary process for employees who have committed a security breach but in case of breaking the law, the penalties are in accordance with illegality of their act identified by point of law.

5.3 Termination of Change of Employment

The objective is to remove access rights of all employees who are terminated their employment or contract in order to secure information system.

To manage Login and User ID correctly and in update, human resource division must inform information technology division to acknowledge immediately if there are events as follows:

- Employment beginning
- Change of employment
- Resignation or termination of executive, employee, and contractor employment or mortality.
- Division transferring
- Job suspending, disciplinary action or idle operation.

All employees and contractors must return all of the Company's assets including assigned computer system, key, employee ID card, access card, computer and peripheral computer, manual and document to superiors before the termination date of employment.

Upon termination or changing position as the company personnel or contractor, relevant employees, contractors, partners, third parties/outsources must be notified the access rights to division's information appropriately.

Article 6
Physical and Environmental Security

6.1 Secure Areas

The objective is to standardize the physical security relating to the area that contains information and information processing facilities owned by the Company.

Information technology division is responsible for formulating the detail of places, protection devices, entry controls to be appropriate for secure premises or areas.

Secure area must be protected by entry controls and must allow only authorized personnel access.

In case of non-information technology employees requesting to access without request in advance, there must be check the necessity to consider the temporary access permission. Anyhow, the persons must show their ID card or other official identification card. Information technology division must record the person information and access request as evidence. (both in case of accepting or denying the access) and must record all Data Center access of external parties together with retaining the records for a minimum of one year.

External parties must exchange their official identification card, for example, ID card, driving license, passport for visitor's division card before getting permission to access. External parties must show the visitor card at all time when being on the office premises. Anyhow, visitor cards are not allowed to transfer the right of ownership or borrowing.

Do not leave the entrance and exit doors of office open or not consent unauthorized person follow to access the office area strictly, except that person is able to show personal card or visitor card in order to protect unauthorized person accessing to the office and secure area.

There must be measures for securing offices, rooms and facilities, for example, high important computer or system must not be set up in the crowded area. Offices or rooms must not put up a nameplate or sign implied to the key system inside. Doors and windows of offices or rooms are always locked. When there's nobody there, the facsimile machines or copying machines are placed separately away from the secure area.

Employees must examine the security of their workplace area every day after work to ensure that safes, cabinets, drawers and equipments are locked properly and keys are kept safely.

Information, media repository, materials and equipment containing confidential information must not be left on the desk, in the meeting room or in the unlock cabinet without attention strictly.

Information, media repository, materials and equipment containing confidential information must not be thrown away in a waste bin without appropriate shredding. Data scrapping and destructing these media repository, materials, equipment must be followed by media and information management procedures manual.

Employees must not allow anyone to move computers or media repository away from their workplace, except for the person who is authorized to operate with the official order of the Company.

To secure premises equipping with and maintaining computer assets, there must be protection against damage from fire, civil unrest and other forms of natural or man-made disaster, in addition to test security system in the secure area once per year at least.

Employees working at internal secure area must be trained and practicing at reasonable time in order to be able to use security devices correctly and appropriately.

Information technology division is responsible for maintaining the premises of damage and threat protection facilities in the area of secure area for a reasonable time.

Information technology division restricts access to the area. If possible, there should be separated between related working area and external party area; for example, loading and delivery area must not in the area of external party access.

6.2 Equipment Security

The objective is to protect unauthorized computer usage and to ensure that computers are protected from the environmental threats, theft and other damages.

Employees or users must arrange and protect all equipments of the Company to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Equipment must be regularly maintained in order to continue its availability and be promptly in use.

Employees or users must coordinate with information technology division in providing contingency plan in case of computer damaged and test the contingency plan at reasonable time.

Employees or users must check all items of equipment containing storage media to ensure that any sensitive data or licensed software has been removed or securely overwritten before disposing or sending the item for maintenance. All this is to protect data.

There must be assigned employees to responsible for computer maintenance and monitoring computer equipment movement in order to prevent data loss or modification.

Article 7

Communication and Operations Management

7.1 Operational Procedures and Responsibilities

The objective is to ensure the correct and secure operation and management of information technology structure.

Information technology division must prepare information technology manual and/or operating procedures for divisions such as a manual of incident informing, recovery, maintenance which detail the procedures and officer or division in charge.

Information technology division must manage all changes to network, computer system, and software every time.

