Cyber Security Policy

United Palm Oil Industry Public Company Limited

effectiveness for the year 2025

Massage from Managing Director

In an era where information technology plays a vital role in business operations, safeguarding data and digital assets has become critically important. Our company recognizes the risks associated with unauthorized access, misuse, or disclosure of information, which can impact our credibility, reputation, and business continuity.

Therefore, we have established this Information Security Policy to define clear and comprehensive practices aligned with best practice. The objectives of this policy are to:

- 🔐 Protect the organization's critical information from internal and external threats
- 👷 Foster a culture of responsible technology use
- 📈 Support efficient and secure business operations
- ⚖️ Comply with relevant laws, regulations, and industry requirements

I would like to emphasize that the cooperation of every employee is essential to ensure this policy is effectively implemented. I encourage all staff to study, understand, and strictly adhere to the guidelines outlined herein, so we can collectively build a secure and sustainable working environment.
Thank you for your continued support.

Respectfully,

(Mr. Sanya Prasertsak)
Managing Director

United Palm Oil Industry Public Company Limited ("the Company")

Information technology is identified as a key tool in driving sustainable business development policies, aiming to integrate operations for growth alongside environmental and social responsibility.

This policy will meet the needs and expectations of all stakeholders through the adoption of modern, effective, and safe practices, tools, and international standards to ensure the Company's operations achieve sustainable success and goals.

Objective

To ensure that the information technology operations of the Company and its subsidiaries are stable, secure and reliable, the Company has established an "Cyber Security Policy".

This policy aims to maintain the highest level of security of the Company's information and information assets, taking into account the prevention of cyber threats and to ensure that the information maintains its confidentiality, integrity and availability in accordance with relevant regulations and laws.

A computer network is established to facilitate employee performance in the organization, ensuring appropriate and efficient use of the computer network, preventing potential problems arising from improper network use, and ensuring that contracted employees and external agencies understand their roles and responsibilities. Furthermore, to ensure that employees, both those hired by the organization and those with external agencies, understand their roles and responsibilities, and to reduce risks arising from theft, fraud, misuse of confidential information, and misuse of equipment, the organization should establish procedures for computer and network use to ensure that employees, both those hired by the organization and those with external agencies, are aware of threats, security-related issues, and their responsibilities, including legally binding responsibilities. They are also required to learn and understand the organization's security policy, and to minimize risks arising from failures in performing their duties.

CYBER SECURITY POLICY

Definitions

“Organization” means United Palm Oil Industry Public Company Limited.

“Employee” means the employees and workers of United Palm Oil Industry Public Company Limited, including other persons assigned by the organization to perform work under the contract.

“Network and Computer System Administrator” means an employee assigned by a supervisor to be responsible for maintaining a computer network, who has access to computer network programs for managing the computer network database, and who is responsible for maintaining the computer system, and who has access to computer programs or other information for managing the computer network, such as computer system user accounts (User Accounts) or email accounts (Email Accounts).

“Information” means anything that conveys meaning, facts, data, or any other information, whether such communication is accomplished through the nature of the item itself or through any other means, and whether it is prepared in the form of a document, file, report, book, diagram, map, drawing, photograph, film, image or sound recording, computer recording, or any other method that makes the recorded information visible, and includes electronic data under the Electronic Transactions Act, including text files, image files, sound files, computer programs, etc.

“Computer system” means a computer device or set of computer devices that are connected to each other and have been set up with instructions, sets of instructions, or other things, and procedures for the device or set of devices to automatically process data, including computers, whether connected or not, mobile phones, etc.

“Computer traffic data” means data about computer system communications, which shows the source, origin, destination, route, time, date, volume, duration, type of service, or other matters related to the communications of that computer system, including log data recorded when accessing the network system, which identifies the identity and rights to access the network, data about the date and time of contact and the machine used to access the service, and
The machines that provide the service, etc.

