-Translated Version-

Cybersecurity Policy

Ubon Bio Ethanol Public Company Limited and Its Subsidiaries

Ubon Bio Ethanol Public Company Limited (UBE) and its subsidiaries (the "Company") implement effective cybersecurity and cyber risk management in accordance with internationally recognized standards. The Company is committed to establishing effective cybersecurity and cyber risk management practices aligned with international standards in order to prevent threats, attacks, information system disruptions, and cyber espionage. This is carried out in accordance with the Information and Communication Technology Policy Standard Practice B.E. 2563 (2020), and the Company has established its Cybersecurity Policy with the following key principles:

1. A Cybersecurity Working Committee shall be established, comprising representatives from relevant functions responsible for cybersecurity across business processes and manufacturing operations at each plant site. The roles, responsibilities, and management procedures shall be clearly defined.

2. The Company shall develop and maintain a cybersecurity governance framework or practice guidelines in alignment with international standards, and shall review applicable laws and regulatory requirements related to cybersecurity at least once a year to ensure ongoing compliance.

3. Cybersecurity risk management shall be conducted based on assessments of threats, vulnerabilities, likelihood, and business impact. Risk treatment shall be aligned with the Company's enterprise risk management framework. The scope of cybersecurity risk management shall cover all organizational assets and personnel, including relevant external parties.

4. Cybersecurity awareness and training programs shall be communicated and provided to employees at least once a year to enhance awareness, responsibility, and understanding of how to respond to cyber threats.

5. Cybersecurity protection and intrusion detection systems shall be implemented across the Company's information systems, together with continuous monitoring. The responsible cybersecurity function shall report cyber threat information to management at least on a quarterly basis.

6. An incident response plan shall be established to ensure timely and effective handling of cybersecurity incidents and to minimize impacts on critical business processes. The plan shall be tested and reviewed at least twice a year.

7. A disaster recovery plan shall be developed to minimize disruption to critical business processes, and shall be tested and reviewed at least once a year to assess its accuracy and effectiveness.

8. Vulnerability assessments and/or penetration testing shall be conducted on information infrastructure and applications for systems exposed to cybersecurity risks at least once a year.

Reviewed and announced on 24 February 2026.

-Signed-

(Mr. Palakorn Suwanrath)

Chairman of the Board of Directors

Ubon Bio Ethanol Public Company Limited