Objectives

1. To ensure the security as well as the operational continuity and efficiency of the Company's information technology and communication systems, 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 to raise awareness of the significance of safeguarding the security of the Company's information technology and communication systems.

3. To prevent users and related parties from committing a wrongful act in accordance with the Computer-Related Offences Act B.E. 2560 (2017).

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 organization's information technology system during their performance of duty and ensure strict compliance with such standards, guidelines, and practices.

The Company recognizes the importance of risk management both from the perspective of a holding company and of an electricity production and distribution business. 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 to 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 organization has deemed it appropriate to define its 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 systems.

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

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

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

"**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 systems 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 systems.

"**Security incidents**" refer to incidents which have happened to the Company's information technology and communication systems or incidents 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, or unauthorized disclosure of material data.

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

"**Information security**" refers to the protection of the security of the Company's information technology and communication systems. 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 or change by unauthorized parties, whether intentional or unintentional.
3. Availability refers to the assurance that data or all information technology and communication systems are ready for service when required.

"**Protocol**" refers to a set of 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 to a program that damages, destroys, alters, or disrupts the information technology and communication systems or causes the systems to operate differently from the 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 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 to the information technology and communication systems

1.1 Access control to user rights

- Users' access rights must be assigned by taking into consideration the roles and responsibilities of users in each division towards the data.
- Each user 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 any authorized person shall consider approving such requests.

1.2 User rights management

- The information technology system administrators assign access rights to the information technology and communication systems 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.
- The 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 systems.

- 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 30 days after the date of receiving the request.
- Unauthorized users are prohibited from intruding into the information technology and communication systems by any means.

1.3 User password management

- The system administrators assign initial passwords to users or use an automatic password generator system, provided that the system must be configured to prevent the display of the 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 five consecutive times.
- The system administrators must prescribe periodic password changes, taking into consideration levels of data classification or mission-dependent materiality. The system must be configured to record the history of password changes to prevent repeated passwords. For example, the finance and accounting system must require a password change at least every three months.

- Users should report username and password issues, such as forgotten usernames or passwords, to the 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 systems to prevent denial of responsibility.
- Users who have received a password for first-time login or a new password must immediately change their password so received.
- Users must create a password and change their password regularly or at least every three months or according to the criteria established by the system administrators. Users must also agree to allow the system administrators to perform any action to ensure the security of the information technology and communication systems.
- Users must keep their password confidential and prevent it from being exposed to others. Users must also not give their password away for any reason, except when a user with approval authority in the information technology and communication systems is unable to perform their duty and may as a result interrupt the continuous operation of the information technology and communication systems, 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 with a combination of regular letters, digits, and symbols.
- Do not provide common passwords, such as abcdef," "aaaaaa," "12345".
- Do not provide 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 any place where are easily noticeable.
- Users must not use the same password for work operations 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 systems without permission.
- Users must immediately change their password if a leak of such password 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 users' roles and responsibilities.
- The system administrators are responsible for validating approvals and assigning user access rights. To request permission to access the work systems, users have to submit a memo and fill out the "IT service request" form as required by the Information Technology Department. As evidence, the form must be approved and signed by a person in authority 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 make a memo and fill out the "IT service request" form as required by the Information Technology Department to have their access 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.
- The system administrators will assign the access rights to the information technology and communication systems which suit the roles and responsibilities of users, with the approval of

a person in authority in writing, and such rights 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 an authorized person to request the granting or revocation of the access 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 systems, and methods of deleting data at each level of data classification must be established.
- Data owners must review the appropriateness of the data access rights of these users at least once a year to ensure that such rights remain appropriate.
- As for data access protocols for each level of data classification, both direct access and access via the work systems, the 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 by 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 or in the event that a computer is taken away for maintenance, data owners must first back up the data onto storage media and delete any stored important data from the computer.