CYBER SECURITY POLICY

Section 1: General Regulations

- The owner of a personal computer is liable for any damages incurred if the computer or its operating system is damaged due to improper use or if it is lost.
- New employees are prohibited from using company computers until they have been approved for use through registration.
- Data owners who wish to publish their data through various channels, such as through the organization's website, must first verify the accuracy of the data. If there are any errors in the content, they will be held responsible for those errors.
- Delete unnecessary data from your personal computer to save memory on the storage media.
- Be careful in using and maintaining your personal computer and network system as you would any other person in using your personal computer and network system, as appropriate.
- Do not install additional computer programs other than those provided by the organization.
- Do not alter or modify any licensed software purchased by the organization.
- Do not install computer programs that infringe on the intellectual property rights of others.
- General employees are prohibited from installing computer programs that can be used to monitor information on the network system.
- Do not install any additional computer programs or computer equipment on the organization's personal computers to allow other people to use the personal computers or the organization's network system.
- Employees' personal computers may not be used on the organization's network unless they have been verified by the Information Technology Department before use.
- In the event that you wish to remove any computer equipment from the office, you must first obtain permission from the person in charge of removing the property.
- Install a UPS for personal computers that use a lot of data and have high usage frequency.
- Do not modify the system settings obtained from the initial installation. This may cause damage to the computer's operation.
- Do not enter the computer network system location (Server room) without permission.
- Computer users must be aware of, understand and strictly comply with the Computer Crime Act B.E. 2560 (2017), announced by the Ministry of Information and Communication Technology on 23 January 2017.

CYBER SECURITY POLICY

Section 2: Regulations for Internet Usage

- Do not download or send obscene or pornographic files.
- Do not download large files unnecessarily.
- Do not use the Internet for work that is not related to your responsibilities and do not use it for unnecessary purposes during times when the network is in heavy use.
- Do not play games, watch movies, or listen to music over the Internet.
- Do not access websites that fall into the following categories:
  1. Gambling
  2. Auction
  3. Criticism related to the nation, religion and the monarchy.
  4. Obscene, indecent, violating the Computer Crime Act (No. 2) B.E. 2560, Section 14.
  5. Other matters related to illegal or immoral or unethical matters.
- Do not use chat programs in chat rooms (such as social networks (Facebook/Instagram/Line/We chat/ whats app/Skype/Twitter, etc.) and except for those sections that are permitted to use them.
- Do not use information obtained via the Internet in a manner that infringes on the copyright of the owner of that information.
- Do not use the Internet to send, distribute or distribute the following:
  1. Electronic publications that infringe the copyright of the owner
  2. Confidential information of the organization to unauthorized persons
  3. Unauthorized personal information
- Do not use the Internet to participate in activities that damage the image and reputation of the organization.

CYBER SECURITY POLICY

Section 3: Regulations for E-mail Usage

- Employees or unauthorized persons are prohibited from accessing other people's email information without permission.
- Do not register with the email address provided by the organization on any website that is not related to the organization's work.
- Do not send emails that are considered spam.
- Do not send emails that are in the form of chain letters.
- Do not send emails that violate the law or the rights of others.
- Do not intentionally send emails containing viruses to other people.
- Do not forge or conceal your email address when sending emails to others.
- Do not send e-mail that interferes with the use of another person's computer system.
- Do not forge other people's email addresses.
- Do not receive or send e-mail on behalf of another person without permission.
- Do not use offensive language when sending e-mails.
- Do not send emails with file sizes larger than those specified by the organization.
- Do not send confidential corporate emails unless the company has implemented encryption methods for the emails.
- Please be careful to specify the recipient's email address correctly.
- Please include the sender's name in every email you send.
- Be careful to limit the number of email recipients to those who need to know.

Note: This Section 3 is an offense under the Computer Crime Act (No. 2) B.E. 2560, Section 4.

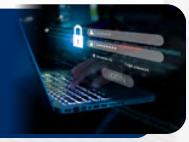
CYBER SECURITY POLICY

Section 4: Regulations for Preventing Misuse of Resources

- Employees must not use the network system for the following purposes:
- For illegal acts or to cause damage to computer data or computer systems related to national security, public safety, national economic security, or public services.
- For actions that violate public order or good morals
- To disclose confidential information obtained from operations to the organization, whether it is information of the organization or of an external person.
- To commit an act that is a violation of the intellectual property of the organization or of another person.
- To obtain information about other people without permission from the owner or the person with rights to such information.
- To express personal opinions on matters relating to the operations of the Organization to any website address in a manner that creates or may create a misunderstanding.
- For any other purpose that may conflict with the interests of the organization or may cause conflict or damage to the organization.
- To falsify computer data that will cause damage to others or the public.
- To disseminate or forward that fake computer data to others.
- To enter false computer data that will cause damage to national security or cause panic among the public into the computer system.
- To enter any computer data into a computer system, where such data is considered an offense against national security or an offense related to terrorism under the Criminal Code.
- To introduce any computer data into the computer system that is obscene in nature and that computer data may be accessible to other employees or the general public.
- To disseminate or forward computer data that is obscene in nature to others.
- To create, edit, add or modify images electronically or in any other way that may cause damage to others.
- To store computer data that is an image of another person and that image is an image created, edited, added or modified by electronic means or any other means that could cause damage to that person.

