EAST EUROPEAN UNIVERSITY

EEU

Information technology and software platforms and systems management policy

Approved by: the order №08/01-08 -February 7, 2019 of the Rector of the University

Updated: Representative Board Resolution №05 – August 25, 2020

1. Objectives of the document

The purpose of the Information Technology and Software Platforms and Systems Management Policy Document is to define policies and procedures related to the management of information technology and information security, in the activities of the Eastern European University (hereinafter - the University) and nformation technology infrastructure and development mechanisms, consumer rights and responsibilities.

2. Scope of the document

The Information Technology and Software Platforms and Systems Management Policy (hereinafter referred to as the "Policy") is mandatory for use by all persons who have a legitimate right to use the University Information Technology and resources in their administrative, academic or teaching / learning activities. Also for all duly invited persons who are entitled to access the University's computer resources.

3. Regulatory documents

The information technology and software platforms and systems management policy is based on the legislation in force in Georgia, the standards in the field of information and communication technologies, the relevant legislation on intellectual property and personal data protection, and the internal regulations of the University.

Information technology and software platforms and systems management policy

1. General requirements for policy application

Eastern European University makes extensive use of information and communication technologies, software platforms and systems in the educational and governance processes to carry out its declared mission, ensuring the efficient and secure operation using modern and high-tech infrastructure. between them:

- □ Uninterrupted and secure access to the Internet and to the University's internal resources (software platforms and systems, corporate mail) must be provided to any student and staff of the University, using both wired and wireless technologies;
- □ For data protection and effective management, protected data and application servers should be used, which can be located both in a specially arranged space on the territory of the University, as well as based on the contract with a contractor company, using protected cloud technologies;
- □ Development of software platforms and systems is a priority of the University, they should be used as much as possible in the educational and governance processes of the University, which require flexible data management, security, and limited access to personal information, the use of software platforms and systems is mandatory in the management of teaching processes, personnel, and finances.
- □ In the information-communication system, any software or hardware resources should be accessed using reliable password system, and using reliable information security standards, methods, and protocols.

2. IT Management Policy Objectives

The goal of IT management policy is to promote the protection of key information characteristics (confidentiality, accessibility, integrity) at the University, which in turn ensures the effectiveness of information risk management and business continuity.

It sets out general approaches and rules for the use of computer and information resources in university governance, education and research processes, on the basis of which information technology management procedures will be formed.

The areas of information security policy protection at the University are:

- □ University Information Technology Infrastructure;
- □ Basic data and information available at the university;
- □ Persons who use and / or administer information systems;

As a result of the policy implementation, it should ensure that:

1.1. **Physical security** - Information assets should be controlled to prevent unauthorized access to, interference, theft or damage to information assets. It is mandatory to ensure the protection of computer systems and networks through physical, technical, procedural and environmental safety control mechanisms. The University does physical access control over devices that contain or process highly critical and / or sensitive information. Such devices are placed in a physically protected place.

1.2. **Management of information security incidents** - Identification of security incidents should be ensured, it also involves studying each incident, identifying their sources (internal, external) and forms (DDoS, Keylog, etc.) and responding adequately, as well as making recommendations as needed.

1.3. **Management of communications and operations** - Information processing equipment must be constantly monitored to ensure its correct and safe use. Network monitoring is performed 24 hours a day. The step-by-step structure of the ongoing processes is as follows:

- □ Damage notification;
- □ The operator identifies and eliminates damage from the control panel;
- □ If necessary, the operator goes to the place of damage
- □ If the damage could not be repaired, notify the administrator
- □ The administrator conducts network diagnostics
- □ The operator notifies the customer of the estimated dates of damage and repair;

1.4. **Control over malicious programs** - The system should be constantly monitored and the security system constantly updated, To prevent the use of malicious or fraudulent programs in critical systems as well as the spread of viruses inside and outside the university;

1.5. **Systems, applications and data backup** - Systematic maintenance and backup of all critical systems, applications and data should be carried out systematically;

1.6. **Computer network management** - Both wired and wireless network systems must be constantly monitored at both the physical and network levels, in order to timely detect and eliminate the fact of intrusion of a unknown, unauthorized user into the system.

