UNIVERSITETI "UKSHIN HOTI" PRIZREN
Rruga e Shkronjave Nr. 1, 20000
Prizren, Republika e Kosovës;
Tel:+383(0) 29 - 232 140;
Homepage: www.uni-prizren.com

REGULATION

FOR SERVICES OF INFORMATION TECHNOLOGY (IT)

Prizren, Maj 2022

Based on the article 23 paragraph 1.2 and 1.3 of the statute of the University "Ukshin Hoti" Prizren and in accordance with the Law of Higher Education of the Republic of Kosovo, the Governing Council of the University in the meeting held on the date of 23.05.2022, approves:

Regulation for services of information technology (IT)

Article 1
Purpose and purview

1. The purpose of this Regulation is to define the criteria and the terms that must be met by the University for the organization and operation of their systems of information technology (hereafter IT), which enable the reduction of the operational risk that may be caused by the misuse of the IT systems, also to maintain confidence on those systems on the support of the University's activities.
2. This Regulation is applied at the University.

Article 2
Definitions

1. All the terms at this regulation have the same meaning with the terms defined at article _ of Law No._____ of the University, or/and the following definitions for the purpose of this regulation:

   1.1. **University** – University "Ukshin Hoti" Prizren

   1.2. **Client** – University management, members of Governing Council, permanent and temporary academic personnel, administrative personnel, and students.

   1.3. **Information system** – means a complete technological group that consist of infrastructure (software and hardware components), organizations, people and the procedures for collecting, storing, processing, transmitting, displaying and using the data and information;

   1.4. **Software components** – means all types of operative system, software apps, tools for software development and other software systems;

   1.5. **Hardware components** – means computer equipment's, equipment for computer networks, devices for data storage and the rest of technical equipment that serve as a support to operate the information system;

   1.6. **Users of the information system** – means all people who are authorized to use the information systems (students, full time employees, part time employees, visiting personnel, guest users, students from exchanging programs);

   1.7. **External service provider** – means a natural or legal person, who according to a written agreement provides external services to the University;

   1.8. **Assets** – means information (such as database, contracts and agreements, system documentation, research information, users manuals, training materials, operating or support procedures, plans to continuous teaching activity, audit trails, and archived information); Software assets (software apps, software systems, tools for software development, etc.); Hardware assets (computer equipment, communications equipment, removable media, and other equipment);

Services (computer and communications services, general services); Personnel (along with the qualifications, skills and the experience); Sacred (as University reputation).

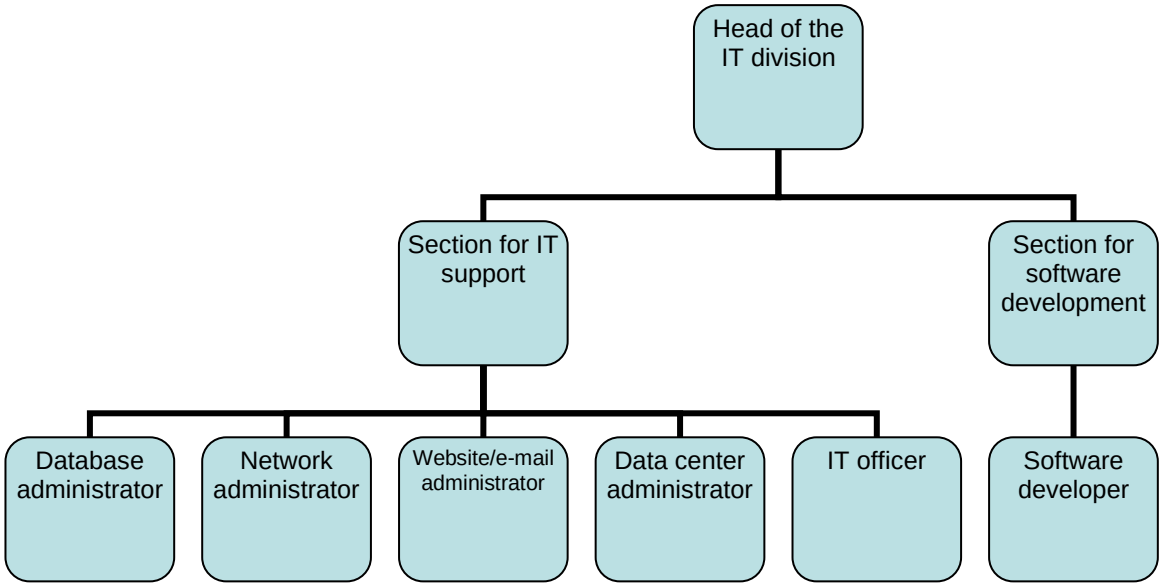
1.9. **Clear desk** – means removing all confidential documents and assets from the working desk during the not supervised period and at the end of the work shift.

