



Information Security Policy

of

CK Power Public Company Limited and its Affiliated Companies



CK Power Public Company Limited and its Affiliated Companies
Information Security Policy

Content

DOCUMENT CONTROL	1
1. OBJECTIVES.....	2
2. SCOPE.....	2
3. DEFINITION.....	2
4. POLICY STATEMENT	3
4.1. ORGANIZATIONAL CONTROLS	3
4.2. PEOPLE CONTROLS.....	11
4.3. PHYSICAL CONTROLS.....	12
4.4. TECHNOLOGICAL CONTROLS	15
5. SUPPORTING DOCUMENT.....	19



CK Power Public Company Limited and its Affiliated Companies
Information Security Policy

Page 1 of 19

Revision No. 01

Effective date
November 27,2025

Document Control

Document Approvals

This document has been reviewed and approved by:

Prepared by	Reviewed by	Approved 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

History

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

Revision	Description	Effective Date
1.0	First creation	01 September 2022
2.0	Update to ISO/IEC 27001:2022 template and adding NIST CSF 2.0	01 August 2025
2.1	Update to company definition and improve parts of the content.	27 November 2025

1. Objectives

- The aim of this information security policy is to provide the management with direction and support for information security, and also outline the common basis for conducting an operation based on good information security practice for all employees of the organization, and external parties dealing with the organization.

2. Scope

This policy applies to:

- All resources and assets, which concern to the CK Power's information security

3. Definition

- **Company:** refers to CK Power Public Company Limited and its affiliates. Affiliates include subsidiaries and associated companies that are under the Company's control and supervision, both existing and to be established in the future.
- **User:** refers to an individual authorized to use, manage, or maintain 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.
- **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.

- **Incident:** refer to an unplanned interruption event or that could pose a threat to confidentiality, integrity, and availability of the organization's IT assets.
- **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.
- **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.

4. Policy Statement

4.1. Organizational Controls

4.1.1. Policies for information security

- The information security related policy and procedure shall be defined and approved by steering committee. It shall be published and communicated to all employees and relevant external parties after an approval.
- The information security shall be reviewed annually or if significant change occurs. The management's approval shall be obtained for the revision in the policy.

4.1.2. Information security roles and responsibilities

- Roles and responsibilities related to information security of each position in the organization shall be defined.

4.1.3. Segregation of duties

- Areas of defined roles and responsibilities shall be segregated. Conflicting of roles and responsibility shall not occurred.

4.1.4. Management responsibilities

- Management shall ensure that employees, contractors and external parties are aware of their responsibilities as defined in information security policies.

4.1.5. Contact with authorities

- Appropriate contacts with relevant authorities shall be maintained.

4.1.6. Contact with special interest groups

- Appropriate contacts with special interest groups of other specialist security associations shall be maintained.

4.1.7. Threat Intelligence

- Information security threats shall be gathered from credible sources, such as Thailand Computer Emergency Response Team (ThaiCERT), trusted vendors, industry groups, and open-source threat feeds. This information shall be analyzed to produce actionable threat intelligence relevant to the organization's environment.
- Threat intelligence shall be used to inform decisions such as security configuration changes, detection rules (e.g., IDS/IPS), and incident response planning.
- Threat sources shall be reviewed at least once a year to ensure they remain relevant and reliable.
- The organization shall document the threat intelligence process and maintain a log of key threat indicators, including source, date received, classification (e.g., TLP), and action taken.

4.1.8. Information security in project management

- Information security shall be addressed in project management. The project management shall require information security objectives, information security risk assessment and information security as a part of all phases of the applied project methodology.

4.1.9. Acceptable use of assets

- Acceptable usage of organization's asset shall be established.

4.1.10. Inventory of information and other associated assets

- All information and associated assets, including hardware, software, services, and data, shall be identified, documented, and maintained in an inventory.
- Each asset shall have an assigned owner and be reviewed at least once a year.

- The inventory shall be protected against unauthorized access and kept accurate to support information security.
- The organization shall maintain representations of authorized network communication paths and data flows, including both internal flows between systems and departments, and external flows involving third parties and cloud services.
- These representations shall be documented (e.g., data flow diagrams, network maps) and reviewed at least annually or upon significant changes to architecture or services.

4.1.11. Return of assets

- Employees shall return all of organization's asset in their possession back upon termination or change of employment.

