CK Power Public Company Limited and subsidiaries

Re: Guidelines for information security

Effective as of November 21, 2019

Objectives

1. To ensure the security as well as the operational continuity and efficiency of the Company's information technology and communication system, which will in turn ensure the credibility of transactions in accordance with security standards for electronic transactions.
2. To provide guidelines for executives, system administrators, and system users and raise awareness of the significance of safeguarding the security of the Company's information technology and communication system.
3. To prevent users and related parties from committed a wrongful act in accordance with the Computer Crime Act B.E. 2560.
4. To establish standards, guidelines, and practices for executives, users, system administrators, and external organizations working for the Company in order to raise awareness of the significance of safeguarding the Company's information technology systems during their performance of duty and ensure strict compliance with such standards, guidelines, and practices.

CKPower recognizes the importance of risk management both from the perspective of a holding company and of an electricity producer and distributor. The risk management process constitutes a key factor that enables the Company to prepare for and respond changes in the business landscape in a suitable and timely manner as well as accommodate opportunities for future business growth in a sustainable way.

Scope

To ensure that the information technology system of CK Power Public Company Limited is suitable, efficient, secure, and continuously functional and to prevent potential issues that may arise from improper use of the information technology system and other threats, the Company has deemed it appropriate to define an information technology security policy that prescribes standards, guidelines, and procedures across various aspects of information technology security and threat prevention.

Definitions

"**Company**" refers to CK Power Public Company Limited

"**User**" refers to an individual authorized to use, manage, or maintain the Company's information technology and communication system.

"**System administrator**" refers to the director of the Information Technology Department or any individual assigned to supervise the management of the Company's information technology and communication system.

"**Officer**" refers to personnel of the Company and external parties authorized to access the Company's information technology and communication system.

"**User rights**" refer to the authorization assigned to users to access the Company's information technology and communication system.

"**Asset**" refers to the Company's computer data, computer systems, or information technology and communication assets, such as network equipment and copyrighted software.

"**Access control**" refers to the control and restriction of the rights to access the Company's information technology and communication system related to the provision of services and data as required by usage, with prevention of unauthorized access by both internal and external individuals.

"**Information security**" refers to the maintenance of confidentiality, integrity, and availability of the data in the Company's information technology and communication system.

"**Security incidents**" refer to incidents in the Company's information technology and communication system that are suspected to ultimately compromise or damage it, leading to a violation of the Company's information security policy, such as authorizing access to a third party, failure to set a password for system access, disclosure of material documents to an external party, malware,
network intrusion, and unauthorized disclosure of material data.

"**Unwanted or unexpected security incidents**" refer to incidents that are unwanted by system administrators or incidents that damage the Company's information technology and communication system and are not anticipated by system administrators, such as malware, software errors, network intrusion, alterations or loss of material data, alternations of the webpage, unauthorized disclosure of material data, denial-of-service attacks, disruption to computer systems and networks, and other incidents that violate the Company's security policy.

"**Information Technology Department**" refers to a unit that carries out operations related to the Company's information and computer systems and serves as the Company's information center. It is responsible for conducting studies and analysis to improve the Company's information and computer systems and collaborating with or supporting other relevant units in various operations.

"**Computer data**" refers to data, texts, commands, programs, or other entities in a computer system that can be processed, including any electronic data according to laws on electronic transactions.

"**Computer system**" refers to a computer device or a set of computer devices that are functionally connected, with prescribed commands, programs, or other entities and instructions that enable the computer device or the set of computer devices to process data automatically.

"**Communication network**" refers to a system used in communication, connection, or transfer of information between the Company's information technology systems. The connection may be either via wire or wireless. Communication networks include local area networks (LAN), wide area networks (WAN), an intranet, and the internet.

"**Intranet**" refers to an internal communication network that connects computer systems in an organization for the purpose of communication and exchange of data and information within the Company.

"**Internet**" refers to a communication system that connects the Company's computer systems with the global internet network.

"**Information**" refers to data that has been processed and organized and can be in the form of numbers, texts, or graphics that are easily understood by users and can be utilized in planning, decision making, and other purposes.

"**Information technology and communication system**" refers to the Company's system consisting of computer systems, databases, and networks that officers who use the system, system developers, system administrators, and the Company's executives jointly utilize to determine objectives, gather, store, and process data, and send obtained results or information to system users and the Company's executives, so that they can be used in planning in support of operations, decision making, management, analysis, and performance monitoring of different units at different levels in the Company.

"**Password**" refers to letters, characters, or numbers that are used for identity authentication to control access to data and data systems in order to ensure the security of data and of information technology and communication system.

"**Information security**" refers to the protection of the security of the Company's information technology and communication system. It consists of the three following basic properties:

1. Confidentiality refers to the act of keeping data confidential and allowing only authorized individuals to access such data.
2. Integrity refers to the assurance that the data will not be subject to any action that results in alteration by unauthorized parties, whether or not such an action is deliberate.
3. Availability refers to the assurance that data and all information technology and communication systems are ready for service when required.