Article 3
Information technology management

1. Information technology management must include the following requests:
   1.1. Should have the functionality, capacity and performance to provide the support that is required by teaching activities;
   1.2. Provides appropriate data validation control, during processing, and during data extraction, to prevent inaccuracies and inconsistencies on data and information;
   1.3. Provides information on real time, accurate and complete, for making decisions of the teaching activities and the risk management, to provide security and steady functioning of the University;
2. University will monitor, adjust and improve constantly the process of IT managing, to reduce the exposure to danger and maintaining its security and functionality.

Article 4
Organizational structure of IT management

1. University must establish an organizational structure of IT unit (IT division) with a sufficient personnel number and adequate, to make sure that IT division is efficiently managed. Sharing tasks must be based on ISO IEC 20000-1 standard with responsibilities and competencies clearly defined for the process of IT management. This unit must document regular informative reports at least on three-month basis for the senior management of the University.
2. This division has this structure:



1. Head of the division

   i. Database administrator,

   ii. Network administrator,

   iii. Website/e-mail administrator,

   iv. Data center administrator,

   v. Software developer,

   vi. IT officer

IT division is responsible for these services:

2.1. Provides access on the official electronic mail (e-mail) for the clients. This service is provided based on the administrative instruction no. 04/2010 for the use of the official electronic mail in the institutions of the Republic of Kosovo (appendix no.1)

2.2. Provides supporting services (helpdesk) for the clients related to the use of software and hardware and is based on administrative instruction no. 03/2010 for the use of software and hardware (appendix no.3)

2.3. Provides maintenance services for the official website. This service is based on the administrative instruction No. 01/2011 for the use of the internet on the institutions of the Republic of Kosovo (appendix no.4)

3. In cases of delegation of IT functions to the external provider (contractor), University must appoint at least one internal employee specialized on the field of information technology, as responsible for coordination and the smooth running of the IT functions.

4. University must assign a person responsible for information security, who will manage the security of the information system and to coordinate policies and processes for the

security of the information related to technological functions and platforms.

Article 5
Policies and Procedures of IT management

1. IT division is responsible for approving policies for technology and information security and annually must assess policy adequacy and perform their review.
2. The University defines goals, strategies and the security requests, for the activity of IT systems, defines polices for technology and information security, also procedures for the field processes. These procedures must be approved by Governing Council of the University.
3. University in accordance with the strategy of teaching activities approves strategies to develop the IT system.
4. In case that University secures all or one part of its activities (or systems), from IT external providers, then University approves an internal procedure to delegate functions to ensure compliance with the requests of this regulation for security and the proper functioning of these systems.
5. The internal procedure to delegate functions according to paragraph 4 of this article must include at least, the following elements:
   5.1. Identifying functions that will be delegated and the assessment of the impact that delegation of those functions will have;
   5.2. Procedures for functions delegation, including criteria for selecting the recipient of the delegated functions;
   5.3. Deadlines and reporting methods of the recipient of the delegated functions, to the University;
   5.4. Ways of monitoring the recipient of the delegated functions, by the University;
6. Policies and procedures for IT management must at least define the following elements:
   6.1. Administration and operation of IT systems;
   6.2. Organizational structure for IT management;
   6.3. Hardware infrastructure of IT field (configuration diagrams);
   6.4. Classification of documentation and the protection of systems and data;
   6.5. Data system backup;
   6.6. Managing systems change;
   6.7. Managing incidents;
   6.8. Risk management of IT systems;
   6.9. Defining security mechanism of IT systems;
   6.10. Managing third parties.

Article 6

IT systems development and procurement

1. To decrease the risk, University must follow the trend of software development by making sure to use only the updated and supported versions from their providers.
2. University approves internal procedures for the way how it executes the developments, changes and testing on its IT systems. IT systems are put on *live* operation, only after the specialized employee that verifies the application of procedures and the system proper functioning gives his documented approval.
3. The external provider during the implementation and work on the systems shall not in any way have access on the systems versions that are *live* except *read only* access with a special approval and monitoring by the University. Contractors and other external parties have to test all the changes in a testing environment.

