UNIVENTURES

INFORMATION TECHNOLOGY SECURITY POLICY

Announcement of
Information Technology Security Policy

Univentures Public Company Limited ("the Company" or "UV") provides information technology system which consists of work systems, network systems and data systems of the Company and its subsidiaries (collectively referred to "UV Group"), as well as computers and peripheral equipment in the office for the employees of UV Group to use in their assigned duties, to increase the convenience and speed of work , used to search for information and communicate both internally and externally. In this regard, in order to use the information technology system of UV Group to be efficient, secure, and maximize benefits. Therefore, the Company has established an Information Technology Security Policy of UV Group. Details are as follows:

1. Objectives of applying the policy
    - 1.1 To create confidence and security in the use of information technology systems ("IT Systems") of UV Group.
    - 1.2 In order to be able to use IT systems of UV Group with the highest efficiency and effectiveness.
    - 1.3 To disclose to all employees of UV Group for acknowledgment and strictly adhere to the policy.
    - 1.4 To define standards, guidelines and practices for executives, employees, system administrators and third parties working for UV Group to realize the importance of maintaining security in the use of IT systems of UV Group.
2. Material topics of IT Security Policy of UV Group are as follows:
    - 2.1 Access control and security
        - 2.1.1 Controlling access and use of IT systems of UV Group
        - 2.1.2 Management of access rights
        - 2.1.3 Management of access to confidential information
        - 2.1.4 Access control to the server room
        - 2.1.5 Server room security
        - 2.1.6 Management of network security
        - 2.1.7 Management of wireless network security
        - 2.1.8 Controlling access to operating systems, application software and utility software
        - 2.1.9 Security of electronic mail ("E-mail")
        - 2.1.10 User responsibilities
    - 2.2 Data backup, data recovery and IT Contingency Plan
        - 2.2.1 Establishment of a backup systems for important data in IT systems
        - 2.2.2 Preparation of plans and data backup systems in case of emergency situations
        - 2.2.3 Determination of data backup periods and audit periods
        - 2.2.4 Data backup system test
        - 2.2.5 Determining the responsibilities of data backup systems administrator
        - 2.2.6 User responsibilities
    - 2.3 Audit, risk assessment and internal information control
    - 2.4 Raising awareness and regulations of security in IT security systems of UV Group
    - 2.5 Guidelines on computer software that UV Group or its employees procure/ create/ develop

3. Assigning responsible persons
   3.1 Assign UV Group's top executive to be responsible for any risks, damages or harm arising in the event that the computer systems or IT systems are damaged or dangerous in any way to UV Group or anyone due to a defect, neglect or violation of compliance with the IT Security Policy.
   3.2 Assign the executive of IT Department to be responsible for ordering according to UV Group's IT Security Policy.
   3.3 Assign the director of IT Department to be responsible for monitoring, supervising, assigning.
   3.4 To verify compliance with the policy and make recommendations to employees or outsources working for UV Group to be efficient, the Company has designated IT Department, system administrators, responsible persons and designated persons to be responsible for the implementation of this policy. IT Security Policy is reviewed at least once a year and disclosed to the employees of UV Group every time when there is a policy change.
4. In order to raise awareness of the threats and impacts caused by IT systems use without caution or ignorance, the Company requires knowledge and understanding of the matter to be provided to UV Group's employees with the following methods:
   4.1 Organize training to provide knowledge and understanding of user responsibilities regarding IT security of UV Group for employees to be aware of
   4.1 Disclosing the IT Security Policy via UV Group's intranet so that all employees can easily access it.
5. This policy is regarded as the standard for the security of UV Group's IT systems to serve as a guideline for operating electronic methods to be safe, reliable, in accordance with relevant laws and regulations. The Company requires all employees of UV Group to strictly adhere to this policy.

In this regard, it shall be applied from the date of this announcement onwards.

Announced on 1 January 2022

-Mr. Khumpol Poonsonee-

(Mr. Khumpol Poonsonee)
President

Information Technology Security Policy of UV Group

The Company has established IT Security Policy of UV Group in order to control, supervise and set standards for the use of IT systems for UV Group's employees to comply with the following practices:

Section 1 Access control and security

Clause 1.1 Access to UV Group's IT system must be controlled and limited by the 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.

Clause 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.

Clause 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.

Clause 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 the event that a person who does not have a relevant duty needs to access the said room, names, times and reasons for entering the area must be recorded for later review and there must be someone responsible for the server room to supervise access control in such area.

Clause 1.5 Security of the server room. A fire extinguishing system of the type used for computers and electronic equipment must be installed in such rooms to minimize damage to the equipment when needed. It has installed an air conditioning backup system and an emergency power backup system to be sufficient according to the level of importance of various work systems and set a maintenance cycle for the equipment so that the work system and the network can provide continuous service.

Clause 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.

Clause 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.

Clause 1.8 Controlling access to work systems, operating systems, applications and utility software to prevent unauthorized access. It requires those who will have access to use it to be approved by IT Department first, including having to have a procedure to verify identity (Authentication) by entering an account to identify with a username and entering the password before accessing. Access to critical systems requires specific rights to perform tasks within the scope of duties with the approval of the supervisor or the person who has the right to approve in writing or request rights from UV Group's rights request system to record it as evidence in the audit and to regularly review the rights granted. UV Group's computers that are connected to the Internet have an antivirus program installed, or there is a compulsory route to connect to the Internet through the control system, monitoring system and security system as specified by UV Group.

Clause 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.

Clause 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.

Section 2 Data backup, data management and IT contingency plan

Clause 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.

Clause 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.

Clause 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.

Clause 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.

Clause 2.5 The media and 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.

Clause 2.6 UV Group's employees are responsible for not backing up personal data or information that is not relevant to UV Group's operations into UV Group's data systems, as well as keeping UV Group's data in a secure place so that the backup system can restore UV Group's data back and to prevent any malicious person from using such data in a way that causes damage to UV Group.

Section 3 Audit, risk assessment and internal information control

"Inside Information" means UV Group's data and/or that of customers within UV Group that is material to changes in the price of securities that have not yet been disclosed to the public or the Stock Exchange of Thailand, including data that has been known due to the job position or a position capable of knowing the facts or being a UV Group employee.

Clause 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.

Clause 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.

Clause 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.

Section 4 Raising awareness and regulations of security in IT security systems

Clause 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.

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

Clause 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.

Clause 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.

Clause 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.

Section 5 Practices relating to computer programs that the Company or employees provide/ create/ develop

Clause 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.

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

Remark Practices or regulations related to IT Security Policy is a part of this policy.

****