The document was approved by Order No. 67
of the Rector of the University on March 17, 2020
Amendments made by the order #165, dated July 11,
2020 and # 1302 , dated February 26, 2021 by the Rector of the University.

Information Technology Management Policy and Procedures of Ltd European University

Objectives of the

This document defines the information technology management policy and procedures of Ltd European University (hereinafter - "University"), which are aimed at the effective and safe use of computer and information resources in the management, educational and research processes of the University, also, at determining the rights, responsibilities and information security of the User of the University Information Technology (hereinafter - the User).

1.1 Goal of the Policy

The University Information Technology Management Policy sets out general approaches and rules for the use of computer and information resources in the University management, educational and research processes, and forms the basis for IT management procedures, including the safe use of systems.

1.2. Policy Distribution Area

The IT management policy is binding on all the persons involved in the management, educational and research processes of the University, who have legitimate access to the University's computer, network and information resources. Also, for all individuals who have appropriate invitation and use their own computer and other electronic means of communication to access the University resources.

1.3. General Principles

a) Information technology management policy is based on the active legislation of Georgia, standards and principles in the field of information and communication technologies.

b) All members and groups of the University community have the opportunity to access the information and communication systems of the University without any restrictions.

c) The use of information-communication systems or resources of the University is allowed only for the authorized user, for which he/she is obliged

to use own personal account, within the authority established by the rules and the agreement. Administration and use of personal accounts is monitored by the Information Technology Service.

d) The information and communication equipment owned or used by the University is transferred to a user for temporary use during the term of the employment and/or educational services agreement (hereinafter - the agreement). User is obliged to use the existing information-communication equipment and/or software of the University only for lawful purposes, which do not contradict the current legislation of Georgia and the internal legal acts of the University.

e) The University ensures protection of copyright, as well as intellectual property rights in general for software, databases and other works represented electronically (literary, musical or artistic works, photographs, films, videos, etc.), which are developed by its students, academic, invited and scientific staff, also, by other individuals and legal entities and placed in its information-communication systems. The institution also ensures appropriate procedures to prevent copyright infringement.

1.4. Information Security

a) University information and communication systems should be arranged in such a way as to ensure the protection, security and integrity of each user's personal data, so that other users can not browse electronic files and databases without the consent of the owner, as well as create a copy, modify or delete information.

b) Except for the information-communication system administrator (head of the information technology service), all users are prohibited from monitoring the information resource without the permission of the University Rector, as well as from changing the system parameters.

Similar approach is taken in terms of access to the management, teaching and scientific databases of the University, programs and applications.

c) The University shall, in accordance with due procedures, ensure that users do not transfer (without the consent of the University Management) to third parties the information protected in the University's information and communication resources, own and/or other user's account settings and information containing personal data, also, data that is the University property and is confidential, commercial secret and/or protected by copyright.

d) The University usually does not check the material transmitted by the users in the computer network and/or does not restrict in any way. In exceptional cases (for system troubleshooting, monitoring and elimination of viruses and other malicious programs, and in other cases prescribed by law), the University reserves the right to openly monitor the use of user information resources and work sessions that are notified to them.

e) The University reserves the right to restrict the infringing user's access to the University's information resources in case of violation of the rules for use of computer resources. In case of a particularly serious violation, a user's personal computer will be immediately disconnected from the information and communication systems of the University after sending the relevant message.

1.5. Data Protection

a) It is mandatory to ensure protection of computer systems and networks by the mechanisms of physical, technical, procedural and environmental safety control.

b) The University provides centralized storage, protection, archiving and creation/backup of administrative, educational, scientific information and data. The University is not responsible for the protection of files or data, which are stored in users' personal computers or outside the University system and/or

are not kept in accordance with the relevant rules. However, the institution provides information to users about the risks and supports them within its competence.

c) The University information-communication systems, as well as personal computers and communication systems must be protected from viral and other cyber-attacks.

d) The University ensures data security, storage of reserve copies and data recovery by carrying out appropriate procedures. Also, the University ensures data recovery and integrity in case of power outages, unauthorized access and other force majeure situations.

1.6. Information security incidents

a) The University shall ensure identification of information security incidents, which shall also include the study, description of each incident, prevention of risks, including incidents, and in case of their materialization - the adequate response.

b) In the event of incidents and outages of information and communication systems, appropriate procedures should be provided for the rapid transmission of information about the problem to the Information Technology Service and to persons whose rights are most likely to be violated. Also, its elimination and proper documentation/description should be ensured.

