Announcement No. 4/2023
Office of the Managing Director

CYBERSECURITY AND INFORMATION SECURITY POLICY (REVISED EDITION NO. 1/2022)

Document Ref.: DMT/P/CS/006/23

Pursuant to the resolution of the Information Technology Governance Committee Meeting No. 14/2022 held on 12 December 2022, the revised Cybersecurity and Information Security Policy was approved as follows:

Information technology systems are developing rapidly and play an increasingly important role in organizational operations. The use of advanced information technology for transactions and communications has also created an environment conducive to cyber threats and cybercrime, whose impacts may spread rapidly and have become increasingly severe. Such threats can cause damage at the individual, organizational, and national levels. Accordingly, preventing and responding to threats or risks relating to information security and cybersecurity is of critical importance.

This Policy is established to ensure that the Company's information technology and communications systems are secure, reliable, and capable of effective operation; that electronic activities are conducted securely and credibly; and that the Company's personnel understand the importance of information security and comply strictly with this Policy.

Definitions

1. Personnel means the Company's employees, workers, and contracted personnel.
2. Asset means anything that has value to the Company.
3. Information security means the preservation of confidentiality, integrity, and availability of information, including authenticity, accountability, non-repudiation, and reliability.
4. Access to or control over the use of information means the authorization, assignment of rights, or delegation of authority to personnel to access or use networks or information systems, electronically or physically, including equivalent authorization for external parties, together with requirements intended to prevent unauthorized access.
5. Undesirable or unforeseen information security incident means an undesirable or unforeseen security situation that may result in the Company's information systems being intruded upon or attacked, or their security being threatened.
6. Computer Center means the server room (Data Center), communications network room (Network Room), and disaster recovery site (DR Site).
7. Cybersecurity means measures or actions established to prevent, respond to, and reduce risks arising from cyber threats, whether originating domestically or internationally, that may affect national security, economic security, military security, or public order.

8. Cyber threat means any unlawful act or operation using a computer, computer system, or malicious program with the intention of harming a computer system, computer data, or other related data, where such act constitutes an imminent danger likely to cause damage to or affect the operation of a computer, computer system, or related data.
9. Critical information infrastructure means a computer or computer system used by a government or private-sector entity in activities relating to national security, public safety, national economic security, or infrastructure serving the public interest.
10. Office means the Office of the National Cyber Security Agency.
11. Regulatory or supervisory authority means a government agency, private entity, or person legally vested with duties and powers to regulate or supervise the operations of a government agency or a critical information infrastructure organization.

The following cybersecurity and information security guidelines are based on ISO/IEC 27001:2013.

1. Information Security Policy
Objective

To provide direction and management support for the Company's information security in alignment with business operations and the information security policy.

Guidelines

1.1 The Company shall maintain a written information security policy approved by the Company's management.
1.2 The information security policy shall be reviewed at least once a year or whenever appropriate.

2. Organization of Information Security
Objective

To strengthen the effective management of the Company's information security by clearly defining personnel responsibilities for information security governance and by establishing measures to review internal units and external parties that directly or indirectly interact with information assets.

Guidelines

2.1 Responsibilities for the Company's information security shall be clearly defined.
2.2 An information security committee or working team shall be established.
2.3 A formal approval process shall be established for the use of information-processing facilities, and compliance with that process shall be controlled.
2.4 A current contact list shall be maintained for relevant organizations, such as the Royal Thai Police, cybersecurity coordination centers, and Internet service providers, for information security coordination when necessary.
2.5 Information security risks associated with external service providers shall be assessed.

3. Asset Management
Objective

To prevent damage to information assets by maintaining an inventory of the Company's assets, classifying them by importance, establishing appropriate controls, and assigning clear accountability.

Guidelines

3.1 An inventory of information assets shall be prepared and kept accurate and up to date,

3.2 Information assets shall be classified according to confidentiality level, value, legal requirements, and importance to the Company.

3.3 Asset labels or records shall identify relevant details and the person responsible for each inventoried information asset.

3.4 Personnel shall take responsibility for assets entrusted to them by the Company as though such assets were their own.

4. Human Resource Security

Objective

To ensure that personnel are appropriately recruited, understand and perform their assigned roles and information security responsibilities, receive role-appropriate awareness and training, and are properly managed when employment or duties change or end. Violations or negligence relating to information security shall be handled formally and fairly.

Guidelines

4.1 Information security responsibilities shall be assigned to personnel in accordance with the Company's information security policy.