Article 7
Delegating IT function to external service providers

1. University is responsible to assure that IT activity is done in accordance with all the requests defined by this regulation even in cases when all or part of IT activities, is provided from external IT service providers.
2. Before selecting the external IT service provider, the University must undertake the following activities:
   2.1. Carrying out risk assessment of University operations that can come from using an external service, offered during the processing of University activities;
   2.2. Defining the minimal standard that the external IT service provider must fulfill and which must be harmonized with the plan of continuous teaching activities;
   2.3. Defining the necessary measures to avoid conflict of interest;
   2.4. Defining the way of monitoring the service and the operation quality of the company, financial situation and risk profile through periodical testing, of compliance with the security policy of the information system;
   2.5. To make the right assessment of the external IT service provider activities on legal and financial perspective also on the way it manages the security of information system defined on this regulation;
   2.6. Defining the coordinated management of security incidents.
3. The agreement between the University and the external IT service provider must be define by a written contract which among others must include:
   3.1. Information of the parties that made the agreement (University and the external IT service provider);
   3.2. The rights and obligations of the arrangement parties;
   3.3. Description of delegated functions;
   3.4. Time line of providing services;
   3.5. Agreement on the quality of service;

3.6. Hiring IT service provider to do their activity in accordance with legislation in force, requirements, regulators, as well as the approved policies of the University;

3.7. The notice period for the contract termination, which is adequate to find alternative solutions;

3.8. Handling and maintaining data confidentiality;

3.9. Provision that defines that the external IT service provider, will be subject to supervision by the University regarding to delegated IT activities;

3.10. Obligating the external IT service provider, to inform University immediately for any fact that might have an important impact in its ability to do his activities efficiently and effectively according to the law in force requirements;

3.11. The right of the University to be informed regarding the progress of the delegated functions by the external IT service provider, as well as the right of the University to give general or special instruction in regard with performing the delegated functions;

3.12. The right of the University, to inspect and control the activities of the external IT service provider regarding the delegated IT activities.

4. The external service provider may not subcontract services unless is defined on the main agreement signed between the University and this service provider.

5. University is obligated to manage risks that arise as a result of contracting relations with the external service providers, whose activities deal with information system that is in use by the University. University is obligated to constantly monitor the method and quality of activities contracted from the external provider.

Article 8
Risk management for information systems

1. University sets criteria for the acceptable risk regarding the use of its own IT systems according to ISO standard 27005.

2. At least once a year or in any case of important changes of security requests of IT, University conducts risk analysis of the IT systems to ensure that this risk is kept within the acceptable limits regarding the University activities. Risk analyses results are documented.

3. Risk management of the information system must include the entire information systems of the University integrated in all its development stages.

4. Risk management of the information system must include the annual plan of awareness for University employees for the adequate use of services offered through the

information system of the University.

Article 9
Security of information systems

1. Security of the IT systems will be based on defining the fulfillment of the following criteria:
   1.1. Confidentiality: information must be accessible only for the authorized users;
   1.2. Integrity: maintaining the accuracy and completeness of the information system;
   1.3. Availability: access on IT system at any time for the authorized users.
2. University must manage constantly the security process of the information system.
3. University must identify and monitor the needs for security for the information system, at least based on the results of risk assessment of that system and the obligation that arise from internal acts or contractual relation.
4. University must define criteria, methods and procedures for information classification based on the sensitivity and critical level – regarding the possible consequences if their confidentiality is breached, integrity and availability.
5. Information security and all activities related to it, must comply with all applicable laws that deal with institution's information and operation.

Article 10
Physical security of information systems

1. University must undertake necessary protection measures to prevent any unauthorized physical access, interferences or damages of information, processing information devices and operations of the University, based on ISO standard 27002.
2. University must establish access and work procedures for the security zones for all employees and external parties. Security zones must be protected through access control to ensure that only authorized employees have access.
3. Devices must be maintained to be protected from failure, to provide constant availability and integrity and to be supported from interruptions as result of failure of the auxiliary equipment, natural catastrophes, malicious attacks, or accidents etc.
4. Security measures must be set even for devices that are used and located outside of the University buildings, depending on the location risks must be considered when determining necessary controls.
5. All devices that contain information must be verified to make sure that all data and licensed software are removed prior to disposal, destruction or reuse, to prevent the recovery of the original information.
6. All users must be aware of the security requests and procedures to protect the unsupervised devices.
7. University must set criteria, methods and procedures for a clean desk in order to protect

the information.

8. Contractual obligation for the employees and external IT service providers must reflect the University policies for the information security. All employees and external IT service providers must understand the responsibility for the roles they are considered.
9. Where appropriate for application, University will define that employees and external service providers will retain the information obtained during the exercise of their activity even for a certain period of time after the termination of the contractual agreement with the employee or external IT service providers.
10. University, must define actions and measures that has to undertake in case of a breach of security requirements by the employees or external IT service providers.