2. Information Technology Management Procedures

2.1. Create a User Account

a) For the use of the University's computer resources and e-mail, there are user accounts with ordinary and special rights.

b) The user with special rights (administrator) is determined by the head of the Information Technology Service, while all other members of the University community have a regular user account.

c) According to the list of new employees provided by the Human Resources Management Service, the Information Technology Service creates computer and e-mail accounts for each employee.

d) Right after registration, e-mail and learning process management system accounts are created for each new student.

e) Change in student status does not affect an e-mail account. Upon graduation of the University or termination/suspension of the status, limited rights to access to the University's computer resources are determined through his/her account.

2.2. Create and use a password

a) Password is an important component of information and network security. Username and password serve to verify user authentication.

b) The password has a text value. As soon as the account is created, each user receives a one-time password from the administrator and is obliged to change it during the first use.

c) In order to create a password, it must be considered that the password:

1. Should contain uppercase and lowercase letters of the Latin alphabet (e.g. a-z, A-Z);
2. Length (number of characters) must be at least 8 alphabetic-digital characters;
3. There should not be words of any natural language (name and surname of a person, names of pets, cities and others, computer terms, orders, names of establishments, etc.; dates of birth, addresses, telephone numbers, etc.; words like these: aaabbb, qwerty, zyxwvuts, password, 123321, secret1, 1secret, etc.);

d) For password protection a user should take into account that he/she:

1. Should not use the same password for the University accounts and other accounts (e.g., personal e-mail account);
2. Should not share the University account passwords with others, including administration representatives, assistants, staff or colleagues (e.g., even while on vacation), family members. All passwords are personal information;
3. Should not write or store passwords electronically;

4. Should not send the password by email or any other means of communication (e.g. telephone).

e) An employee of the Information Technology Service may request a user password to resolve any issues arising.

f) If the user suspects that his/her password has been revealed, he/she should immediately inform the Information Technology Service.

2.3. Right to access of user account and restriction

a) The right of the user is a set of rules for access to computer resources, which determines the actions to be taken on the data: read, write, execute, modify, administer.

b) User is given access only to the specific resources needed to perform his/her immediate job/academic duties. Rights are defined (changed and/or revoked) by the immediate supervisor. Users are prohibited from using resources other than shared resources without authorization.

c) If a user changes position at the University and/or amendments is made to his/her job description, it is obligatory to review the user's access rights.

d) User is not allowed to share his personal accounts and passwords with others. User is responsible for the actions performed with his/her account. Users are responsible for any unauthorized actions carried out through the computer under the auspices of the University.

2.4. Electronic mail of the university

a) Email is one of the most important means of internal and external communication for users. E-mail, which operates under the domain @eu.edu.ge or @esu.edu.ge, is the property of the University and may be used for business purposes only. Avoiding, not accepting or deleting the contents of the letter does not release the email account holder from responsibility.

b) According to the Law of Georgia on Personal Data Protection, correspondence from the individual e-mail accounts of the University staff and students is their personal information and is not subject to substantive monitoring, except as provided by law.

c) In case of any questions regarding the operation of the e-mail system, users should contact their immediate supervisor and/or the University Information Technology Service.

d) The following type of e-mail account is used at the University:

1. Individual report of the University staff and students. Account is formed by a combination of name and surname. In case the mentioned combination is busy, a serial number is added (according to the order of registration). For students, the account is created using the 4-digit ID of the database, in case of coincidence, the letters "GE" are added;

2. Research, scientific, cultural, social projects and other special postal reports of separate structural units (faculty, department, etc.) are formed in agreement with the relevant services and on the basis of their application.

The e-mail account is suspended in the following cases:

1. Termination and/or suspension of the contract with the University;
2. Liquidation/reorganization of a separate structural unit;
3. Inappropriate use of the University e-mail;
4. While disseminating information prohibited by this policy and the legislation of Georgia;
5. When a third party access is detected.

e) In case of temporary suspension of the University e-mail account, the Information Technology Service is obliged to inform about this fact to both the account holder and his/her immediate supervisor. The restriction is lifted after the elimination of its causes and is notified to both the account holder and his/her immediate supervisor.

