# Information Technology Systems Usage Policy

**Objectives**

1 This policy has been created for Thaifoods Group Public Company Limited's employees or third parties who access the computer system of Thaifoods Group Public Company Limited (the "Company"), including the access of the Internet via the organization's network, and this policy must be strictly adhered to.

2. The Company reserves the right to inspect, collect evidence, and take appropriate action if a violation of the information system usage policy is found.

3. Definition of Computer Systems and accessories as follows:
    - 3.1 Computer system
    - 3.2 Computer
    - 3.3 Accessories
    - 3.4 Software
    - 3.5 Intranet network
    - 3.6 Internet network
    - 3.7 Remote access
    - 3.8 Application Program
    - 3.9 Viruses, malware, or undesirable sets of instructions

**General Section**

1. The Company's computer system, computer, and connection equipment for services related to the Company's business only is not allowed to be used for business unrelated to the Company's business.

2. Access to the Company's computer system and Internet connection requires following the procedure for asking for access permission by registering for access according to the procedures of the organization.

3. When requesting permission to access, the direct superior or authorized person of the user shall be the requester by following the procedures for requesting access to the system as specified.

4. Users agree and sign to confirm that they follow the computer system usage policy and internet connection, and agree to the changes, if any, by giving their consent to each modification.

5. This computer system usage and Internet connection policy is part of all user operational requirements and will be regarded as a violation of work discipline.

6. If a user is in violation of the computer system usage and Internet connection policies, they will be punished in accordance with employee regulations, including the possibility of initiating legal proceedings if the violation violates national law.

7. Users shall not use internet systems, downloaded files, or shared folders in the case of suspected viruses, malware, or undesirable sets of instructions.

**Section 1: Regarding General Usage Regulations and Property Ownership**

1. Various information that was made is considered the property of the Company. Receiving, sending, recording, and generating information using the Company's various systems is considered ownership by the Company.

2. The Company can monitor each person's usage as appropriate for the administration objectives and security of the network system.

3. Users must notify the Company of suspicious activity or improper or unauthorized computer use.

4. Various information of the Company, user must store this information in a device or system provided by the Company only and not collect outside the Company, such as by depositing files with a synchronization service provider, depositing files online, etc.

5. The Company reserves the right to inspect the network and various systems intermittently without prior notice. This right includes checking the website that the user has accessed via the internet, group chat, news, downloading and uploading documents via the internet, and receiving and sending email.

**Section 2: Security and Confidential Information**

1. Information in electronic or other forms, such as information contained on the Internet or intranet and contact information with networks outside the Company, should be used following the Information Technology Systems Usage Policy.

2. The password must be kept in a secure location and not told to anyone else. Users are responsible for any passwords they possess. System and user passwords must be changed at regular intervals to ensure the highest level of security. The period of change must be every 90 days, and the password setting must contain at least 8 characters of letters, numbers, and special characters.

3. The computer must be equipped with an automatic password screensaver for security reasons and must be logged off or shut down when not in use.

4. Portable computers have a high risk of data loss. Users must use these computers with caution.

5. Users are not permitted to use the Company's email address to leave their name for receiving information outside the Company unless this is done exclusively in connection with assigned tasks.

6. Every computer that a user connects to the Internet, intranet, or extranet must be virus checked against the current database used to protect against viruses.

7. Users must be careful when opening email attachments from unknown senders because there may be hidden viruses, ransomware, or Trojan viruses.

**Section 3: Computer System Usage and Internet or Intranet Connection**

1. The Company operates under the laws of Thailand; therefore, the use of computer systems and Internet connections by employees must comply with the Computer Crimes Act (B.E. 2560) and other related laws.

2. The Company does not support or permit the Company's users to violate the Computer Crimes Act (B.E. 2560) and related laws.

3. The Company provides a username (User ID) and password (Password) to users who must use the computer system and connect to the Internet individually. Moreover, there are rules for using passwords, such as the length of characters or the period, which change for a new password in the interest of overall system security.

4. User's password is a preventive measure and protects the confidentiality of the organization. The Company does not allow the disclosure of personal passwords to others, and all users are required to strictly protect the passwords of the organization.

5. The Company does not allow the use of names and passwords together on all computers and systems.

6. Users may be assigned to access other working systems required by the Company. Users must abide by the rules of system usage, keep their names and passwords, and shall not disclose them to others unless they are approved in writing by their direct superiors.

7. If it is necessary to cancel using username and password, the user shall notify the superior directly to request cancellation, which must be done immediately before canceling use.

8. Computers and peripheral devices are the property of the Company. Users are responsible for maintaining their availability, which includes updating operating systems, antivirus programs, and any undesirable sets of instructions.

9. Computers or peripheral devices other than those of the Company are not allowed to be used to connect to the Company's network.

**Section 4: Email Usage, Conversation, and Other Electronic Communications, Mail, Chat, and Other Digital Communication such as File or Facsimile Sending**

1. In electronic communication, whether it is electronic mail, conversation, or any communication, this is regarded as sending a formal letter and must comply with the following rules of receiving and sending letters of the Company, namely:
    A) Regarding the confidentiality of documents, it is forbidden to send confidential documents by electronic mail unless they are encrypted and confirmed by computer authorities.
2. It is forbidden to send false, defamatory, or insulting information, as information that causes damage to the Company or any other person.
3. It is forbidden to send pictures or messages related to pornographic matters.
4. Transmission of any information must comply with the Computer Crimes Act (B.E. 2560) and other laws.
5. If the information submitted violates the Computer Crimes Act (B.E. 2560) or the Company regulations, it must be reported directly to the superior or the computer department officer.
6. Use polite messages in electronic mail, chat conversations, or other electronic communications.
7. It is forbidden to send any email or electronic communication (SPAM email) without specifying the sender's name.
8. Users are not allowed to use any other email not specified by the Company.

**Section 5: Organization's Website Usage and Internet Access**

1. User is prohibited from porting image files or any data onto the Company's system or other systems as follows:
    A. Violation of the Computer Crimes Act (B.E. 2560) and other laws
    B. Not related to the Company's business.
2. User is prohibited from downloading the following photos or information:
    A. Violation of the Computer Crimes Act (B.E. 2560) and other laws
    B. Not related to the Company's business.

**Section 6: Application Usage and Other Programs**

1. Access to various programs must be approved by the information technology department, and the direct superior shall be the requester for permission to access.
2. Use the program specified by the Company only.
3. Users are prohibited from installing any programs on computers or computer systems in the Company, including any other peripheral devices, without the direct consent of the computer department and their superiors.
4. Users are prohibited from using or installing unlicensed programs.

**Section 7: File or Folder Sharing**

1. The purpose is to collect information or share information among users.

2. User is prohibited from storing the following types of information or photos on the Folder Sharing System:

    A. Violation of the Computer Crimes Act (B.E. 2560) and other laws
    B. Not related to the Company's business.

3. Users are prohibited from storing programs on the Folder Sharing System.

4. It is prohibited to use any information or anything that is copyrighted by the Company without permission.

5. User is prohibited from storing information unrelated to the Company on the folder - sharing system.

If a violation of the provisions of these regulations causes or may cause damage to the Company or any person, the Company will consider taking disciplinary and legal action against violators as appropriate. Moreover, the Information Technology Department reserves the right to immediately suspend the use of such personnel without prior notice.

**Policy Review and Improvement**

The Company requires this policy to be reviewed regularly, at least every year or when significant changes occur, to be consistent with the Company's operations.

Announcement on January 1st, 2026