CKPower
ENDLESS ENERGY

# Information Security Policy

# of

# CK Power Public Company Limited and its Affiliated Companies

## Table of Content

DOCUMENT CONTROL ........ 1

1. OBJECTIVES ........ 2

2. SCOPE ........ 2

3. DEFINITION ........ 2

4. POLICY STATEMENT ........ 3

4.1. Information security policies ........ 3

4.2. Internal organization ........ 3

4.3. Human resources security ........ 4

4.4. Asset management ........ 5

4.5. Access control ........ 6

4.6. Cryptography ........ 8

4.7. Physical and environmental security ........ 8

4.8. Operation security ........ 9

4.9. Communications security ........ 10

4.10. System acquisition, development and maintenance ........ 10

4.11. Supplier relationships ........ 11

4.12. Information security incident management ........ 11

4.13. Information security aspects of business continuity management ........ 11

4.14. Compliance ........ 11

5. SUPPORTING DOCUMENT ........ 12

# Document Control

## Document Approvals

This document has been reviewed and approved by:

| Prepared by | Reviewed by | Reviewed by |
|---|---|---|
| (Mr. Anucha Prapadnirattisai……………………………….)<br>Date (01 /09 /2022) | (Mr. Umnath Chuencharoen……………………………..)<br>Date (01 /09 /2022) | ( Mr. Burahan Madae……………………………..)<br>Date (01 /09 /2022) |
| Document Control | ISMA | ISMR |

## History

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

| Revision | Description | Effective Date |
|---|---|---|
| **1.0** | **First creation** | |
| | | |
| | | |
| | | |

## 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.
- **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. Information security policies

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.

4.1.2. Review of the policies for information security

- 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.

### 4.2. Internal organization

4.2.1. Information security roles and responsibilities

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

4.2.2. Segregation of duties

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

4.2.3. Contact with authorities

- Appropriate contacts with relevant authorities shall be maintained.

4.2.4. Contact with special interest groups

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

4.2.5. 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.

4.2.6. Mobile devices and teleworking

- Mobile devices which include smart phone and tablet are not allowed to use without authorization.
- Remote access can be done by only employee of the organization via laptop or notebook provided by the organization.

## 4.3. Human resources security

4.3.1. Prior to employment

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

4.3.2. During employment

- **Management responsibilities:** Management shall ensure that employees, contractors and external parties are aware of their responsibilities as defined in information security policies.
- **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
- **Disciplinary process:** A formal disciplinary process shall be established

4.3.3. Termination and 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.

### 4.4. Asset management

4.4.1. Responsibility for assets

- **Inventory of assets:** asset shall be identified and documented. It shall be reviewed at least once a year to maintain the accuracy of the inventory.
- **Ownership of assets:** owner of all asset shall be identified and documented.
- **Acceptable use of assets:** acceptable usage of organization’s asset shall be established.
- **Return of assets:** employees shall return all of organization’s asset in their possession back upon termination or change of employment.

4.4.2. Information classification

- **Classification of information:** information shall be classified in terms of its values, legal requirements, sensitivity and criticality to the organization.
- **Labelling of information:** information shall be labelled with appropriate procedure as classified.
- **Handling of assets:** information shall be appropriately handled based on its classification.

4.4.3. Media handling

- **Management of removable media:** removable media, which includes device that can store data, be inserted and removed from system, shall be managed and controlled.
- **Disposal of media:** media shall be securely disposed when no longer required e.g. securely wipe out.

- **Physical media transfer:** media containing information shall be appropriately protected from unauthorized access, misuse and corruption during transportation based on its classification.

### 4.5. Access control

4.5.1. Business requirement for access control

- **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.
  - 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.
  - 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 to keep it up-to-date and accurate.
- **Access to networks and network services:** access to network and network services of the organization shall be provided with appropriate authorization based on operation needs.

4.5.2. User access management

- **User registration and de-registration:** user registration and de-registration process shall be established and implemented.
- **User access provisioning:** access right shall be differently provided to each type of user based on the operation needs.
- **Management of privileged access rights:** privileged access right shall be restricted and controlled.
- **Management of secret authentication information of users:** password and other secret authentication information shall be given to user in secure manner and also handled as sensitive information.
- **Review of user access rights:** user access rights shall be reviewed at least once a year.
- **Removal or adjustment of access rights:** user access rights shall be removed upon termination of their contract or agreement, or adjusted upon their change of employment.

