The Electricity Generating Public Company Limited

Information Technology and Cyber security Policy

Document ID :	SP-0123-0002
Version Number :	1.0
Document Effective Date :	1 October 2021
Document Ownership :	Information Technology Division
Document Approver :	Kulit Sombatsiri

Version History

Version No.	Description and reason for change	Revised by	Revised date
1.0	Initial release		

ISO/IEC 27001:2013 Standard Requirements

This document is developed to align with ISO/IEC 27001:2013 standard (Clause 5.2: policy , Annex A.5:Information security policies) , Thailand's Cybersecurity Act B.E. 2562 (2019) and Thailand's Personal Data Protection Act B.E. 2562(2019)

Document Sign-off

Role	Name – Last name	Signature	Designation	Date
Authored by	Boonchot Boonkue		VP-Infrastructure Development	20 Sep 21
Reviewed by	Wutirat Chungsangsatiporn		SVP-Information Technology	22 Sep 21
Approved by	Kulit Sombatsiri		Chairman of Board of Directors	24 Sep 21

1. Introduction

Electricity Generating Public Company Limited (EGCO), or EGCO Group, has organized an information technology system of the EGCO Group to support its personnel to achieve their objectives. Business goals and in accordance with good corporate governance principles and the management of information technology systems to be efficient for the best benefit and fairness. Realizing that information is an important resource. There is a need to take precautions to ensure security. There are measures to prevent the leakage of important information. Access control and use of information are to align with the appropriate policies and practices.

1.1 Objective

The information technology and cyber security policy has been developed in accordance with the framework of the ISO / IEC 27001: 2013 standard , Thailand's Cybersecurity Act B.E. 2562 (2019) and Thailand's Personal Data Protection Act B.E. 2562(2019) with the following objectives:

1. To provide management direction and support for the information security management program as well as continuous improvement and in accordance with relevant laws and related security requirements.
2. To ensure all EGCO's employee and other who's authorized to access the ECGO's information system and comply with correctly policy property, appropriately and safely
3. To protect EGCO's information from loss, destruction, unauthorized modification, smuggling or unauthorized access disclosure of sensitive information, As well as ensures that EGCO's information are confidential, integrity and availabilities.

1.2 Scope

This document policy for IT scope is applied to all EGCO's employees and all user who is given the privileged to gain access to EGCO's system and use information processing facilities. They shall be acceptable committed and apply this security policy, principles, and practices, and cybersecurity policy.

1.3 Regular review

We are committed to maintain and review of the policies for information security in order to maintain information security (confidentiality, integrity, and availability) depend on business need at least once a year

1.4 Definition

1) “EGCO Group/Organization” means to Electricity Generating Public Company Limited (EGCO) and Subsidiary of EGCO that employee are subject to.
2) “Line Manager” means to a person with direct managerial responsibility for a particular employee.
3) “Employee” means to a person employed for wages or salary, staff and executive level, including intern, contractors, and special worker undergo agreement with Organization.
4) “User” means to all employees, contractors, vendors and any third-party relationship of the Organization who have the authorized to access Organization’s assets and information system.
5) “External Party “means to a person or another company who provide services to organization have the authorized to access Organization’s assets and information system for example
   - Business Partner
   - Outsource
   - Supplier
   - Service Provider
   - Consultant
6) “Information” means to an asset that, like other important business assets such as business information, source code, image, voice that have sensitive information, is essential to an organization’s business and consequently needs to be suitably protected.
7) “Media” means to a device kept electronic information e.g. CDs, Tape, Hard disk, Thumb drive etc.
8) “Endpoint Devices” refers to mobile computing devices such as laptops, smartphones are used by the staff or vendors in performing work for organization.
9) “Information Technology System” means to all communications system, or, computer system used in the operation of company including all hardware, software, and peripheral equipment.
10) “Access Rights” means to the permissions that are granted to a user can access to organization’s system or otherwise access a computer file. The level of access right often depends on the role in the company e.g. Admin access right can change

configuration or setting of server, User access right can access basically service system that organization provide and Special Access right assign specific permission depend need to use to access the system.

11) “Service Level Agreement” means to the level of service expected by a customer from a supplier including roles and responsibilities, period of service, condition in the agreement.

12) “Security” means to any processes or activities of control to maintenance of system and important information to prevent unauthorized access from attacker both of insider and hackers to damage the business services.

13) “Threat” means to an events, sources, actions, or inactions that could potentially lead to harm of your organizations information security assets.

14) “Vulnerability” means a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions, insufficient control) within a computer system.