Information technology and communication division must document changes every time and communicate to relevant divisions to be acknowledged the detail on changes.

Information technology division is in charge of defining information and network operating responsibilities clearly to avoid misuse or unauthorized of the Company's assets.

7.2 Third Party Service Delivery Management

The objective is to implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

Formal contracts must be provided to control third party security service. These contracts must define as follows:

- The agreed policy and control upon the Company's information security
- Scope, detail and service level agreement
- Physical and logical control measures documentation
- To ensure that the system of third party service provider is able to secure information in 3 aspects; confidentiality, integrity, and availability
- The agreed upon connecting network to external party

- Types of information that external parties are allowed to access and requesting the Company's information process in case of requiring additional information.
- Non-disclosure agreements
- Borrowing and requesting the Company's equipment
- Legal agreement such as privacy and information protection
- Information technology division assigned to audit and inspect the service provided by third party according to the agreement
- Information technology division is responsible for managing changes to third party service providers.

7.3 System Planning and Acceptance

The objective is to minimize the risk of system failures.

Information technology division must continuously monitor and analyze current resource capacity upon its appropriateness followed by the documentation, guidelines of capacity management.

Information technology division must plan resource capacity management once a year at least regarding to consider future capacity requirements (for example; the next year requirement, speed-up CPU, larger hard disk capacity, current usage performance, technology changing).

Information technology division must establish acceptance criteria for new or purchased information systems including to test prior to acceptance in accordance with the system acceptance guidelines.

7.4 Protection against Malicious and Mobile Code

The objective is to set a guideline for controlling and protecting users from misappropriation usage of system, software, information and wireless communicating electronic devices such as mobile phone, tablet, and laptop.

Computer, laptop, wireless communicating electronic devices and information operated on the Company's network must be registered and set up right of use followed by security policy before usage approval. The following details of mobile device registration must be included:

- Submission date and registration request date
- Types of devices
- Device serial number (ex: MAC Address)
- Data owner, system administrator and approved person
- Device usage necessity
- Usage right specification

Clients and laptops must be installed updated anti-virus program approved by information technology division and enable to activate the program during in-use. These are followed by malicious software controlling management guideline.

Server providing anti-virus service must be updated latest pattern regularly. All service providing computer, desktop computer and laptop must be updated latest pattern by the server providing anti-virus service.

Server providing anti-virus service configuration documentation must be revised every 6 months.

Employees must not download shareware or free ware directly from the internet without information technology division approval. After approval, employees must scan software with virus scanner program before using.

Within division, all files downloaded from attaching in e-mail, disk copying, or file sharing must be scanned to detect virus.

Users must not create, keep or publish any malware; for example, virus, warm, Trojan horse, e-mail bomb against the Company's computer system.

Users must not interfere or interrupt anti-virus software action. Files related to work are only permitted to be transferred on organization's network. Anyhow, users should receive file only from known sources and through possible communicate channels. Furthermore, users must scan received file to detect virus with organization's anti-virus software before opening the files.

All servers must be turned off the function connecting the internet except when necessary to prevent malware affecting to key information on servers.

Users must not installed portable programs such as different Active code (Java, ActiveX) from the incredible sources.

7.5 Information Back-up policy

The objective is to be a guideline for back-up procedures in order to restore in case of incident occurrence such as natural disaster, system failure.

Information technology division must set the frequency of information backups subjected to its important and risk acceptance identified by data or system owner. These are followed by back-up information management guideline.

Information technology division must maintain back-up system or equipment to be effectively available using

Information technology division must provide physical access control of back-up storage. Backup media must be protected in line with the important level of information.

Information technology division must set the period of back-up according to the level of risk management.

Information technology division must provide the backup and restore data procedures for all systems including documentation and auditing periodically.

Information technology division must provide backup and data restoration registration records each time.

Backups of essential information must be tested periodically to ensure that information can successfully be retrieved from the backup media.

Information technology and communication division must record the holding backup media at site storage and audit every year.

Procedures of holding backup media and site storage of backup must be audited at least once a year.

Backup media must be labeled at least with the following details:

- System name
- Created data date

- The important level of data
- Information administrator contact

7.6 Network Security Management

The objective is to the information in networks and supporting infrastructure.

Information Technology division must define the responsibilities, the practice when there are the incident or security breach and offender detection.