4.5.3. User responsibilities

- **Use of secret authentication information:** employee and individual who may hold password or other secret authentication information of the organization shall follow the practices of the organization.

4.5.4. System and application access control

- **Information access restriction:** access to information is provided based on need-to-know basis.
- **Secure log-on procedures:** authentication process shall be established for an access to each system and application of the organization.
- **Password management system:** password management and its complexity requirement are defined and documented.
- **Use of privileged utility programs:** utility program shall be restricted and controlled. It shall be allowed only for administration access rights.

## 4.6. Cryptography

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

## 4.7. Physical and environmental security

4.7.1. Physical entry control

- Physical entry control shall be implemented to ensure that only authorized person can access to that area. Visitor who needs to access an area of the organization shall be escorted by employee. Physical access log shall be reviewed on regular basis.

4.7.2. Equipment security

- **Removal of assets:** equipment shall not be taken off-sit without prior authorization and approval from authorized person or asset owner.
- **Secure disposal or re-use of equipment:** equipment shall be securely disposed.
- **Clear desk and clear screen policy:** all information shall not be left on desk.

## 4.8. Operation security

4.8.1. Operational procedure and responsibilities

- **Documented operation and responsibilities:** procedure related to an operation shall be documented, maintained and made available to all users who need.
- **Change management:** changes of the organization which may affect information security of the organization shall be controlled.
- **Capacity management:** use of resource shall be regularly monitored and planned to ensure the future capacity requirement.
- **Separation of development, testing and operational environment:** development, testing and operational environment shall be separated.

4.8.2. Protection from malware

- **Control against malware:** detection, prevention and recovery controls to protect against malware shall be implemented and keep it up-to-date.

4.8.3. Backup

- **Information backup:** information shall be backed up regularly, and backup information shall be tested regularly.

4.8.4. Logging and monitoring

- **Event logging:** user activities shall be recorded, kept and reviewed regularly.
- **Protection of log information:** log shall be protected from unauthorized access and tampering.
- **Administrator and operator logs:** administrator activities shall be recorded.
- **Clock synchronization:** information processing systems of the organizations shall be synchronized to trusted time source.

4.8.5. Control of operational software

- **Installation of software on operational systems:** software installation shall be done by IT team or with an approval of IT team.

4.8.6. Technical vulnerability management

- **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.
- **Restriction on software installation:** software installation shall be performed by IT team or with an approval of IT team.

4.8.7. Information system audit considerations

- **Information system audit controls:** an audit activity on information processing facilities shall be carefully planned to mitigate the risk that may occur during audit.

## 4.9. Communications security

4.9.1. Network security management

- An internal network system shall be secured from unauthorized access and modification
- An internal network system shall be segregated to control an access to service, system or information within the organization.

4.9.2. Information transfer

- An information shall be transferred into secure manner and suitable with their class of information defined by the organization

## 4.10. System acquisition, development and maintenance

- A security requirement shall be defined when establishing new information processing system or project.
- User acceptance test of tool or software provided to customer of the organization shall be done.

## 4.11. Supplier relationships

- 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.
- 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.
- The service and other deliverables from supplier shall be reviewed and evaluated to ensure that supplier does not exceed SLA or any specifications.
- Supplier shall comply with all applicable law and regulation.

## 4.12. Information security incident management

- An incident response plan shall be defined.
- Roles and responsibilities with an incident response plan shall be defined and communicated to an individual.
- Evidence of an incident that occurred shall recorded as knowledge base.

## 4.13. Information security aspects of business continuity management

- The organization shall plan and document business continuity plan. This plan shall be tested and its result shall be evaluated for an improvement at least once a year.

## 4.14. Compliance

4.14.1. Compliance with legal and contractual requirements

- **Identification of applicable legislation and contractual requirement:** applicable laws and regulations are identified and maintained. Operations of the organization shall not against the applicable laws and regulations
- **Intellectual property rights:** employees shall ensure that the use of intellectual property is not against the contract with property owner and applicable laws
- **Protection of records:** all records of the organization shall be secured with appropriate control
- **Privacy and protection of personally identifiable information:** personal identifiable information shall be protected at least as required by applicable laws and regulation
- **Regulation of cryptographic controls:** cryptographic control shall be used and complied with relevant agreement, legislation and regulations.

4.14.2. Information security reviews.

- 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

## 5. Supporting Document

- N/A

It is hereby announced for general acknowledgment and action.

(Dr. Thanong Bidaya)

Chairman of the Board of Directors