საქართველოს ეროვნული უნივერსიტეტი სეუ
GEORGIAN NATIONAL UNIVERSITY SEU

GEORGIAN NATIONAL UNIVERSITY SEU

Strategic Development Planning methodology

2020
TBILISI

Article 1. General Provisions

1. This document defines the information technology management policy of Georgian National University SEU (hereinafter referred to as the University), information technology management procedures, information technology infrastructure and development mechanisms, university administrative activities and educational process, administrative and operational rules of electronic learning management systems of reg.seu.edu.ge and emis.seu.edu.ge.

2. Adherence to these rules shall be mandatory for all persons who use the information technologies and resources of the University in their administrative, academic, or student activities.

3. The user of the University information technology (hereinafter referred to as the user) shall be obliged, in addition to this rule, to comply with the requirements established by the legislation of Georgia regarding the protection of intellectual property, information technology security, and personal information.

Chapter I. Information Technology Management Policy

Article 2. Objectives of Information Technology Management Policy

1. Information security policy shall ensure the establishment of information security control mechanisms at the University.

2. Areas of information security policy protection shall be:

A) IT infrastructure of the University;

B) Basic data and information available at the University;

C) Persons using or administering information systems;

D) Persons who manage key data and information.

3. Policy shall determine:

A) The protection of the University in terms of confidentiality, integrity, and accessibility of information;

B) Responsibilities for information security.

Article 3. Physical Security

1. The University shall exercise control over information assets to prevent unauthorized access, interference, theft, or damage.

2. It shall be mandatory to ensure the protection of computer systems and networks through physical, technical, procedural, and environmental safety control mechanisms.

3. The University shall exercise physical access control over devices that contain or process highly critical and/or sensitive information. Such devices shall be placed in a physically protected place.

Article 4. Information Security Incidents

1. The University shall be obliged to identify security incidents, including the study, description, and adequate response to each incident.

2. Those responsible for the operation of the University Information Technology System shall periodically report on information security incidents, their sources (internal, external), their forms (DDoS, Keylog, etc.), along with correction and optimization recommendations.

Article 5. Communications and Operations Management

The University shall carry out constant control over information processing devices to ensure their correct and safe use.

Article 6. Development and Planning of a New System

In the process of planning and implementation of systems, the technical and functional capabilities of the systems should be taken into account, so as not to hinder the proper operation of critical systems.

Article 7. Control Over Malicious Programs

Control of critical systems is essential to prevent the use of malicious or fraudulent software.

Article 8. Protection Against Viruses

1. The University shall carry out appropriate control to prevent the spread of viruses both inside and outside of the University.;

2. Backup of all critical systems, applications, and basic data shall be done synchronously on the university google drive.

Article 9. Computer Network Management

1. Mac addresses of computers and devices connected to both the physical and wireless network at the University, which belong to the University assets, are pre-written in the router, which assigns a pre-selected IP address.

2. Devices that do not belong to the University's assets and use the University Wireless Network (Wi-Fi) shall use a dedicated network that allows them to access only the pre-selected category of websites.

Article 10. Security Systems in Design for Testing

Systems shall be tested in an isolated environment to protect critical systems from accidental destruction and/or damage.

Article 11. Business Continuity Management

1. The business continuity strategy developed and its functioning should ensure the reduction of the risk of sudden interruption in the process of information processing of the University and its timely recovery.

2. In case of failure of the main router, the backup router shall be switched on within 10 minutes after the result.

3. In case of failure of external servers, their backups shall be activated within 5 minutes, so as not to disrupt electronic services.

Chapter II - Electronic Management System of University Educational Process

Article 12. Description of the Educational Process Management System

1. University e-services system reg.seu.edu.ge shall provide support, communication, information processing, and protection of the existing educational and administrative activities of the University.

2. General functions of the system:

A) Automation of educational process management in the university

B) Financial module automation

C) Electronic case management

D) Library

C) Human resource management

3. The system uses md5 s type encryption with encrypted users' (staff, student) passwords.

4. System users shall be:

A) Administrative, academic, and invited staff

B) Student

Article 12. System Security

1. The system code is written on a specially allocated local server (https://bitbucket.org/) where a new module added to the system shall be tested and then the verified code is uploaded to the main server.

2. Actions logs shall be stored on the server with the following data: author of the action, time of action, action performed, IP address.

3. In case of failure of the main server, the backup server shall be automatically activated to ensure business continuity, replicating with the main server.

4. System data shall be automatically saved to the university google drive once a day.

5. Reservations of external servers serving the electronic services management system shall

be made twice a day.

Article 13. Development Mechanisms

1. The network infrastructure of the university shall be arranged according to modern standards. The University shall be constantly taking care to bring its infrastructure in line with new standards in the event of a change in standards.

2. The code of the existing educational process management system shall be written according to the existing standards; with the change of standards, the software approach and the ways of its solution change shall alternate as well.

3. The University shall provide information resources development, improvement, process optimization and monitoring through the IR unit resources and outsourcing the relevant services.