1.7 Communication network access control

This control applies to individuals who access the communication networks, and also systematically prevents intrusion and allows access to information systems only to which services are authorized to be accessible. The system administrators must design the communication networks 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, etc. Therefore, security measures must be established as follows:

- Users can access only services in the information systems to which they are authorized to access.
- Users wishing to access the communication networks must submit a request by filling out the "IT Service Request" form and receive a written approval from the director of the Information Technology Department or an authorized person.
- The system administrators must register for assignment of the user rights to access to the communication networks which suit the roles and responsibilities of each user before their access to the communication networks. These access rights must be reviewed at least once a year.
- The system administrators must register every device that is connected to the communication networks by filling in a computer and communication network device registration form in the "IT Service Request" System or any form provided by the system administrators.
- The system administrators must 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/groups must be segregated for access prevention and access control, namely, public sections, internally connected sections, sections related to vital assets or

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 to 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, password encryption, self-selection of frequency channels.
- Computer data traffic must be stored in compliance with the Computer-Related Offences Act B.E. 2560 (2017).
- 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.
- The communication networks must be kept under surveillance.
- The configurations of communication network devices must be backed up.
- Software or firmware patches or releases 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 the communication networks.
- Control on internal access to communication networks and network connection must be implemented.
- Requests for installing connecting points to networks of the network control room must be made in writing and approved by the director of the Information Technology Department or an authorized person.
- Users' network access rights and use rights must be overseen and improved regularly.

- Devices for filtering received and sent data, such as emails, file transfers, interactive access, chats, and access to applications, must be provided.
- A limit on the length of day or time for an authorized connection 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, routers, etc.
- 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, rights to IP addresses for the network connection of devices and network users must be established.
- Protocols and ports for each user group must be established, such as HTTP, FTP, SMTP, and TELNET.
- VLANs must be established to control and assign the access rights.

1.9 User identification and authentication

- Users' identities must be authenticated by providing their username and password to access the networks.

1.10 Installation of firewall devices for network security

- The 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 an authorized person.

- Every communication network must be set to a default “deny-all” setting.
- 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.
- The 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 an 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 whenever the firewall settings are changed.
- The 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 the 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)

- The IDS/IPS are 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 tries to access or do something unauthorized or when a user tries to abuse their privileges.
- The IDS/IPS must be installed to cover the Company's entire computer systems 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 flows in and out of the IDS/IPS must be stored for at least 90 days.
- The system administrators must regularly check and update patches and signatures of the IDS/IPS at least once a month or whenever a new signature update is available.
- The system administrators must inspect incidents, computer traffic data, usage behavior, 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 to the chain of command as soon as it is detected.
- The 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 remote access methods for the information technology and communication systems or computers must be first approved by the director of the Information Technology Department or an authorized person, subject to the firewall service request form, and must be under stringent control before they are used. Users must also strictly comply with the access requirements.
- To be granted permission to have remote access to the information technology and communication systems or computers via communication networks, users must provide proofs of reason or operational necessity and must also obtain the approval of the director of the Information Technology Department or an authorized person.
- For remote access to the information technology and communication systems or computers via computers, portable computers, portable computing devices, or mobile communication devices, there must be strict control over the engaged firewall ports for access to the systems and clear frequency channel division.
- Remote users' identities must be authenticated by providing their username and password. Such access to the information technology and communication systems or computer system via the Internet will also be verified to authenticate users' identities.
- Instead of passwords, special authentication tools must be stringently deployed for access to the information systems related to data at the internal level as well as the "confidential" level or higher, such as the use of token when operating outside the organization.

1.13 Wireless communication network access control

- The 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.
- The system administrators must choose appropriate transmission power for the working area and inspect whether the signals leak out of the area.
- The system administrators must change factory default SSID (Service Set Identifier) settings, usernames, and passwords as soon as access points are deployed.
- The 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).
- The 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.
- The system administrators must install firewalls between wireless communication networks and the Company's internal communication networks.
- The 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 systems when it is not in use for a certain period of time.
- The information technology and communication systems must be set to suspend operation and deactivate when there is no activity within a period of 60 minutes to prevent unauthorized data access.
- A mechanism for deactivating applications and automatic connections to systems when it is not in use 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 a session-timeout for a connection to the information technology and communication systems for various operations when the user has remained inactive on such systems for over 60 minutes.

