



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

Contents

DOCUMENT CONTROL 1

1. OBJECTIVES..... 2

2. SCOPE..... 2

3. DEFINITIONS..... 2

4. POLICY DESCRIPTION 3

4.1. GENERAL..... 3

4.2. CORPORATE INFORMATION..... 3

4.3. CORPORATE EQUIPMENT..... 4

4.4. CORPORATE WORKING AREA 7

4.5. EMPLOYEES OF THE ORGANIZATION 8

4.6. DATA LEAKAGE PREVENTION..... 9

4.7. WEB USAGE AND FILTERING COMPLIANCE 10

4.8. EXCEPTION..... 11

5. SUPPORTING DOCUMENTS 11



CK Power Public Company Limited and its Affiliated Companies
Acceptable Use Policy

Page 1 of 11

Revision No. 01

Effective date
November 27, 2025

Document Control

Document Approvals

This document has been reviewed and approved by:

Prepared by	Reviewed by	Reviewed by
(... Mr. Chalermchad Homat ...) Date (08 /09 /2025)	(... Mr. Umnath Chuencharoen ...) Date (08 /09 /2025)	(... Ms. Pimsiri Pochanaphanich ...) Date (08 /09 /2025)
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 September 2022
2.0	Update to ISO/IEC 27001:2022 template and adding NIST CSF 2.0	1 August 2025
2.1	Update to company definitions and improve parts of the content.	November 27, 2025

1. Objectives

- This Policy aims to establish appropriate guidelines for the acceptable use of information technology (IT) in accordance with applicable laws and regulations, as well as relevant security requirements, and aims to safeguard the organization's and employees' assets from security risks or misuse, such as unauthorized disclosure of information, network or service system intrusion, or any other unlawful actions.
- This Acceptable Use Policy is issued under the authority of CK Power Public Company Limited's and its subsidiaries Information Security Policy and forms part of the Company's Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022 requirements.
- This Policy must be reviewed annually or upon significant changes. Updates must be documented and version-controlled.

2. Scope

This Policy applies to:

- All resources and assets related to CK Power Public Company Limited's information security.
- All individuals who use the resources and assets defined above.

3. Definitions

- **Company** refers to CK Power Public Company Limited.
- **User** refers to any individual authorized to use, manage, or maintain the Company's IT and communication systems.
- **System administrator** refers to the Director of the IT Department or any individual authorized to supervise the management of the Company's IT and communication systems.
- **Employees** refer to personnel of the Company, including external parties authorized to access the Company's IT and communication systems.
- **User rights** refer to permissions granted to users to access the Company's IT and communication systems.
- **Asset** refers to the Company's assets, including servers, client devices, network infrastructure, system and application software, data, as well as other computer subsystems and components that are owned or used by the Company, or that are under the Company's responsibility. The use of an information system also includes the use of all internal and external services, such as Internet access, e-mail.

- **IT Department** refers to the 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, as well as collaborating with or supporting other relevant work 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 a combination of letters, numbers or symbols that are used to authenticate identity and control access to data and data systems in order to ensure the security of data and the IT system of the Company.
- **Electronic mail (e-mail)** refers to a system that individuals use to receive and send messages via computers and connected communication systems. Such messages may include texts, images, audio, graphics, or animations, and can be sent 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 effective information security, this Policy addresses 4 key areas as follows:

- **Corporate information** is the most critical asset and must be protected to preserve:
 - Confidentiality
 - Integrity
 - Availability
- **Corporate equipment** refers to IT resources provided by the organization, such as computers/laptops, networks, and electronic information. Therefore, all employees and relevant personnel have a duty to safeguard the organization's information and information systems to the best of their ability.
- **Corporate working area** refers to an area where employees and relevant personnel operate, which may be vulnerable to information security breaches if not properly secured.
- **Employees of the organization** refer to personnel who are responsible for safeguarding organizational information. Therefore, they must be knowledgeable in protecting such information from unauthorized access or breaches, whether working in the office area, from home, or while traveling for off-site working.

4.2. Corporate Information

- **Classification and confidentiality:** All information/data must be assigned a confidentiality level and classified in accordance with the organization's Information Classification and Handling Procedure.

