-Translated Version-

Information Technology Policy
Ubon Bio Ethanol Public Company Limited and Its Subsidiaries

To ensure that the use of computers and network systems within Ubon Bio Ethanol Group is conducted in an orderly manner and delivers maximum benefit to the Company's operations, as well as to prevent any violation of the laws governing electronic transactions and computer-related offenses.

1. This policy shall be called the "**Information Technology Policy**" governing the use of computers and network systems to maintain the security and integrity of information technology systems of Ubon Bio Ethanol Public Company Limited and its subsidiaries.

2. This Policy shall become effective on 24 February 2026 and shall remain in force thereafter unless amended or repealed by the Company.

Chapter 1
Definitions

---

3. In this Information Technology Policy, the following terms shall have the meanings set forth below:

"Organization" means Ubon Bio Ethanol Public Company Limited and its subsidiaries.

"Computer and Network Systems" means client computers, server computers, peripheral devices, and network equipment that connect computers within the Organization to enable shared use of resources. The term shall also include software applications, data and information that are not designated as public information, as well as Internet and Intranet network communication channels within the Organization.

"Client Computer" means a desktop computer, laptop computer, or any other device capable of connecting to the Organization's network.

"Computer Data" means data, messages, instructions, sets of instructions, or any other information stored in a computer system in a form that can be processed by such computer system, and shall include electronic data as defined under the laws governing electronic transactions.

"User" means any person who has been authorized to use the Organization's computer and network systems.

"Head of System Administration" means the Head of the Information Technology Department or any person designated by management to coordinate and oversee the maintenance and administration of the Organization's computer and network systems.

"System Administrator" means an officer of the Information Technology Department or any person designated by Information Technology Management to be responsible for the administration, maintenance, management, or operation of the Organization's computer and network systems.

"Malicious Software" means any computer program and/or electronic data designed with the intent to disrupt, interfere with, damage, or gain unauthorized access to computer systems, whether directly or indirectly. Such software includes, but is not limited to, computer viruses, spyware, worms, and Trojan horses.

Chapter 2
General Provisions

---

4. The Information Technology Department shall be responsible for assigning User Accounts to Users.

5. No person shall access or use the Organization's computer and network systems without authorization from the Head of System Administration or a System Administrator.

6. To ensure that the Information Technology Policy remains current, appropriate to operational practices and changes in technology, and in compliance with relevant laws and regulations, the Policy shall be reviewed at least once a year, or as necessary when deemed appropriate due to any changes.

Chapter 3
Computer and Network Usage Policy

---

7. Users, the Head of System Administration, and System Administrators shall have the duties to comply with the Organization's policies as follows:

    (1) To use the Organization's computer and network systems efficiently and for the maximum benefit of the Organization.

    (2) To maintain and safeguard the Organization's computer and network systems to ensure that they remain functional, reliable, and cost-effective in their utilization.

    (3) Not to use the Organization's computer and network systems to engage in any acts that constitute offenses under the laws governing electronic transactions, the laws on computer-related crimes, or any other applicable laws, which may cause damage to individuals, the Organization, or third parties.

Chapter 4

User Obligations in the Use of computer and Network Systems

---

8. Users shall not use the Organization's computer and network systems for the following purposes:

   (1) For any unlawful acts, or acts that cause damage, distress, or nuisance to other persons.

   (2) For any acts that are contrary to public order, good morals, or public decency.

   (3) For commercial profit-seeking purposes.

   (4) For the disclosure of confidential information obtained through the performance of duties for the Organization, whether such information belongs to the Organization or to third parties.

   (5) For acts that constitute infringement of copyright or intellectual property rights of the Organization or any other person.

   (6) For accessing or obtaining information of other persons without authorization from the owner or the rightful data owner.

   (7) For sending or receiving information that may cause or is likely to cause damage to the Organization, including but not limited to chain letters, or information received from third parties that is unlawful or infringes the rights of others when forwarded to Users or other persons.

   (8) For any acts that interfere with or disrupt the Organization's computer network systems or those of other Users, or that cause the Organization's computer network systems to become unavailable or operate abnormally.

   (9) For expressing personal opinions relating to the Organization's operations on any website in a manner that may cause or is likely to cause misunderstanding or misrepresentation of facts.

   (10) For any other acts that may be contrary to the Organization's interests, or that may cause conflict or damage to the Organization.

9. Users who are the owners of User Accounts shall be responsible for any consequences arising from the use of their User Accounts in connection with the Organization's computer and network systems, except where it can be proven that such damage was caused by the actions of another person.

