UNIVENTURES

INFORMATION TECHNOLOGY GOVERNANCE POLICY

Information Technology Governance Policy

Univentures Public Company Limited ("**the Company**") recognizes the importance of information technology as a key tool to support the enhancement of organizational capabilities in both management and business operations. Therefore, to ensure the efficient, secure, and reliable operation of information technology within the Company and subsidiaries (collectively referred to as "**UV Group**"), and to maintain the confidentiality, integrity, and availability of information and information technology assets, as well as to ensure compliance with relevant laws, regulations, practices, and international standards, the Company has established an Information Technology Governance Policy to guide all departments and personnel at all levels within UV Group.

1. Objectives

   This Information Technology Governance Policy is established for the following purposes:

   - Establish a framework for the governance, operation, and management of information technology ("**IT**") at the organizational level, providing a clear operational framework for all stakeholders, both internal and external.
   - Train and educate UV Group's personnel to comply correctly with all relevant IT laws, policies, practices, and regulations of regulatory agencies and UV Group itself.
   - Prevent problems or damage to assets, business operations, or the reputation and credibility of UV Group that may arise from the inappropriate use of IT, emergency situations, or various threats.

2. Scope

   This policy applies to all directors, executives, and employees at all levels of the Company and subsidiaries, as well as external service providers (outsourced) contracted by the Company or subsidiaries to perform information technology services, and external persons or entities authorized to access, provide services to, or use any network systems, operations, or assets in UV Group's IT systems.

3. Relevant definitions

   - **The Company** means Univentures Public Company Limited.
   - **Subsidiary** means a business in which Univentures Public Company Limited directly or indirectly holds more than 50% of the total number of shares with voting rights or has control over the business.
   - **UV Group** means Univentures Public Company Limited and subsidiaries.
   - **Information** means to data, facts, news, and knowledge that have been recorded, processed, or handled in any way, and which can be used for management, planning, decision-making, and other purposes.
   - **Assets in IT system** refer to assets or things within or used with UV Group's IT system, both tangible and intangible, such as hardware, software, computers, servers, IP addresses, domain names, and various licensed software.
   - **Inside information** means confidential business information or important information of UV Group that has not been disclosed to the public or the Stock Exchange of Thailand and that affects the price of the Company's shares or the decision to buy or sell the Company's shares, which personnel of UV Group and related persons have access to such information from their positions or from a position that allows them to know the facts or from being employees.

- **Artificial Intelligence (AI)** means a technology developed to enable computer processing systems, robots, machines, or various electronic devices to possess characteristics or behaviors similar to humans, according to human-defined objectives. This includes learning, perceiving and responding to the environment, reasoning, and problem-solving. The Company provides and implements AI for use by executives and employees within UV Group.

4. **Duties and Responsibilities**

In order to effectively manage this IT Governance Policy, the Company has defined the duties and responsibilities of the relevant departments and individuals as follows:

(1) **The Board of Directors**: Approves and oversees the policy in accordance with the Company's strategic goals and good corporate governance principles, and review policy to ensure they are appropriate to changes in the business environment and relevant laws.

(2) **Senior Executives:**

- Allocate sufficient and appropriate personnel, budget, and technology for operations related to IT governance to achieve the objectives of this policy.
- Monitor and supervise relevant departments to ensure they implement the policy, including establishing guidelines, principles, and procedures related to IT governance.
- Promote education and understanding among UV Group's personnel to ensure compliance with IT Governance Policy correctly and appropriately.

(3) **Information Technology Department**:

- Control, monitor, and advise UV Group's personnel on compliance with this policy, as well as other laws and policies or practices related to IT governance.
- Monitor technological trends and threats, including changes in relevant laws and standards, in order to develop or recommend ways to improve the efficiency and security of UV Group's IT systems.
- Support training or review activities on knowledge and best practices related to IT governance for UV Group's personnel.

(4) **Employees**:

- Comply with IT Governance Policy, including all relevant laws and policies related to IT governance.
- Inform their supervisor or IT Department when they discover any actions that violate the law, this policy, or other policies and/or practices of UV Group related to IT governance.
- Participate in training or review activities related to IT governance organized by IT Department or Human Resources Department of the Company or subsidiaries.