15) “Technical Vulnerability” means any weakness within an organization’s information systems, internal controls, or system processes that can be exploited by cybercriminals.

16) “Access control” means to the process of granting or denying specific requests to obtain and use information and related information processing services and enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances), not limited to external party who have accepted and comply to security control.

17) “Security Incident” means to event that unwanted or unexpected could lead to loss or disruption to an Organization’s operations, services or functions such events are likely caused by intrusion or hackers.

18) “Information security risk” means to event that could lead to loss of confidentiality, loss of Integrity and loss of Availability to an Organization’s operations, services or functions.

19) “Cyber” shall include data and communication from the service providing or application of the computer networks, internet system, or telecommunication networks including the usual service provision of satellite and other similar network systems which are generally connected.

20) “Cyber threats” means to any action or unlawful undertaking by using the computer, computer system, or undesirable program with an intention to cause any harm to the

computer system, computer data, or other relevant data, and be an imminent threat to damage or affect operation of the computer, computer system, or other relevant data

21) "Cybersecurity" means to any measure or procedure established to prevent, cope with, and mitigate the risk of Cyber Threats from both inside and outside the country which affect national security, economic security, martial security, and public order in the country.

2. Information Security Protection Strategy

2.1 Security Principles

There are security principles for achieving the following objectives.

- Confidentiality is to protect the confidentiality of information It prevents unauthorized access and disclosure of information. This includes personal or proprietary information of the organization.
- Integrity is to ensure that information must not be altered, modified or destroyed by unauthorized persons.
- Availability is to ensure that authorized users can access the information system and taken continuity services.
- Accountability define the duties and responsibilities of the individual Including the liability and acceptance of the results of acting in accordance with that role
- Authentication is to ensure that access rights to computer systems and information must go through a complete identity verification process.
- Authorization is to ensure that the provision of access to information system as required (Least Privilege) and complies with the Required (Need to Know Basis) requirements as permitted.

2.2 Information Security and Cybersecurity Risk Management

Risk management is the shared responsibility of management and employees at all levels. And this needs to be continued even if the risks cannot be eradicated.

The risk management process must consist of the following main steps:

- Identifying potential risks and impacts on information security and cybersecurity
- Risk assessment

- Risk management
- Risk monitoring and reporting

3. Information Security and Cybersecurity Policy Applicability

This document, information security directives, cover the main point of the information security and cybersecurity policy set. It sets the tone of expectations towards policy compliance within EGCO.

3.1 Information Security Policy Enforcement Mechanism

In order to manage new information security and cybersecurity policy deployment as well as existing information security policy updates, a sunrise period shall be established for implementers to align themselves to the new/revised policy statement.

Managers are responsible for modifying their work processes and implementing new controls to align their team responsibilities with the new updates in the security policies while ensuring that the rest of the work processes and control implementation aligned with the existing security policies are still operating effectively within their area of responsibility.

Audit program shall be used as a means to provide independent review of information security controls and processes put in place to demonstrate the effectiveness of the information security policies.

3.2 Handling of Technical Controls Obsolescence

In the event where the obsolete technical control proves to be a critical risk to organization and has to be removed immediately, otherwise, the affected policy can be updated with an effective date to enforce a faster transition.

3.3 Handling of Policy Deviations

Any deviation from the baseline information security policies (i.e. general environment, OT environment and IT environment) shall be reviewed. The deviation shall be communicated with the interested parties and shall be reviewed on a yearly basis.

4. Policy Directives

The policy directives provide the highlights of security concerns are as follow.

4.1 General Security Management

Objective: to ensure that the responsibilities and authorities for roles relevant to information security are assigned, apply and be aware of the information security policy, where the following control principles apply,

- EGCO Group shall identify the applicable legislative and regulatory security requirements as well as customer security obligations to protect the information.
- EGCO Group shall be establish control expectations on the handling of classified information based on its characteristics and purpose shall be in place; suitable mechanism for storing and protecting such information shall be defined.
- User who having access to EGCO's information and information processing facilities shall be made aware of the acceptable usage as well as information security requirements of the EGCO's assets associated with information and information processing facilities and resources.
- User shall apply the information security and cybersecurity policy and be made aware of the minimum expectations of having to attend regular information security education and training.
- Transfer of information both internally and externally through formal information transfer agreements as well as through the use and review of confidentiality and non-disclosure agreements, especially via electronic messaging, shall be protected and secured; mechanism to enable the transfer shall be defined.
- User shall be made aware of the duty to protect intellectual property rights and reporting weaknesses observed, suspected or confirmed information security events in the EGCO Group as quickly as possible.

