Tel. : 044-666928-9
Fax. : 044-666212-3
Website. : www.nerubber.com
E-Mail. : ner@nerubber.com

Policy Code No. IT001

Revision No. 04

Effective Date: 7 October 2567

Information Technology Governance and Management Policy

1. Information System Access Control

The Information System Access Control Policy is a crucial part of organizational security, aiming to prevent unauthorized access to data and resources, as follows:

1.1. System administrators shall permit users to access requested information systems only upon approval from the responsible person/data owner/system owner and supervisor, solely based on necessity of use.

1.2. External individuals requiring access rights to the department's information systems must request and receive written approval from the relevant line executives.

1.3. System administrators must define data and system access rights appropriate for usage, and regularly review user accounts and access rights. They are responsible for user operations within information systems and consistent access right reviews, as follows:

1.3.1. Establish criteria for granting access to information usage related to permission and authorization:

1.3.1.1. Define rights for each relevant user group (User Access Management), such as:

- Read-only
- Create data
- Edit
- No rights

1.3.1.2. Define criteria for suspending rights and granting authorization in accordance with the established User Access Management.

1.3.1.3. Users who wish to access the company's information systems must register their information with the assigned system administrator, except for visitor status.

*** For visitors, a separate user account will be provided for Internet access only, using a dedicated IP range for visitors.

1.3.2. Print a list of active users in the system, separated by department/section, and submit the list to the department supervisor for review of names and access rights to ensure accuracy.

1.3.3. Correct data and rights as notified by the line executive or department supervisor.

1.3.4. Procedures for revoking user access rights: Upon receiving the employee resignation notification from Human Resources, rights must be suspended within 7 days, or within 15 days when there is a job position change.

1.4. System administrators must install a system to record and monitor information system usage, and inspect security breaches to information systems. They must also maintain detailed records of information system access and changes to rights as evidence for inspection, in accordance with the Computer-Related Crime Act of 2550 (2007) and its 2560 (2017) amendment, which stipulate: "Service providers must retain computer traffic data for no less than 90 days from the date the data enters the computer system. However, in necessary cases, an official may order a service provider to retain computer traffic data for more than 90 days but not exceeding 2 years, specifically for individual cases and occasions."

1.5. System administrators must arrange for recording entry and exit to information system locations (server rooms).

1.6. System administrators must allocate appropriate space on the server for users.

1.7. System administrators must back up the server data.

1.8. System administrators must restrict the connection of computers to various data storage devices such as Flash Drives, Smartphones, External Hard Disks, etc.

1.9. System administrators must implement Multi-Factor Authentication (MFA) to enhance security for identity verification before accessing important programs or sensitive data sets such as ERP or E-Mail.

1.10. Employees or users must receive training on Cyber Security and methods to prevent cyberattacks such as Phishing, Scammer, Spam, and Social Engineering.

1.11. System administrators must prepare a Disaster Recovery Plan (DRP) to cover system recovery procedures in case of disasters or cyberattacks.

1.12. System administrators must prepare a Business Continuity Plan (BCP) to define guidelines and procedures for business operations in the event of a business disruption.

1.13. The Information Technology Department must review this policy annually, or whenever there are changes in technology or new systems, to ensure that the security standards currently used by the company maintain effective security standards or operational coverage for prevention or operation.

2. User Access Management for Internal Network

The User Access Management Policy for internal networks, based on the Zero Trust Security principle, aims to prevent unauthorized access to data and resources, ensuring secure and efficient data access. Crucially, it mandates verification and authentication of users and devices every time resources are accessed, whether within or outside the company's network, as follows:

2.1. User Registration: Defines procedures for new user registration, including verification and approval of access rights.

2.2. User Account Management: Defines access rights based on user roles and responsibilities, including regular review and auditing of access rights.

2.3. Password Management: Defines secure password creation policies and periodic password changes.

2.4. Network Access Control: Defines network and internal network resource access rights based on data criticality levels.

2.5. Access Monitoring and Logging: Records and monitors data access activities to prevent security breaches.

2.6. Authentication: Users must authenticate with a username and password before accessing the network.

3. Wireless LAN Access Control

The Wireless LAN Access Control Policy aims to prevent unauthorized access to the wireless network and to maintain data security within the network, as follows:

3.1. Wireless Access Point Signal Control: Controls wireless access point (AP) signals to prevent leakage outside the wireless network usage area or to minimize leakage.

3.2. Changing Default Settings: System administrators must change the default SSID (Service Set Identifier) settings provided by the manufacturer to prevent unauthorized access.

3.3. SSID/VLAN Separation: Defines separate SSIDs/VLANs for general internet users and users who access internal systems such as File Share, Programs, Database, Printer.

3.4. IP/VLAN Separation per Building/Floor: Defines separate IPs/VLANs for each building or floor to prevent the spread of computer viruses.