"**Protocol**" refers to step-by-step details that must be followed to achieve the standard defined in accordance with the objective.

"**Guideline**" refers to an instruction that is not compulsory but is recommended to facilitate the achievement of goals.

"**Malware**" refers a program that damages, destroys, alters, or disrupts the information technology and communication system or causes the system to operate differently from prescribed commands.

"**Electronic mail (e-mail)**" refers to a system that individuals use to receive and send messages via computers and connected communication systems. The data that is sent can be either letters, images, graphics, animations, or sounds. Senders can deliver news to a single recipient or multiple recipients. The standards for the reception and delivery of such data include SMTP, POP3, and IMAP.

Guidelines for the Company's Information Security

1. Security of the access control of the information technology and communication system

1.1 User access rights control

- User access rights must be assigned with consideration to the roles and responsibilities of users in each division towards the data.
- Users must submit an access right request to the Information Technology Department either in writing or via the IT Service Request System.
- The Director of the Information Technology Department or authorized person shall consider the approval of such requests.

1.2 User rights management

- Information technology system administrators assign access rights to the information technology and communication system that suit the user's service access and roles and responsibilities according to the Company's regulations. Such access rights are to be reviewed whenever users are transferred/transition to a new position in the Company or resign or retire on a regular basis or at least once a year.
- System administrators must assign rights and passwords to new user accounts for their first-time use for authenticating the identity of users of the information technology and communication system.
- When a new officer is recruited, the Human Resources Department/the affiliated unit must immediately submit an access rights request to the Information Technology Department either in writing or via the IT Service Request System so as to create a user account and assign user rights as requested.
- When an officer resigns or when their roles and responsibilities indicated in the user right request are changed, the Human Resources Department/the affiliated unit must immediately submit a rights revocation request to the Information Technology Department either in writing or via the IT Service Request System to withdraw the rights of the individual who resigns or change their rights in the system or temporarily deactivate their account before deleting all the information of the officer within seven days of receiving the request.
- Unauthorized users are prohibited from intruding into the information technology and communication system by any means.

1.3 User password management

- System administrators assign initial passwords to users or use an automatic password generator system. The system must not display passwords on the screen.
- The system must require users to change their password during their first login.
- The system must allow users to provide incorrect passwords no more than six times (accounting and finance system).
- System administrators must prescribe periodic password changes, taking into consideration levels of classification or mission-dependent materiality. The system must also record the history of password changes to prevent repeated passwords. For example, the finance and accounting system must require a password change every 90 days.
- Users should report username and password issues, such as forgotten usernames or passwords, to system administrators either in writing or via the IT Service Request System.
- The password must be given to the user in a secure way along with the "Password Guidelines." The user must also be informed that they must strictly follow the guidelines.

1.4 Use of user passwords

- Users must use their own username and password to access the system to prevent denial of responsibility.
- Users who have received the password for first-time login or a new password must immediately change their password.
- Users must create a password and change their password regularly or at least every 90 days or according to the criteria established by system administrators. Users must also agree to allow system administrators to perform any action to ensure the security of the information technology and communication system.
- Users must keep their password confidential and prevent it from being exposed to others. Also, users must not give their password away for any reason, except when a user with authority in the information technology and communication system is unable to perform their duty and may as a result interrupt the continuous operation of the information technology and communication system, in which case an interim must be appointed for that period as evidence for verifying the use of rights. Once the interim has completed their duty, the user who is the password owner must immediately change the password.
- The password must contain 8 characters or more and include a combination of regular letters, numbers, and symbols.
- Do not use common passwords, such as abcdef," "aaaaaa," "12345."
- Do not use personal information in passwords, such as first and last names, date of birth, address.
- Do not use words that can be found in dictionaries as passwords.
- Do not use personal passwords in accessing shared folders on a computer network.
- Do not use computer software that automatically store personal passwords.
- Do not write down or store personal passwords in a place that leaves them easily noticeable.
- Users must not use the same password for work and personal use.
- Users must immediately log off when not using the system to prevent others from using their right of access to the information technology and communication system without permission.
- Users must immediately change their password if a leak is suspected.

1.5 User access management

- Users must be authorized by officers responsible for data and work systems.
- Data owners and/or system owners will authorize users to access only the part of the system that is suitable to the roles and responsibilities.
- System administrators are responsible for validating approvals and assigning user access rights. To request permission to access the work system, users have to submit a memo and fill out the IT service request form as required by the Information Technology Department. As a record, the form must be approved and signed by an authorized individual who is a data owner and/or a work system owner.
- A registration procedure for new officers has been prescribed. In case of job transfer/transition/resignation/retirement within the Company, the affiliated unit/user is required to fill out and record the IT service request form as required by the Information Technology Department to have their rights granted or revoked.
- New users or affiliated units must fill out the IT service request form for registration. The form must be approved by the head of their affiliated units and then submitted to the Information Technology Department.