4.2 Endpoint Management

Objective: to ensure the security of the use of endpoint devices usage in organization.

EGCO Group shall

- establish control expectations on information security and cybersecurity requirements in endpoint devices used within Organisation’s operating environment and teleworking sites in order to minimise risk of having interception and hacked.
- implement authentication mechanism to protect information being accessed from teleworking sites.
- appropriate user awareness program shall be established to help user to stay vigilance against endpoint risk.
- enforced security control over company’s devices and personal devices to prevent information stored within these devices from being misuse for personal gains.
- backup of company's information shall adhere to guidelines and control expectations to prevent from loss of data's due to man-made/natural disasters.

4.3 Human Resource Security

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

EGCO Group apply to

- all employees shall undergo screening process to determine the suitability of the position prior to employment.
- all employees, contractors and vendors who works in the EGCO Group, physically or remotely, must have work agreements in place prior work commencement and relevant policies, processes and awareness about information security shall be made available to them.
- disciplinary process shall be enforced in the event of security violation
- information security obligations shall survive beyond the tenure of service engagement for terminating staff or staff changing their roles and respossibilities within the EGCO Group.

4.4 Physical Security and Environmental Management

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

EGCO Group shall

- clearly identify and separate physical areas with different risk exposures in terms of user accessibility into sensitive and/or critical systems and implement the security control for each area.
- establish control expectations to protect physical security perimeters, protect physical entry and restrict physical movement within the restricted area to prevent unauthorized physical access, damage and interference to the Organisation's information and information processing facilities.
- ensure control processes are defined to manage the authorised personnel, vendors and contractors operating within the physical premise.
- regular maintenance and inspections on the protection control systems shall be performed to minimise the disruption of services and utilities necessary for the Organisation's operations.

4.5 Equipment Security and Maintenance

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

EGCO Group shall

- define the control processes for maintain a listing of non-portable assets (i.e. appliances, computing desktops and servers) that have information storage or processing capability, assigning the ownership and keeping track of asset movement and lifecycle, including those that are off-premise. Authorisation shall be sought for equipment being removed from its intended location.
- establish control expectations and processes to protect Organisation equipment, both onsite and offsite against loss, damage, theft or compromise of assets and interruption to the Organisation's operations.
- be verified all items of equipment having storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

4.6 Logical Access Management

Objective: To limit access to information and information processing facilities.

- All authorised personnel who need to have access to Organisation's assets, information and system shall go through a formal user access management process based on need-to-know basis.
- Users who no longer require access to the resources shall be removed as soon as possible.
- Regular reviews of user access rights including employees, contractors, and external party users shall be conducted.
- Administrative accounts shall be managed securely and the overall control over these accounts shall not be handed over to the outsourced service provider.
- Authentication mechanism implementation must commensurate with the risk exposure in which the Organisation resource is exposed to as well as the available resources and information exposure upon successful authentication.

4.7 Network Management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

EGCO Group shall

- clearly identify and separate network zones of different risk exposures and establish control processes to authorise users to access the network and network services.
- establish control expectations to secure data transmission between operating sites, partners as well as remote users.
- identified security mechanisms, service levels and management requirements of all network services and included in network services agreements, both internally and externally.
- establish control processes for network monitoring to detect unauthorised network intrusions as well as network availability.

4.8 Operations Management

Objective: To ensure correct and secure operations of information processing facilities.

EGCO Group shall

- maintain a configuration management database for effective operations.
- appropriate documented the standard operating procedures for operational needs and made available.
- implement monitoring mechanisms and processes to allow effective response towards incidents and management of computing resources where applicable.
- establish control mechanisms to centralise and secure the logs for further log analysis.
- backup and testing of information and data shall be conducted regularly in a manner that commensurate to the sensitivity and criticality of the information in order to protect against the loss of information or data for any possible disruptive event.
- synchronised to a single reference time source for all relevant information processing systems within an Organisation.
- be tested prior to execution and ensure the implementation of rollback guidelines where updates, additions, or changes to operational software and applications.

4.9 System Administration

Objective: To define minimum security control and standard guideline for operations of information processing.

EGCO Group shall

- be implemented the control mechanism to allow effective implementation of policies and security controls to the system and network devices of interest.
- be used change management process to manage all changes made to the system and network devices.
- establish control processes to monitor the trend the resource growth.
- define standard baseline configuration(Hardening) for all system and network devices used in the operating environment.
- carefully plan to implement information system audit control and to minimize disruptions to business processes.

