Nova Organic Public Company Limited
190/4 Moo 8, Naikhlongbangplakot,
Phrasamutchedi, Samutprakan 10290
Tel +66 (0) 2-417-1130
Tax ID : 0107564000201

-Translation-

Information Technology Security Policy

Nova Organic Public Company Limited

Execution No.	00
Effective Date	12/07/2021
Prepared by	..... (Ms. Haruethai Sirisinvibul) Company Secretary
Approved by	..... (Mr. Prakit Tangtisanon) Chairman of the Board of Directors

บริษัท โนวา ออร์แกนิค จำกัด (มหาชน)
190/4 หมู่ที่ 8 ตำบลในคลองบางปลากด
อำเภอพระสมุทรเจดีย์ จังหวัดสมุทรปราการ 10290
เลขประจำตัวผู้เสียภาษี : 0107564000201
โทรศัพท์ +66 (0) 2-417-1130
www.nova-organic.com

Table of Content

			Page
1	Explanatory		3
2	Objectives		3
3	Scope of Enforcement		3
4	Definition		3
5	Roles, Duties, and Responsibility		5
6	Section 1	Information Technology Supervision and Management	6
7	Section 2	Policy determination, measures, and a management structure to maintain the security of information system, information asset management and access control to data and Information system	10
8	Section 3	Security of Information Communication via Computer Network and Security of operation related to Information Technology System	23
9	Section 4	Other Criteria	32
10	Appendix and Updated Information		34

1. Explanatory

Nova Organic Public Company Limited recognizes the importance of information technology adoption in business management. Hence, the Company has established this policy to provide the good corporate governance practice and management framework based on the principles of the rules and practices of information technology system provision, as well as information system security practices in accordance with the Securities and Exchange Commission's guidelines and other related laws. The Information Technology Policy is defined as follow:

1) Information Technology Resources Allocation and Management Policy
2) Information Technology Risk Management Policy
3) Information Technology Security Policy

2. Objectives

The Information Technology Security Policy is being implemented to ensure that the Company has a corporate-level information technology supervision and management framework that fulfil the Company's requirements, and that information technology can support and develop business operations, risk management, and enable the Company to achieve its core objectives and goals by appropriately using resources and risk management in accordance with good corporate governance.

3. Scope of enforcement

This Information Technology Security Policy applies to Nova Organic Public Company Limited. Previous policies, guidelines, regulations, and directives will continue to be in effect as long as they do not contradict or are in conflict with this Policy.

4. Definition

Terms	Definition
Company	Nova Organic Public Company Limited
Chief Officer	Chief Officer of Nova Organic Public Company Limited
Management	Director and Chief Officer of various divisions of the Company
Policy	Information Technology Policy

Terms	Definition
Information Technology Division	The division under the Company's structure responsible for information technology.
User	Full-time employees, contractual employees, external service providers, business partners or customers.
External service providers	Third party persons hired by the Company to provide the services related to information systems, and information technology systems.
Personnel	Staffs or employees under information technology division and external service providers
Methodology	Procedures for managing information technology
Information Technology Resources	1) Information Technology System 2) Personnel 3) Computer equipment
Information Assets	1) System-type information assets such as computer networking, computer systems, and information systems. 2) Equipment-type information assets such as computer device, computer equipment, data storage, and any other devices 3) Information assets such as data information, electronic information, and computerized information 4) Copyright information assets such as developed assets or the right of use granted by the product owner.
Data Processing Facilities	Equipment, systems, or environments that are required or contribute to the complete, accurate, and efficient processing of data.

5. Roles, duties, and responsibilities

5.1 Board of Directors

5.1.1 Define the Company's Information Technology Policy

5.1.2 Supervise management to comply with the policy in accordance with the requirements of the Company, as well as supporting and developing business operations, risk management to achieve its core objectives and goals

5.1.3 Review or update the Policy at least once a year, or when there are any incidents that may significantly affect the supervision and management of information technology.

5.2 Management

5.2.1 Define guidelines, principles and regulations relating to the Policy

5.2.2 Monitor, control and supervise relevant parties in accordance with the Policy.

5.3 Information Technology Division

5.3.1 Monitor users to properly comply with the relevant Company's Policies and regulations and in the event of any wrongful practices, the case shall be reported to management

5.3.2 Communicate the Policy to users, related business operators in an easily accessible manner so that such personnel can understand and follow such Policy correctly.

Section 1

Information Technology Supervision and Management of the Company

1.1 Information technology risk management encompasses risk identification, risk assessment, and risk control to the Company's acceptable level by establishing cooperation from all parties to gain an understanding of information assets in order to maximize the efficiency of operations involving information assets.