In the event that information and IT systems of UV Group are damaged due to defects, negligence, or violations of IT Governance Policy, including laws and policies or practices related to IT governance, this constitutes an offense subject to disciplinary action according to the Company or subsidiaries' regulations or the terms of the employment contract, and may also result in penalties as prescribed by relevant laws, rules, regulations, or orders.

5. Policy

5.1 Allocation and Management of Information Technology Resources

In order to ensure that the allocation and management of IT resources are aligned with the corporate strategy, the Company requires senior executives, IT Department, and related departments of the Company or subsidiaries to:

(1) Establish criteria and factors for prioritizing IT plans to align with the corporate strategy or business objectives.

(2) Define the duties and responsibilities of IT Department and personnel for the allocation and management of IT resources.

(3) Prepare and approve an IT budget that is consistent with the overall budget and corporate strategy.

(4) Provide sufficient human resources for IT work and continuously develop the skills of such personnel, including considering hiring external IT providers when necessary.

5.2 Information Technology Risk Management

(1) Establish IT risk management in accordance with the corporate risk management policy.

(2) Establish IT system security measures to ensure UV Group's information systems are always available, which is part of UV Group's business continuity management.

(3) Establish a system for managing events that may affect information system security, defining clear management procedures and responsible parties to ensure that such events are resolved or addressed correctly, efficiently, and within a reasonable timeframe.

(4) Establish an IT asset management system, specifying responsible parties and responsibilities to ensure that critical IT assets are adequately protected.

5.3 Information Technology System Security

The Company has established an IT Security Policy and Procedures to control, monitor, and standardize the use and operation of information and IT systems within UV Group, as well as to provide guidance for UV Group employees and related parties. This policy covers the following areas:

(1) Access control and security of IT systems

(1.1) Access to UV Group's IT system must be controlled and limited by IT Department in accordance with operational necessity, be appropriate in a hierarchical manner and according to the right to have access only, as well as to maintain, store, protect work systems and important information in accordance with this policy, including being legally related and having to keep evidence of rights requests, can be examined.

(1.2) Access to UV Group's IT system requires user registration, which is authenticated only by using the account name and password in their own company domain. Employees are prohibited from sharing their own account names in the domain with other employees and a password must be securely set in order to verify identity in the use of the system, identify who is responsible for the recording of such transactions in the system, and use it to determine hierarchical access to information according to the right to have access. It is also used to identify the use of traffic routes in UV Group's network.

(1.3) Access to information by level of importance and the storage of information in the work system must have a hierarchy of importance, classified by function, task, department. Methods for managing and protecting each type of information are defined, including accessing and safeguarding sensitive personal data (as defined in the Personal Data Protection Act) and establishing procedures and practices for dealing with sensitive data before selling, replacing or reusing the device.

(1.4) Access control of the server room is intended to control the security of system, network system and UV Group's information by limiting access to rooms in which networking equipment or equipment used in UV Group's IT system is installed and stored. In cases where unauthorized persons need access to such rooms, the Company requires that the name, time, and reason for access be recorded for later investigation, and that a designated server room officer be responsible for overseeing and controlling access to such areas.

(1.5) Security of the server room. The Company requires the installation of a fire suppression system suitable for computer and electronic equipment in the server room to minimize damage to equipment when it is needed. It also requires the installation of a backup air conditioning system and an emergency power backup system adequately commensurate with the importance of the various systems, and requires regular maintenance of equipment to ensure the continuous operation of the systems and network.

(1.6) Controlling network access from both internal and external networks. Requires those who will access to use must be approved by IT Department first and must have an identity verification procedure by entering an account to identify with a username and password in the domain before accessing. The connection path between UV Group's computer network and the Internet is enforced through the control system, monitoring system and security system as specified by UV Group. The network system is designed by demarcating the boundaries (Zone) in use to be able to protect against threats safely and effectively and can be inspected in case abnormal events occur.

(1.7) Controlling access to wireless networks to prevent access to UV Group's IT system. Before accessing, a verification procedure (Authentication) is required by entering an account to identify with a username and enter the password in the domain In the case of being a contact with UV Group (Guest), it is necessary to obtain approval for use via the registration system for using the wireless network of UV Group (Guest Wi-Fi) or the use of a Media Access Control Address of the connected device to request approval and register with IT Department before use.