10. Users shall keep their User Accounts strictly confidential and shall not disclose, transfer, sell, or distribute their User Accounts to any other person without authorization from the Head of System Administration.

11. Users shall log in using their own User Accounts and shall log out of the system upon completion of use or whenever temporarily suspending usage.

12. The setting, use, and maintenance of passwords shall be in accordance with the following guidelines:

(1) Passwords shall consist of no fewer than eight (8) characters and must include a combination of numeric characters, lowercase letters, uppercase letters, and special characters.

(2) Passwords shall not be based on the User's name, surname, family members' names, persons with personal relationships, dictionary words, or telephone numbers.

(3) Password reuse is not permitted until the password has been changed at least five (5) times.

(4) Upon first login, Users shall immediately change the initial password provided.

(5) If an incorrect password is entered five (5) consecutive times, the User Account shall be temporarily suspended. The User shall contact the System Administrator to unlock the account.

(6) Passwords for accessing the Organization's computer and network systems shall be changed every ninety (90) days.

(7) Users should not use automatic password-saving programs (Save Password) on client computers used within the Organization.

(8) Users shall not write down or store passwords in any location that is easily visible or accessible to others.

(9) Passwords used for accessing the Organization's computer and network systems shall be treated as strictly confidential and shall not be disclosed or made known to any other person.

13. Users shall not import, disseminate, or transmit any false computer data, including obscene or pornographic data, and shall not create, edit, modify, or alter images of other persons by electronic means or any other means in a manner that misrepresents such persons.

14. For the security of the Organization's computer and network systems, Users shall comply with the following:

(1) No computer programs capable of network traffic monitoring or data interception shall be installed on any computer systems.

(2) No additional software or hardware shall be installed on the Organization's computers for the purpose of enabling third-party access to the Organization's computer and network systems.

(3) Computers assigned to Users shall be shut down after completion of work or when not in use, except for server computers that are required to operate continuously on a 24-hour basis.

(4) All data received from both internal and external sources shall be scanned using the Organization's approved antivirus or malicious software detection tools prior to use. If

malicious software is detected, it shall be promptly removed or the affected data shall be deleted immediately.

(5) Internet usage that consumes excessive bandwidth or is unrelated to work duties during working hours is prohibited, including but not limited to large file downloads, online gaming, online chatting, and streaming of music or video content.

(6) Users shall not open email attachments from unknown or suspicious file types capable of executing programs, regardless of whether the sender is known or unknown, including but not limited to .exe, .com, .bat, .vbs, .scr, and .hta files.

(7) Unnecessary computer data shall be deleted from the Organization's computer systems to optimize storage space and system efficiency.

(8) Users shall not enter areas where computer network systems are installed without prior authorization from the Head of System Administration or a System Administrator.

(9) Upon termination of employment or cessation of User status, Users shall return all assets related to the use of the Organization's computer and network systems, including data, copies of data, keys, access cards, and any other relevant items, to the Organization.

Chapter 5
Computer and Network Connection and Usage

---

15. Any person who wishes to connect computers and/or devices to the Organization's computer and network systems shall obtain prior authorization from the Head of System Administration or an authorized person, and shall strictly comply with this Policy.

16. No person shall move, install additional equipment, or perform any actions on core network equipment, including routers, switches, or any devices connected to the Organization's main network infrastructure, unless prior authorization has been granted by a System Administrator.

Chapter 6
Duties of System Administrators

---

17. System Administrators shall have the following duties:

(1) To install computer systems and network infrastructure of the Organization, including encryption systems, intrusion detection and prevention systems, malicious software

protection and removal systems, as well as any necessary hardware and software to ensure secure and stable operation of computer and network systems.

(2) To monitor and supervise the use of the Organization's computer and network systems to ensure proper and efficient operation. In the event that any abnormality is detected, System Administrators shall promptly take corrective action and immediately prevent or mitigate potential damage.

Where such abnormality results from non-compliance with this Policy by Users, System Administrators shall promptly instruct the relevant User to cease such activity immediately. Where necessary to prevent or mitigate damage to the Organization, System Administrators may suspend the User's access to the computer and network systems, subject to appropriate access control procedures.

(3) To install and update security patches and software required to correct system vulnerabilities and to ensure that computer and network systems remain secure and up to date.

(4) To review the security status of server systems and computers every four (4) months.

(5) To change passwords for server and network access every ninety (90) days or as necessary for security purposes.

(6) To perform full data backups of critical information at least once per month and to conduct data recovery testing every six (6) or twelve (12) months.

(7) To retain system usage logs (Log Files) for not less than ninety (90) days, stored on at least one separate computer system from the main servers, and to review access logs every ninety (90) days.