CYBER SECURITY POLICY

Section 5: Password Creation Guidelines



- The passwords assigned by the organization must be kept confidential.
- Passwords must be set to have the following properties:
  - Must be at least 8 characters long.
  - Mix of regular, uppercase, numbers and symbols.
  - Do not set your password based on your own name or surname, or that of a family member or person with whom you are closely related.
- Do not use computer programs to automatically remember your passwords (Save Password).
- Do not write down or save your password in a place where it is easily visible to others.
- Do not allow other people to access the computer network from your own user account.
- If you need to share your password with others for work, change your password immediately after completing the process.
- Groups of users who use the same user account and password will be jointly responsible for any damage or problems that occur with the accessed system.
- If you wish to cancel your username and password, please notify your supervisor directly to request cancellation. This must be done immediately upon termination. The assigned Information Technology Officer must cancel the username and password immediately upon receiving notification of cancellation.

CYBER SECURITY POLICY

Section 6: Access and Usage of Servers

- Do not enter the server room without permission.
- Employees are prohibited from entering the server room area without related activities.
- Food and drinks are prohibited in the server room.
- External persons entering the premises must wear their Visitor ID cards at all times so that they can be clearly seen, unless they are company employees.
- Record the entry and exit of the host machine room (Server) by outsiders in the host machine room entry and exit logbook every time.
- If you find any abnormalities in the server room, such as missing property or signs of intrusion, please immediately notify the Information Technology Manager.
- Do not bring any recording-capable devices into the server room, such as mobile phones, digital cameras, or video cameras.
- Please strictly follow the instructions of the server room staff.

CYBER SECURITY POLICY

Section 7: Information Management Guidelines

- For information in paper form, use a shredder to destroy confidential or high-priority documents.
- Protect confidential or high-priority documents printed on the printer to prevent unauthorized access.
- Confidential or high-priority documents should be classified separately and provided with adequate security.
- Copies of confidential or high-priority documents may be made only with the owner's permission.
- Be careful when distributing or distributing confidential corporate documents to recipients who have a need to know about them.
- Please verify the accuracy of the document before using it.
- Document owners must provide adequate security measures for confidential or high-priority documents to be sent by mail.

CYBER SECURITY POLICY

Section 8: Electronic Information Resources (e.g., electronic files, web data, e-mail, voice mail, multimedia content)

- Confidential or high-priority electronic data must be classified separately and protected with adequate security.
- Copies of confidential or high-priority electronic information may be made only with the permission of the owner.
- Be cautious about distributing or distributing confidential electronic information of the organization to recipients who have a need to be aware of the electronic information.
- The owner of electronic data must verify the accuracy of the electronic data before using it.
- Owners of confidential or high-priority electronic information are prohibited from transmitting such information by post unless they use the encryption method prescribed by the organization.
- Send the computer to be sold to the Information Technology Department to format the electronic data on the computer's hard disk.
- No one is allowed to copy data stored on the computer outside the company by any means (such as saving it to various storage media such as floppy disks, hard disks, CDs, DVDs, Handy Drives / Flash Drives, etc.), as such action is against the Computer Crime Act (No. 2) B.E. 2560, Section 18.

Note: If anyone needs to take such information out of the company, they must notify their supervisor and obtain permission first. Otherwise, it will be considered as having improper intentions.

CYBER SECURITY POLICY

Section 9: Guidelines for Reporting Security Incidents

- Have the staff immediately notify the Information Technology Department when they see any security incidents, including:
- Malicious programs
- The system was compromised via the network.
- Important information has been changed or lost.
- Unauthorized disclosure of sensitive information
- Misuse of sensitive data
- Misuse of information technology resources
- Finding weaknesses in the software, system, or hardware in use
- The system was attacked and unable to provide service.
- Information technology resources were stolen
- Allowing external parties to access the organization's systems
- Secretly installing software to steal data or spy on network data or
- Other incidents that violate the organization's security policies
- Cooperate and facilitate supervisors or network administrators in investigating security incidents and/or personal computer and network system security incidents, and strictly follow the instructions of supervisors or network administrators.

CYBER SECURITY POLICY

Section 10: Penalties

- In the event that an employee violates this Information Technology System Usage Policy, resulting in damage to the organization or damage that may be proven to occur, as determined by the organization's management, the employee who committed the offense acknowledges and agrees that the organization may impose appropriate punishments on the employee, including a warning, a written notice, a penalty, or termination of employment, in accordance with the organization's regulations.
- In the event of serious damage resulting from intentional or grossly negligent acts that cause damage to the organization, the employee who committed such wrongdoing is aware of and consents to the organization being able to act in accordance with the above clause, including agreeing to compensate the organization for the actual damages incurred as a result of such wrongdoing.