1.2 Allocate and manage information technology resources that cover the allocation of sufficient resources to conduct business operations and establish guidelines to support them in the event that resources cannot be allocated as defined, such as:

1.2.1 Personnel allocation has been planned or a personnel allocation policy is in place.

1.2.2 Human Resource Department shall:

1) Make a public announcement and hire employees in accordance with the policy
2) Notify the system administrator to properly and adequately prepare the information assets in accordance with the policy

1.2.3 System Administrator shall:

1) Allocate, transfer or purchase information assets based on the position of responsibility
2) Implement the control of information assets registered book and make copies of related documents for separate storage for verification purposes, such as tax invoices of computer devices, computer equipment, and copyrights (licenses). In case of asset transferring from the head office to a branch office, a control document must be copied and kept separately.

1.2.4 The Procurement Department is responsible for acquiring Information Assets (In case of lack of spare information assets)

1.2.5 Accounting/Finance Department is responsible for registering information assets.

1.2.6 Others

1.3 Supervision of information systems relating to human resources

1.3.1 Prior to the start of employment

1) Employees' responsibilities in relation to information security must be determined by the Company. In terms of personnel qualifications in accordance with assigned duties, the Human Resources Management Division must verify all candidates' qualifications before hiring them as Company employees. Criminal records or other records must be checked in light of the circumstances.
2) The Human Resource Management Division shall determine the terms of employment, including working conditions and responsibilities for the Company's information security.
3) In order to ensure the most accurate and up-to-date management of User ID, the Human Resource Management Division must notify the responsible division as soon as the following is discovered:
    - Employment
    - Change of conditions of employment
    - Resignation and termination of personnel
    - Rotation
    - Suspension, disciplinary or suspension of duties

1.3.2 During Employment

1) Providing officers with information security education and training at least once a year
2) As part of their orientation, new employees must be trained in Information Security Policy. Such training must be recorded and stored in the system.
3) The responsible division must inform about the Information Security Policy and its changes in relation to information system security.

1.3.3 Position change or termination of employment

1) The responsible division must change and deliver information so that the Information Division can deal with user’s rights regarding the use of information

systems as their employment status changes. The data must be collected so that they can examine the history of changes in those information systems.

2) Upon termination or change of employment condition, users must immediately return Company assets in connection with his/her duties with the Company, such as information systems equipment, information and copies of information, keys, identification cards, any in-out passes, or equipment that belong to the Company.

1.4 Allocation and management of information technology resources

To achieve the mission's goals, the Company requires that information technology resources be allocated and managed in accordance with the Company's strategic plan. The following are the defined strategies and operational action plans:

1) Define guidelines and factors for prioritizing information technology plans, such as fit with the Company's strategic plan, impact on business operations and urgency level
2) Prepare and approve information technology budgets in accordance with the Company's overall budget and strategy
3) Provide adequate manpower for performing information technology function, provide or develop personnel skills, and hire information technology expert
4) Manage risks in the event that insufficient resources are allocated to information technology operations, whether personnel, budgets, or demands that exceeds the limit
5) Define the roles and responsibilities of personnel under the Information Technology Division in the allocation and management of the Company's information technology resources
6) Assets including computer equipment and data accounts stored in different location of the Company must be registered and clearly categorized in order to determine the value of assets, specifying the owners of each asset, and auditing those assets for the specified period at least once a year
7) If any division uses software assets for the Company operations without paying royalties, they must be recorded in the registered book and a copy must be submitted to the Information Division, which is in charge of managing the Company's data and assets in order to identify, track, and investigate vulnerabilities that could jeopardize information security

8) A responsible division must be in charge of compiling a list of computer equipment, network equipment, software, or rented computer systems
9) The assets must be used with care and maintenance in accordance with their intended usage
10) Restrict the access to data, information system, and data processing facility
11) Implement physical and environmental security to prevent people without relevant authority from accessing computer network locations, which can damage information devices or affect confidential or sensitive information.

Section 2

Policy determination, measures, and a management structure to maintain the security of information system, information asset management and access control to data and information system

2.1 Implementation of information system security policy and procedures

2.1.1 Setting up the intrusion prevention system (Firewall)

2.1.2 Installing antivirus software, antispyware, malware, and security patch updates

2.1.3 Assigning information access or usage rights to each user's host computer or group of users

2.1.4 If the use of a peripheral device via a USB port is required, the request for permission to use must be documented and approved by the authorized person or the management before being submitted to the system administrator for processing

2.1.5 The right to use and the use of storage media and various portable computer devices containing confidential information belonging to the Company (such as thumb drives, CD, and DVD) must be carefully determined and used. Personal belongings must be registered and approved by a supervisor, authorized person, or executive and submit to the system administrator before using such belongings

2.1.6 Information pertaining to the Company's operations, whether stored on the user's computer or on host computers managed by administrators, must be backed up on a regular basis in order to recover the data when problems arise.