- System administrators will assign appropriate rights of access to the information technology and communication system according to the roles and responsibilities of users. The rights must be approved by an authorized individual in writing and will be reviewed on a regular basis, or at least once a year, or upon job transfer/transition/resignation/retirement, or in the event that the affiliated unit submits a memo to the director of the Information Technology Department or authorized person to request the granting or revocation of rights.

1.6 Data access management according to data classification

- The system must be maintained. Data classification, data storage protocols, access control protocols for both direct access and access via the work system, and methods of deleting data at each level of confidentiality must be established.
- Data owners must review rights of access of these users at least once a year to ensure that they remain suitable.
- According to data access protocols for each level of data classification, including both direct access and access via the work system, system administrators must assign user accounts and passwords for user authentication at each level of data classification.
- Data classified as “confidential” and above that is sent or received via public network must undergo encryption according to international standards, such as SSL, VPN, and HTTPS.
- Data security measures must be put in place when a computer is taken out of the area of the department. In the event that a computer is taken away for maintenance, data owners must first back up the data to storage media and delete any important data stored from the computer.

1.7 Communication network access control

This control applies to individuals who access communication networks. It systematically prevents intrusion and allows access to information systems only to authorized individuals. System administrators must design a communication system according to the group of information technology and communication systems in operation, user group, and group of information systems, such as internal zone, external zone, and DMZ zone. Therefore, security measures must be established as follows.

- Users can access only services in the information system for which they are authorized to access.
- Users wishing to access the communication network must submit a request by filling out the form in the IT Service Request System and receive a written approval from the director of the Information Technology Department or authorized person.
- System administrators must register user accounts and set appropriate network access permissions according to the roles and responsibilities of each user before their first use. These access permissions must be reviewed at least once a year.
- System administrators must register every device that connects to the communication network by submitting a computer and communication network device registration form in the IT Service Request System.
- System administrators provide network management system software that can perform equipment identification at the levels of IP address, computer names, and MAC address.
- Network diagrams must be created and regularly updated.

- Communication networks must be segregated for protection and access control into sections/groups, namely public sections, internally connected sections, sections related to vital assets, and hazardous sections, and information service groups, user groups, and information system groups.
- VLAN is employed in each section/group of communication networks, such as information service groups, user groups, and information system groups
- Gateways are installed to keep communication networks segregated and control data communicated between them.
- Equipment in communication networks must be set so as to enable the control or screening of data communicated between the networks.
- Control and prevention measures must be put in place to ensure security, such as user authentication, passwords, self-selected frequency channels.
- Computer data traffic must be stored in compliance with the Computer Crime Act B.E. 2560.
- The functioning of the communication networks and network equipment must be inspected on a daily basis.
- Settings and configurations must be correct, appropriate, and current.
- Surveillance must be implemented for communication networks.
- The settings of network devices must be backed up.
- Patches and releases for system software and firmware must be updated.
- The equipment and the server computer that provide services in the Company's communication networks must be inspected for vulnerabilities.
- Penetration testing must be conducted on communication systems.
- Control on internal access to communication networks and network connection must be implemented.
- Requests for installing connecting points to the computer system and network control room must be submitted in writing and approved by the director of the Information Technology Department or authorized person.
- Users' permission to access or use networks must be overseen and adjusted regularly.
- Devices for screening received and sent data, such as emails, data folders, interactive access, chats, and access to applications, must be provided.
- Limits on the time of the day or periods of time for connection permission can be imposed as deemed necessary.

1.8 Network routing control

- Network routing must be controlled on network devices, such as core switches, edge switches, and routers.
- Gateways must be made available to validate the start and end points at control points between internal networks through the use of proxy servers or network access controllers (NAC).
- Appropriate protocols, permissions, and IP addresses for the network connection of devices and network users must be established.
-Protocols and ports for each user group must be specified, such as HTTP, FTP, SMTP, and TELNET.
- VLANs must be specified for permission control and setting.

1.9 User identification and authentication

- Users must authenticate their identity by providing their username and password to access the network.

1.10 Installation of firewall devices for network security

- System administrators are responsible for managing, installing and configuring all firewalls; changing the settings of firewall devices each time, such as parameters; configuring service settings; and configuring network settings so that they can be connected to the Company's communication networks, with the approval of the director of the Information Technology Department or authorized person.
- The default settings of every communication network must be set to deny-all.
- All unauthorized connections to the internet or internet services via any route must be blocked by firewalls.
- Access to firewall devices must be given only to individuals authorized to manage them.
- All inbound and outbound traffic data of firewall devices must be stored on the devices.
- Stored traffic data must be reliable and encrypted to prevent editing or alteration. Traffic data must be stored for at least 90 days.
- System administrators must inspect incidents, traffic data, usage behavior, and activity and record the amount of network access data on a daily basis.
- To specify internet services for clients, firewall ports will be opened for connection to authorized basic programs. If there arises a need to use programs other than those specified, a special port opening must be submitted in writing and approved by the director of the Information Technology Department or authorized person. In configuring services in the server computer of each section of a communication network, the firewall must be configured to allow only connection ports that are necessary for the service and must be individually specified to server computers that are in service.
- Server computers that provide service to information systems must not allow internet connection, except when necessary on a case-by-case basis.
- The settings of firewall devices must be backed up every week or every time the settings are changed.
- System administrators are authorized to suspend the use of computers with usage behavior that violates policies or with a program whose operation poses security risks until it is rectified.
- Remote login from outside through a communication network to a server computer or devices on internal communication networks must be logged on the list of operations according to the firewall service request form and must be approved by system administrators first.
- Violators of the firewall security policy will face an immediate suspension of their internet access or connection to internal communication networks.