- **Use and protection of confidential information:** Employees must use the information/data in accordance with the Information Classification and Handling Procedure.
- **Use of shared folders:** Sharing confidential information via shared folders is prohibited without permission from an authorized person.
- **Employees must not disclose confidential information** to any external parties unless the disclosure is permitted under a valid Non-Disclosure Agreement (NDA).
- **Confidential information stored on any device or server** must be protected using encryption methods approved by the organization to prevent unauthorized access (Data-at-Rest Encryption).
- **Use of storage media containing the organization's confidential information:**
 - Storage media and portable devices, such as USB flash drives, that contain the organization's confidential information must be carefully maintained and used.
- **Information backups:**
 - The organization's business-related information, whether stored on the user devices or servers managed by the system administrators, must be backed up regularly.

4.3. Corporate Equipment

4.3.1. Device usage

- All IT devices and related data-processing equipment provided by the organization are intended for the organization's business operations. Limited personal use may be permitted within defined limits, provided that it does not interfere with the user's responsibilities.
- Employees are responsible for using computers and other equipment of the organization with due care, and must treat them as if they were their own assets.
- Corporate equipment must always be protected by the operating system passwords prior to access and configured to automatically lock the screen or log out after a period of inactivity.
- Devices that connect to the organization's data/IT systems must be protected in accordance with the organization's security measures, such as installing anti-malware software, enabling firewalls, updating security patches, and other necessary controls.
- Employees are strictly prohibited from allowing unauthorized individuals to install any hardware or software on the organization's computers.
- The organization's computers must not be modified, nor may any equipment, whether hardware or software, be installed, without permission from an authorized person.
- System access permissions must be reviewed quarterly to ensure they align with each individual's current job responsibilities.

4.3.2. Software usage

- Employees are prohibited from installing or distributing pirated software on the organization's computers and IT systems.
- Employees are prohibited from installing or using software for personal purposes or copying any software without authorization.



CK Power Public Company Limited and its Affiliated Companies
Acceptable Use Policy

Page 5 of 11

Revision No. 01

Effective date
November 27, 2025

- If any software that is not part of the organization’s standard is installed, whether with permission or installed independently, the organization must not be held liable for any resulting consequences.

4.3.3. E-mail usage

- E-mail users must use only the e-mail account assigned by the organization.
- User e-mail accounts must be protected by passwords to prevent account takeovers and unauthorized use.
- Shared or functional e-mail accounts, such as sales@company.com, may be set up for specific purposes. At least one employee must be designated as the primary responsible person, and access rights must be clearly defined.
- E-mail and attachment sizes are subject to limits under the organization’s policy. If exceeded, the users’ message will be rejected (bounced) by the system.
- Users must regularly delete unnecessary e-mails from their inboxes to ensure compliance with the organization’s storage limits.
- Users are prohibited from using the organization’s e-mail accounts to engage in illegal activities, immoral conduct, or actions that may compromise national security, including matters related to religion, or politics.
- Users must not use the organization’s e-mail accounts to publish sensitive information on public online platforms, such as forums, blogs, newsletters, unless the information is job-related or part of their work.
- Users must compose e-mail content carefully, whether sending it on their own behalf or on behalf of the organization.
- Users are strictly prohibited from spoofing e-mail content, signatures, or e-mail addresses of others.
- Automatic forwarding of e-mails outside the organization is prohibited unless permitted by an authorized person.
- Users must not send unsolicited e-mails, such as spam, product advertisements, chain letters, or e-mails containing fraudulent content.
- Users must not send or forward e-mails containing any images or content that are obscene, defamatory, disrespectful, damaging to others, including those that are racially discriminatory, threatening, or pornographic.
- Users must not open attachments or URLs from unknown sources, and must exercise special caution when it is necessary to open files or click links from unrecognized senders, as such content may contain viruses or malicious programs, such as e-mail bombs or phishing software.

4.3.4. Internet usage on the organization's network

- Internet usage is intended solely to support users in searching for information, knowledge, and communication with external parties, customers, and business partners, to increase the efficiency of the organization's operations and services.
- Users must not use the Internet to perform any illegal activities or to harm the organization's reputation, and improper Internet usage must be deemed a disciplinary violation and may result in legal proceedings.
- To comply with laws governing electronic transactions, access to the Internet must be only through channels provided by the organization. The organization reserves the right to monitor the user's Internet usage and access logs.
- Users are prohibited from clicking on advertisements or pop-up windows generated by spam to access any websites, as those websites may contain malicious programs or may steal information on the user's computer without their knowledge or permission.
- Users are prohibited from accessing, using, downloading, modifying, or reproducing pornographic content, pirated software, or any other inappropriate or illegal materials.
- All sensitive or confidential data transmitted over the network must be communicated through secure channels, such as HTTPS, TLS, or VPN, to ensure data protection during transmission.