3.5. User Registration and Access Rights for Wireless Network: Registers and assigns user access rights to the wireless network appropriate for their duties and responsibilities before system use, including regular review of access rights.

4. User Responsibilities

The User Responsibilities Policy aims to ensure that users are aware of their duties and responsibilities in using the organization's information systems correctly and securely, as follows:

4.1. Password Usage: Users are responsible for protecting, maintaining, and keeping confidential their username and password. Each user must have their own unique username and must not share it with others or disclose it.

4.2. Password Definition: Passwords must be at least 8 characters long, consisting of at least 1 uppercase letter, 1 lowercase letter, 1 special character, and 1 number, etc.

4.3. No Personal Information in Passwords: Do not use personal information for personal passwords, such as one's own name or surname, family/company member's name, birthdate, phone number, etc.

4.4. Password Change Frequency: Passwords must be changed every 3 months.

4.5. No Automatic Password Saving: Do not use computer programs to automatically save personal passwords ("Save Password") on personal computers owned by the user.

4.6. No Visible Password Records: Do not write down or record personal passwords in locations easily observable by others.

4.7. Initial Password Security and Delivery: Initial passwords for users must be difficult to guess, and password delivery to users must be secure.

4.8. Authentication Prior to Access: Users must authenticate themselves every time before using assets or information systems. If there is an authentication problem, whether due to a locked password or any error, users must immediately notify the system administrator by following these guidelines:

4.8.1. All types of computers must perform authentication before accessing the information system every time.

4.8.2. For Internet usage, authentication must be performed, and data must be recorded, allowing for the identification of the individual user.

4.9. Users must protect, maintain the confidentiality, accuracy, and availability of data, as well as documents, computer storage media, or various information prone to unauthorized access.

4.10. Confidential or sensitive data under the possession and care of the department must not be disseminated, altered, duplicated, or destroyed without permission from the line executive, supervisor, or authorized person.

4.11. Users are responsible for safeguarding company data and shall be held partially responsible for any loss, misuse, or unauthorized disclosure of such data.

4.12. Users have the legitimate right to store, use, and protect their personal data as they deem appropriate. The company respects personal rights and does not permit any individual to infringe upon personal data without the consent of the user possessing that data, in accordance with the PDPA principles.

4.13. Do not open or use any type of online entertainment programs, such as watching movies/listening to music and games, etc., during working hours.

4.14. Do not use company assets provided for work to disseminate data, messages, images, or anything that violates morality/national security and laws, causing harm to others.

4.15. Users will receive the following Internet speeds:

General Users Upload : 5 Mbs.
Downloads : 5 Mbs.
** 1 user can use 2 devices simultaneously.

Executive Users Upload : 10 Mbs.
Downloads : 20 Mbs.
** 1 user can use 10 devices simultaneously.

4.16. Users must save data only in the areas provided by the company or department.

4.17. Computers or notebooks must only have endpoint protection software provided by the company installed.

5. Assets Management

The Asset Management Policy aims to ensure that the management of organizational assets is efficient and aligned with business objectives, as follows:

5.1. Users are strictly prohibited from entering the computer and network control rooms, which are restricted areas, unless authorized by the system administrator.

5.2. Users must not remove any equipment or parts from the computer and network control rooms unless authorized by the system administrator.

5.3. For external individuals or non-authorized personnel entering the computer and network control rooms, a system administrator must always be present or accompany them.

5.4. Users must not connect any tools or other devices to the network for personal business purposes.

5.5. Users must not copy or duplicate copyrighted files without permission, and users must not use or delete other people's files under any circumstances.

5.6. Users must destroy important data on data storage devices and files before disposing of such devices. Techniques for deleting or overwriting sensitive data on storage devices must be used before allowing others to reuse those devices to prevent access to confidential information. Consider the following data destruction methods for each type of storage media:

Type of Storage Media	Destruction Method
Paper	Use a paper shredder.
Flash Drive/ Hard disk/ Solid State Drive (SSD)	- Destroy data on Flash Drives according to DOD 5220.22 M standard of the U.S. Department of Defense, which is a data destruction standard by overwriting existing data multiple times. - Use smashing or crushing methods to damage the device.
CD/DVD	Use a shredder.
Tapes	Use smashing or crushing methods to damage or burn for destruction.

5.7. Users are responsible for the assets provided by the company for their use, treating them as their own. All asset lists for which the user is responsible, as well as the receipt or return of assets, will be recorded and inspected every time by assigned personnel.

5.8. Users are obligated to compensate for damages if assets are damaged or lost due to the user's negligence, according to the asset's value.

5.9. Users must not lend computers or notebooks to others under any circumstances, unless such lending is approved in writing by the line executive/supervisor.