1.11 Installation of intrusion detection and prevention systems (IDS/IPS)

- IDS/IPS is installed to inspect or monitor incidents arising from abnormal usage of the organization's computer systems or communication networks, such as attempts to undermine the confidentiality, integrity, and availability of data or evade the security system of the information technology and communication system. Such intrusions arise when intruders access the system via the internet or when an internal user accesses or performs something unauthorized or when a user tries to abuse their privileges.

- IDS/IPS must be installed to cover the Company's entire computer system and communication networks as well as all traffic data routes to external and internal communication systems.
- All computer systems accessible via external communication systems or the internet must be validated by IDS/IPS.
- Computer traffic data that goes in and out of the IDS/IPS system must be stored for at least 90 days.
- System administrators must check and update patches and signatures of the IDS/IPS system at least once per month or whenever a new signature update is available.
- System administrators must inspect incidents, traffic data, usage behavior, and activity and record the amount of network access data on a daily basis.
- The IDS/IPS operates under basic control rules of the firewalls used for accessing the information technology and communication system.
- All behavior usage, activity, or incidents that pose risks of system intrusion and attack, as well as suspicious behavior and attempts to access the system, whether successful or unsuccessful, must be reported to supervisors up the chain of command upon detection.
- System administrators are authorized to terminate any connection to a communication network of a computer with behavior that poses risk of intrusion to the information technology and communication system without prior notice to the user and report such termination to the supervisor.

1.12 Remote communication network access control

- Permission to remotely access the information technology and communication system or computers via communication networks must be given on the basis of necessity. Firewall ports or communication systems must not remain open when not necessary, and remote access to the information technology and communication system must be immediately disabled when not in use.
- Any methods for remotely accessing the information technology and communication system or computers must be approved by the director of the Information Technology Department or authorized person according to the firewall service request form, and stringent control must be put in place before they are used. Users must also strictly comply with the access requirements.
- To be granted permission to remotely access the information technology and communication system or computers via communication networks, users must show proofs of reason or operational necessity and must obtain the approval of the director of the Information Technology Department or authorized person

-For remote access to the information technology and communication system or computers via computers, mobile computers, mobile computing devices, or mobile devices, there must be strict control of the engaged firewall ports and clear frequency channel division.

- Remote users must authenticate their identity by providing their username and password. Such access to the information technology and communication system or computer system via internet will also be verified to authenticate users' identity.

- Instead of passwords, special authentication tools must be deployed for accessing information technology systems related to data at the internal level as well as the confidential level and up, such as the use of token when operating outside the organization.

1.13 Wireless communication network access control

- System administrators must designate proper placement of access points to ensure that their signals do not extend outside the working area so as to prevent attackers from transmitting or receiving the signals from outside the building or controlled perimeter.
- System administrators must choose appropriate transmission power for the working area and inspect whether the signals leak out of the area.
- System administrators change factory default SSID (Service Set Identifier) settings, usernames, and passwords as soon as access points are deployed.
- System administrators must configure encryption settings between signal receivers and access points to impede interception and ensure security. The minimum requirement is WPA (Wi-Fi Protected Access).
- System administrators must select a MAC address or a username and password for a user authorized to access wireless communication networks and give permission only to devices with the defined MAC address, username, and password.
- System administrators must install firewalls between wireless communication networks and the Company's internal communication networks.
- System administrators must deploy software or hardware to verify the functionality of computers/devices authorized to connect to wireless communication networks and store computer traffic data of wireless networks for at least 90 days.

1.14 Access control in operating systems

This control applies to individuals who access operating systems under the Company's communication networks. To protect the security of data and resources, the following security measures have been established:

- Users must authenticate their identity by providing usernames.
- User authentication will be automatically activated from Active Directory (AD) or a RADIUS server upon accessing an operating system.

1.15 Installation of utility software for operating systems

- Do not install pirated software.
- Install only task-related programs and do not install non-work-related programs.
- The Information Technology Department specifies session timeout for the information technology and communication system when it is not in use for a certain period of time.
- The information technology and communication system must be set to suspend operation or deactivate when there in no activity within a period of 3,600 seconds to prevent unauthorized data access.
- A mechanism for deactivating applications and automatic connections to systems when not used within the defined period of time must be put in place.

1.16 The Information Technology Department establishes limitations of connection time for the information technology and communication systems or applications with high risks or high significance to ensure security as follows.