4.2 Information security awareness, knowledge, and training shall be provided to personnel.

4.3 Personnel shall return information assets when employment ends or duties change.

4.4 Access rights to information and information assets shall be revoked when employment ends or duties change.

4.5 Disciplinary measures shall apply to personnel who violate the Company's information security policy or guidelines and cause damage to the Company.

5. Physical and Environmental Security

Objective

To prevent unauthorized physical access to information security equipment and important information assets. Such assets shall be located in secure, controlled areas and protected against unauthorized access, damage, disruption, theft, and other threats, including where equipment is used off-site or is portable.

Guidelines

5.1 Physical access controls shall be designed for work areas requiring physical security protection (Secure Areas).

5.2 Entry and exit controls shall be implemented for secure locations or areas, and access shall be permitted only to authorized persons.

5.3 Protection shall be provided against threats such as fire, flood, earthquake, and other human-made or natural disasters.

5.4 Mechanisms shall be established to prevent failures of systems and supporting utilities, including electricity, air-conditioning, and backup power systems.

5.5 Equipment shall be maintained to ensure continuous and reliable operation.

5.6 Work areas shall be kept secure. Important documents and removable storage media, such as flash drives, shall not be left unattended when not in use and shall be managed in accordance with the confidentiality classification of the information.

5.7 Computers shall be secured when unattended to prevent unauthorized access.

5.8 Rules shall be established for the use of the Computer Center.

6. Communication and Operations Management

Objective

To ensure that communications and operations involving information assets are appropriately controlled, monitored, and tested; that important information is backed up; that storage media and information exchanges are controlled; and that process responsibilities are clearly assigned.

Guidelines

6.1 Operating procedures relating to information security shall be documented, maintained, and kept available so personnel can perform their duties correctly.

6.2 Measures for detection, prevention, and recovery shall be implemented to protect information assets against malicious software.

6.3 Important information shall be backed up and backup data shall be tested regularly.

6.4 Measures shall be implemented to protect against computer-network threats and to secure applications operating on networks.

6.5 User activities, system service denials, and information security-related events shall be logged regularly.

6.6 Procedures shall be established for regular monitoring of system use and information asset use.

6.7 The operations of external service providers shall be monitored and reviewed.

6.8 Storage media shall be managed appropriately.

6.9 Information exchanges shall be managed securely through documented procedures. Where information is exchanged with an external service provider, a confidentiality or non-disclosure agreement shall be executed.

6.10 Future information-resource capacity requirements shall be planned to support increased system usage.

6.11 Logs relating to system administration shall be retained.

6.12 System and equipment clocks shall be synchronized with a reliable time source.

7. Access Control

Objective

To control access to data, information systems, networks, and other information assets so that access is granted only to authorized persons through appropriate registration, de-registration, authorization, and periodic review processes, together with proper creation, use, storage, and destruction of important documents and storage media.

Guidelines

7.1 Access to information shall be controlled and restricted according to business need.

7.2 A formal password management process shall be established for personnel, including controlled password allocation.

7.3 Communication ports used for system inspection and configuration shall be protected.

7.4 Access rights and controls over information use shall be reviewed at defined intervals.

7.5 Privileged access rights shall be managed and used only when necessary.

8. Information System Acquisition, Development and Maintenance

Objective

To ensure the effective and secure acquisition, development, and maintenance of information technology systems throughout the system development life cycle. Security requirements, procurement and engagement criteria, support controls, development controls, cryptographic measures, security reviews, and technical vulnerability management shall be established to prevent error, loss, unauthorized alteration, and misuse.

Guidelines

8.1 Input data validation and output data validation shall be implemented for applications to ensure that information is accurate and appropriate before processing.

8.2 Access to application source code used within the Company shall be restricted to prevent unauthorized changes.

8.3 Information concerning vulnerabilities shall be monitored, and vulnerability assessment and testing shall be performed on systems in use.

8.4 Encryption measures shall be applied to protect the confidentiality of important information.

8.5 For critical information systems, development, testing, and production environments shall be segregated.

8.6 Test data shall not be actual production data and shall not adversely affect personal data.

8.7 System developers shall submit requests for approval of new system development or modifications to existing systems, including sufficient details for review by authorized persons.

8.8 Both internal developers and external service providers shall comply with security requirements, including confidentiality, data integrity, availability, user identification, authentication, authorization, event logging, and continuity of information technology services.

8.9 Baseline security requirements shall be included in engagements of external service providers for new system development, enhancements to existing systems, and the procurement of processing, network, and security equipment.

8.10 Controls shall be established for information transmitted or exchanged in online transactions.

9. Information Security Incident Management

Objective

To ensure that undesirable or unforeseen information security incidents are handled effectively through systematic and timely reporting, notification, response, defined roles and procedures, compliance with applicable rules and laws, and continual improvement to prevent recurrence.

