International Teaching University of Management and Communication

ALTERBRIDGE

The Policy of Informational Technologies

Reviewed by Academic Board, minutes #2, on 05/03/19
Approved by the Rector's order #O/1-01/08 of 07/03/2019

1. Field of Action and Responsibilities

1.1. This procedure regulates the rule, procedure and policy of general safety of information technologies developed by the Information Technologies Service at the University of International Management and Communication. The Information Technologies procedure is a collection of norms established by the Teaching University, which aims to establish the uniform behavior of conducting, using computer means and communications technologies on the balance sheet of the Teaching University. The rule of protection of information technologies has been approved by authorized persons of the university and the rules in it are mandatory for the employee who has direct communication with the existing information and telecommunication technologies, regardless of location and work place of the employee.

1.2. The management reserves the right to periodically revise the existing procedure without the notice and permission of the employees. Information about procedure changes will be available to the employees through the information exchange mechanisms of the university.

1.3. Information Technologies staff is responsible for the implementation and protection of the procedure and, as well, every employee of the Teaching University is responsible for its implementation.

2. The Rule of Use and Obligations

2.1 Only the staff of the Teaching University and interns, who have "user" status, have the right to use the computers and programs of the university.

2.2 The use of computers and programs of the university by the third-party is inadmissable.

2.3 In case of damage to hardware or software error, each employee is obliged to immediately inform the IT service. Information Technology Service is responsible for solving the problem in time.

2.4 At the end of each working day it is recommended to turn off the computer and peripheral equipment attached to it.

3. The Rules of Using Technics

3.1 Technical equipment will be transferred to the teaching university staff in temporary use and is the property of the university.

3.2. In case of loss of office equipment belonging to the Teaching University, the employee is obliged to immediately inform the direct supervisor and the Information Technology Service. Information Technology Service is responsible for blocking user information

3.3 It is forbidden:

3.3.1. Transferring computer of its equipment to the other person without special permission;

3.3.2. Connecting additional, internal or peripheral equipment to the computer without the permission of IT Service.

3.3.3. Dismantling the computer or other communicational technologies or moving to another placeo without written permision.

3.4. The user is obliged to:

3.4.1. In case of physical damage of the computer hardware pay the costs of the damage.

3.4.2. In case of loss of delivered hardware pay the cost of it.

4. Terms of Using the Software

4.1. Each computer has only the necessary software installed. Additional software can be installed only in case of the obligatory need of it for the staff to execute the imposed work and there is an agreement of HR Management Office of the Teaching University. The right to install the software has only the staff member of IT Service.

5. Terms of Using the Internet and Document Exchange

5.1 The Internet is an important instrument for carrying out the activities of the Teaching University. It is available for every staff member and its use it allowed only for need.

5.2 Based on the interests of the Teaching University, IT Service has the right to limit the use of social networks and access to other prohibited Internet resources set by the management.

5.3 It is prohibited:

5.3.1. The use of non-ethic, immoral, pornographic, terrorist, spy and other prohibited web-pages by Georgian legislation.

5.3.2. The use of dating, entertainment, gambling and other similar web-pages, which are not directly connected to the activities of the Teaching University.

5.3.3. Downloading audio and video files, which are not directly connected to the university activities.

5.3.4. It is prohibited to use the Internet with other sources (mobile phone or tablet computer) at the university (Wi-Fi). Except for the cases that are caused by the workplace necessity. Otherwise, it is permissible to use wireless networks for guests. Internet source (Wi-Fi) password is only available for staff and is intended for university's computers, tablet hardwares and mobile phones. Internet source (Wi-Fi) can be used by alternatives (mobile phones or tablets). The password shall be available for students, academic saff and guests.

5.4 Document exchange program is an page for unviersity's staff which is intended for internal use and it is prohibited to diclose the information.

6. The Terms of Using E-mail

6.1. Based on the request of the Human Resources Service, an IT staff employee creates an e-mail and "user" with password required to register new employee in the information system. After that, the employee is responsible for the change of the primary password and therefore the security of the information as well as the safe keeping/archiving of its personal files.

6.2. Every employee is obliged to check the official e-mail of the Teaching University periodically with the given username.

6.3. E-mail of the employee is employee's property, which is given by the university for temporary use.

6.4. The use of e-mail is only allowed for the purpose of activities related to the university.

6.5. If the letter is written in Georgian language oonly UNICODE shall be used with (Sylfaen) shrift.

6.6. For the uninterrupted use of e-mail it is recommended to delete/archive long letters in every 6 months.

6.7. In every letter sent by the employee there should be a signiture according to the rules of the univerity.

6.8. Despite the existence of antivirus, all consumers are obliged to remove the e-mail from the suspicious, unknown sender's address

6.9. It is prohibited to:

6.9.1. Send the letters about the university's and employees' financial of other confidential information to third-partes.