4.1.12. Classification of information

- Information shall be classified in terms of its values, legal requirements, sensitivity and criticality to the organization.

4.1.13. Labelling of information

- Information shall be labelled with appropriate procedure as classified.

4.1.14. Information transfer

- Information shall be transferred in a secure manner appropriate to its classification. This includes use of encryption protocols (e.g., TLS, IPSec, SFTP), secure email gateways, and access-controlled channels. Data transfer activities shall be logged and monitored for unauthorized activity.

4.1.15. Access control policy

- An access to information, information processing systems, and other IT assets shall be provided based on business purposes and, need-to-know and need-to-use basis.
- An access right to information, information processing systems, and other IT assets shall be limited for accounts to the bare minimum permissions needed to perform their work.
- An access to information, information processing systems, and other IT assets systems shall be provided in according with their information classification.

- An account using for access to information, information processing systems, and other IT assets shall be distinguished from other account and can identify to owner of the account.
- High privilege account shall be provided only when there is a need to use and an approval from asset owner or authorized person is needed.
- An account and secret authentication information provided by the organization shall be handled with care.
- All activities performed during an access to information, information processing systems, and other IT assets shall be logged. These logs shall contain at least an information that can be used to identify an individual, timestamp and activity performed.
- An account that is not required shall be removed from system.
- An account is provided for an individual. It cannot be shared with another person.
- An account and its access right shall be reviewed at least once a year or when there is position change, employee leave or other situation which may affect the right to access to information, information processing systems or other IT assets

4.1.16. Identity Management

- User registration and de-registration process shall be established and implemented.
- Password management and its complexity requirement are defined and documented.

4.1.17. Authentication information

- Password and other secret authentication information shall be given to user in secure manner and also handled as sensitive information.
- Employee and individual who may hold password or other secret authentication information of the organization shall follow the practices of the organization.
- Password management and its complexity requirement are defined and documented.

4.1.18. Access rights

- Access right shall be differently provided to each type of user based on the operation needs.
- User access rights shall be removed upon termination of their contract or agreement, or adjusted upon their change of employment.
- User access rights shall be reviewed at least once a year.

4.1.19. Information security in supplier relationships

- Both pre-contract and after-contract information shall be treated as confidential information.
- Supplier shall follow the information security related policy and so other policy and code of conduct of the organization.
- Supplier shall comply with all applicable law and regulation.
- Lines of communication shall be established and maintained for identifying, escalating, and resolving cybersecurity risks originating from suppliers or external parties.
- These shall be integrated into the broader incident response and risk management workflows.

4.1.20. Addressing information security within supplier agreements

- In supplier contract shall address confidentiality agreement and security requirement of the organization, for example:
 - Supplier shall comply with all applicable law and regulation.
 - Supplier shall not lead the organization to a cyber-attack or an action against law or regulation.
 - Prior notification is needed when there is a change in supplier organization that may affect the organization.

4.1.21. Managing information security in the (ICT) supply chain

- The organization shall establish and implement processes to manage information security risks in the ICT supply chain.
- All ICT suppliers shall be identified and assessed based on their criticality.
- Security requirements shall be included in supplier agreements, and due diligence shall be performed before engagement.
- Supplier services and security practices shall be regularly monitored. Changes, incidents, and end-of-contract transitions must be managed to maintain information security throughout the supplier relationship.

4.1.22. Monitoring, review and change management of supplier services

- The service and other deliverables from suppliers shall be reviewed and evaluated to ensure that suppliers do not exceed SLA or any specifications.

- The organization shall maintain a list of critical external suppliers, services, and capabilities it depends upon. These dependencies shall be reviewed regularly and communicated to relevant internal stakeholders for inclusion in risk assessments, continuity planning, and cybersecurity strategy.

4.1.23. Information security for use of cloud services

- The organization shall establish and enforce processes for the secure acquisition, use, management, and termination of cloud services.
- Cloud service providers must comply with the organization's information security requirements, including data protection, access control, and incident handling.
- Security responsibilities between the organization and the provider shall be clearly defined in agreements.
- Periodic reviews shall be conducted to ensure ongoing compliance and risk mitigation throughout the cloud service lifecycle.