- Define session-timeout for connections to the information technology and communication system used in operation when the user is not using the system for over 3,600 seconds

1.17 Application access control applies to access to the Company's information technology system and applications. To ensure data security, the following security measures have been established:

- Operating environments must be separated. Server computers installed with significant operating systems are designated to the server zone, while server computers for general users, which are sensitive to interference and at great risk and must thus be specially monitored, are designated to the demilitarized zone (DMZ).
- User authentication before accessing the system must be implemented in accordance with "guidelines for user password management" and "guidelines for permission management."
- Passwords must be encrypted by the system to prevent them from being exposed to others.
- Automatic session time-out must be put in place for when no user response is detected for over 3,600 seconds.
- Data classified as confidential in databases must be encrypted.

2 Guidelines for control room and network room management

2.1 Physical security management

The data center, which is an area that houses the information technology and communication system, is divided into key zones as follows:

- Server and server equipment zone
- Air-conditioning system zone

2.2 Physical entry controls for control and network rooms

- Processes for permission request, authorization, and access control for control and network rooms must be put in place.
- A system that automatically logs the date and time of each entry in relation to each individual must be put in place for verification later when necessary.
- The use of ID cards and fingerprints or ID cards and password for the authentication of authorized individuals must be implemented as part of physical entry controls for control and network rooms.
- The operation of external parties in control and server rooms must be supervised and monitored until its completion to prevent loss of assets and unauthorized physical entry.
- External parties must wear visible identification throughout the entire duration in control rooms.
- Unauthorized persons are not allowed in important areas or zones in control rooms.
- Foster understanding and awareness of rules and regulations that must be followed while in control rooms.
- Permissions must be reviewed regularly, and permission to access control rooms must be immediately revoked upon any change

2.3 Equipment siting and protection in control and network rooms

- Each type of equipment must be sited in designated areas.
- No food and drinks are allowed in control rooms.

- The environment of control rooms must be inspected, surveilled, and maintained to prevent damage to equipment inside, such as by checking and keeping the temperature and moisture at normal level.

2.4 Supporting utilities in control and network rooms

- Supporting utilities for the Company's information technology and communication system must be sufficiently provided and include the following: power and backup power system, precision air conditioning system, access control system, environmental monitoring system, closed-circuit television system, equipment and network cabling systems, KVM switches, and emergency power system.
- Supporting utilities must be regularly inspected or tested to ensure normal functionality and reduce risks of failure.

2.5 Cabling security in control and network rooms

- Conduits must be used to prevent interception or damage from cutting.
- Power cables must be segregated from communication cables to prevent interference.
- Equipment cables must be labeled to prevent cutting wrong cables.
- A complete, correct, and current diagram of communication cables must be created.
- Cable racks and cabinets must be securely bolted to prevent access by external parties.

2.6 Equipment maintenance for control and network rooms

- Maintenance must be carried out at three-month intervals.
- Manufacturers' maintenance recommendations must be followed.
- Each maintenance must be logged for inspection or assessment later.
- Issues and defects must be recorded for assessment and improvement of relevant equipment.
- The operation of computer system maintenance companies must be controlled and supervised. Off-site equipment repair must be controlled to prevent loss and unauthorized data access.
- Access to equipment containing material data by maintenance companies must be approved to prevent unauthorized data access.

3 Security for the use of computers

3.1 Use of computers by users

- Assignment, change, and storage of user passwords must be in accordance with Item 1.4: Use of user passwords
- Users must log off immediately when not using the information technology system to prevent others from using it. In case of suspected leak, users must immediately change their passwords.
- Unauthorized individuals are not allowed to intrude or access the information technology system by any means.
- Users are not allowed to install other software or programs into work computers or install additional network equipment or connect the operating computer network with other networks outside the Company or bring their own personal computers to use with the Company's information technology system, unless permitted by system administrators.
- Files in work computers must not be shared except on a work system prescribed by the Company. If necessary, file sharing must be enabled only for the required duration and immediately disabled once it is no longer in use to prevent potential damage to the computer system and data.

- Users must not download any data or programs that are not related to work or from unreliable websites with dubious security.

3.2 Use of personal computers

- Authorized personal computers are the Company's assets and must therefore be used carefully and efficiently.
- Programs to be installed in personal computers must be approved by the Company or lawfully copyrighted. Users are prohibited from copying, installing, or altering any programs and installing them on personal computers that do not belong to the Company or illegally giving them to others for use.
- Media such as CD, DVD, and flash drives that are used with personal computers outside the information technology system or are from dubious data sources must not be used with personal computers operating in the information technology system without prior inspection and virus removal.
- Users are responsible for ensuring the safety and security of personal computers operating in the information technology system.
- Antivirus programs must be installed, and virus databases in personal computers must be regularly updated.
- Users must turn off the personal computers that they use when the task is completed.
- Users must not use personal computers that do not belong to the Company with the Company's information technology system, unless permitted by system administrators.
- Users must scan attached files in emails or files downloaded from the internet with an antivirus program before using them.
- Users must inspect any data containing malware that damage, destroy, or alter data, computer systems, or other programs or cause them to operate differently from prescribed commands.
- Users must make backups of personal computers in other storage media, such as CD, DVD, and external hard disks.
- Backup media must be stored in a suitable place where they are free from risk of data leak. Data recovery testing should be conducted regularly. Backup media that are no longer in use must be formatted, so that any backups inside can no longer be used.
- Assignment, change, and storage of user passwords must be in accordance with Item 1.4: Use of user passwords