5.10. Users have the right to use assets and various information systems provided by the department solely for company purposes.

5.11. The appropriate basic computer set for general users should consist of:

OS : Windows 10 Pro or higher

Programs Office : Microsoft Office Home &Business 2021or higher

CPU : Intel core i3 gen 12th หรือ Ryzen 3 gen 5th or higher

Ram : DDR4 8 GB or higher

SSD : 240 GB or higher

Monitor (จอ) : 21” or higher

UPS (Uninterruptible Power Supply) : Must provide power backup for at least 5 minutes or more.

6. Software Licensing and intellectual property and Preventing Malwares

The Software Licensing and Intellectual Property and Preventing Malware Policy aims to ensure that software usage within the organization is legally compliant and secure from cyber threats, as follows:

6.1. The company places importance on intellectual property. Therefore, users may request to use licensed software or software for which the department holds a license, based on necessity for their duties. Users are prohibited from installing or using any unlicensed software. If a copyright infringement is detected, it will be considered a personal offense, and the user will be solely responsible.

6.2. Software provided by the department to users is considered essential for work. Users are prohibited from uninstalling, changing, modifying, or duplicating it for use elsewhere, unless authorized by the department head or an authorized person with copyright ownership.

7. Drone

The Unmanned Aircraft (Drone) Usage Policy aims to ensure that drone operations are safe and legally compliant, as follows:

7.1. Registration and Authorization: Drone users must register and obtain usage permits from relevant authorities, such as the Civil Aviation Authority of Thailand (CAAT) and the National Broadcasting and Telecommunications Commission (NBTC), to ensure legal drone operation.

7.2. Flight Control: Defines areas and altitudes for drone flight, such as prohibiting flights in restricted areas or near airports, and requiring flights at specified altitudes.

7.3. Safety Measures: Requires the installation of anti-collision systems and automatic flight control to prevent accidents and collisions with obstacles.

7.4. Training and Certification: Drone users must undergo training and receive certification from relevant authorities to acquire the knowledge and skills for safe drone operation.

7.5. Legal Compliance: Adherence to laws and regulations related to drone usage, such as the Air Navigation Act B.E. 2497 (1954) and Ministry of Transport announcements.

8. CCTV Policy

The CCTV System Usage Policy aims to ensure that CCTV usage is legally compliant and maintains the security of personal data, as follows:

8.1. The company installs CCTV systems for the safety of employees and assets.

8.2. The company installs CCTV systems to prevent and investigate potential incidents such as theft, property damage, or accidents.

8.3. Defines areas requiring camera installation, such as main entrances, storage rooms, parking lots, operational areas, etc.

8.4. Avoids installing cameras in highly private areas such as restrooms or employee changing rooms.

8.5. CCTV data shall be stored for a minimum of 60 days.

8.6. Data Access Rights:

8.6.1. Executives (business owners) or authorized directors of the company.

8.6.2. Responsible persons appointed by the Chief Executive Officer or authorized directors of the company:

- Security officers
- System administrators (System administrators: Information Technology Department)

8.6.3. Persons authorized by executives (business owners) or authorized directors of the company.

8.6.4. For external individuals:

- Government officials: If CCTV footage is requested for investigation purposes, a written request is required.
- General external individuals: If CCTV footage is requested, a written request and a daily logbook entry are required.

8.7. Employees and external individuals must be informed about CCTV installation through clearly visible signs or announcements.

8.8. In cases where relevant laws or regulations apply, consent from affected employees or individuals must be obtained before installation.

8.9. Regular maintenance of CCTV equipment is required to ensure efficient operation:

- For maintenance, all systems must be serviced at least once per quarter.
- In case of equipment malfunction:
- If the problem can be resolved internally, it should be fixed immediately upon discovery of the malfunction.
- If it cannot be resolved internally, the contractor or outsource provider must be immediately notified for repair.

Tel. : 044-666928-9
Fax. : 044-666212-3
Website. : www.nerubber.com
E-Mail. : ner@nerubber.com

9. AI System Usage

This policy aims to define guidelines for the use of Artificial Intelligence (AI) within the company, to ensure that AI usage is efficient, secure, and compliant with laws and ethics.

9.1. The company must provide training and knowledge about AI usage to employees.

9.2. Employees or users must receive training on the risks and methods to prevent security breaches from AI usage.

9.3. Inspection results and problems found from AI usage must be reported to the management.

9.4. Testing and impact assessment of AI usage must be performed.

Therefore, this policy is hereby announced for widespread acknowledgment on 7 October 2567.

- Mrs. .Jarunee Jongwattanasak -	- Mr. Chuwit Jungtanasomboon -
(Mrs. Jarunee Jongwattanasak)	(Mr. Chuwit Jungtanasomboon)
Acting deputy chief executive officer of corporate development	Chief Executive Officer