2.5. Privacy Protection

a) The computer network of the University belongs to the University and is used for academic, research and administrative activities.

b) The University uses various measures of protection for the security of its own computer resources and its user accounts.

c) The University may monitor the activities and reports of individual users of the University network or computer resources, including the content of individual sessions and communications without prior notice when:

1. The user voluntarily makes available to everyone the information he/she posts through internet resources, websites or blogs;
2. It appears that the user account is unusually active, which is not required with permissions.

d) Any such monitoring of communications, except as required by the user or by law or the need to respond to an emergency, must be authorized in advance by the University Rector. After each such action, the measures taken will be informed and explained to the user.

2.6. Copyright Rights:

a) The University shares the requirements of Georgian law on copyright and related rights. Software and databases in the University computer network are owned or licensed by the University or a third party and are protected by copyright.

b) User is prohibited to:

1. Create a copy of programs for use in the University Network or distribution outside the University;
2. Do unauthorized download of copyrighted works and use them on the University computer network and/or through other information resources;
3. Sell the University data and/or programs;
4. Use the software for non-educational purposes and/or financial gain;

5. Publicly disclose the programs (e.g. program code) or data without the permission of their authors/owners.

c) When connecting to the University network, all users are obliged to protect the copyright of the works, which are usually placed on the supplier's website. If the user does not agree to the specific copyright, it does not mean that the copyright does not apply to this work.

2.7. Data Protection

a) All data and information systems of the University must be protected in accordance with the current legislation of Georgia.

b) Access to information resources of the University is determined by the rights of the user.

c) The user must comply with those restrictions imposed not only by the University, but also by other users and third parties, which do not contradict the information technology management policy of the University.

2.8. Protection against viruses and malware

a) Viruses and malware designed to harm, steal, modify, and otherwise damage the electronic information, endanger the University information security.

b) On all computers and laptops of the University, which are connected to the computer network of the institution, shall be installed software (with appropriate settings) with protection against viruses and malware recommended by the Information Technology Service.

c) It is not allowed to deactivate the software for protection against viruses and malware independently. Its settings should be neither changed, nor should the frequency of automatic updating of the database be reduced, so as not to decrease the effectiveness of protection.

d) Information about all viruses that are automatically detected and destroyed should be reported to the Information Technology Service as an information threat.

2.9Disposal of electronic data

a) The purpose of the University Information Technology Management Policy is to protect confidential data and ensure compliance with software licensing agreements, thus, it is important to manage the University's electronic data when moving computer resources.

b) All computers and digital storage devices owned by the University must be processed accordingly before their ownership form is changed (such as, but not limited to: sell, give away, write off, etc.). When processing computers and digital storage devices, all University-related data on the devices and licensed software must be deleted or the device itself must be physically destroyed.

c) All computers and digital storage devices that need to have changed their ownership form, must be provided to the Information Technology Service for processing;

d) If the hard drive is damaged or can no longer be used due to inactivity, it needs to be disassembled and physically destroyed.

e) All computers and storage devices ready for write-off are stored in a safe place;

f) If a third party uses the University's computer equipment, they must comply with the University's electronic data management policy.

2.10. Management of computer network

a) The University reserves the right to inspect and review all aspects of its computer systems and networks, including individual session and report files. The purpose of this inspection is to detect computer network problems, viruses and other malicious software, to determine whether the user is violating the University IT Management Policy or applicable law.

b) All computer and communication devices connected to the University network are subject to this policy, regardless of whether this device is the University property.

c) Monitoring of the University network, internet connection or computer resources of the University can be carried out only by the employees of the Information Technology Service.

d) Authorized staff of the University Network and Internet Inspection shall not disclose confidential and personal information obtained during the network monitoring process without the permission of the University Administration.

2.11. Internet and wireless connection

A) All buildings of the institution are covered by wireless network. Optical internet is introduced in the buildings. It is available to all students, academic and administrative staff.

B) In order to ensure business continuity, the University has a backup Internet backup works in parallel with the main Internet and in case of damage or disconnection of the main Internet, the University will continue to use the Internet without interruption.

C) The University's wireless networks are managed, monitored and operated by the Information Technology Service.

D) Users' access to the wireless network can be free or limited. The restriction is allowed only for protection due to the specifics of the structural unit activity.

E) Regardless the wireless network has restricted or free access, it should be accessed using WPA2/ PSK technology and AES encryption with the appropriate password in order to protect the information transmitted in the network from unauthorized access;

F) Wireless network passwords are set by the Information Technology Service.

G) The password of the wireless network can be accessed by anyone, written on an information board or placed in any visible place.

H) The password of the wireless network with limited access will be revealed only to those users who need access to the mentioned network due to their business activities and they are obliged not to pass the password to anyone else without the consent of the IT service.