Information Technology division must record the detail of significant changes and inform relevant parties to be acknowledged in case of changing and modifying network.

There must be managed relevant activities appropriately and ensured that these are in line with the control of information transmitted on the Company's network and infrastructure.

All networks of the Company connecting to other networks must use facilities or Package Filtering program such as Firewall or any hardware including being able to detect virus.

Information technology division must limit the number of connections between external parties and the Company's network and set the connection to specified computer and system particularly. The particular computer and system should be separated from practical organization's physical and logical network. Unauthorized parties are not permitted to use computer or networking of the Company.

Users must not install modem with their own computers or equip with any part of the Company's network without information technology approval.

External party must not connect external computers or any facilities to the Company's computer system and network. If necessary, they must request appropriate approval in advance.

Users must not strictly install any hardware or software related to network services; for example, Router, Switch, Hub and Wireless Access Point without permission.

Users working on the Company's network must not connect to external network through modem or interlock equipment while connecting to organization's network.

7.7 Media Handling

The objective is to prevent potential destruction to the Company's media storage.

There must be procedures and authorized right in place for the management of removable computer media.

Disposal of document and media must be approved by data owner and appropriately recorded.

Information technology division must record the media distribution and authorized person request.

Information technology division must handle and store security of system documentation.

7.8 Exchange of Information

The objective is to protect information and software loss including to prevent information from unauthorized modification and misuse.

Information technology division must provide methods of transferring media (information or software) securely.

Information technology division must provide methods of electronic information accessibility including transferring electronic information on network.

Information technology division must place formal exchange procedures to protect the exchange of information among organizations.

7.9 Monitoring

The objective is to detect unauthorized information processing activities.

Information technology division must produce audit logs recording user activities, system exceptions, and information security events regularly.

Information technology division must monitor use of information processing facilities regularly to detect any incidents.

Information technology division must specify to protect audit logging information or other incidents relevant to the information technology usage in order to prevent unauthorized changes or correction.

Information technology division must produce administrator and operator logs recording.

Information technology division must produce fault logging related to information usage, analyze and take appropriate action.

Information technology division must synchronize the clocks of all relevant information processing systems within the Company with an agreed accurate time source.

Article 8
Access Control

8.1 Business Requirement for Access Control

The objective is to control access to information securely.

Information technology division must establish an access control policy and information requirements for access to control the authorized accessibility.

Information technology division must identified the access right of information and information system to suit for usage and the responsibilities of users prior to use information system including review the access right periodically. Anyhow, users must be approved by system administrator upon the necessity.

Only system administrators are able to change the access right of information and information system.

Information technology division must record and monitor the Company's information system usage and be on guard against security breach of essential information and information system.

8.2 User Access Management

The objective is to prevent unauthorized access to information systems.

There must be a formal user registration for new users to grant necessary access to information system and revoke access when; for example, staff resign or change position.

According to information access guideline, users must be strictly reviewed and considered to be approved as the Company's practice.

There must be assigned the access right for each information system and separated by duty.

Users must prove their identity any time when log on information system.

Information technology division must secure users' password regularly.

Information technology division must review users' access rights of information system at regular interval (such as at least once per 6 months).

The record of access log and log files must be kept for at least 5 years.

8.3 User Responsibilities

The objective is to prevent unauthorized user access of information system.

System administrator must identify the users' access right of each information system and separate the access right by responsibilities. The practice is defined within the "Information Access Control and Use of Password Management" documentation.

Employees must be required to follow the information access control, password creation, password changes, password removal and use of password control as established by the Company.

If necessary to grant privileges to users meaning that the highest level of right must be cautious of controlling the privileges users by considering the following factors:

- There should be consented and approved by superior and system administrator of the system.
- There should be strictly control of use such as assigned the control of use only for necessary case.
- There should be set the effective period and disabled when overdue.
- There should be strict password changes; for example, when no need to use or when necessary to use for a long term, password should be changed every 6 months etc.

Users are responsible for maintaining their username and password including personal information required for changing user account to use system securely.

Passwords must be changed upon first login and change at regular interval as stated in Password Standard practice.

Passwords must be secured as stated in Password Standard practice.

Passwords are confidential. Users are responsible for secure passwords and must not use a joint password or strictly not share their own passwords with anyone including family members when users bring their work home.

Users must be responsible for all activity performed with their personal User ID and passwords. If users suspect that whether their own user ID and passwords are hacked, users must inform information technology division to reset all passwords immediately.

