UNIVENTURES

Notice of Regulations for Computer System Usage

Univentures Group has provided computers for employees to use on their assigned tasks including setting up system and network related to internet usage and e-mail transaction to increase convenience of information search, task assignment, and communication of both internal and external. In order to ensure that the usage of computer system is effective and provides optimum benefit for the Group, regulations for computer system usage are set as follows:

Section 1
Usage of Electronic Mail (E-mail)

Article 1 The Company allows usage of company e-mail within company activities only.

Article 2 Sending an e-mail that consists of message or picture or audio or any kind of form that causes damages to others is considered as an extreme violation to the Company's policy. The employee must take responsibility for the damages by his/her own in which the Company will not provide any support.

Article 3 Disclosure or publishing of the Company's confidential information without related duties or responsibilities is considered as an extreme violation to the Company's policy. The employee must take responsibility for the damages.

Article 4 Attached file must not exceed the size specified by the Company.

Article 5 Regarding sending of attachment to multiple employees such as sending picture file or video file that exceeds the specified size, instead of file attachment, the Company has set alternative methods of file sharing or link sharing or placing file in folder set by the Company then sending e-mail to inform accessibility to the file.

Article 6 All employees hold responsibilities in cautious inspection of receive-delivery of file attached with e-mail in order to reduce the risk of external attack from malicious personal. If an e-mail with computer virus is opened, employee must inform Information Technology staff immediately to proceed with solution.

Article 7 In order to provide work convenience, employees can access company e-mail from outside the company. In this regard, all employees are responsible for secured usage and maintaining of user login and password for e-mail and must not use user login and password on any external computers that are subjected to risk of computer virus or malicious personal that can elicit information.

Article 8 Because e-mail is currently a channel with risk of external attack, the Company gives authority to Information Technology department to set e-mail system to reject attached file of some email addresses with high risk and also to oversee e-mail usage policy in other aspects that will help increase stability and security to the Company.

Univentures Public Company Limited
22nd Floor, Park Ventures Ecoplex, 57 Wireless Road, Lumpini
Patumwan, Bangkok 10330, Thailand

บริษัท ยูนิเวนเจอร์ จำกัด (มหาชน)
57 ปาร์คเวนเชอร์ อีโคเพล็กซ์ ชั้น 22
ถนนวิทยุ แขวงลุมพินี เขตปทุมวัน กรุงเทพฯ 10330

Tel: 66 (0) 2643-7100
Fax: 66 (0) 2256-0505
www.univentures.co.th

Section 2

Internet Usage within Company

Article 9 The Company allows usage of internet as tool for obtaining knowledge or information searching in order to achieve work objective only.

Article 10 Usage of internet to deliver or publish illegal information is prohibited.

Article 11 The Company prohibits any employee that is not responsible or not assigned to use internet to publish confidential information externally. This is considered as extreme violation to the Company's policy and the employee must take responsibility for the damages.

Article 12 Accessing websites that refer or involve with illegal matters or may cause damages to the Company is prohibited.

Article 13 The Company prohibits usage of unauthorized chat programs including audio, visual, and message type with personnel outside company network system because it can be channel for information leakage and it unnecessarily consumes internet bandwidth of the Company.

Article 14 Do not download file with size exceeding the size specified by the Company because it will cause slower operation of the major system of the Company. If it is necessary, please inform Information Technology staff to consider appropriateness and offer suggestion for action.

Article 15 For work convenience, employees can use internet within the company network in which it must be done through login with domain user only in order for the system to be able to identify personnel according to the Computer Crime Act.

Article 16 Regarding usage of other program types such as social network programs which must access internet, the programs must have capability to be accessed via login with domain user only in order for the system to be able to identify personnel according to the Computer Crime Act. The programs must not request high level of authorization that will reduce security of the company network such as request for local admin authorization.

Article 17 Employees can use intranet system to reserve meeting room, projector, and vehicle. Employees can also use it to place file for sharing such as company certificate forms of each department. If employees want to revise department content by themselves, employees can send request of additional authority to Information Technology department for approval and procedure for additional authorization.