Guidelines

9.1 Information security breaches and incidents shall be recorded so that lessons can be learned and necessary preventive measures can be prepared.

9.2 Undesirable or unforeseen information security incidents shall be reported.

9.3 Personnel and software shall be provided to monitor information security breaches.

10. Business Continuity Management

Objective

To prevent disruption of the Company's activities and failure of critical information systems by establishing, testing, and regularly improving business continuity plans to minimize impacts on the Company.

Guidelines

10.1 Risks that may affect business continuity and cause disruption or failure shall be assessed.

10.2 Business continuity plans shall be prepared to ensure that business can continue if information systems are disrupted or fail.

10.3 Business continuity exercises shall be conducted to verify that business can continue if information systems are disrupted or fail.

10.4 Adequate resources shall be prepared and made available when business continuity plans must be activated.

11. Compliance

Objective

To prevent violations of legal, regulatory, contractual, and business requirements relating to information assets by establishing appropriate compliance review processes and controls over audit activities and audit tools.

Guidelines

11.1 Supervisors shall oversee and control the work of their subordinates to ensure compliance with the Company's information security policy.

11.2 Measures shall be established to prevent personnel from using information-processing facilities for improper purposes or without authorization.

11.3 Information systems shall be audited regularly to ensure compliance with the Company's information security standards.

11.4 The Company shall maintain a personal data protection policy.

12. Cryptographic and Key Management

Objective

To apply appropriate and effective encryption to protect confidentiality, prevent data falsification, and preserve data integrity.

Guidelines

12.1 Measures shall be established for encrypting important electronic information of the Company.

12.2 Internationally recognized cryptographic algorithms shall be used. Proprietary or self-developed encryption methods shall be avoided to ensure that the algorithms employed are secure.

12.3 Cryptographic algorithms and key lengths shall be reviewed at least once a year to ensure continued security.

12.4 A cryptographic key management process shall cover key generation, storage, distribution, and replacement.

13. Mobile Device and Teleworking

Objective

To ensure the secure use of mobile communications devices and secure work performed outside the Company's premises.

Guidelines

13.1 The use of mobile devices within the Company shall be controlled, including controls for access to the Company's network, such as device registration.

13.2 Personal mobile devices may connect only to information systems and networks that implement authentication controls.

13.3 Personal mobile devices used for work outside the Company shall comply with access-control requirements and connect to the Company's information systems only through channels provided by the system owner.

13.4 Personnel shall receive awareness guidance regarding the use of personal mobile phones, smartphones, tablets, and notebook computers.

13.5 Remote access shall be restricted and shall require approval from the Information Technology Department.

13.6 Users outside the Company shall be authenticated before being permitted to access the Company's computer networks and information technology systems.

14. Supplier Management

Objective

To protect Company assets that may be accessed by external service providers and to ensure that external service levels conform to agreed service-level commitments.

Guidelines

14.1 External service providers requiring access to important Company information shall sign a confidentiality agreement.

14.2 The performance of external service providers shall be monitored to ensure compliance with service-level agreements.

14.3 Information security risks associated with external service providers' operations shall be assessed.

15. Cybersecurity Management

Objective

To prevent, respond to, and reduce risks arising from cyber threats and to define response guidelines and cybersecurity measures for information security events or undesirable or unforeseen security incidents.

Guidelines

15.1 Cybersecurity risk assessments of critical information infrastructure shall be conducted by assessors, and cybersecurity audits shall be performed by internal auditors or independent external auditors at least once a year.

15.2 A cyber threat response plan shall be established for responding to cyber threats and cybersecurity incidents.

15.3 A responsible unit shall be designated to monitor and respond to cyber threats and cybersecurity incidents.

15.4 Cyber threats and cybersecurity incidents relating to critical information infrastructure shall be monitored.

15.5 Where a cyber threat has a material impact on the Company's systems, the incident shall be reported to the Office and the relevant regulatory or supervisory authority, and the cyber threat response plan shall be implemented.

15.6 Where a cyber threat occurs or is expected to occur against an information system under the Company's responsibility, relevant information, computer data, computer systems, and surrounding circumstances shall be examined to determine whether a cyber threat exists. If a threat is confirmed or reasonably anticipated, the Company shall prevent, respond to, and reduce the risk in accordance with the cyber threat response plan and promptly notify the Office and the relevant regulatory or supervisory authority.

15.7 The Company shall coordinate and cooperate with the Office in preventing, responding to, and reducing risks arising from cyber threats.

Announced on 4 January 2023

(*Signed*)

(Dr. Sakda Panwai)
Managing Director