2.1.7 Backups must be kept in at least two locations, such as the headquarters and the branch.

2.1.8 Users are responsible for using the Company's computers and devices with care and protecting them as their own assets. When working outside the premises, the user must take care of and be accountable for the computer equipment assigned by the company.

2.1.9 The operating system password must be used to protect all of the Company's computers, portable computers, and host computers. The computer must be Log Off when not in use.

2.1.10 Before being installed on the Company's information technology system, software used to process and store confidential or sensitive information for the Company, whether derived

from user-generated content or purchased, must be properly inspected, controlled, and approved by the division responsible for such system or information.

2.1.11 Users must use network resources wisely and refrain from downloading/uploading data or anything else unrelated to work. When using the Internet, users are not permitted to click on pop-up advertising windows or visit any website unrelated to the work because there could be a program on the user's computer that steals information from the user's computer. The users are not allowed to use the website that is unrelated to the Company's work or business. The use must not be defamatory to the Company or other people, nor must it be related to illegal acts or the computer-Related Crime Act. The Company reserves the right to inspect and record a user's computer usage history in order to verify inappropriate access.

2.1.12 Organize training to educate users on the importance of preventing and creating security for information assets, as well as the practices, procedures, and risks involved. This includes informing users about new laws, regulations, policies, and changes that affect the Company's information assets.

2.1.13 Updating information technology assets registered book regularly.

2.1.14 The policy should be reviewed and updated at least once a year and to update the process and operational procedures to reflect the changed policy.

2.2 E-mail usage

2.2.1 The email account must be protected with a password.

2.2.2 All e-mail accounts and e-mails (including personal emails) created and maintained on the Company's computer system or networking system are the assets of the Company.

2.2.3 The mailbox size of the user on the central server is limited. When the e-mails storage is extent and approaching the set area size, the system will send an alert to users. Users will be unable to send and receive emails as usual if the size of the e-mail exceeds the limit. If the email and attachments file larger than the limit, the user will receive a notification letter that the e-mail could not be sent. Users must always delete unnecessary emails from their mailboxes in order to keep the Company's e-mail storage at the size specified.

The user is required to keep email that is relevant to the job and email that is required by laws only.

2.2.4 Do not use the Company's email account to engage in any illegal activities, violate any Act, regulations, and Computer-Related Crime Act B.E. 2560 (2017), or violate any Company's policies. If it is discovered that a user has submitted information in violation of the Computer-Related Crime Act B.E. 2560 (2017) or the Company's regulations, the supervisor or computer division officer must be notified promptly.

2.2.5 E-mail software should always be configured to include the sender's signature. The signature must include the following information: name and surname, position, division's name, company's name, and phone number. The disclaimer message must be included in all Company emails. In the case of an email sent to a customer, payment information such as account number and account name, as well as the type of payment account, must be confirmed to prevent data theft, internet scams (Phishing Mail) from obtaining information or deceiving customers to pay through other channels.

2.2.6 When sending electronic mail, having a conversation, or any other type of communication via electronic mail, the user must carefully craft the email's contents and use a polite message. The users shall aware that the email is being sent on behalf of the Company. The user is strictly prohibited from sending or forwarding any email that contains content or images that disparage other people, racism, intimidation, obscenity, sexual provocations, or emails that raise cultural or religious concerns, including emails that jeopardize national security or the monarchy, or any other file that is unrelated to work and has a negative impact on the Company.

2.2.7 Users must take extra precautions when opening attachments received from senders they do not recognize because viruses, e-mail bombs, and phantom programs may be contained in attachments (Trojan horses).

2.2.8 When antivirus software alerts the user that the computer is infected with a virus, the user must suspend sending e-mail immediately until the computer is restored to normal operation.

2.2.9 Communication via electronic means, whether it is an electronic letter, a conversation, or any other form of communication, is considered a single formal mailing that must adhere to the Company's letter delivery rules:

1) Maintain document confidentiality by establishing a standard for sending e-mails or files with specific words to prevent the document from being delivered outside of the Company
2) Prohibit from sending confidential documents via email except they are encrypted and confirmed by the computer division.

2.2.10 Do not send wrongful information or information with possibility to harm the Company or third parties.

2.2.11 Do not send electronic mail or any other electronic communication in which the sender's name is not specified (SPAM e-mail)

2.2.12 Employees are not permitted to use any other e-mails that are not required by the Company.

2.2.13 Establish guidelines for naming work files in the same format for easy understanding and in order according to the Company's internal notices.

2.3 Risk Management Policy

2.3.1 The Information Technology Division must identify information technology risks (IT-related risk).

2.3.2 Risks must be evaluated based on likelihood or frequency, as well as their significance or impact.

2.3.3 Risk indicator must be defined for significant risks as specified in 3.2.1, as well as monitoring and reporting of such indicators so that risk can be managed appropriately and on timely basis.