4.1.24. Information security incident management planning and preparation

- The organization shall establish and maintain an incident management plan that defines roles, responsibilities, and procedures for identifying, reporting, responding to, and recovering from information security incidents.
- The plan shall be communicated and regularly reviewed.
- The organization shall utilize a standardized methodology for evaluating cybersecurity risks, including criteria for impact, likelihood, and risk ranking.
- This method shall be documented and consistently applied across functions such as risk assessment, incident analysis, and supplier onboarding.
- The organization shall identify and evaluate strategic opportunities related to cybersecurity, such as investments that reduce long-term risk or improve business resilience. These opportunities shall be considered alongside traditional threat-focused risk assessments

4.1.25. Assessment and decision on information security events

- All reported information security events shall be assessed promptly to determine their nature and potential impact.

- Events shall be classified appropriately to decide whether they constitute security incidents requiring formal response.

4.1.26. Response to information security incidents

- Information security incidents shall be responded to according to documented procedures to contain, mitigate, and recover from the impact.
- Timely communication with stakeholders shall be ensured.
- During information security incidents, designated personnel shall share relevant information with internal stakeholders (e.g., executive management, IT teams) and external parties (e.g., regulators, customers, law enforcement) in accordance with predefined criteria and confidentiality obligations.
- All disclosures must be documented, approved, and communicated through authorized channels.

4.1.27. Learning from information security incidents

- After incident resolution, a review shall be conducted to identify root causes and lessons learned. Findings shall be used to strengthen controls and prevent recurrence.

4.1.28. Collection of evidence

- Procedures shall be established for the secure collection, handling, and preservation of evidence related to information security events, ensuring it is admissible and reliable for legal or internal investigation purposes.

4.1.29. Information security during disruption and ICT readiness for business continuity

- The organization shall plan and document a business continuity plan. This plan shall be tested and its result shall be evaluated for improvement at least once a year.
- The plan shall account for critical objectives, capabilities, and services that external stakeholders (e.g., customers, regulators) depend upon.
- These dependencies shall be identified, prioritized based on impact, and considered in recovery and continuity strategies.
- Cybersecurity risk management objectives shall align with business continuity and strategic business goals.

- These objectives shall guide prioritization of mitigation, recovery, and investment decisions.

4.1.30. Legal, statutory, regulatory and contractual requirements

- Applicable laws, regulations, and contractual obligations related to cybersecurity and privacy shall be identified, documented in a compliance register, and reviewed at least annually or when significant regulatory changes occur.
- The organization shall assign responsibility for monitoring regulatory changes, assessing their cybersecurity implications, and ensuring updates are reflected in the ISMS.
- Operations of the organization shall not violate applicable legal or regulatory requirements, and changes in such requirements shall trigger appropriate policy or control adjustments.
- The organization's cybersecurity risk activities and outputs, including residual risk levels and treatment plans, shall be integrated into its enterprise risk management (ERM) framework to ensure consistent decision-making across business domains.

4.1.31. Intellectual property rights

- Employees shall ensure that the use of intellectual property is not against the contract with property owner and applicable laws

4.1.32. Protection of records

- Records shall be protected against loss, destruction, falsification, unauthorized access, and unauthorized release through appropriate security controls, in accordance with legal, regulatory, and business requirements.

4.1.33. Privacy and protection of personally identifiable information (PII)

- Personal identifiable information shall be protected at least as required by applicable laws and regulation

4.1.34. Independent review of information security

- An internal audit shall be conducted to review a compliance with policy and procedure of the organization at least once a year
- Technical review for asset within ISMS scope shall be done at least once a year

4.1.35. Compliance with policies, rules and standards for information security

- The organization shall ensure all personnel and relevant parties comply with the established information security policies, rules, and standards.
- Compliance shall be regularly reviewed and enforced through audits and disciplinary measures when necessary.
- Findings and results from internal audits, technical reviews, security incidents, tabletop exercises, and operational process monitoring shall be used to identify opportunities for improvement in the organization's cybersecurity risk management.
- Improvement actions shall be tracked, prioritized, and integrated into planning, training, and control enhancement activities.
- Where relevant, suppliers and third parties shall be included in these evaluations and improvement planning cycles.

4.1.36. Documented operating procedures

- Operating procedures related to information processing and security shall be documented, reviewed, and made available to authorized personnel.
- These procedures shall ensure consistent and secure operations.