3.3 Use of mobile computers

- Authorized mobile computers are the Company's assets and must therefore be used carefully and efficiently.
- Programs to be installed in mobile computers must be approved by the Company or lawfully copyrighted. Users are prohibited from copying, installing, or altering any programs and installing them on mobile computers that do not belong to the Company or illegally giving them to others for use.
- Users should study and follow manuals closely for safe and efficient usage.
- Users must not modify or alter any components of mobile computers and must maintain their original and ready-to-use condition.
- Mobile computers must be put in bags for mobile computers when transported to prevent damage from impact, such as a fall from a desk or from users' hands.

- For non-touch screen computers, avoid using fingers or hard objects such as pencils to touch the screen as it may be scratched or damaged.
- Do not place an object on top of the screen and the keyboard.
- Screens should be wiped as gently as possible and wiped in the same direction, not in a circular motion, which can cause scratches.
- Users are responsible for prevent the loss of mobile computers. For instance, mobile computers should be locked when not in use and not left unattended in public places or any location where there is a risk of loss.
- Mobile computers must not be stored or used in places with high levels of heat/moisture/dust and must be protected from falls or impacts.
- Usernames and passwords must be assigned for accessing the operating system of mobile computers.
- Assignment, change, and storage of user passwords must be in accordance with Item 1.4: Use of user passwords
- Users must turn off the mobile computers that they use when the task is completed or when they are no longer in use.
- Users must make backups of mobile computers in other storage media, such as CD, DVD, and external hard disks.
- Backup media must be stored in a suitable place where they are free from risk of data leak. Data recovery testing should be conducted regularly. Backup media that are no longer in use must be formatted, so that any backups inside can no longer be used.

4 Security for the use of the internet and electronic mail

4.1 Use of the internet

- System administrators must register computers connected with the Company's internet system to make it possible to locate the unit of the Company in which a computer is being used.
- Users/Human Resources Department must submit a written request for access rights and password for authentication in the Company's internet system. Each user must protect and prevent their access rights and password from being used by others and take responsibility for any ensuing damage in case of violation of the Computer Crime Act without deniability.
- Users must not use the internet while using multimedia data or downloading non-work-related data or taking up bandwidth.
- System administrators must route computer connections to the internet through security systems, such as proxies, firewalls, ISP, and IDS.
- Before accessing the internet through a web browser on personal computers, mobile computers, and mobile computing devices, antivirus programs must be installed and vulnerabilities in the operating system in which the browser must be patched first.
- Users must not use the Company's internet for personal business or to access inappropriate websites, such as those that are contrary to good morals, are against the nation, religion, and monarchy, or pose social threats.
- Users are assigned rights to access data in accordance with their roles and responsibilities to ensure network efficiency and the data security of the Company as approved by system administrators.
- Users are prohibited from disclosing confidential information related to the Company's business that has not been officially announced on the internet.

- Users must exercise caution in downloading programs from the internet and must not commit an intellectual property infringement.
- Users must immediately log off the internet after use to prevent use by others.
- Users must strictly comply with the Computer Crime Act.

4. Use of electronic mail

- System administrators must register computers connected with the Company's internet system to make it possible to locate the unit of the Company in which a computer is being used.
- Users must use the Company's email system only to receive and send emails related to the Company.

- Users must exercise caution in using emails so as not to damage the Company, cause annoyance to others, or act in contrary to good morals and must not exploit the use of the Company's email system.
- Users must immediately log off the email system after use to prevent use by others.
- Before opening attached files in emails, users must always scan such files with an antivirus program.
- Users must not open or forward an email or a message received from an unknown sender.
- Users must inspect their email inbox on a daily basis and organize their files and emails to keep them to a minimum.
- Users must regularly make backups of vital data in emails.

5 Security of asset and network management

5.1 Computer data management

5.1.1 Defining data types

- Character data refers to data consisting of letters and numbers not used for calculations, such as document numberings.
- Numerical data refers to numbers used exclusively for calculations, such as numbers of goods ordered.
- Graphic data refers to still images, animations, drawings, photographs, and video images, such as document scans.
- Audio data refers to sounds and other data that can be perceived by hearing, such as sound recordings of a meeting.

5.1.2 Defining levels of data classification

Level 1 - Public data

Public data refers to data that is accessible by the general public without any restrictions, data that does not affect the Company's operations and can be made available to the public, or data that must be disclosed as required by the law. The disclosure of this data, either in part or in its entirety, does not negatively impact the Company. An example is the data published on the Company's website.