1.7. **Planning-development of a new system** - In the process of planning and implementation of systems, the technical and functional capabilities of the existing systems should be taken into account, so as not to hinder the smooth operation of critical systems, for which systems are tested in an isolated environment to protect critical systems with vital impotence from accidental destruction and / or damage.

3. Right and restriction of user account access

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

The customer is only allowed access to the specific resources needed to perform his / her immediate job / academic duties. Rights are defined (changed and / or canceled) by the head of his department (service). Users are prohibited from using any computer resource other than shared resources without authorization.

If the user changes position and / or responsibilities at the university, the user's access rights must be reviewed. The user must use only those objects, accounts, access codes, privileges and / or information of the computer resources for which he / she is authorized according to the responsibility of his / her new position.

4. Consumer rights and responsibilities

All members and groups of the university community have the opportunity to always have access to the University information and communication systems without restrictions.

The use of information-communication systems or resources of the University is allowed only for the authorized user, for which he is obliged to use his personal account, in accordance with the established rules and within the powers defined by the contract. The personal accounts are administered and monitored by the Information Technology Management Department.

The information-communication equipment owned or supervised by the University will be transferred to the customer for temporary use during the term of the employment or study contract (hereinafter referred to as the contract). The 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 legislation of Georgia and the charter of the University. It is also not allowed to be used to slander or insult any person.

The University provides to protect the copyright and intellectual property rights of the works (literary, musical or artistic works, photographs, films, videos, etc.) submitted by its students, academic and scientific staff as well as other individuals and legal entities in electronic format in its information-communication systems and provides appropriate procedures to prevent copyright infringement.

5. Information security

University information-communication systems should be arranged in such a way as to ensure the protection and integrity of entrepreneurial, work, personal, private information and data, for which any customer[1]

□ Without the consent of the owner Can not: Browse, back up, modify or delete electronic files and database information

[1] except to the information-communication system administrator, in accordance with the current legislation

- □ Change system settings
- □ Gain access to university management, teaching and research databases, programs and applications without proper permission.
- □ Do not transfer information protected on the University Information and Communication Resources to third parties without proper permission; own or other user account settings and information containing personal data, as well as data that is the property of the University and is confidential, commercial secret and / or protected by copyright.

The University does not normally review or in any way restrict the material transmitted by users on the computer network. However, 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 about which he is informed.

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

6. Data protection

Data is classified according to information security according to the risks, its confidentiality, value and the level of impact on the activities of the university. All university data should be classified according to the following three types:

- □ **Limited** - Unauthorized disclosure of data is associated with high reputational and organizational risks, and altering or destroying them may result in long-term disruption of the University sctivities or disclosure of personal information. Limited data is protected by state law and confidentiality agreements between entities (E.g. staff personal information, student academic data, university financial information, etc.). The highest level of security should be used for limited data.
- □ **Private** - Unauthorized disclosure of data is associated with moderate risks and their modification or destruction may or may not result in temporary disruption to the University. Private information includes regulatory and management information in the university's internal document management system. Normally, all university data that is not explicitly classified as limited or public data should belong tolimited data and should be protected according to the average level of security.
- □ **Public** - Unauthorized disclosure, alteration or destruction of data is associated with high risks. Examples of public data are: announcements, messages, course syllabus, press releases, newsletter, newspapers, magazines, websites, scientific papers and more. Low levels of security are required to protect public data.

Access to university information resources is determined by user rights. Users must comply with restrictions imposed not only by the University but also by other users and third parties that do not conflict with the University IT Management Policy.

It is mandatory to ensure the security of computer systems and networks through physical, technical, procedural and environmental control mechanisms, for which it centralizes the storage of information and data, archives and backups, and restores data integrity in case of force majeure.

University information and communication systems, both personal computers and communication systems, must be protected from viral and other cyber-attacks.

The University is not responsible for the protection of users 'files or data stored on users' personal computers or outside any other university system and / or protection files or data stored without proper rules however, it provides information to users about the risks and provides support within its competence.

7. Copyright

The University shares the requirements of Georgian law on copyright and related rights[2].

