Acceptable Use Policy

of

CK Power Public Company Limited and its Affiliated Companies

CK Power Public Company Limited and its Affiliated Companies

Acceptable Use Policy

Table of Content

Document Control

Document Approvals

This document has been reviewed and approved by:

Prepared by	Reviewed by	Reviewed by
(Mr. Anucha Prapadnirattisai) Date (___ /___ /_____)	(Mr. Umnath Chuencharoen) Date (___ /___ /_____)	(Mr. Burahan Madae) Date (___ /___ /_____)
Document Control	ISMA	ISMR

Version History

The following is a list of revisions made to this document:

Revision	Description	Effective Date
1.0	**First creation**	

1. Objectives

To establish appropriate guidelines for the use of information technology, in accordance with laws and regulations, as well as related security requirements, and to protect the assets of organizations and employees from security risks or misuse, such as unauthorized disclosure of information. Hacking into networks or service systems or any unlawful action, etc.

2. Scope

This policy applies to:

- All resources and assets, which concern to the CK Power's information security
- An individual using the resources and assets defined above.

3. Definition

- **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.
- **Employees:** 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 assets includes all servers, clients, network infrastructure, system and application software, data, as well as other computer subsystems and components which are owned or used by the organization, or which are under the organization's responsibility. The use of an information system also includes the use of all internal or external services, such as Internet access, e-mail, etc.

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

4. Policy Description

4.1. General

To ensure data security with key element 4 sections include:

- Corporate information is the property that is most important and must be protected to preserve:
  - Confidentiality
  - Integrity
  - Availability
- Corporate equipment is the provision of information technology services that require computers/ laptops, networking, and electronic data. Therefore, it is the duty of all employees and related persons to maintain the security of the information and information systems of the organization to the best of their ability.

- Corporate working area is the operating area of employees and related parties; these areas may be subject to information security breaches. If not properly protected
- Employees in the organization are employees who are responsible for organization's information. Therefore, employees need to know how to protect information/data from information/data breaches whether while working in the office area, working at home or while traveling to work offsite.

4.2. Corporate information

- Classification and confidentiality must be identified for all information/data in accordance to Information Classification and Handling Procedure.
- Use and protection of confidential information.
  - Employees must use the information/data in accordance with Information Classification and Handling Procedure.
- Share folders are not allowed to exchange sensitive information without permission from the authorized authority.
- Employees must not disclose classified information to third parties unless the disclosure is covered by the Non-Disclosure Agreement (NDA).
- Use of media that contains confidential information.
  - Media and mobile devices such as Thumb-drive where organization's confidential information is recorded. It must be carefully maintained and used.
- Information/data backups
  - Information related to the business operations of the organization, either on the user's computer or the administrator-maintained Server, must be backed up regularly.

4.3. Corporate equipment

- Device usage
  - All information technology systems and related information/data processing equipment provided by the organization. It is intended to be used in the business operations of the organization. The use of systems and equipment for personal errands. Permission is allowed to be used to a limited extent as appropriate, which must not interfere with or hinder the user's responsibilities.
  - The employee is responsible for the use of the computer. and equipment of the organization carefully and protect them as their property.
  - An organization's information device must always be protected by the operating system password when anyone wants to access it and must be automatically protected by a Screen Saver password or log off the device every time the device has been idle for some time.
  - Portable computers with organization’s information/data stored must be protected equal to computers used within the organization i.e., installing anti-malware software, enabling firewall, updating security patch and any others.
  - Employees must not allow unauthorized persons to install any hardware or software on the computer of the organization is strictly prohibited.
  - The organization's computer equipment must not be tampered or installed any additional equipment (both hardware and software) before obtaining permission from authority.
- Software usage
  - Employees are prohibited from installing or disseminating pirated software on computers and organization’s information technology systems.
  - Employees are prohibited from installing and using software for personal use or copying without authorized.
  - Installing any software other than the organization's standard program whether authorized or installed manually, the organization is not responsible for the outcome.

- E-mail usage
  - E-mail users must have their own e-mail account which is an e-mail provided by the organization.
  - User e-mail accounts must be password protected to prevent account takeover and misuse of e-mail.
  - E-mail accounts with special purposes, such as sales@company.com, may be created as the party's central e-mail account and/or for sharing by more than one user. At least one employee must be appointed to act as the owner of the e-mail account, and details must be specified for who can access the e-mail account.
  - The size of e-mails and attachments has been limited. If the e-mail and attachments are larger than the limit. Users will receive a bounce letter.
  - Users must always remove unnecessary e-mails from their mailboxes. To maintain the e-mail storage area according to the size specified by the organization.
  - Users are prohibited from using an e-mail account to perform any acts related to illegal, moral, or potentially detrimental to national security. Religion, monarchy.
  - Users are prohibited from using an e-mail account to publish any sensitive information in the electronic community, such as web boards, blogs, bulletins, etc., unless the information is relevant or part of its work.
  - Users must draft the contents of the e-mail with caution. Always regardless of whether you are an exporter of e-mails on behalf of the organization's representatives.
  - Users are strictly prohibited from spoofing messages in e-mails, e-mails, signatures in e-mails or e-mail accounts of other people.
  - Auto-forward to outside organization is prohibited except authorized persons.
  - Users are prohibited from sending e-mails that the recipient does not require. For example, junk mail, advertising products (Spam Mail), chain e-mail, or any fraudulent e-mail.