Project manager of new system within the Company must examine to ensure that their in charge system is in line with this policy and relevant supporting document. They must coordinate with system administrator to control and configure system settings in accordance with the relevant regulations before adoption.

Reset password must be processed only by the Company's standard procedures to ensure that this correspond to users' requirement and system administrator also has the access right to request users' information and prove users' identity as appropriateness.

On the contrary, uses may be requested by information technology division to change a new password in case of the password becoming unsecured, predictable or easy to be hacked. Anyhow, users must also verify the source of request to ensure that the request isn't deceptive.

There must be defined the unattended equipment protection.

Employees must set the papers, documentation or media containing essential information controlling to be not left on the desk or at unsafe place when not in use as well as desktop controlling to be not displayed any key information whenever it is not in use.

8.4 Network Access Control

The objective is to control access the Company's networked service.

Information technology division must establish the access control of network and networked service policy especially to prevent unauthorized access.

Information technology division must prevent access auditing ports and configuration ports covering both physical prevent and networked access prevent.

Information technology division must segregate networks in groups of information services classified by users and information such as internal zone, external zone etc. in order to systematically control and firewall.

The segregation in networks must be developed in network diagram format which details the scope of internal and external network and updated regularly.

Information technology division must restrict the access right to control users using only authorized network.

Information technology division must restrict sharing network routing.

8.5 Operating System Access Control

The objective is to prevent unauthorized access to operating system.

Information technology division must set a log-on procedure to be secured such as configuring the operating system access to fail when users entering incorrect password more than 3 times etc.

Information technology division must assign system users to prove their identity before gaining access to the system.

Information technology division must provide checking quality of password systems or methods and force users to change passwords at the specified time.

Information technology division must establish the control of using system utilities to prevent unauthorized access which are as follows:

- Prove personal identity before access
- Segregate utility program and system program
- Restrict the use of utility program to be only for assigning person.
- Log the access of utility program such as system users

Information Technology and communication function must disable the time-session of clients when clients are inactive for a defined period by screen lock, re-establishment of the session with only a valid password provided.

8.6 Application and information access control

The objective is to prevent unauthorized access to information and information system.

Information Technology and communication function must control the use of information in information system that is assigning access right to execute such as authorized to write, read, delete. There must be defined the users granted to execute and reviewed executed information to ensure that only necessary content is available.

Assigning user account right to execute in the privileges level such as root or administrator must be considered to assign users as the necessary and define the appropriate time frame of access corresponding to the responsibilities.

External parties must consent to comply with the Company's ICT Security Policy strictly before being permitted to access information system.

Information Technology division must segregate the key or risky information system such as segregation of internet and intranet using within the Company.

8.7 Information Technology Access Control

The objective is to prevent unauthorized access to information.

Access to information right must be controlled and considered to approve upon necessary to secure information effectively including segregate users' right and duty.

8.8 Mobile Computing

The objective is to control use of mobile computing and tele-working facilities to perform securely.

Measures must be adopted to protect data and information asset within mobile computing (notebook, palmtops, laptop) and different medias when off-site working; for example,

- Set password to lock screen.
- Set password to protect significant data.

Article 9

Information System Acquisition, Development and Maintenance

9.1 Security Requirements of Information Systems

The objective is to secure the information systems.

Information technology division must specify obviously the requirements for security system, both in-house developed and commercial system.

The division responsible for information technology system must analyze information technology system regarding any risk exposures that may cause data damage, by emphasizing on the following issues;

- Action procedure prior to the damages, such as information back-up, back-up network system

- Action procedure after the damages, such as information recovery plan, information recovery period.

9.2 Correct Processing in Applications

The objective is to prevent information errors occurred by data correctness, loss, and incorrect modification.

Information system developer must validate data input which are detecting range values input, detecting characters input, detecting the integral field of data input etc. in order to ensure the completeness and not lead to system damage.

Information system developer must analyze area of risk to identify potential risk that damage data.

Information system developer must established practice for computing checks and controls to detect errors.

Information system developer must established practice for detecting data transferring in the information system to ensure that data in information system is safe and completely correct.

Information system developer must set the procedures of detecting, testing, and computing to ensure that the system is validated and the output is accurate.

9.3 Security of System Files

The objective is to operate the information activities securely.