Level 2 - Internal data

Internal data refers to data that the owner has deemed can be made available to personnel within the company, but not to external users as it can damage the Company. The disclosure of such data depends on the discretion and approval of the owner or may be required by law. Examples of such data are data in the Company's personnel system and registration system.

Level 3 - Confidential data

Confidential data refers to data that the Company has deemed cannot be made available to every user. Such data is restricted to relevant parties that need it for their operation and accessible on a need-to-know basis. The data is essential to company operations, is considered internal data, and cannot be legally disclosed to unrelated external parties, as it may cause damage to the Company. The disclosure of such data must be approved by the owner of the data or required by the law. Examples of such data are data on salary and disciplinary actions.

Level 4 – Highly confidential data

Highly confidential data refers to internal data used by authorized users of the Company. Such data requires special access codes and cannot be disclosed to the public as the data is vital to the Company's operations and may cause severe damage to the Company. The disclosure of such data must be approved by the owner of the data or required by the law. Examples of such data are traffic data and e-mail data.

Level 5 - Top secret data

Top secret data refers to internal data used only by high-level executives of the Company. Such data requires special access codes and is used in making key deliberations and decisions within the Company. The disclosure of such data to outsiders is forbidden as it is highly sensitive and may cause severe damage to the Company, unless required by the law.

5.1.3 Control of data request, use, verification, and access.

- Officers of the Information Technology Department are not authorized to grant data access to requesters without permission from the director of the Information Technology Department or authorized person, except during a system development process where officers of the Information Technology Department and contractors are responsible for transferring data to the new system.
- In the event that the data requester is an internal unit and the data owner is another internal unit, the requester must submit a memo requesting permission to the unit that owns the data. Officers of the Information Technology Department will provide the required services related to such data only when notified of the permission.
- In the event that the data requester is an external agency, whether a government or private agency, and there exists no prior agreement between the agencies, a written request for permission must always be submitted. If there exists a prior agreement, the data access must be supervised to ensure that the scope of requested data is as specified in the agreement.
- In the event that data requests are submitted to the Company by individuals or juristic persons and there already exist guidelines or protocols established by the Company, the process can be conducted according to such guidelines or protocols.

5.1.4 Defining access time and channels

Internal users can access data via the intranet and the internet. External users can access data via the internet as per agreements between agencies. Data published via the internet can be accessed 24 hours a day.

5.2 Computer system management

- Create an asset control inventory in the computer system
- Specify names and IP addresses in the computer system
- Clearly assign an officer in charge of creating and altering parameters in the system program.
- Any abnormal use or alterations of the parameters detected must be immediately rectified and reported the officer in charge.
- Services must be allowed only as needed. If such services present risks to security systems, additional measures must be implemented.
- Patches of essential systems must be regularly installed to eliminate any vulnerabilities in system software, such as DBMS and web servers.
- Tests should be conducted on system software related to security and overall operational efficiency prior to installation and after maintenance.
- Computer system equipment must be maintained to ensure operational efficiency. Regular maintenance of computer system equipment must be conducted according to schedule specified in the maintenance contract.

5.3 Program management

- Create an inventory of programs
- Register programs for use with license owners
- Update programs to newer versions when new versions are released
- Control versions of applications
- Install licensed programs or freeware/open source programs only as needed.

5.4 Communication network management

- Segregate networks/groups (VLAN/Zone).
- Create an inventory of communication network usage controls.
- Create a communication network diagram and scope.
- Inspect communication networks to ensure operational efficiency.
- Control routing and prescribe access methods for the Company's communication networks.
- Install systems to prevent intrusion and irregular use of the communication networks
- Conduct penetration tests against the communication networks and compile reports of such tests.
- Assign individuals in charge of setting or changing parameters for the communication networks and connected devices.
- Revise such parameters at least once a year.
- The communication networks must be maintained to ensure operational efficiency. Regular maintenance of the communication networks must be conducted according to schedule specified in the maintenance contract.

5.5 Asset management

- Establish an asset inventory that contains the following:
- Officer in charge
- Asset types

5.6 Requisition of computer and network devices

- Users must submit a request for computer and network devices via the IT Service Request System or submit a requisition form, detailing the items required, storage/installation sites, to the officer in charge for approval.
- The officer in charge reviews the request and its appropriateness according to the process and seeks the approval from the unit that is the asset owner or assigned individuals.
- Once the request is approved, the officer in charge must specify the storage/installation sites of the equipment in the IT Service Request System or the computer and network device requisition form to record a device history.

5.7 Computer and network device maintenance request

- Upon encountering irregularities in the working of a device or are unable to use the device, users must submit a maintenance notice to the maintenance personnel by filling out relevant information in the IT Service Request System.
- The officer in charge analyzes damage to the device with the data submitted through IT Service Request and actual testing of the device, taking into consideration its warranty period. If the warranty is still valid, the device can be sent for maintenance by the supplier service center without incurring extra costs detailed in the warranty. If the device is out of

warranty, it is up to the discretion of the officer in charge to either repair or dispose of the device, depending on the conditions.