(1.8) Controlling access to work systems, operating systems, databases, applications, and utility software to prevent unauthorized access. Access requires prior approval from IT Department, which includes a procedure for verifying identity (authentication) by entering a username and password before access is granted. Access to critical systems requires specific rights, which must be approved in writing by a supervisor or another authorized individual. Alternatively, rights can be requested through UV Group's rights request system to serve as evidence for audits. Access rights must be revoked upon a change in responsibilities or resignation, and the granted rights must be reviewed regularly. Furthermore, computer networks connected to the internet must be equipped with antivirus software. Internet connections must be routed through control systems, monitoring systems, and security systems.

(1.9) The Company establishes the security of UV Group's electronic mail (e-mail) system and defines the duties and responsibilities of users in the use of UV Group's e-mail system. UV Group's e-mail is only used for contacting tasks related to UV Group's mission and requires IT Department to impose prohibitions, precautions and rights of use that take into account UV Group's IT security systems.

(1.10) To prevent unauthorized access to UV Group's IT system, including disclosure or theft, the Company requires UV Group's employees to be responsible for setting and changing the password for logging in to UV Group's IT system in accordance with the control policy of IT Department, not keeping the computer screen on without preventing others from to using it instead, and to keep and maintain assets in UV Group's IT system in a safe place to prevent malicious people from using such assets in a way that causes damage to UV Group.

(1.11) To mitigate the risk of vulnerabilities that could be exploited to attack systems, IT Department is required to continuously manage the installation of operating system patches. For the Company's critical ERP systems, IT Department must manage the installation of necessary software and operating system patches in a timely manner. These patches are to be tested in a secure environment before being deployed. In cases where critical systems cannot be patched, IT Department must identify this in the IT security exceptions list for monitoring and risk management according to established management processes.

(1.12) To monitor and ensure that patches in the ERP system, the Company's critical system, are continuous and effective, IT Department is required to conduct or coordinate an examination of the results of software and operating system vulnerabilities at least once a year and submit a report of the assessment results to the executives for signature to acknowledge and consider management as appropriate.

(2) Data backup, preparedness for emergencies and cyber threats

(2.1) The Company requires that there be a backup system for important data in UV Group's IT system in order to be able to provide continuous, stable, secure services. The backup system is always checked and maintained in a ready-to-use condition by prioritizing the backup of UV Group's IT system as needed, from greatest to least, including assigning responsibilities to employees who inspect and maintain the backup system.

(2.2) The Company requires regular backup of important work systems in UV Group's IT system by considering the backup frequency, method and technology used in the backup to suit the importance of the data in UV Group's work system, as well as considering keeping UV Group's work system and important information ready for use at another secure location, preparing an IT contingency plan and preparing a back-up processing system to support UV Group's main transactions to be able to proceed continuously.

(2.3) IT Department shall agree with the data owner to set the backup frequency and the period of data retention, which must ensure that UV Group's data and databases are backed up regularly, completely and continually, ready to be reused within the specified time frame when an emergency occurs.

(2.4) IT officers are responsible for backing up data, verifying backed up data and data recovery, including assessing and reviewing preparedness plans in case of emergency situations, as well as defining responsibilities and procedures for dealing with emergency situations that arise. Access to UV Group's data backups and data retrieval is required to be performed only by authorized personnel of UV Group and system administrators.

(2.5) The storage media and storage systems used to keep UV Group' s data backups and important databases must be tested at least once a year and results of the testing must be reported to the senior management of IT Department. This ensures that work systems and data can be restored at any time or when an emergency occurs.

(2.6) Employees are responsible for keeping UV Group's data securely stored in a designated location so that the backup system can recover UV Group's data and prevent malicious individuals from using such data in a way that would harm UV Group. Employees are prohibited from backing up personal data or data unrelated to UV Group's operations to UV Group's data system.

(2.7) Establish a Business Continuity Plan and Disaster Recovery Plan for Information Technology Systems as a guideline, including preparing backup processing systems and resources required to connect to the main and backup networks so that UV Group's main transactions can continue to operate continuously.

(2.8) In response to an emergency situation of IT system that affects UV Group's business operations, the Company has established a working group and personnel to manage when an emergency occurs and has clearly defined roles, responsibilities, necessary procedures, and communication methods to comply with the prepared plan.

(2.9) Establish a Cyber Incident Response Plan, and develop a plan that covers information, as well as critical infrastructure components of business systems and networks that are necessary for UV Group's core business activities. There must be annual rehearsals and reviews to ensure that the plan can be effectively applied in real situations. The executives and related employees must be aware of and understand the specified procedures.