2.3.4 Specify the duties and responsibilities of the responsible person as well as the person in charge of information technology risk management.

2.4 Physical Security

2.4.1 Access control must be provided in the area where security is required.

2.4.2 Only those who have been authorized are permitted to enter and exit. If a person who is not a system administrator requests to enter the area without obtaining permission to do so, the reasons and necessities must be considered before allowing or temporarily prohibiting a person from entering the area. Individuals must present an identity card or other government-issued card or attach a Plant Visit Gate Pass as evidence. System administrator must record the accessible request or store a Plant Visit Gate Pass as evidence (Both in case of permission and prohibit to enter the area). Third-party access to the server room/data center must be recorded and stored for at least one year (or as appropriate).

2.4.3 No equipment or parts are removed from the Server Room/Data Center unless obtaining approval from system administrator. Connection of any other tools or devices to the network for personal purposes is prohibited. Under no circumstances, use or delete other people's data files is not allowed. Copy of licensed data files could not be done before permission is granted.

2.5 Using network from computer that are not the Company’s information assets must be approved by the system administrator. If the unauthorized use of network is discovered, system administrator can immediately disconnect from networking. If the user installs or publishes pirated software on the Company's data assets, the user will be held accountable for the unintentional offense.

2.6 In order to supervise the external service provider, an agreement to regulate information technology services by third-party as follow.

2.6.1 External service providers must accept the Company's information security policy and be subject to information security regulations in order to prevent unauthorized access to the Company's information assets.

2.6.2 Scope, particulars, and Service Level Agreement.

2.6.3 Physical and logical documentation for control measurement.

2.6.4 Establish policies for suppliers or vendor on information disclosure, accessible to the information for work, authorization to the server and databases, borrowing or requests for

the use of the Company's equipment, other external device extensions, as well as third-party networking agreements, in accordance with the Company's notification.

2.6.5 When it is necessary for IT Outsourcing to access the Company's data or assets, security requirements for the Company's information must be developed in accordance with the Company's data confidentiality requirements, data security regulation, legal requirements such as privacy and data protection in which the Company communicates and enforces before allowing the access.

2.6.6 System administrators shall monitor, review, and evaluate external services on a regular basis in accordance with the terms specified in the agreement.

2.6.7 The system administrator oversees the change management in the provision of services by third-party service providers, including evaluating service providers, to ensure that the system of third-party service providers maintains information security in all three areas: confidentiality, integrity, and availability.

2.6.8 System administrator shall supervise the third-party service provider's performance in accordance with the agreements provided with the business operator.

2.6.9 When the Service Agreement for a critical system is changed, the security risk assessment must be conducted.

2.6.10 Upon a change in management, including improving or modifying the information technology system, there must be a responsible person and authority to change, control, improve, or modify the Company's information technology system.

2.6.11 Separation of development, test, and operational facilities necessitates the storage of operational evidence for later review.

2.6.12 To avoid work impact, defining the measures to segregate the computer working system for development, testing, and service is needed.

2.6.13 Define measures to control the transfer of working systems from development units to service devices.

2.6.14 Prevent unauthorized access to software tools and utilities used in the creation of working systems.

2.6.15 Requires user accounts to be separated for the system used for development, testing, and actual work.

2.6.16 The development and maintenance of information systems necessitates the security of information system development processes in order to develop or modify information systems that are processed correctly, completely, and in accordance with the needs of the user, as well as maintaining information system security throughout the development process.

2.7 Business Continuity Management Policy

2.7.1 The Company requires that the security of information systems be part of the Company's business continuity management so that the Information system is always in a ready-to-use condition.

2.7.2 Information Technology Division must prepare a plan to address the uncertainty and disasters that may occur to the information system in accordance with the Company's Crisis Management Plan.

2.7.3 Audits and assessments of potential information system risks must be carried out at least once a year.

2.7.4 Emergency preparedness plans must be reviewed at least once a year.

2.7.5 The availability of the backup information system must be checked at least once a year.

2.7.6 Preparation of backup processing equipment (Redundancies)

2.8 Management of incidents that may affect the security of information systems of the Company.

2.8.1 The Company shall define procedures for managing events that may compromise information system security, as well as assigning people with the necessary knowledge, skills, and experience to be in charge, and providing rapid and timely reporting of incidents through individuals or entities responsible for informing incidents and flaws in information system security. This is to ensure that the event and sensitive information system security concerns are handled properly.

2.8.2 In reaction to occurrences involving the Company's security, responsibilities and procedures must be established.

2.8.3 Communication channels must be defined to clearly report the security situation of the information system.

2.8.4 If the user notices something that could jeopardize the information system security, he/she must notify it to the Information Technology Division.