The software and databases on the University computer network are owned or licensed by the University or a third party and are protected by copyright, licensing and contract rules, and other laws. The user is obliged to respect and comply with the terms of the software use and distribution licenses, which include the following prohibitions:

1. Creating a copy of programs for use in the University network or distributing it outside the University;
2. Unauthorized download of copyrighted works and use of them in the university computer network and / or through other information resources;
3. Sale of data and / or programs;
4. Use of software for non-educational purposes and / or financial benefit;
5. Disclosure of programs (eg program code) or data without the permission of their authors / owners.

When connecting to the University Network, all users are required to follow the copyright of their work, which are usually posted on the supplier's website in the form of a contract agreement. If the user does not agree to the specific copyright, it does not mean that the copyright does not apply to this work.

[2] Articles 6,19 – https://matsne.gov.ge/index.php?option=com_ldmssearch&view=docView&id=16198#

Information and communication technology management procedures

2. Create and delete a user account

There are accounts with ordinary and special rights for users (see "Access and Restriction of User Account Access") for the use of the University's computer resources and e-mail.

The customer with special rights (administrator) is determined by the head of the IT department, while university students, academic and visiting staff, as well as support staff have a regular user account

2.1. Create a user account

According to the list of new employees provided by the Human Resources Management Service, the Information Technology Management Department creates a computer and e-mail account for each employee. A account of teaching programs is created for the teaching-scientific academic staff of the faculty upon the recommendation of the head of the faculty.

When registering a new student, a personal e-mail account is created, which is used for both communication and access to university e-resources.

2.2. Cancel accounts

According to the list of employees leaving the university submitted by the Human Resources Service, the Information Technology Support Service cancels the relevant accounts of these employees.

A change in student status does not affect their email account. Upon graduation or termination of the status of the University, the limited rights of access to the University's computer resources are determined by its account.

3. Create a password

A password is an important component of information and network security, and the username and password together serve to verify the authenticity of the user, as well as the protection and management of his personal and university corporate information;

The password is a text value and the following parameters must be considered for creation:

1. Must contain uppercase and lowercase letters of the Latin alphabet (Eg.: a-z, A-Z);
2. Must contain numbers, arithmetic operations and / or other symbols (Eg.: 0-9, @#$%^&*()_+|~-=\`{}[]:";'<>?,./);
3. Length (number of characters) must be at least 8 alphabetic-digital characters;
4. No words should be used: Surname, first name, cities names, computer terms, dates of birth, telephone number, names of institutions, etc .;

5. Use and manage the password

Each user receives a one-time password from the administrator as soon as the account is created and is obliged to change it during the first use.

Each user should consider the following issues when using the password:

□ Immediately change the temporary password received from the system administrator;

□ Do not use the same password for university accounts and other accounts (E.g., personal email account);

□ Do not share university account passwords with others, including administration representatives, staff, or colleagues (E.g., even while on vacation), family members;

□ Do not keep a password on paper or in electronic form;

□ Do not send the password by e-mail or any other means of communication (eg mobile);

□ Do not use the "Remember me" option in browsers;

□ Do not leave password-protected resources (email, e-dean, etc.) open while you are not at work.

In case of suspicion of forgetting the password, as well as disclosure, or attempting to gain unauthorized access by other persons, immediately contact an IT Management Officer who will provide a temporary password.

In some cases, an employee of the Information Technology Management Department may request a user password if requested assistance, however once the problem is eliminated the password is subject to change.

4. University Email

The e-mail, which operates under the domain @ eeu.edu.ge, is the property of the University and can be used only for business purposes and is a means of internal and external communication for students and staff.

According to the Law of Georgia on Personal Data Protection [3] ,correspondence from the individual e-mail accounts of university staff and students is their personal information and is not subject to substantive monitoring.

If users have any questions regarding the operation of the e-mail system, users should contact their immediate supervisor and / or the University IT Management Department.

When using e-mail, it is not allowed:

□ Spreading obscenity, insults and slander, fraud, intimidation, falsification, creating illegal pyramid schemes or spreading malicious computer programs, etc .;

□ View, copy, modify or delete email accounts or files without the permission of the account holder or any other person;

□ Open attachments to messages sent from suspicious addresses, which are direct sources of viruses and malware;

□ Sharing your e-mail account passwords with other people or trying to find another person's account password;

□ Distribution of letters as part of commercial activities, political campaign distribution and e-mail use.