(2.10) In order to effectively respond to cyber threat incidents, the Company has established a working group and personnel to handle and respond to cyber-attacks, with clear roles, responsibilities, necessary procedures and communication methods defined so that relevant employees understand their roles and can perform their duties correctly and quickly when a cyber threat occurs.

(3) Audit, risk assessment and internal information control

(3.1) The Company requires UV Group's IT risk assessment by providing UV Group's internal auditor or an independent external auditor at least once a year in order for the Company and departments to be aware of the level of risk and security in IT systems of UV Group.

(3.2) The Company requires all departments to organize their work and place of work to maintain internal information of UV Group. Do not disclose that information to persons unrelated or not necessarily known. Using or submitting internal data to be done by the responsible person or authorized by the authorized person only.

(3.3) Employees working on UV Group's inside information are prohibited from disclosing inside information, directly or indirectly, to any person. Unless assigned as a responsibility and authorized by the authorized person only.

(4) Raising awareness and regulations of security in IT security systems

(4.1) Organize employees' training on practices in accordance with UV Group's IT Security Policy on a regular basis and disclose knowledge of laws and regulations related to the use of IT systems.

(4.2) Disclose UV Group's IT Security Policy on UV Group's intranet so that all employees can easily access it.

(4.3) Provide preventive measures by providing knowledge of the practices on how to use and precautions in the use of UV Group's IT systems, including setting penalties for employees when found to have committed an offense or improper use of IT system, such as suspension of access or suspension of the right to use.

(4.4) Employees are obliged to strictly implement this policy. Violators do not comply with this policy in any way or infringement of copyright in the use of computer programs of UV Group for their own benefit or any person other than their obligations or for the benefit of UV Group. It is a violation of employee discipline.

(4.5) If a computer or any computer equipment damaged or lost, the Company requires employees, the responsible person to possess or an assigned person to notify the executives or persons assigned to act on their behalf immediately to continue to troubleshoot or mitigate the damage.

(5) Practices relating to computer programs that UV Group or employees provide, create, develop

(5.1) Creating or developing programs for use by UV Group, it must be approved in writing by executives or authorized persons assigned by UV Group.

(5.2) Computer programs created or developed by employees as employees of UV Group, the license of such computer program belongs to UV Group.

(5.3) Batch processing shall be carried out under appropriate controls, including a batch schedule and post-processing data validation, as well as data backup measures and monitoring systems to prevent potential damage from processing errors.

(5.4) When UV Group implements computer programs related to artificial intelligence ("**AI**") in operations, it is required to comply with AI Governance Policy and Practice, taking into account data security. This includes prohibiting the use or disclosure of internal information, confidential data, important documents, or information that may affect UV Group's operations, as well as personal data, when using AI. Furthermore, the accuracy of data obtained from AI must be verified before use, and approval for the use of secure AI within UV Group must follow established procedures.

(6) Management of external IT service providers

(6.1) To ensure that the operations of ERP service providers or other systems the Company has assessed as being equally critical to the Company's business operations comply with the security requirements set forth in the Company's policies, prior to selecting a service provider or contracting with the service provider, IT Department is authorized to inspect and evaluate the service contract to ensure that the services provided comply with the Company's security requirements.

(6.2) Establish a system for managing, monitoring, inspecting, and regularly evaluating the performance of the ERP system providers or other systems that the Company deems equally critical to business operations, in order to prevent potential risks arising from the operations of external service providers.

6. Policy Review

The Company requires that this policy be reviewed annually or whenever significant changes occur and that any revisions or changes to the policy be presented to the Board of Directors for approval.

7. Relevant Policies and/or Practices

Directors, executives, and employees are responsible for acknowledging, understanding, and complying with the Company's policies, practices, and other manuals related to IT Governance, such as:

- Information Technology Security Policy and Procedures
- Artificial Intelligence Governance Policy
- Artificial Intelligence Governance Practice
- Code of Business Ethic
- Policy, practices, and regulations regarding personal data protection
- Work regulations, manuals, and operating procedures

This Information Technology Governance Policy was approved by the Board of Directors at Board Meeting No.3/2026 - 2027 on 14 May 2026 and is effective from 15 May 2026 onwards.