4.3.5. Social media usage

- Employees must not present themselves as representatives of the organization in any form of communication unless they are explicitly authorized to do so.
- Employees should exercise caution when posting on their personal social media accounts, as such content may impact the organization's image.
- Employees must not post or share any confidential, copyrighted, or proprietary information belonging to the organization or its employees, customers, suppliers, partners, or competitors.
- Employees must promptly notify the organization if they come across any online content that is defamatory, or inappropriate related to the organization, or violates laws, the organization's policies, rules, regulations, or ethical standards.

4.3.6. Secure use of passwords

- Each user must be assigned a unique user account to access the organization's systems and services.
- System administrators must change their passwords every 90 days.
- Regular users should change their passwords periodically at appropriate intervals.
- Passwords must be secure in accordance with the following requirements:

- Passwords must be at least 8 characters and include a combination of letters, digits, and symbols.
- Do not use simple or commonly used passwords, such as “abcdef,” “aaaaaa,” or “12345”.
- Do not use personal information as passwords, such as first name, last name, date of birth, or address.
- Do not use dictionary words as passwords.
- Passwords are confidential information. All users are responsible for keeping their passwords secret and must not disclose them to others.
- Users must not share their accounts or allow others to access their accounts under any circumstances.
- Users must not write down or record passwords in locations that are easily visible to others.
- Users are responsible for any actions taken through their user accounts and passwords. They may not deny responsibility in the event of any undesirable incidents.
- If a user account or password is suspected to have been compromised, the password must be changed immediately.
- Prior to creating a user account, the user’s identity must be verified and confirmed by the Human Resources Department, and approval must be obtained from the relevant manager.
- User authentication information must be transmitted only through encrypted communication channels, such as VPN or HTTPS, to ensure data protection during transmission.

4.4. Corporate Working Area

4.4.1. Physical security

- Third-party visitors must present their valid ID issued by government agencies, such as a national ID card, driver’s license, or passport, along with the organization’s visitor pass, before being granted access to the working area.
- Third-party visitors must have a visitor pass and be accompanied by an employee of the organization at all times while inside the working area. The visitor pass must not be transferred or lent to others.
- Employees must not leave working area doors open or allow others to tailgate into the area unless they present a valid visitor pass. This is to prevent unauthorized access to working areas or security-controlled zones.
- Employees must immediately notify the security guard if they encounter any unfamiliar individuals or anyone in the working area without a visitor pass.

- Employees should supervise and provide guidance to those visitors or collaborators at all times during their stay in the working area.
- Employees should conduct a daily security check of their working area after working hours to ensure that file cabinets, drawers, and equipment are properly locked, and that keys are securely stored.
- Information, media, materials, or equipment containing confidential information must not be left unattended, whether on meeting desks, in meeting rooms, or in unlocked cabinets.
- Media, or equipment containing confidential information must not be discarded in the trash without undergoing proper destruction procedures.
- PCs and laptops must be locked or set to automatically shut down or sleep when left unattended.
- Confidential information must not be left visible on screen or in memory without protection. Systems must enforce automatic screen locks and appropriate session timeouts.
- While handling sensitive information, employees must close related applications after use and ensure that the information cannot be accessed through screen sharing, screen capture, or memory scraping.

4.5. Employees of the Organization

4.5.1. Compliance with rules and policies

- All employees must be informed of, understand and strictly comply with the Acceptable Use Policy.
- Information created, stored, or transmitted through the organization's information system must be considered the assets of the organization, except where such information is the property of customers or external parties (e.g., licensed third-party software or proprietary data). Such information may be disclosed or used as evidence in investigations without prior notice to employees.
- The organization reserves the right to access, review, and monitor employee e-mails without prior notice when necessary. Employee information must not be disclosed unless required by a court order, legal obligation, or with the consent of the employee.
- Employees are prohibited from using the organization's assets and IT systems in any manner that violates the laws of the Kingdom of Thailand or international law.
- Employees are prohibited from infringing copyrights or using pirated software, including the use, reproduction, or distribution of copyrighted materials, such as images, music, articles, books, documents, or software on or through the organization's IT systems.
- All employees must stay informed of proper password practices and remain updated on emerging threats or scams that could lead to data theft.