2.8.5 Information system security incidents must be notified in accordance with the severity of the issue. If there is a significant impact on a large number of users, the notification must be given as soon as possible.

2.8.6 Security breaches must be documented, at the very least in relation to the nature of the occurrence, volume, and the amount of damage with aiming to set a precedent case and plan for protection.

2.8.7 Evidence must be collected and stored according to the rules or criteria that will be used in court proceedings.

2.9 Standards for physical security and environmental control

2.9.1 Supervision access control and control of the server computer room surroundings requires extra carefulness. Important computer equipment, such as servers and network equipment, must be stored in computer centers or restricted areas. Only necessary personnel, such as computer operators and system administrators, will be permitted access to the computer center.

2.9.2 If a person who does not have a regular relevant duty request to occasionally access the computer center, there should be strictly controlled, for example, by assigning computer center employees to maintain a continual monitor during the working hours.

2.9.3 A computer center access log must be recorded, such records must contain personal details and access time, and such records should be checked regularly.

2.9.4 For ease of working and efficient access to vital computer equipment, the computer center should be divided into different sections such as network zone, server zone, and printer zone. The section of the computer center that require access by personnel from multiple divisions, such as the section that keeps reports produced by the computer division to

distribute to other divisions, or the section that keeps video providing marketing advice, should be separated from the computer center.

2.9.5 Information Classification

2.9.5.1 Classification of Information

1) The Company must implement information asset classification and hierarchize information confidentiality by establishing a class of confidentiality according to the laws and the Company's requirements to consider the appropriate class of confidentiality.
2) The Company's internal entity must categorize information and assets, information used in the Company operations, and determine the hierarchy of information confidentiality and information assets.

2.9.5.2 Labeling of Information

1) The Company must maintain control over information in the form of documents that are properly prepared, controlled, and maintained starting from labeling, retention, reproduction, distribution, and destruction, as well as the establishment of a protocol for personnel and related parties to follow in order to ensure that information is properly controlled and secured.
2) The Information Technology Department and related agencies must attach a label to all computer equipment in accordance with the property account registration and the procedure for use.

2.9.5.3 Handling of Asset: Assets must have a policy governing the implementation of administrative procedures to ensure that important information of the Company's is not leaked.

2.9.6 Media handling

2.9.6.1 Management of Removable Media

1) The Information Technology Department must provide operational procedures for the management of the media used to record and maintain moving

information in writing, as well as communicate with users within the Company to follow.

2) Management of movable recording materials must be consistent with defining a confidential information hierarchy.

2.9.6.2 Disposal of Media

1) The Information Technology Department must establish a procedure for destroying the recording media to prevent leakage of confidential or sensitive information.

2) The Information Technology Department must set a standard for controlling the destruction of recording media based on internationally recognized standards.

2.9.6.3 Physical Media Transfer: Information Technology Department must establish operational procedures or agreements to maintain information security in the event of the movement of the recording media from the installation or operating area.

2.10 Damage protection

2.10.1 Fire protection system.

1) A fire alarm device, such as a smoke detector or heat detector, must be installed to prevent or suppress fires in a timely manner.

2) The primary computer center must be equipped with an automatic fire suppression system, for subordinated computer center, there must be equipped with at least a fire extinguisher for initial firefighting.

2.10.2 Electrical outage protection

1) A system must be prevented from being damaged by current inconsistency.

2) A backup power system is required for critical computer systems for continuity of operations.

2.10.3 Temperature and humidity control system: The environment must be controlled to the optimum temperature and humidity. The air conditioner temperature should be

set, and humidity should be set to suit the specifications of the computer system, as the computer system may malfunction under improper temperature or humidity conditions.

2.10.4 Water leak alarm system: In the event of lifting the floor of the computer center to install air conditioning systems as well as wiring and network cables below, water leakage warning systems should be installed in the areas with water pipes to prevent or suppress water leakage in time. In addition, if the computer center is in a place at risk of water leakage, it is advisable to regularly observe whether there is a water leak.

2.11 Information Security Structure

2.11.1 The Company's Information Security working team has been established with representatives from various divisions to be members of the working team.

2.11.2 Risk assessment must be conducted at least once a year or when there are significant changes considering internal context, external context, stakeholders, vision, mission set by the Company.

2.11.3 Criteria for acceptable and unacceptable risks must be set to be the guideline for risk management arising in the assessment of risks.

2.11.4 Policy must be reviewed at least once a year to reflect internal context changes, external context, stakeholders, vision, mission, and prospects of future risks that may affect the Company's information security.

2.11.5 The declared policy must be evaluated in order for improvement of policy and the strategic plan to be aligned with current and potential future threats.

2.11.6 An Information Security Policy must be written in accordance with the approved objectives and scope in order to be enacted and implemented for the entire company, applying to all Company personnel who work with information assets.