1.17 Access control to the technology systems, application software and applications applies to access to the Company's information technology systems, application software, 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 user right 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 60 minutes.
- Data classified as confidential in databases must be encrypted.

2 Guidelines for computer control 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 computer control and network rooms

- Processes for permission requests, right assignment, and controls of physical entries control for computer 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 or fingerprints or ID cards and password for the authentication of authorized individuals must be implemented as part of physical entry controls for computer control and network rooms.

- The operations of external parties in the computer control and network rooms must be supervised and monitored until its completion of the missions in order to prevent any loss of assets or unauthorized physical entry.
- External parties must wear a clearly visible identification badge throughout the entire duration in the control rooms.
- Unauthorized persons are not allowed in the important areas or zones in the control rooms.
- Fostering understanding and awareness of rules and regulations that must be followed while in the control rooms.
- Permissions must be reviewed regularly, and the right to access the control rooms must be immediately revoked upon any change in the right.

2.3 Equipment sitting and protection in the computer control and network rooms

- Each type of equipment must be sited in designated areas.
- No food and drinks are allowed in the control rooms.
- The environment of control rooms must be inspected, kept under surveillance, 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 the computer control and network rooms

- Supporting utilities for the Company's information technology and communication systems 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, computer network equipment and network cabling systems, KVM (Keyboard, Video, Mouse) switches, and emergency power system.
- Supporting utilities must be regularly inspected or tested to ensure normal functionality and reduce risks of failure.

2.5 Electric wiring and communication cabling and other cables in the computer control and network rooms

- Various signal conduits must be installed to prevent any signal interception or damage from cutting the signal cables.
- Power cables must be segregated from communication cables to prevent any cable interference.
- Signal cables on equipment 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 the computer 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 a subsequent inspection or assessment.
- Issues and defects must be recorded for assessment and improvement of the relevant equipment.
- The operations of computer system maintenance service companies must be controlled and supervised. Off-site equipment repair must be controlled to prevent any loss or unauthorized data access.
- Access to equipment containing material data by maintenance service companies must be approved to prevent any 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 5.1.4: Use of user passwords.

- Users must log off immediately the information technology system when not in use to prevent others' continued access to the system. In case of a suspected leak of password, 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 any other software or programs on the operating computers or install additional network equipment or connect the operating computer network with other networks than the Company's networks or bring their own personal computers to use with the Company's information technology system, unless permitted by the system administrators.
- Files in the operating 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 systems 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 on 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 giving them to others for illegal use.
- Media such as CD, DVD, 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 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 the 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 data from personal computers in other storage media, such as CD, DVD, external hard disks, One Drive, etc.
- 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 5.1.4: Use of user passwords.
- In case of damaged assets or imperfect assets due to staff's negligence, staff is responsible for the damages to the Company's assets subject to the assessed penalty fees.

3.3 Use of portable computers

- Authorized portable computers are the Company's assets and must therefore be used carefully and efficiently.

- Programs to be installed on portable computers must be approved by the Company or lawfully copyrighted. Users are prohibited from copying, installing, or altering any programs and installing them on portable computers that do not belong to the Company or giving them to others for illegal use.
- Users should carefully study and follow manuals for safe and efficient usage.
- Users must not modify or alter any components of portable computers and must maintain their original and ready-to-use condition.
- Portable computers must be put in bags for portable computers when transported to prevent damage from impact, such as a fall from a desk or from users' hands, etc.
- For non-touch screen computers, users must 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, to prevent scratches on the screens.
- Users are responsible for preventing the loss of portable computers. For instance, portable 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.
- Portable 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 systems of portable computers.
- Assignment, change, and storage of user passwords must be in accordance with Item 5.1.4: Use of user passwords.
- Users must turn off the portable computers when the task is completed or when they are no longer in use.
- Users must make backups of data from the portable computers in other storage media, such as CD, DVD, 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.
- In case of damaged assets or imperfect assets due to staff's negligence, staff is responsible for the damages to the Company's assets subject to the assessed penalty fees.