- User activities, including email and Internet usage, must be logged and subject to periodic review to detect policy violations.

4.5.2. Reporting of information security breaches and vulnerabilities

- All employees are responsible for promptly reporting any actual or suspected information security violations, vulnerabilities, or inappropriate activities within the organization to enable timely mitigation.
- Employees who identify or acknowledge any system malfunctions or software errors must immediately report the matter as a security incident.
- Employees who discover any damage or malfunction in hardware or equipment must immediately report the matter as a security incident.
- Employees must immediately isolate the affected devices if a security breach is suspected and report the incident to the IT Department for containment and impact mitigation.
- All security incidents must be recorded, and any related digital evidence must be properly preserved in accordance with the Incident Management Procedure.
- Incident-related metadata, such as timestamps, source IPs, and audit logs, must be retained in a complete and accurate manner, protected from unauthorized modification, and must be fully auditable retrospectively.
- The IT Department is responsible for notifying relevant internal teams and, where applicable, external parties (e.g., regulatory authorities or business partners) in accordance with the Incident Management Procedure. All notifications must follow the organization's established communication protocols and escalation procedures.

4.5.3. Policy communication and acknowledgement

- All employees, contractors, and external users of the organization must receive training on this Acceptable Use Policy during the onboarding process and at least once annually thereafter. The organization must retain documented evidence that each user has read, understood, and acknowledged compliance with this Policy.
- Personnel in technical roles, such as system administrators, software developers, or information security officers, must receive role-specific cybersecurity training at least once annually.
- Violation of this Policy may result in disciplinary action, including termination of employment, and in some cases, may also lead to legal proceedings in accordance with applicable laws.
- Disciplinary measures must be proportionate to the severity of the violation and consistent with the organization's disciplinary procedures.

4.6. Data Leakage Prevention

To prevent the unauthorized disclosure or leakage of the organization's information, all users must strictly adhere to the following acceptable use practices:



4.6.1. Prohibited data transfers

- Users must not transfer, upload, or share internal or confidential information via personal email accounts, public cloud storage platforms (e.g., Google Drive, Dropbox, iCloud), or unauthorized messaging applications (e.g., LINE, WhatsApp, Telegram).
- The use of file-sharing tools or data synchronization services must be limited to organization-approved platforms with appropriate access controls and encryption.

4.6.2. Use of removable media

- The use of USB drives, external hard disks, and other portable media is restricted. Where permitted, such media must be encrypted and require approval from the IT Department.
- Users must not copy the organization's data to any personal devices or media without authorization.

4.6.3. Information disclosure

- Users must not disclose any confidential, personal, or critical information of the organization to external parties unless formally authorized.
- Transmitting documents labeled "Confidential" or higher classification outside the organization's network requires prior approval.

4.6.4. Printing and screen capture

- Users must not print, capture, or record sensitive content unless such actions are part of authorized job responsibilities and in accordance with the organization's data classification guidelines.
- All printed materials must be securely stored and properly disposed of in accordance with the organization's procedures.

4.6.5. Awareness and compliance

- Users are responsible for recognizing and avoiding behaviors that may result in data leakage.
- Violations of these guidelines may result in disciplinary action, including access restrictions, or legal liability under applicable laws and the organization's policies.

4.7. Web Usage and Filtering Compliance

Users must not attempt to bypass web filtering mechanisms or access websites classified as harmful, inappropriate, or unrelated to the organization's business.

- Access to websites related to illegal activities, pornographic content, unauthorized streaming, or anonymous proxy services is strictly prohibited.



- The use of browser extensions or VPNs to circumvent web filtering policies constitutes a violation of this Policy.
- If access to a blocked website is required for legitimate business purposes, users must request exceptional approval from the IT Department.
- Violations of this Policy may result in access revocation, disciplinary actions, or legal consequences.

4.8. Exception

Any exception to this Policy must be subject to the risk management process for risk acceptance.

5. Supporting Documents

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

It is hereby issued and must take effect for the acknowledgement and compliance of all personnel this hereby revokes the previous Information Security Policy issued on 20 February 2023, and replaces it with this revised Acceptable Use Policy (Revision No. 1), which has been reviewed and approved by the Company's Board of Directors Meeting No. 7/2025 held on 27 November 2025.

-Signature-

(Dr. Thanong Bidaya)

Chairman of the Board of Directors