4.2. People Controls

4.2.1. Screening

- Background verification checks on all candidates shall be carried out in accordance with applicable laws, regulation and ethics, and needs of business requirement

4.2.2. Terms and conditions of employment

- Contract or agreement with employees and contractors shall state their responsibilities for information security and protection of organization's information

4.2.3. Information security awareness, education and training

- Awareness and training shall be provided to all employees at least once a year e.g. sending security awareness content email

4.2.4. Disciplinary process

- A formal disciplinary process shall be established



4.2.5. Responsibilities after termination or change of employment

- Termination or change of employment formal process shall be established and implemented with a combination of return of asset and user access right review process.

4.2.6. Confidentiality or non-disclosure agreements

- The organization shall identify and implement confidentiality or non-disclosure agreements with employees, contractors, and relevant third parties. These agreements shall reflect the organization's requirements for protecting sensitive information and be reviewed periodically.

4.2.7. Remote working

- Remote access can be done by only employee of the organization via laptop or notebook provided by the organization.

4.2.8. Information security event reporting

- The organization shall establish a clear and accessible process for reporting observed or suspected information security events.
- All personnel and relevant parties shall report such events promptly through designated channels to enable timely assessment and response.

4.3. Physical Controls

4.3.1. Physical security perimeters

- Security perimeters shall be defined and implemented to protect areas that store or process critical information. These include barriers such as physical locks, access cards, and alarmed zones, aligned with infrastructure segmentation policies.

4.3.2. Physical entry control

- Access to secure areas shall be restricted to authorized personnel only, using authentication methods such as key cards or biometrics.
- Visitor access shall require escort and registration. Access logs shall be monitored and retained.

4.3.3. Securing offices, rooms and facilities

- Critical workspaces and system areas shall be locked when unattended.
- Physical layout and building controls shall support secure operations and prevent unauthorized access.

4.3.4. Physical security monitoring

- CCTV and intrusion detection systems shall be deployed in key locations and monitored continuously.
- Logs and recordings shall be retained and reviewed as per internal policy or regulatory requirements.

4.3.5. Protection against physical and environmental threats

- Facilities shall be protected from fire, flooding, and other physical/environmental threats through smoke detectors, water sensors, surge protection, and HVAC systems.
- Business continuity plans shall cover these scenarios.

4.3.6. Working in secure areas

- Personnel shall follow defined rules when working in secure areas, including prohibitions on personal devices, requirements for proper identification, and adherence to clean environment protocols.

4.3.7. Clear desk and clear screen

- Workstations and documents must be cleared of sensitive information when unattended.
- Screens must be locked when inactive.
- Paper documents must be stored securely outside working hours.

4.3.8. Equipment siting and protection

- Equipment shall be located to minimize exposure to unauthorized access, accidental damage, or environmental hazards.
- Server racks must be locked and cable routes concealed.



4.3.9. Security of assets off-premises

- Off-site use of devices must be pre-approved and tracked. Assets must be encrypted or physically secured, and loss or theft must be reported immediately via the incident response process.

4.3.10. Storage media

- Storage media shall be protected throughout its lifecycle, including acquisition, transport, storage, and disposal. Transfer must align with classification level and usage controls.

4.3.11. Supporting utilities

- Critical systems shall be supported by backup power and cooling. UPS, generators, and redundant HVAC shall be tested regularly to ensure readiness for operational disruption.

4.3.12. Cabling security

- Power and data cables shall be securely routed and shielded to prevent unauthorized interception or damage.
- Access to switch panels and backbone lines must be restricted.

4.3.13. Equipment maintenance

- Regular maintenance shall be performed on all equipment to ensure operational integrity.
- Only authorized personnel may perform servicing.
- Maintenance records shall be documented and reviewed.

4.3.14. Secure disposal or re-use of equipment

- All data storage devices must be sanitized using secure deletion tools or physical destruction prior to disposal or reassignment.
- Disposal actions shall be documented and subject to verification.

4.4. Technological Controls

4.4.1. User end point devices

- The organization shall protect information accessed, processed, or stored on user end point devices by implementing appropriate security controls, such as encryption, access restrictions, and malware protection.
- Usage of such devices shall comply with the organization's security policies.
- Mobile devices which include smart phone and tablet are not allowed to use without authorization.

4.4.2. Privileged access rights

- The allocation and use of privileged access rights shall be strictly controlled and limited to authorized personnel.
- Privileged accounts shall be granted based on business needs, formally approved, regularly reviewed, and monitored for misuse.