Article 18 All employees are responsible for using internet with cautions to reduce risk of attack from malicious personnel or from computer virus.

Article 19 Because internet is currently a channel with risk of external attack, the Company gives authority to Information Technology department to oversee and monitor access to risky websites and also to manage internet usage policy in other aspects that will help increase stability and security to the Company.

Section 3

Data Storage within Network Drive on File Server

Article 20 All important working material must be stored within the Company's network drive only.

Article 21 The Company has set network drive for each type such as drive sharing data between departments, drive for sharing data within departments, drive for storing specific data for individuals in which they are differentiated by letters clearly representing each drive such as drive H:, drive I: in order to provide security, customization of authority to access data, and data recovery by Information Technology Department.

Article 22 Personal data or files not related to work or files that illegally violate copyright such as music files (MP3, WMV, AAC, etc.), movie files, and pornographic pictures are prohibited from storing in network drive on file server because they require unusual file size for storage, violate copyright and laws, and may contain virus attachment into network system of the Company.

Article 23 In the event that there is demand to access network drive of other department or to create additional network drive to share usage with other department, the employee has to send request for additional authorization to Information Technology Department for further submission to management for approval. This submission must be completed prior to any procedures every time.

Article 24 All employees hold responsibilities to use network drive prudently, deliberately, and cautiously in order to create efficiency for usage of file server and mitigate risks from attack by malicious outside individuals or computer virus.

Article 25 The Company gives authority to Information Technology Department to manage, monitor access, and specify employee quota of each department on network drive. In this regard, the aforementioned management must align with the Company's policies and agreement of the department that owns such information.

Section 4

Computer and Computer Programs Usage

"Computer" is defined as personal computer operating stand alone or connecting in network type as well as notebook and server computer.

"Computer Program" is defined as work system, command, command set or other matter that is applied with computer in order to operate computer or create a particular result.

Computer is an equipment that the Company has provided to employees to use on the Company's work and it is the major equipment to use for accessing the Company's work system. Consequently, it is an important tool that needs to have rules and regulations for usage as follows:

Article 26 Employees must not use the Company's computer in any other matters apart from their working tasks that have been assigned by the Company.

Article 27 Employees must examine for computer virus or unknown programs every time when external media of every type such as CD, DVD, USB thumb drive, and SD Card are used with the Company's computer in order to prevent damages to computer system or to the Company's data.

Article 28 Employees must contact staff of Information Technology Department immediately when unknown programs are found in computer or it is found that there are computer virus with external media to be used with computer which can result in damages to computer system or loss of the Company's information.

Article 29 Installation or usage of non-copyright programs is prohibited as they may contain computer virus and they violate copyright laws. If there is demand to use copyright programs, there must be request for purchase approval from head of department and from Information Technology Department according to policy of "Approval request for purchase or development of programs".

Article 30 Installation of programs and computer games not related to work into the Company's computer is prohibited because the installation may impact operating efficiency of programs within the computer, may impact work system, and may contain computer virus that attaches into network system of the Company.

Article 31 No individuals shall act in violation of copyright of the Company's computer programs including duplication, adaptation, disclosure, revision, or any actions defined by laws to be considered as copyright infringement.

Article 32 Installation of programs received without compensation from internet, training workshop, or other methods onto the Company's computer without authorization is prohibited. In every case, there must be notification and approval request to Information Technology Department.

Article 33 Installation of any computer equipment that the Company did not provide is prohibited. If there is demand for usage or installation, notification and approval request to Information Technology Department must be made every time in order to prevent damages to the Company's computer and network system.

Article 34 Employees must not arbitrarily relocate any computer equipment. The management of any equipment must be in accordance to the Company's policy which will be managed and controlled by Information Technology Department and Administration Department.

Section 5

Accessibility Control and System and Information Security

Article 35 Accessing work system and information of the Company must be done with personal identification through using domain user and password of each employee only. Employee must not share domain user with other employee and must set the password securely in order for the Company to record transaction in work system, identify responsible individual for such transaction, and prevent information access from user who does not have authorization to access.