4 Security for the use of the Internet and electronic mail

4.1 Use of the Internet

- The 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 individual's authentication in access to 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 for using multimedia data or downloading non-work-related data and taking up the bandwidth.
- The system administrators must route computer connections to the Internet through security systems, such as proxy firewalls, IPS, and IDS.
- Before connecting to the Internet through a web browser on personal computers, portable computers, and portable computing devices, antivirus programs must be installed and vulnerabilities in the operating system in which the browser is installed 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, monarchy, or pose social threats.

- Users are assigned rights to access data sources in accordance with their roles and responsibilities to ensure network efficiency and data security of the Company as approved by the 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 any access by others.
- Users must strictly comply with the Computer Crime Act.

4.2 Use of electronic mail

- The 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's business affairs.
- Users must exercise caution in using emails so as not to damage the Company, cause annoyance to others, or act in contradiction 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 any access by others.
- Before opening attached files in emails, users must always scan such files with an antivirus program.
- Users must not open or forward any email or 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 data containing the digits 0-9 used exclusively for calculations, such as numbers of goods ordered.
- Graphic data refers to still images, animations, drawings, photographs, and video images, such as images of scanned documents.
- Audio data refers to sounds and 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 such data, either in part or in its entirety, does not negatively impact the Company. For example, the data published on the Company's website.
- Level 2: Internal data

  Internal data refers to data that has been deemed by the owner of the data to be made available to personnel within the Company, but not to external parties as it may cause damage to the Company. The disclosure of such data must depend on the discretion or approval of the owner of the data or may be required by law. For example, data in the Company's personnel system, data in right and juristic act registration system.

- Level 3: Confidential data

  Confidential data refers to data that has been deemed by the Company not to be made available to every user. Such data is restricted to relevant parties that need it for their operation only and their access is on a need-to-know basis for their operation. The data is essential to the Company's 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 may be required by the law. For example, salary data, disciplinary action data.

- Level 4: Highly confidential data

  Highly confidential data refers to internal data used by certain 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 the disclosure of such data may cause severe damage to the Company. The disclosure of such data must be then approved by the owner of the data or may be required by the law. For example, computer traffic data, 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 external parties 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, or access.

- Officers of the Information Technology Department are not authorized to grant data access to data requesters without permission of the director of the Information Technology Department or authorized person, except during a system development process when officers of the Information Technology Department and contractors are responsible for transferring data to the new system.

- In the event that a data requester is an internal unit of the Company and the data owner is another internal unit of the Company, the unit as the data 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 no prior memorandum of agreement between the agencies has been made, a written request for the Company's permission must always be submitted whenever a request is made. If a prior memorandum of agreement has been made, the data access must be supervised to ensure that the scope of requested data is as specified in the memorandum of agreement.
- In the event that data requests are submitted to the Company by individuals or juristic persons, guidelines or protocols established by the Company existing, such established guidelines or protocols must be followed.

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 and in accordance with the memorandum of agreements between the agencies. Data published via the Internet can be accessed 24 hours a day.

5.2 Computer system management

- Specify names and IP addresses in the computer system.
- Clearly assign an officer in charge of setting, changing or altering parameters of the system program.
- Any abnormal use or alterations of parameters detected must be immediately rectified and reported to the officer in charge.

- Services must be allowed only as needed. If such services as needed present risks to security systems, additional measures must be implemented.
- Patches of essential systems must be regularly installed to eliminate any vulnerability 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 rectification or 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 a program access control inventory.
- Register programs for use with license owners.
- Update programs to newer versions when new versions are released.
- Control versions of applications.
- Install licensed or free programs (freeware, open source programs) only as needed for usage.

5.4 Communication network management

- Segregate networks/groups (VLAN/Zone).
- Create an inventory of communication network access controls.
- Create a communication network diagram and scope.
- Inspect usage of 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 prepare reports of such penetration tests.

- Assign individuals in charge of setting, changing or altering parameters of the communication networks and connected devices.
- Revise such parameters at least once a year.
- Maintain the communication networks 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 management inventory that contains the following:
- Officer in charge;
- Asset types.