2.11.7 Encourage information security training at least once a year to raise information security awareness.

2.12 Mobile devices and teleworking

2.12.1 Mobile Computing and Communication

1) The Information Technology Department must develop appropriate measures to support the security of mobile communication devices based on the risks of the device being connected to the Company's computer network and when the device is taken off-site.
2) Users who use mobile communication devices to connect to the Company's information systems must comply with the Information System Security Policy and be strictly aware of information security.

2.13 External operations (Teleworking)

2.13.1 All users working from outside the Company must adhere to the Information System Security Policy in the same way that employees work within the Company.

2.13.2 Users who access the Company's data while working outside the Company or logging in remotely must obtain reasonable permission from the information's owner division and affiliated division.

2.13.3 Users who want to log in remotely must obtain permission from the administrator.

2.14 Provision of Equipment or Information Systems (Redundancies)

2.14.1 The Company must be in charge of determining the requirements for maintaining the availability of high-priority information systems.

2.14.2 The Company must direct the installation of a backup information system, backup device, or backup system to support adequate services to ensure proper business continuity.

2.15 Compliance

2.15.1 Compliance with legal and contractual requirements

1) The Information Technology Department must collaborate with the Legal Department and Human Resource Management Department to collect the law, regulations, guidelines, and requirements relating to information security, which must be documented for written operational requirements and kept up to date.

2) All personnel are strictly responsible for complying with the requirements specified.
3) Employees of the Company are prohibited from using the Company's assets and information systems and do any act that contradicts to the Laws of the Kingdom of Thailand and international law under any circumstances.

Section 3

Security of Information Communication via Computer Network and Security of operation related to Information Technology System

3.1 Security measures for information communication via computer network systems

3.1.1 Establish a written operating procedure including the preparation of an information technology system operation manual with at least the following details:

- Operating manner in the server room
- Turning on and off the system including turning on-off the server, turning on-off the system.
- Shutting down the service system
- Backup
- Equipment maintenance
- Managing storage media, which includes labeling, deletion, recording on media, and data retrieval.
- Submitting work to be processed in the computer system and troubleshooting issues
- The process of bringing data into a processing system, known as data processing, and show the result of using utility application
- Reporting and resolving issues
- Dealing with failures of computer systems, work systems, and networks
- System and network recovery

The Information Technology Division must establish accountabilities and responsibilities, such as the procedures in the event of an unexpected incident or a security breach, and how to perform offender inspections.

3.1.2 Significant modifications must be documented and communicated to other relevant divisions, and the Information Technology Division must distribute and supervise functionally operate in accordance with the Company's guidelines. To keep it up to date, the operating manual should be examined and revised on a regular basis, especially if the network system changes.

3.1.3 The Company's complete network system, which is connected to other network systems, must deploy package filtering devices or programs, such as firewalls or other virus-detection equipment. External service providers must have a strategy in place to screen out websites that is unauthorized under the Computer-Related Crime Act. If the user needs to browse unauthorized websites, he/she should obtain appropriate approval prior the use.

3.1.4 Ensure that relevant activities are managed effectively and that controls of information carried via the network and through the Company's infrastructure are enacted.

3.1.5 Users are not allowed to connect their computer to a modem or any other equipment or program that provides network services, such as a router, switch, hub, or wireless access point or connected to any point on the Company's network system without approval from the Information Technology Division.

3.1.6 Third parties are prohibited from connecting a computer or any other external device to the Company's computer and network systems. In the event of a requirement, a proper request for approval must be made at all times.

3.1.7 It is forbidden for users to connect to an external network through modem or other connection device while linked to the Company's internal network.

3.1.8 Collecting computer traffic data in accordance with Computer-Related Crime Act.

3.1.9 Maintaining and improving computer networks in good operating order. In the event that a systemic issue occurs, the network administrator has the right to revoke access to the computer or network in order to prevent damage.

3.1.10 Computer Network Management

3.1.10.1 Network Controls: Network Administrator must execute control and supervision over the administration of the computer network to protect against threats and maintain the security of information systems and applications running on computer networks, including information that is exchanged on the network.

3.1.10.2 Network Controls: Whether it is a service from within or outside, Network Administrators must include security features, service levels, and all administrative requirements of network services in network service agreements.

3.1.10.3 Segregation in Network: The Information Technology Department must offer appropriate segregation on the computer network system, taking into account the needs of network users, the impact on information security, and the level of value of data on the network.

3.1.11 Control the level of access to information technology systems according to duties and responsibilities.

3.1.12 Determine the policy for gaining access to the internal system so that the user's identity can be verified.

3.1.13 Establish a policy for assessing database on a regular basis by categorizing data into two categories: unneeded data and expired data and setting a time limit for checking and inspector. If the data is no longer used, it must be changed to archive history.