(8) To regularly monitor communication ports of the network systems and promptly close any unnecessary ports.

(9) To manage and maintain user accounts for Internet services, email accounts, and systems including Internet/Network access, Microsoft 365 (Email, OneDrive, SharePoint), SAP, VPN, or any other systems to ensure accuracy and currency.

User account management shall include the following:

(9.1) Creation of new user accounts (new employees), including Email, Internet/Network, Microsoft 365, SAP, and VPN access, in accordance with the operational procedure manual entitled "Request for Internal System Access."

(9.2) Provision of Internet access for visitors via Wi-Fi shall require completion of a usage request form through the Company's reception staff, in accordance with the operational procedure manual entitled "Internet Access Request for External Users."

Relevant terms and conditions shall be attached to the request form to ensure compliance with the Group's Internet usage policy.

(9.3) Email accounts shall be registered by Information Technology officers. Email addresses shall be generated based on the user's first name followed by the first letter of the surname. In cases of duplication, additional letters of the surname or sequential identifiers shall be used.

(9.4) In the case of resignation, upon approval of the resignation by management, employees shall submit an asset clearance form and system access termination request. The Information Technology Department shall verify IT assets and revoke system access rights, including Email, Internet/Network, Microsoft 365, SAP, VPN, and other systems (if any), in accordance with the operational procedure manual entitled "IT System Deactivation Procedure."

(9.5) In case of employee termination, the Human Resources Department shall notify the IT Department after the effective termination date. The IT Department shall then proceed to revoke system access rights and verify IT asset return. System access shall be terminated for Email, Internet/Network, Microsoft 365, SAP, VPN, and other relevant systems under the Ubon Bio Ethanol Group. The IT Department shall reset credentials and notify the employee's supervisor. Email accounts shall be retained only upon written approval from the supervisor and shall be deleted within thirty (30) days in cases of resignation without completion of the normal resignation process.

(10) To maintain and service computer systems, network infrastructure, and shared drives of the Organization.

(11) To report system service performance and usage, including observations and recommendations, to higher management for awareness or decision-making regarding system improvement and administration efficiency.

(12) For wireless communication systems, System Administrators shall:

(12.1) Implement encryption technologies for wireless communications with a minimum standard equivalent to WPA (Wi-Fi Protected Access).

(12.2) Ensure that wireless network devices include secure user authentication mechanisms to prevent unauthorized access.

(12.3) Install and maintain intrusion detection systems, including firewalls or equivalent security tools.

(12.4) Install, maintain, and regularly update antivirus and malicious software protection systems.

(13) Change management of IT systems shall include impact assessment, approval from authorized personnel, careful implementation, and post-implementation review.

(14) IT incident and problem management shall include recording of incident reports, resolution methods, categorization and prioritization of issues, status tracking, target resolution time, actual resolution time, and performance measurement criteria to support continuous improvement of IT service efficiency and management.

18. The Head of System Administration and System Administrators shall comply with the following:

(1) They shall not engage in any act that violates the privacy or personal data of Users whose information is stored in computer systems, without reasonable justification.

(2) They shall not disclose any information obtained in the course of their duties that is deemed confidential or should not be made available to any person, without reasonable justification.

Chapter 7
Information Security Policy on Backup and Data Recovery

Objective

This Policy establishes standards for data backup and data recovery of information systems and ensures preparedness for emergencies or any incidents that may cause damage to information assets, enabling system recovery within twenty-four (24) hours.

Backup and Data Recovery Procedures

(1) Procedures for data backup and recovery shall be properly established for both software systems and information data within each individual system. Backup and recovery procedures shall be defined separately for each system.

(2) Backup data shall be stored on appropriate storage media, which shall be clearly labeled to indicate the system name, software system, date, time of backup, and responsible personnel. Backup data shall be stored at an off-site location, separate from the primary operating site, and backup media shall be regularly tested.

(3) A business continuity and emergency preparedness plan shall be established.

(4) Emergency response drills shall be conducted at least once per year.

Chapter 8
Technical Vulnerability Management

The designated unit responsible for the Organization's information systems shall ensure that the Organization's systems are assessed for potential technical vulnerabilities in accordance with the following principles:

(1) Penetration testing shall be conducted on critical systems connected to untrusted networks. Such testing shall be performed by an independent party separate from the Information Technology function, based on risk assessment and business impact analysis, as follows:

(1.1) For high-criticality systems, penetration testing shall be conducted at least once per year, or whenever significant changes are made to the system.

(1.2) For other critical systems, penetration testing shall be conducted at least once every three (3) years.