5.6 Requisition of computer and network devices

- Users who intends to requisition computer and network devices must submit a request via the IT Service Request System or submit a computer and network device requisition form, detailing the items required, including storage or installation site, to the officer in charge for approval.
- The officer in charge reviews the requisition 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 requisition request is approved, the officer in charge must newly record data on the storage or installation site of the equipment in the IT Service Request System or the computer and network device requisition form as a device history.

5.7 Computer and network device maintenance request

- When any users find a malfunction of a device or are unable to use a device in their operation, the users must give a maintenance notice to the officer in charge by filling out relevant information in the IT Service Request System.
- The officer in charge analyzes damage to the device from the data submitted through the IT Service Request System and from the self-testing of the device, as well as taking into consideration supporting data, especially its warranty period. If the warranty is still valid, the officer in charge can send the damaged device for maintenance by the supplier service center without incurring any costs detailed in the warranty. If the device is out of warranty, the officer in charge must exercise his discretion to consider whether it should be either repaired or disposed of, depending on the extent of the damage to the device.
- During the repair or maintenance of the device, if a replacement is available, the officer in charge must deliver such replacement to the user and must be responsible for recording data on replacement devices in the IT Service Request System.
- After having received the repaired device, the officer in charge must re-test the device to recheck the previously malfunctioned part before returning the same to the user, whereby the officer in charge must fill out the device test and maintenance form in the IT Service Request System or the computer and network requisition form, and return the repaired device together with such documents to the user.

5.8 Taking the Company's assets off-site

- A request for permission must be recorded before the equipment or assets are taken out of the premises as evidence in order to prevent loss, including record of further information upon the return of assets.
- The officer in charge must take care of the Company's equipment or assets as their own ones.

5.9 Disposal of computer and network devices

- If the device is too damaged to be repaired and is out of warranty, and when considering the cost of the device against repair costs, the disposal of such device is required. In this case, 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, as the user 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 matter back to the officer in charge.
- The matter must be submitted to the unit in authority to approve the disposal of the device for further consideration.

5.10 Control of printouts from the information technology and communication systems

- 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 printouts off-site as evidence in order 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, application programs or applications, instruction sets, 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 improved or 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.

6.4 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 to work systems or data in databases, must be specified.
- Backup frequencies and methods for such vital work systems, such as full backup or 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 these 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 or educating relevant officers on the protocols or actions that need to be taken in any emergency.

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

6.8 Data must be backed up according to the prescribed data types, frequencies, and backup methods. Backups must be regularly inspected to ensure their completeness.

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

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 recovery plan, another meeting must be held to inform all related parties of such updates.

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

- Preparing forms/printed forms that can be used in place of the forms/printed forms that can be printed from the information technology and communication systems.
- Reverting to the existing plans prior to the adoption of the current information technology and communication system, such as the manual system.
- Once the information technology and communication systems resume normal operations, the data acquired during the emergency must be input into the systems.

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

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 or training must be carried out to ensure that the Company's officers will acknowledge, understand, and refrain from violating the Computer-Related Offences Act B.E. 2560 (2017) and other laws related to information technology, as well as ensuring responsible and appropriate use of the Company's information technology resources.

8.2 An officer responsible for publicly publishing data on the Company's website 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 policies and guidelines must be reviewed and updated to ensure that they meet accepted standards at least once a year.

It is hereby announced for general acknowledgment and action.

(Mr. Thanawat Trivisvavet)

Managing Director

Abbreviation List

The Hypertext Transfer Protocol (HTTP)	: is an application layer protocol for distributed, collaborative, hypermedia information systems.
Media Access Control address (MAC address)	: is a unique code number with hexadecimal. That is attached to the device connected to the network.
The File Transfer Protocol (FTP)	: is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network.
The Simple Mail Transfer Protocol (SMTP)	: is an internet standard communication protocol for electronic mail transmission.
Telnet (TELNET)	: is an application protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.
Database Management System (DBMS)	: is a computer program designed to manage a database, a large set of structured data, and run operations on the data requested by numerous users.
Secure Sockets Layer (SSL)	: is a cryptographic protocol designed to provide communications security over a computer network.
virtual private network (VPN)	: is extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.