3.1.14 Establish remote work standards, such as VPNs and access controls. The accessor must seek for authorization and fill out the form to notify the division.

3.1.15 Establish a policy for notifying the incident by prioritizing it based on its importance to the system, risk, and stakeholders, logging the incident, and reporting the incident to the supervisor for acknowledgement and signature in accordance with the Company's announcement.

3.1.16 Create a form or method for submitting requests to use the server, database, or program in order to record the data in accordance with the Company's announcement concerning data recording.

3.1.17 Information Transfer

3.1.17.1 Information Transfer Policies and Procedures

1) The Information Technology Department must be in charge of supervision, establish information-sharing protocols that are appropriate for the type of communication and the level of information confidentiality.
2) The Information Technology Department is responsible for determining an agreement on information sharing and directing an agreement on information exchange between internal company departments as well as between corporations and their outside agencies.
3) Prior data transfers to third parties, authorization from the data's owner and written control documents such as specified terms of the exchange, sufficiently protected guarantee of information is required.
4) In the event of electronic information sharing via e-mail or instant counter-messaging, policies for managing confidential messages or significant electronic data must be implemented to ensure that they are well-protected against unauthorized access, amendment, and interference, which could result in system halting.
5) Establish confidentiality or non-disclosure agreements, in which management must require personnel and external entities that provide services to the Company to sign a written confidentiality agreement or non-disclosure of the Company's information unless consent has been given in writing on a case-by-case basis and identify the purpose for disclosing information that is relevant to the Company.

3.2 Measures for operational security related to information systems

3.2.1 The Information Technology Division must have control over the use of information in information systems, including assigning permissions to use such as write, read, and delete, allocating groups of people who can use the information, and ensuring that the information under permission to use include only the necessity information.

3.2.2 Setting a time restriction for users to gain access to a higher level of information system, such as Root or Administrator, as needed and appropriate for their task.

3.2.3 Third parties are required to strictly follow the Company's policies prior to being granted access to the Company's information technology system.

3.2.4 Access permissions to information files must be regulated and allowed only when seriously needed to enable the efficient safeguarding and separation of user rights and responsibilities.

3.2.5 Managing the installation of various applications in the information system or on the PCs of employees without interfering with the primary system or causing damage to the integrated system

3.2.6 Information for testing (Test data): The organization must establish a data protection policy in order to protect data for testing. The Information Technology System Development Division and Information Technology Project Management Division are the ones in charge. Users must also refrain from testing the service system with real data stored in the production system. There must be control system if a copy of the data from the production system is utilized for testing.

3.3 Audit of information systems and computer network systems must be conducted at least once a year as follows:

3.3.1 Plan the system audit in relation to the risks that have been identified.

3.3.2 Determine the scope of the system audit's technical aspects to ensure that critical risk areas are covered. The operation must not be harmed as a result of the inspection.

3.3.3 Perform the audit of the system out of working hours if the audit may have an impact on the system's availability.

3.3.4 At least once a year, review and amend the policy, including enhancing procedures and operating procedures to align with the new policy.

3.4 Data Encryption Measures (Cryptographic controls)

3.4.1 Policy on the use of Cryptographic Controls

1) The Information Technology Department shall establish data encryption standards and recommendations for their selection that are appropriate for the organization and the dangers that may arise in each class of confidentiality outlined.

2) Key Management: The Information Technology Department must establish a plan for managing keys used in data encryption, as part of the Key Management Life Cycle, which includes monitoring the consistent execution of such rules and processes.

3.5 Controlling access to the Company's operating system, work systems and data

3.5.1 System Administrators must configure users of all the Company's computers to work together with Active Directory, allowing the AD system to control all users' computers and specifying a user and password to access the operating system of the Company's computers.

3.5.2 For a safe and secure entry, appropriate authentication techniques must be used to control access to the operating system. Furthermore, due to its suitability, the user group has restricted authorization to connect directly to the operating system via the command line.

3.5.3 Review the history of access to information system through the security log on a regular basis.

3.5.4 The user's right to use the system together with username based on Single Sign-On and required activities such as signing in, adding, deleting, and updating data, must be documented.

3.5.5 Assign a security log reviewer, for example, the administrator must verify the security log every two weeks to verify activity that might create risk for information system.

3.5.6 Determine the length of time required to verify and destroy the security log because if it is kept too long, it does not benefit the system. For example, the duration to store the important data must be identified, for example, activity data on the system that apply to the entire company shall be maintained for a period of 1-year and the less important data shall be kept for a period of 6 months, etc.

3.5.7 Technical Vulnerability Management

1) The Information Technology Department must maintain control over the Company's information system to ensure that it is free of technological flaws. At the very least, this should be done once a year.

2) Administrators must periodically monitor and maintain the system's level of information security, which includes checking for vulnerabilities, assessing found vulnerabilities, and repairing and improving weaknesses in information systems.