(2) Vulnerability assessments shall be conducted on critical systems at least once per year, or whenever significant system changes occur. The results shall be reported to relevant stakeholders for awareness and for the development of corrective and preventive measures.

(3) Testing of procedures and processes for managing events that may impact information security shall be conducted at least once per year. Such testing shall include, at a minimum, Cyber Security Drills.

(4) Cyber security incident management processes shall be established and maintained to ensure effective response to information security incidents.

Chapter 9
User Access Management

The purpose of this Policy is to control access to information systems only for authorized users who have completed information security awareness training, in order to prevent unauthorized access, with at least the following requirements:

(1) Users shall be provided with appropriate knowledge and awareness to understand security risks and the potential impacts arising from careless or uninformed use of information systems. Preventive measures shall be implemented as appropriate.

(2) User registration shall include formal procedures for registering users when access to information systems is granted, and for removing users from the registry when access rights are revoked or terminated.

(3) User access rights management shall be implemented to control and restrict access privileges to each information system as appropriate. This shall include standard access rights, privileged access rights, and any other access-related permissions.

(4) Password management for users shall be implemented through a secure and controlled password management process.

(5) User access rights shall be reviewed at least once per year to ensure that access privileges remain appropriate and up to date.

Chapter 10
Software Installation Control on Production Systems

The project owner or the designated unit responsible for the Organization's information systems shall establish operational procedures and control measures for software installation on production systems. Such controls shall restrict users from installing unauthorized software and prevent the installation of unapproved applications. A list of standard software (Software Standard) permitted for installation on the Organization's computers shall be formally documented, regularly updated, and communicated to all Users for acknowledgment and strict compliance.

Chapter 11
Asset Loss, Damage, or Destruction

Asset refers to computers, peripheral devices, or any information technology equipment of the Organization assigned to employees or responsible persons for use.

In the event that any asset is lost, damaged, or destroyed due to negligence, the assigned user or responsible person shall be fully responsible for all associated costs.

The following procedures shall apply:

(1) Employees who experience asset loss, damage, or malfunction shall immediately notify their direct supervisor and submit an incident report to the Information Technology Department. Failure to report such incidents may result in disciplinary warning.

(2) Employees shall submit any damaged equipment to the Information Technology Department for inspection and assessment.

(3) The Information Technology Department shall forward the damaged equipment to an external service provider for repair cost evaluation.

(4) The repair cost estimate shall be submitted to the Human Resources Department, which shall inform the responsible employee and process salary deduction in accordance with the assessed repair cost. The Human Resources Department shall also issue a written notice accordingly.

Chapter 12
Acquisition, Development, and Maintenance of Information Systems

---

Objective

This objective of controlling the development or modification of information systems is to ensure that computer systems developed or changed operate accurately, completely, and in accordance with user requirements. This aims to reduce integrity risks related to data accuracy and system operations. The scope covers the entire process of system development or modification, from initiation and request to implementation and deployment into production systems.

Operational Guidelines

- Procedures for system development or modification shall be formally documented. At a minimum, such procedures shall include request submission, development or modification process, testing process, and system deployment process.
- Procedures for emergency system changes (Emergency Change) shall be established. All emergency changes shall be documented, including justification and approval from authorized personnel.
- Where external individuals or third-party service providers are involved in system design, development, modification, or maintenance and such activities involve personal data, a Personal Data Processing Agreement shall be executed between the Organization and the third party. Such agreement shall require the third party to act only under the instructions of the Organization and to maintain appropriate personal data security measures.
- Procedures and details related to system development and modification shall be communicated to Users and relevant stakeholders, and compliance shall be ensured.
- Requests for system development or modification shall be made in writing, including electronic forms such as email, and shall be approved by authorized persons, such as the head of the requesting department or the designated system owner.
- Impact assessments of significant changes shall be documented, covering operational impact, security impact, and system functionality.

- Applicable legal and regulatory requirements shall be reviewed prior to implementing system changes, as such changes may affect legal compliance obligations.

System Development Practices

- Development environments shall be segregated from production environments, with access restricted to authorized personnel only. This segregation shall also apply to environments involving personal data protection controls. Separation may be implemented either by using separate physical machines or logically separated environments within the same system.
- Requestors and relevant users shall participate in the system design, development, modification, and maintenance processes to ensure alignment with business requirements.
- Security and system availability shall be considered from the earliest stages of system development or modification.
- System testing shall involve requestors, IT personnel, and other relevant users to verify that developed or modified systems operate efficiently, accurately, and in accordance with requirements prior to deployment into production.