Information system developer must control the installation of new software, library software, and patch vulnerability software on the in-used and service delivery facilities. All software must pass the pilot testing before being installed in the production module.

The use of sanitized production data in a testing environment must be authorized by the information owner prior to being used for testing purpose. Sanitized production data must be deleted immediately when testing is completed and recorded as the evidence of testing sanitized production data identified the scope of testing; date, time of testing and involved division. All must be informed over to the information owner.

Information system developer must restrict access to production or service system source code such as

- Source code must not be held in production facilities and must be kept in secured repository.
- Source code in the testing process and in production must be segregated.

9.4 Security in Development and Support Processes

The objective is to maintain the security of information system software and information.

Information system developer must place the procedures in controlling all changes to information system software that is being used or provided service; for example,

- Requests to change must be authorized.
- Requests must be approved by authorized person.
- There must be controlling potential side effect of changing.
- When changes are completed, the receiving inspections must be approved by authorized person.
- All requests must be logged.

When systems are changed, information system developer must review and test to ensure there is no adverse impact on organizational operations and security.

Modification to software packages must be limited to necessary changes and all changes must be tested and documented in order to be usable when modified in future.

Information system developer must prevent opportunities for information leakage; for example, sniffer with external signal cable, falsification, using software that might be leak information.

Outsourced software development contract must be clear and mentioned the agreement of license software, software usage, and system auditing in detail prior to installation including certified system qualification and specifying the area of outsourced software development.

9.5 Technical Vulnerability Management

The objective is to secure information software and information in system in order to reduce risks resulting from exploitation of published technical vulnerabilities.

Information technology and communication function must follow up news information relevant to technical vulnerability of information systems and assess the risk posed by un-patched vulnerability as well as take the measures to reduce that risk.

Article 10
Business Continuity Management

The objective is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems and to ensure their timely resumption.

A process must be developed and maintained for business continuity, managed and revised regularly.

The Company's business continuity process must be tested regularly.

Article 11
Compliance

11.1 Compliance with Legal Requirements

The objective is to avoid breaches of any both of criminal law and civil law, statutory, regulatory or contractual obligations.

Information technology division must study and identify all relevant legal regulatory and contractual requirements to the use of the Company's information technology.

All Employees must acknowledge, be understand, and strictly comply with identified relevant legal regulatory and contractual requirements to the use of the Company's information technology at least as the followings:

- Information technology and communication security policy
- Computer-related Crime Act
- Electronic Transactions Act
- Use of Electronic Transaction in Public Sector Royal Decree
- Copy Right Act

Information created, maintained, or transferred through the Company's information system is regarded as organizational property (except information regarded as clients' or external parties' property including software or facilities guarded by the patent or external parties' property right). The Company is able to disclose or use the information for evidence in detection without user notification.

According to the purpose of managing and securing organization's information technology, the organization reserves the right to inspect the use of computers, computer system, and network by users to ensure that the usage is complied with the policy including access to review and check users' e-mail without user notification. However, the checking is performed when necessary and there must not disclose any users' information except for court decree in accordance with legal enforcement or users' consent only.

All employees must not exploit the Company's asset and information technology system or perform any action against the law of the Kingdom of Thailand and international law under no circumstances.

The use of material covered by intellectual property rights provided by the Company must be complied with copyright formality and beware of piracy.

There must be implemented compliance with software copyright including control of implementation according to obtaining software copyright which are holding software registration as evidence of ownership, regular checking the validation of installed software copyright.

Users must not use, copy, or publish photographs, songs, articles, books or any documents within the scope of piracy or install pirated software in the Company's information technology system strictly.

There should not copy any installed software in the Company's computers for any unauthorized purposes to ensure that employees don't pirate unintentionally or accidentally.

11.2 Reviews of Security Policy and Technical Compliance

The objective is to ensure that systems are in compliance with security policies.

Information technology division must check all system within division for compliance with security policies at the specified time.

Information technology division must check technical detail of systems in use or providing service at the specified time to assess adequacy of security which are system intrusion detection, securing parameter configuration and also system detection by vulnerability scanning and penetration test to detect system defect.

11.3 Information System Audit Considerations

The objective is to minimize interference to/from the information systems audit process.

Information technology division must plan all audit system activities to minimize the risk of disruptions to business processes.

Information technology division must protect software audit tool to prevent any misuse or protect critical information resulted from the software audit tool.