4.10 Cryptographic Management

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

EGCO Group shall

- establish control expectation and processes in determining the sensitivity and critically of the right kind of information to encrypt, in order to prevent unnecessary encryption of information.
- be established Cryptographic controls in compliance with all relevant agreements, legislation, and regulations. The EGCO Group shall ensure that the computers and software used to perform cryptographic functions as well as methods of access to encrypted information are in accordance with the respective countries' authorities.

4.11 Information System Acquisition, Development and Maintenance

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle (system development life cycle). This also includes the requirements for information systems which provide services over public networks.

EGCO Group needs to

- establish control expectations and processes to meet the requirement for new information systems or enhancements to exiting information systems and provide a proper development and testing environment as well as maintaining the integrity of the software used in the production environment. Both physical and logical aspects of the system and software development environment shall be protected and secured.
- establish control expectations and processes to monitor outsourced system development. The EGCO Group shall also protect its interests via licensing agreements, intellectual property, and code ownership when outsourcing system development by following guidelines of this policy.
- implement a comprehensive application testing regime including the embedded security features within, baseline security configuration review and system acceptance testing and prevent incomplete transmission, alteration, unauthorized disclosure, duplication, and mis-routing. Inclusively, data use for testing shall be appropriately selected and sanitized to avoid any unnecessary data leakage through test platforms.

- sufficient protection shall be implemented to prevent public facing systems and applications from being compromised.
- Independent review of the operation and implementation of information security and cybersecurity shall be established to ensure compliance with what is outlined by the Organization. Reviews shall be performed on a regular basis or whenever there are material changes. Reviews shall be initiated and led by the EGCO Group's management, and carried out by independent parties.

4.12 Supplier Security Management

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

EGCO Group shall

- establish audit and/or review processes the services delivered by the Suppliers to ensure both performance as well as information security and cybersecurity obligations are met.
- provided relevant information security policies and processes as well as awareness training to the suppliers so as to help them familiarize with the security expectations of the Organization.
- assessment, establish specifications and mechanisms to secure supply chain technology that interfaces with the suppliers' IT systems.

4.13 Technical Vulnerability Management

Objective: To prevent exploitation of technical vulnerabilities.

EGCO Group shall

- establish the roles and responsibilities for technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment and patching.
- appropriate contacts with specialists , security forums, and professional associations shall be maintained to improve knowledge and receive early security advisories.
- establish control processes to address and manage the discovered vulnerabilities and mitigating them.

4.14 Information Security and Cyber Incident Management

Objective: To ensure a consistent and effective approach to the management of information security incidents and cybersecurity.

EGCO Group shall

- establish roles and respossibilities in managing information security and cyber incidents.
- establish clear reporting channels for reporting information security events and weaknesses and cyber incident.
- establish control expectations and processes to manage information security incidents, events and weaknesses and cyber incidents, as well as collecting evidence for court admissibility.
- perform regular exercises and drills to get the team to be familiarized with the incident response plan.

4.15 Business Continuity and Availability Management

Objective: To protect critical business processes from the effects of major failures of information system by intention or disasters.

EGCO Group shall

- identify the availability and recovery requirements (e.g. recovery time objectives and recovery point objectives) derived from business expectations, minimum business continuity objectives and critical business functions.
- identify technology required to meet the availability and recovery requirements as well as well developing and approving plans detailing the response and recovery of the information systems and business services aligned with the expected availability and recovery requirements.
- provide backup system or technology requires to meet the recovery plan.
- regular tests and updates shall be performed to help recovery team familiarize with the recovery steps as well as to determine the sufficiency of the planned financial and technical resources for recovery.

4.16 Personal Data Management

Objective: To ensure to protect the personally identifiable information as required in relevant legislation where applicable.

EGCO Group shall

- define a privacy policy to allow customers understand about how oorganization use and store their personal information
- establish control processes to protect the personal data and only use them based on legitimate business need.
- destroy the personal data after the use of the personal has expired.
- identify roles and responsibilities of data protection officer(s) or relevant parties with touch points pertaining to visitor, customer and staff personal information shall refer to the following related tactical policies as follows Personal Data Management Policy

5. Compliance

We are committed to comply with all applicable Information Security and Cybersecurity policy as well as information security and Cybersecurity and End User Security Guideline as attachment of this announcement.

Effective date 1 October 2021

Announcement date

Kulit Sombatsiri

(Mr. Kulit Sombatsiri)