Chapter 13
Information Security Incident Management

Objective

This Policy aims to establish a consistent and effective approach for managing information security incidents, including reporting security risk situations, reporting information security vulnerabilities, and reporting incidents or threats that may impact personal data within the Organization's information systems.

Operational Guidelines

- Roles, responsibilities, and procedures shall be clearly defined for responding to information security incidents within the Organization.
- Clear communication channels shall be established for reporting information security status and incidents.
- Users who identify any incident that may affect information system security shall immediately report such incidents to the Information Technology Department.
- Security incident reporting shall be conducted according to the severity level of the incident. In cases where incidents have a severe impact on a large number of users, timely notification and communication shall be issued.

- Information security incidents shall be recorded and documented, including at minimum the type of incident, frequency of occurrence, and associated costs or damages, in order to support future analysis and preventive measures.
- Risk assessments shall be conducted, and potential threats or risks affecting personal data within the Organization's information systems shall be identified, monitored, and reported in accordance with applicable legal and regulatory requirements, including the Personal Data Protection Act (PDPA).
- Evidence related to security incidents shall be collected and properly preserved in accordance with applicable rules and standards for potential use in legal proceedings.

Chapter 14
Access Control and Data Transfer

Objective

This Policy aims to prevent any unauthorized person from accessing, using, disclosing, or modifying information or information system operations without proper rights, authority, or beyond assigned responsibilities.

Operational Guidelines

(1) Data Management

- Information and data shall be classified according to confidentiality levels and business requirements. Data categories shall be defined in accordance with business functions and priority levels, including classification of personal data as "sensitive information." Procedures for handling confidential or sensitive data prior to disposal or reuse shall also be established.
- Transmission of sensitive information over public networks shall be protected by internationally recognized encryption standards, such as SSL (Secure Socket Layer) and Virtual Private Network (VPN).
- Measures shall be implemented to ensure the accuracy and integrity of data across all stages, including storage, input, processing, and output. In cases where data is stored in multiple locations (distributed databases) or in related datasets, controls shall be in place to ensure consistency and accuracy of data across all systems.
- Appropriate security measures shall be applied to protect data, including personal data, when computers are taken outside the Organization's premises (e.g., for

repair). Such measures shall include secure deletion or anonymization of personal data stored on storage media to prevent identification of individuals.

(2) User Privilege and Access Control

- Access to data, sensitive information, personal data, and processing equipment shall be strictly controlled, taking into account operational needs and system security. Access authorization rules shall be defined, and only designated personnel shall be granted access to sensitive or personal data. Users at all levels shall be informed, trained, and required to comply strictly with established guidelines and security requirements.
- Access rights to data, sensitive information, personal data, and information systems (including application systems and internet access) shall be assigned appropriately based on job responsibilities. Access shall be granted on a least-privilege basis, subject to written approval from authorized personnel, and shall be reviewed periodically.
- In cases where privileged users are required, strict access controls shall be enforced. The Organization shall consider the following principles in determining adequacy of privileged access controls:
    - Approval shall be obtained from authorized personnel.
    - Usage of privileged accounts shall be strictly controlled and limited to necessary cases only.
    - Access duration shall be defined, and privileges shall be revoked immediately upon expiration.
    - Passwords shall be changed strictly, such as after completion of required tasks or at least every six (6) months in cases of prolonged usage.
    - When users are away from their workstations or devices, appropriate safeguards shall be applied, such as mandatory system logout to prevent unauthorized access.
    - Users shall not grant access rights to other persons unless temporarily necessary and approved by authorized management. Such access must follow established procedures, including documented justification, defined duration, and immediate revocation upon completion of necessity.

- In cases where access rights are granted to other users for data modification or access (e.g., file sharing), access shall be granted on a need-to-know basis (individual or group access only), and shall be revoked immediately once the necessity ends. Records of such access grants shall be maintained for audit purposes.
- Encryption mechanisms shall be applied to password storage files to prevent unauthorized access, disclosure, or modification.

Chapter 15
Penalties

In the event that Users violate this Policy and such violation causes damage to the Organization, the following disciplinary actions shall apply:

1. The Organization shall take action in accordance with its internal rules and regulations and/or applicable laws and regulations.
2. For non-serious violations, the matter shall be referred to the Human Resources Department and the relevant supervisor for issuance of a written warning.
3. For serious violations, disciplinary actions may include termination of employment and revocation of all employee benefits in accordance with applicable company policies and employee entitlements.

Reviewed and announced on 24 February 2026.

-Signed-

(Mr. Palakorn Suwanrath)
Chairman of the Board of Directors
Ubon Bio Ethanol Public Company Limited