4.1. Email Address

[3] "Law of Georgia on Personal Data Protection – https://matsne.gov.ge/ka/document/view/1561437

The following types of e-mail accounts are used at the University:

- □ Individual account of university staff and students. The account is formed by a combination of first and last name, in case the mentioned combination is occupied, a serial number is added (According to the order of registration); and for students, the account is formed by the 4-digit ID of the base, in case of coincidence, the letter G or E is added.
- □ A separate structural unit (faculty, department, etc.), research, scientific, cultural and social projects and other special postal accounts are formed in agreement with the relevant services and on the basis of their application;

4.2. Suspend or cancel an email account

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

1. Violation of the above policy by university students and staff;
2. Dismissal of an employee from his / her university;
3. Termination of status for a student or transfer to another university;
4. Liquidation / reorganization of a separate structural unit;
5. Internal investigation to establish the fact of improper use of the University e-mail;
6. Dissemination of information prohibited by this policy and the legislation of Georgia;
7. Detection of the fact of access to the account by a third party;
8. In case of technical problems in the information system and network infrastructure;

In case of technical problems, the Information Technology Management Department is obliged to inform both the account holder and his / her direct supervisor about the temporary suspension of the University e-mail account. The restriction is lifted after the elimination of its causes and the account holder and his / her direct supervisor is notified about it.

Short-term access to the user's e-mail is possible, with his / her consent, in special cases:

- □ Ensure the continuity of university activities (eg, the need to obtain information when the user is unavailable);
- □ Diagnose and eliminate technical problems related to the system;

It is not allowed to delete the mail account completely.

The e-mail account of the employee with whom the contract with the University terminated should be suspended; and the former employee handing over his / her e-mail password to the IT Management Department, in order to access his/her account if necessary.

University Computer Network Management

The University Computer Network consists of management and data transmission infrastructure in wired and wireless networks, as well as databases and application management servers, the smooth operation and administration of which is provided by the Information Technology Management Department.

Technical or software upgrades to the network infrastructure and any other scheduled service work that will cause the computer network to malfunction must be performed during non-business hours and notified to all users 24 hours in advance.

4.3. IP address management

Internet addresses (IP) of computer devices are distributed through a networked server (using the DHCP protocol), which is managed, supported and documented by the University IT Management Department.

Each device connected to the University network may be assigned a dynamic or static IP address, including:

- □ As an exception, static IP addresses can be assigned for the proper functioning and security of the network infrastructure.
- □ Dynamic IP addresses are assigned to all computers and mobile devices connected to the university network.

4.4. Network router management and security

The IT department is responsible for the proper installation and maintenance of all routers involved in the University network, as well as for their safety, management, monitoring and periodic auditing.

The network router must meet widely used security standards.

The following should be ensured when the router is operating:

- □ The access password must be stored in encrypted form;
- □ A standardized SNMP protocol should be used for management and monitoring;
- □ An encrypted (ssh) channel should be used for remote router configuration;

The operation and safety of the network router should be monitored 24/365, and periodic safety and performance audits should be carried out at least once a year, whose reports are submitted to the Rector.

4.5. Wireless management

The University's wireless networks are managed, monitored and operated by the Information Technology Management Department.

Wireless network access may be free or restricted.

- □ The password of the free access wireless network can be passed on to anyone, written on the information board or placed in any visible place.
- □ Restricted wireless network password is communicated only to those who need access to the network due to business activities.

Although the wireless network is restricted, free access must be accessed using WPA2 / PSK technology and AES encryption using the appropriate password to protect the information transmitted through the network from unauthorized access.

4.6. Computer network monitoring

All computer and communication facilities connected to the University network are subject to this policy, regardless of whether or not this device is the property of the University.

If there are any violations facts of this policy, unauthorized access to university information technology and computer infrastructure or/and suspicion of abuse, in order to detect computer network technical problems, the presence of viruses and other malicious programs, the University reserves the right to: examine and check all elements of its computer systems and networks, including individual account files and information, without substantive monitoring.

Monitoring of the University Network, Internet Connection or University Computer Resources can only be done by the Information Technology Management Department. Attempts to monitor the network by all other users are not allowed.

Authorized staff of the University Network and Internet Inspection shall not disclose or transfer information obtained during the network monitoring process to third parties without the permission of the University Administration.