3.6 Determine and confirm the user's identity

3.6.1 The user must have precise information that allows him/her to be identified and use proper authentication techniques to back up the identification as the user.

3.6.2 Creating a new user account, modifying an existing account, or canceling an existing account requires the administrator's consent, as well as the consent of the user's supervisor and the system's supervisors.

3.6.3 Requests to add, change, or revoke the account, as well as the right must be done in writing.

3.6.4 Each user must have a unique User-ID that distinguishes them from other users. The user ID that is issued must be able to verify the user and return the verification.

3.6.5 A user must specify name of the user and password to use the computer system of the Company.

3.7 Use of Utility Programs: To avoid copyright infringement or circumvention of security measures that have been implemented or that are already in place, the use of utility programs shall be as follows:

3.7.1 Limit access to the utility program and clearly define the right of use.

3.7.2 Permission to use the utility program from time to time.

3.7.3 Storage of utility programs on external media if not using it on a regular basis.

3.7.4 Remove any unnecessary utility programs from the system.

3.7.5 Only the copyright-licensed utility programs are installed.

3.7.6 Direct access to the various applications must be granted by the supervisor. A notice of usage must be provided, as well as a record of the request.

3.7.7 Require employees to exclusively adopt utility programs and applications that have been approved by the Company.

3.7.8 Employees must obtain permission from the Computer Division and direct supervisors before installing any program or application on a computer or computer system, including other corporate accessories.

3.7.9 Employees are not permitted to use non-copyrighted programs or applications.

3.7.10 If an employee intends to use the program without purchasing a license, he/she must make a request form, which is then approved via the approval chain.

3.8 Determining the system usage time

3.8.1 When a period of inactivity in the usage of the information system occurs, the information system shall be turned off. For instance, the system might be turned off after at least 30 minutes of inactivity. However, if the system is high-risk or high-priority, the period of inactive usage might be shorten as deemed appropriate, or approximately 10 minutes to protect unauthorized access to important information.

3.8.2 For high-risk or high-importance information systems or applications, the longest length of the connection to the information system or application must be limited so that users can

only use it for the specified period, by programming it to run for 3 hours per connection or by allowing users to use it during the Company's normal working hours.

3.9 Protection from information system threats by determine the guidelines to safeguard from malicious software.

Section 4

Other Criteria

4.1 Employees / Users

4.1.1 Strictly follow the employee handbook and Business Ethics Manual.

4.1.2 Under this policy, all employees have the right to use information assets. Violation against this policy which causes or threatens to cause harm to the Company, or another individual may result the employee to be accused disciplinary and legally.

4.1.3 Employees must behave in a nice and suitable manner and follow the standard practices in using the network.

4.1.4 Employees must be cautious when using the network and ensure that no one else has unlawful access to your account.

4.1.5 Employees are required to keep the password confidential and do not use computer programs that automatically remember passwords (Save Password) on personal computers owned by employees in order to prevent outsiders from acquiring and misusing an employee's password and causing damage to the organization.

4.1.6 When an employee's computer is infected with a virus, the employee must immediately notify system administrator so that corrective action can be taken to ensure the safety of computer network systems.

4.1.7 Employees must delete unneeded information from the computer to maximize the data storage.

4.1.8 Employees must coordinate with system administrators to monitor the security of personal computers and computer networks. Employees must also follow instructions about computer and network security.

4.2 Internal control to ensure policy compliance

4.2.1 The Company has set aside a period of time to evaluate information systems by external specialists.

4.2.2 The Company has a policy for compatible devices connection to be able to identify the user and the accessing devices. Such data must be collected in the form that the Company shall further announce.

4.2.3 The Company's operations are governed by Thai laws. As a result, the Company's computer network must be applied in accordance with the Computer-Related Crime Act, B.E. 2560. (2017)

4.2.4 The Company does not support or allow employees to commit offenses under the Computer-Related Crime Act B.E. 2560 and other related laws.

4.2.5 The Company will provide a USER ID and Password to employees who have duties related to the use of computer networks and connection to the internet individually. The rules for setting and using password are notified to employees.

4.2.6 Passwords are the property of the Company. It is forbidden to share passwords with others. Employees are accountable for strictly securing passwords.

4.2.7 The Company forbids the shared use of USER IDs and Passwords.

4.2.8 Employees may be assigned accessibility to other systems required by the Company to comply with the rules of use of the system and to retain their User ID and password without disclosure to any other person unless authorized in writing from the supervisor.

4.2.9 If there is a cause to stop using the USER ID and password, the supervisor needs to be informed as soon as possible of the cancellation.

4.2.10 Computers and accessories are the property of the Company. Employees are obliged to keep them usable. This includes updating the operating system and antivirus or a set of commands as desired.

Appendix and Updated Information