Article 36 Accessing work system and information of the Company requires accessibility control and limitation by Information Technology Department in consideration to necessity for work and level of information security. This also includes control and prevention on using information under wrong purpose.

Article 37 Employees who use work system and information in the Company's system hold responsibilities for actions resulted from domain user of himself/herself in which the domain user must not be disclosed or exchanged with other individual.

Article 38 Accessing network system from outside the network must gain approval from Information Technology Department first and must be used only through securely channels. In addition, there must be security control on other type of portable equipment such as smartphone and tablet for connecting with the Company's network.

Article 39 In the case that there is connection between networks, there must be procedures or equipment for its control, security measures for accessing information with network separated by user group and usage type, as well as controlling and examining procedures in the case of abnormal events.

Article 40 Employees hold responsibilities for setting and changing password for accessing the Company's computer accurately in accordance to policy of Information Technology Department. They must not turn on the computer and leave it without user and without protection from usage by others in order to prevent unauthorized individuals from using computer or accessing the Company's system with employee authorization.

Section 6
Internal Information Control

"Internal Information" is defined as corporate information and/or customer information that is significant to price change of securities, has not been disclosed to public or stock market, and acknowledged by position or status that has ability to acquire these facts or by being employee of the Company.

Article 41 The Company imposes all departments to organize work system and work environment and secure the Company's internal information not to disclose it to individuals who are not related or do not require to know. Using or communicating of internal information will be done by only individuals who hold responsibilities or have approval from person of authority.

Article 42 Employees whose work are related to internal information of the Company must not disclose internal information to any individuals, directly or indirectly, unless they are assigned to be responsible individuals and have approval from person of authority only.

Section 7

Information Backup and Recovery

Article 43 Work system and information in all work systems must have occasional data backup with consideration to necessity and sufficiency of data backup. The work system and information must also be ready to use and contained at another secure location. In addition, there should be back up for processing system in order for the operation of the Company's main business to continue consistently with efficiency.

Article 44 The department who holds ownership of its information will be responsible for determining requirement and period for data backup in which it must be certain that the information and database has been backed up occasionally, completely, and continuingly to be ready for usage within the set period in the case of emergency.

Article 45 Personal information or information not related to work operations of the Company is prohibited from backing up into work system and network system of the Company.

Article 46 Accessibility to backup data of the Company and its usage must be done by only individuals authorized by the Company and administrator.

Article 47 Tool for information storage and backup database must be occasionally tested in which the test result must be reported to management in order to be certain that it can be used anytime or when emergency occurs.

Section 8

Procurement, Development, and Maintenance of Information System

Article 48 Administrators of work system and information system of the Company hold responsibilities to control and manage their accessibility, information of work system, and original programs.

Article 49 Administrators of work system and information system of the Company must provide certainty that the changes in work system or information system from development, procurement, and system test are under control with proper management tools, procedures for change request, and procedures for approval request before operation or usage in accordance to the policy on notification and resolution of issues set by the Company with consideration on information security and system stability.

Article 50 Administrators of work system and information system must review work system settings before actual operation to prevent flaw within information security. In the case that a flaw is found within work system or information system, the abnormal incident must be reported according to the Company's policy on notification and resolution of issue.

Section 9

Procedures related to Computer Programs Created/Developed by the Company or Employee

Article 51 Creation or development of programs to use in the Company's work must obtain approval in written form from executives or individuals with authority assigned by the Company.

Article 52 For computer programs that employee has created/developed, as an employee of the Company, the copyright of such computer programs will be owned by the Company.

Section 10

Compliance to Regulations

Article 53 Employees hold responsibilities to strictly comply with these regulations. Individuals who do not comply with these regulations on any articles or violate copyright in using the Company's computer for own benefits or benefits of others apart from his/her duties or benefits of the Company are considered to conduct disciplinary action.

Article 54 In the case that any computer or computer equipment is damaged or lost, the employee who uses, holds responsibility in ownership, or assigned individual must inform management or person assigned for the duty immediately in order to proceed for resolution, prevention, and damage mitigation.

The compliance to these regulations shall take effects from the date in this notice onwards.

Notice as of July 1, 2018

Mr. Worawat Srisa-an

President