- Users are prohibited from sending or forwarding e-mails containing images or content that contains images or content that are insulting, defamatory, insulting, discrediting others, class racism, intimidation, gambling, or obscenity.
- Users should not open unknown files or URLs or unknown e-mails and be extra careful when they need to open attachments or URL links received from senders they don't recognize. The attachment may contain an e-mail Bomb virus or a phantom program.

- Internet usage on the organization's network
  - Internet use is intended to facilitate users to search for information, knowledge, and communication with third parties, customers, and commercial partners, to increase the efficiency of the organization's work and services only.
  - Users must not use the Internet in any work related to illegal activity and/or discredit the organization, and misuse of the Internet is a disciplinary offense and may be prosecuted under the law.
  - To comply with electronic transaction laws. Internet access must be accessed only through channels provided by the organization. The organization reserves the right to monitor the user's internet usage and internet access log.
  - Users are prohibited from clicking on the ad window to access any website advertised by spam, as these websites may contain malicious programs or may steal information on the user's computer without the user's knowledge or permission.
  - Users are prohibited from visiting, using, downloading, obtaining or reproducing pornography, pirated software, and any other inappropriate or illegal media.
- Social media usage
  - Employee shall not give the impression that you are speaking on behalf of the organization unless you are specifically authorized.
  - Be mindful when posts on your personal social media accounts and pages reflect on the organization.

- Not post or share any confidential, copyright or proprietary information about the organization or other employee, customer, supplier, partner or competitor of the organization.
- Notify the organization if you see any online content about the organization that is disparaging and/or indicates that is against the policy of the organization, law, regulation or unethical content published.

- Secure use of passwords
  - Each user must be assigned a unique user account to access the organization's systems and services.
  - For administrators, make a password change every 90 days.
  - For users, make a password change regularly with appropriate period.
  - Passwords must be secure as below.
    - 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.
  - Passwords are confidential information, and it is the duty of all users to keep them secure. It is forbidden to publish their passwords to others.
  - User accounts are strictly prohibited from sharing or giving others access to their accounts.
  - Do not write down or save personal passwords in places that are easy to notice to other people.
  - Users are responsible for any actions taken through their account and passwords and cannot be denied responsibility in the event of an adverse event.
  - If the user suspects that their account or password has been violated, change the password immediately.

4.4. Corporate working area

- Physical security
  - Third parties must present their identities issued by government agencies. For example, id card, driver's license, passport, etc. along with the contact card of the organization. Before being allowed access to the working area.
  - Third parties must be always accompanied by a visitor card in the working area. Visitor cards do not allow transfer of ownership or borrowing.
  - Employees must not leave the working area door open or allow others to follow into the working area unless the other person can present a contact card to prevent unauthorized access to working areas and security control areas.
  - Employees must notify the security guard immediately. When they see a strange person or a person without visitor card in the working area.
  - Employees should accompany to supervise and advise those who come into contact with them at all times when they are in the working area.
  - Employees should check the security of their working area on a daily basis after work to ensure that file cabinets, drawers and equipment are properly locked, and keys are kept secure.
  - Information, media, materials, and equipment that store secret data must not be left unattended, whether at the desk, in a conference room or in an unlocked cabinet.
  - Information, media, materials, and equipment that store secret data must not be discarded in the trash without proper destruction.
  - PC and laptop shall be locked-off or shut down when screen is left/unoccupied

4.5. Employees of the organization

- Compliance with rules and policies
  - All employees must be informed, understand and strictly comply with the Acceptable Use Policy.
  - Information created, stored, or transmitted on the organization's information technology system is considered the property of the organization, except information that is the property of customers or third parties, including software or other information protected by third-party patents or copyrights, can be disclosed, or used as evidence in investigations of various offenses without prior notice to employees.
  - The organization has the right to access, review and inspect employee e-mails without prior notice as necessary and will not disclose any information of employees unless it is disclosed by court order, in accordance with the law, or with the consent of the employee only.
  - Employees are prohibited from using the organization's assets and information technology systems to act in conflicts with the laws of the Kingdom of Thailand and international law under any circumstances.
  - Employees are strictly prohibited from plagiarism/piracy whether to use or repeat or publish pictures, songs, any articles, books or documents that infringe copyright or install pirated software on the organization's information technology system.
  - All employees must be aware of the correct use of passwords and should update on new ways of scam that will lead to information/data theft.
- Notification of security breaches and weaknesses
  - All employees are responsible for reporting security violations, any weaknesses or inappropriate actions that occur or are suspected within the organization to take timely resolution of the issue.
  - Employees who encounter or acknowledge malfunctions or software errors or weaknesses must report a security breach immediately.
  - Employees who find any hardware or equipment damaged or malfunctioning must report a security breach immediately.

4.6. Exception

Any exception to the policy must be considered by risk management process in order to accept the risk.

5. Supporting Document

- CKP-ISMS-PC-07 Information Classification and Handling Procedure
- CKP-ISMS-PC-10 Risk Management Procedure

Please be informed and comply accordingly.

(Dr. Thanong Bidaya)

Chairman of the Board of Directors