6.9.2. Sending large files via e-mail as inside the university and abroad, which could potentially threaten both the Teaching University and the addressee servers.

6.9.3. Sending the letters which consists slander, agression, indecent or other prohibited information according to the legislation of Georgia.

6.9.4. Loving, sexual and/or discriminating content letters.

6.9.5. In case the user thinks that his/he r e-mail or private files are available for the third-party he/she should inform the IT Service to change all the passwords of the employee immediately.

6.9.6. After the employee leaves the job his/her information from the e-mail is copied/archived fot the reservation until before the expiration of limited period.

7. Using the Identification Information "Username" and Password

7.1. After getting the "username" and password employee is responsible for every implemented action under this username. It is employee's personal responsibility to obey the following rules of using identificational information:

7.1.1. It is prohibited to use other employee's identificational information;

7.1.2. It is prohibited to give your identificational information to other user. If this happens, the responsibility will be on the real owner.;

7.1.3. It is prohibited to see, modify, copy or delete files of other user whitout his/her written persmission;

7.2. Based on the Management request the IT Service has the right to:

7.2.1. Block the user if necessary.

7.2.2. Have an access to internal correspondence (e-mail, communicator, Intranet, etc.) and get the information;

7.2.3. Have an access to the technics on the balance of the university and get the information;

7.3. Terms of using the password:

7.3.1. An employee is obliged to change the password after receiving it. Password should contain 8 symbols including big and small letters, numbers and symbols.

7.3.2. The user is obliged to change the password every 2 months.

7.3.3. The user is obliged to keep the password secretly and not to write it on the places available for others.

7.3.4. The user is obliged not to give the password to the third-party (direct supervisor, other employee, etc.) who can use it in an abusive way.

7.3.5. During the break or temporary leave of the working place use the temporary blocking combination (+ L) of the computer.

8. Publicity of Completed Actions

8.1. The direct purpose of computer equipment and the Internet to employees is to use them for their official purposes.

8.2. The Teaching University Management reserves the right to monitor the results of any activity of the employee while using the computer equipment in the temporary use. Monitoring is subject to employee browsing websites, social networks, news services, downloaded and uploaded files and all other communications tools that can be used. Monitoring is aimed at optimizing the University's resources and strengthening internal security.

9. The Procedure for Keeping and Transmitting Information by the Employee

9.1. It is prohibited to retain the information provided by the law on personal and "state secrets".

9.2. Restriction also applies to information that may be granted in the future as a "classified secret".

9.3. The storage, processing, transmission and printing of secret information shall be carried out on the computer isolated from the internal and external network.

9.4. Working information and documentation should be maintained on the internal stationary computer. The user is also obliged to restrict critical information on the hosted website.

9.5. It is not permitted to store information and documentation on electronic transmitting devices (CD-DVD, USB FLASH, USB HDD, etc.) without interference with the Information Technology Service.

9.6. Transfer of working information and / or documentation to the internal network should be made only by corporate e-mail, shared folder or other internal services.

10. Obligation to Inform the Information Technologies Department on Personnel Issues

10.1. Human Resources Management Office is obliged to inform the Information Technologies Service about staff changes in the Teaching University to avoid violating the norms of safety, registrations and other policies of registered users.

10.2. Human Resources Management Office is obliged to give the Information Technologies Service information about: name and surname, position, job, internal phone number, mobile number and photo.

11. Technical Support Policy implemented by the Information Technology Service

11.1. An IT staff member is obliged to inform his / her direct supervisor in case of access to the Server Room of the Teaching University.

11.2. Employees of Information Technology Service are obliged to document any changes made to server and network equipment.

11.3. Teaching University staff requests technical support directly through the central technical support portal of the Teaching University.

11.4. The technical support request by the phone is provided only in critical situations.

11.5. The technical support request should be pre-prepared and approved.

11.6. Upon request of technical support the user is obliged to receive the information on the Self-Service Portal and pass the steps mentioned on it. In the absence of information, the user has the right to

request technical support.

11.7. In case of failure of computer hardware on the balance sheet of the University of Teaching, its owner is obliged to inform the Information Technologies Service.

11.8. If computer equipment needs to be replaced / renovated and transferred to IT services, the carrier is obliged to:

11.8.1. Migrate to unassisted local disk space and / or texts of the university files on the specially allocated host and / or cloud space allocated to him / her on the database.

11.8.2. Only official files should be migrated. In case of discovery of non-official files, the owner is obliged to transfer the files to the personal storage device. Otherwise, the Information Technology Service is authorized to destroy those files.

11.8.3. The user is obliged to sign the pre-prepared and approved document that relieves the Information Technology Service in case of loss of damage / loss of files and physical damage to the equipment.

12. Final Provisions

1. This document shall enter into force from the moment of the entry into force of the Order issued by the Teaching University.

2. Changes and amendments to this document are made by the Rector's Individual-Legal Act.