4.4.3. Information access restriction

- Access to information and associated assets shall be restricted based on business requirements and the principle of least privilege.
- Controls shall be implemented to ensure only authorized users can access information relevant to their roles.

4.4.4. Secure authentication

- A secure authentication and authorization process shall be applied.
- The process applied shall be suit for criticality of information; classification of the information, information processing systems, and other IT assets.

4.4.5. Capacity management

- Use of resource shall be regularly monitored and planned to ensure the future capacity requirement.

4.4.6. Protection against malware

- Detection, prevention and recovery controls to protect against malware shall be implemented and keep it up-to-date.

4.4.7. Management of technical vulnerabilities

- All equipment shall be patched or up-to-dated or perform an action to manage vulnerabilities based on a recommendation from relevant external parties shall be considered to ensure that there is no effect on equipment or software as regular basis or at least once a year.

4.4.8. Configuration management

- System and security configurations of hardware, software, and networks shall be defined, documented, implemented, and regularly reviewed to maintain integrity and reduce vulnerabilities.

4.4.9. Information deletion

- Information shall be securely deleted from systems, devices, and storage media when no longer required, in accordance with its classification and applicable retention policies.

4.4.10. Data masking

- Data masking techniques shall be applied to protect sensitive data in non-production environments or when full data visibility is not required, ensuring compliance with privacy and security requirements.

4.4.11. Data leakage prevention

- Controls shall be implemented to detect and prevent unauthorized transmission or disclosure of sensitive information across systems, networks, and devices.
- Data in use, particularly sensitive or confidential information, shall be protected against unauthorized access or manipulation through appropriate technical controls.
- These may include memory-level protections, virtualization/containerization, screen protection, and role-based masking during active data processing.

4.4.12. Information backup

- Backup copies of critical information, software, and systems shall be created, protected, and tested regularly to ensure availability and integrity in the event of data loss or system failure.

4.4.13. Redundancy of information processing facilities

- Redundancy measures shall be implemented for key information processing facilities to meet availability requirements and ensure business continuity during system disruptions

4.4.14. Logging

- User activities shall be recorded, kept and reviewed regularly.
- Log shall be protected from unauthorized access and tampering.
- Administrator activities shall be recorded.

4.4.15. Monitoring activities

- The organization shall monitor networks, systems, and applications to detect abnormal activities and potential security incidents. Monitoring shall be continuous, risk-based, and aligned with legal and regulatory requirements.

4.4.16. Clock synchronization

- Information processing systems of the organizations shall be synchronized to trusted time source.

4.4.17. Use of privileged utility programs

- The use of utility programs that can override system or security controls shall be restricted and tightly controlled.
- Access shall be limited to authorized personnel, logged, and regularly reviewed to prevent misuse.

4.4.18. Installation of software on operational systems

- Only authorized personnel shall install software on operational systems.
- All installations must be approved, documented, and comply with security standards to prevent unauthorized or malicious software.

4.4.19. Networks security

- The organization shall protect its networks and network devices through appropriate security controls to prevent unauthorized access, ensure data integrity, and maintain system availability.

4.4.20. Security of network services

- Security requirements for all network services shall be identified, agreed upon, and implemented.
- Service levels and controls shall be monitored to ensure ongoing protection.

4.4.21. Segregation of networks

- Networks shall be segmented based on security and operational requirements to limit access, reduce risk exposure, and contain potential threats.

4.4.22. Web filtering

- Access to external websites shall be controlled through web filtering mechanisms to reduce exposure to malicious or inappropriate content and enforce acceptable use policies.

4.4.23. Use of cryptography

- The use of cryptographic shall be controlled and suitably applied to an information as classified.
- A cryptographic key used for an encryption shall be controlled to protect the data from unauthorized access or manipulation.

4.4.24. Change Management

- Changes to information systems, applications, and infrastructure shall follow a formal change management process to ensure they are assessed, approved, tested, and documented to prevent unintended security impacts.



CK Power Public Company Limited and its Affiliated Companies
Information Security Policy

Page 19 of 19

Revision No. 01

Effective date
November 27,2025

4.4.25. Protection of information systems during audit testing

- Audit and assurance activities involving operational systems shall be carefully planned and authorized to avoid disruptions or compromise to system security, integrity, or availability during testing.

5. Supporting Document

- N/A

It is hereby announced for general acknowledgment and action this hereby revokes the previous Information Security Policy issued on 20 February 2023, and replaces it with this revised Information Security 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