- During the maintenance of the device, if a replacement is available, the officer in charge must notify the user. A requisition form for computer and network devices must be filled out, detailing the items required, installation sites, and submitted for approval by the officer in charge. The officer in charge must specify the storage/installation sites of the equipment in the IT Service Request System or the computer and network device requisition form to record a device history.
- After having received the repaired device, the officer must inspect the device to recheck the previously malfunctioning part, fill out the maintenance form in the IT Service Request System or the computer and network requisition form, and return the device to the user along with such documents.

5.8 Removal of the Company's assets

- Keep records of permissions prior to the removal of assets to prevent loss and record further information upon the return of assets.
- The officer in charge must take care of the Company's equipment and assets as if they were their own.

5.9 Disposal of computer and network devices

If the device cannot be repaired and is out of warranty, disposal may be necessary considering the cost of the device against repair costs. The officer in charge must fill out the "computer and network device return form" to be acknowledged and approved by the officer who is the task/project owner or supplier.

- The officer who is the task/project owner is responsible for reviewing the return of the device. They may approve the return by signing the "computer and network device return form" or not approve the return, in which case they must state the reasons and send the request back to the officer in charge.
- The request must be submitted to the unit in charge of approving disposal for further consideration.

5.10 Control of printouts from the information technology and communication system

- Assign printing permissions.
- Assign an officer in charge of controlling access to printouts.
- Ensure secure storage of documents related to the system.
- Dispose of unused or misprinted documents.
- Keep records of permissions prior to taking out printouts to prevent loss.

6 Security for data backup and recovery

6.1. Data storage and backup systems must be available for each data type, such as operating system programs, applications, programs, and data. At least one such system must be kept in a separate location to ensure security and operational continuity.

6.2 A person in charge must be designated for making backups, checking the availability, accuracy, and completeness of data at least once a year, and recording inspection details. Any loss, inaccuracy, or incompleteness of data detected must be immediately rectified.

6.3 The frequency of backing up data of a work system must be prescribed, and backups of such data must be made according to the prescribed frequency. (Backups should be made more frequently for work systems with frequent changes, and at least one set of backups must be stored off-site.)

- A correct data backup and recovery process as well as software must be prescribed.
- A backup that is created must be inspected for its completeness.
- Data recovery testing should be conducted at least once a year. Functional testing must also be conducted on all work systems.
- An emergency plan must be formulated to ensure systems can be recovered within a prescribed amount of time. Disaster recovery guidelines are as follows:
- All of the Company's vital work systems must be identified. A list of such systems must be created and must always be updated to reflect new vital work systems.
- Such vital work systems must undergo risk assessment, and measures must be established to reduce detected risks. The risk assessment report must be updated at least once a year.
- Data types, such as software related work systems or data in databases, must be specified.
- Backup frequency and methods for such vital work systems, such as full backup and incremental backup, must be prescribed.

6.5 A disaster recovery plan must be formulated and must include the following:

- The assignment of roles and responsibilities of all related parties
- Risk assessment for vital work systems and measures for reducing such risks as prolonged power failure, fires, earthquakes, and protests that render work systems inaccessible
- Protocols for work system recovery
- Protocols for data backup and recovery tests
- At least one readiness test per year

6.6 Raising awareness and educating relevant officers on the protocols and actions that need to be taken in an emergency

6.7 The recovery plan must be updated at least once a year.

6.8 Data must be backed up according to prescribed data type, frequency, and backup method. Backups must be regularly inspected to ensure their completeness.

6.9 A test should be conducted at least once a year to check whether data in backups can be fully recovered. Any issues during the recovery test must be rectified and recorded, with the solutions documented.

6.10 A meeting must be held to inform all related parties of the details of the data recovery plan. If there are updates to the plan, another meeting must be held to inform all related parties of such updates.

6.11 A plan should be formulated for an emergency in which electronic means cannot be employed in order to ensure operational continuity.

- Forms/printed forms that can be used in place of the forms/printed forms that can be printed from the information technology and communication system must be prepared.
- Revert to the procedure prior to the adoption of the current information technology and communication system, such as the manual system.
- Once the information technology and communication system resumes normal operations, the data created during the emergency must be input into the system.

7 Security for risk assessment of the information technology and communication system

7.1 A risk management committee of the Information Technology Department shall be appointed to:

- prioritize risks
- formulate risk management plans
- carry out risk management plans

7.2 An inspection and risk assessment with regard to information technology and computer system security must be conducted at least once a year.

8 Fostering information technology security awareness

8.1 Public relations activities and training must be carried out to ensure that officers will acknowledge, understand, and refrain from violating the Computer Crime Act B.E. 2560 and other laws related to information technology, as well as use the Company's information technology resources responsibly and appropriately.

8.2 An officer responsible for publicly publishing data on the Company's website must be designated. The Company must carry out the publishing itself and must not allow other parties to perform the task on its behalf.

8.3 The Company's information technology security policy and guidelines must be reviewed and updated to ensure that they are current and meet accepted standards at least once a year.

Please be informed and comply accordingly.

(Mr. Tanawat Trivisvavet)

Managing Director