Article 11
IT asset management

1. The university must identify all IT assets.
2. The university must maintain an inventory for all assets with all necessary information, including the model of the asset, format, and location, information for backup (when applicable), information for the license and the value for the teaching activity.
3. University must define and document the ownership and the classification of all assets related to the information processing.
4. The owner of the asset will be responsible for:
   4.1. To ensure that the information and assets related to the information processing are classified based on the sensitivity;
   4.2. To define and regularly review restriction on access and classification.
5. University must define rules for the acceptable use of the information and the assets related to information processing.

Article 12
Computer network management

1. The university computer network must be managed and controlled in order to protect the system of information and applications. University must implement control to ensure protection of the confidentiality and integrity of the information on the network and the protection of services from unauthorized access based on ISO standard 27002.
2. For computer network management University must define:
   2.1. Procedures for the use and management of network services and devices in order to restrict access on network services and applications;
   2.2. Establishing special controls to protect the confidentiality and integrity of the data that passes through public or wireless networks;
   2.3. The technology applied for the security of network services such as authentication, encryption and network connection controls;

2.4. Groups of information services, users and information systems must be isolated from public networks;

2.5. Special controls must be applied to the access of external service providers in cases of the need for interconnections (with third parties).

Article 13
User access management

1. University will manage the access to the information systems through relevant internal procedures for managing users' access rights. The internal procedures must contain criteria for access, authorization, identification and authentication of users based on ISO standard 27001.
2. Every user must be unique and the system must define the criteria for setting the password based on ISO standard 27000. Prior to granting access on the information systems, internal University employees as well as external service providers, must sign a confidentiality and non-disclosure agreement.
3. University has to make sure that the authorization of users' access on the information systems is done by the persons responsible for those systems and to be based on the principle the lowest possible access in the system, enabling to perform the work tasks. University should review at least on six months basis the users access rights on the high importance systems, based on the risk assessment and at least on annual basis for all other systems.
4. On the rights of users' access management, University must specifically authorize privileged access and/or remote access on the information system. Every access and privileged user's activity and remote access must be monitored.
5. Remote access on the information system should be enabled on the two-factor authentication method. Communication between the remote devices that will access the information system must have end-to-end encryption measures for each communication session.
6. University has to monitor and store information security events on their infrastructure based on ISO standard 27001.

Article 14
Internal audit of information system

1. Requests define by the Regulation for the internal controls and audit are applied to information system audit.
2. Activity of the IT field must submit to at least periodic annual review that focuses on risk based methodology.
3. IT audits must be performed by competent persons within the internal audit function or external persons contracted for this purpose.

Article 15

Information backup

1. Information backup must be done according to University's internal procedures.
2. Internal acts according to 1st paragraph of this article must contain at least the following elements:
   2.1. Determining the necessary level of information backup;
   2.2. Maintaining accurate and complete data on information backup, as well as documented procedures of backup;
   2.3. Model (Full, incremental, differential) and the frequency of the backups based on the complexity of teaching activity.
3. The schedule to establish backups must be made by ensuring that all information and the software will be recovered in case of disasters or device failures.
3. Backups must be stored on a second location, in a proper distance to not be exposed to the same threats as the central location.
4. Backups should have the proper level of physical and environmental protection, in accordance with the applied standard at the central location.
5. Backups must be tested regularly, ensuring that they are reliable and useable when needed.
6. Backups should be protected from unauthorized access by encryption.
7. The duration to store the information must be done according to the legislation in force.
8. Any contracted service submits to the same information protection rules that apply to University's internal (not contracted) services.

Article 16
Database

1. Requirements defined by Administrative Instruction no. 01/2010-MAP on access security, the Regulation for the minimal security requirements are applied for the database.
2. Beside the requirements from the 1st paragraph of this regulation, University must define the terms for personnel access and authorized third parties to access servers' room in case of emergencies.
3. The server room must be restricted for access to authorize personnel only and to be monitored by recording entry/exit of staff and external persons within this room.

Article 17
Continuity of operation in emergency situations

1. In order for all IT systems to operate uninterrupted, University must establish a process for constant work.
2. University must approve a plan that will analyze the interruption of activities, that will

contain at least:

2.1. Processes that have priority as well as the necessary resources for these processes;

2.2. The final activities that must be reached (Service Delivery Objective);

2.3. The last time of recovery (Recovery Time Objective);

2.4. The last recovery point (Recovery Point Objective).

3. University must approve on yearly basis the Plan for Activity Continuity, also the Disaster Recovery Plan, which regulates the creation of condition for the recovery and availability of the information system resources, necessary to perform the critical activity processes.

4. The Plan for teaching Activity Continuity and the disasters recovery plan must include at least the following requirements:

4.1. Procedures that must be followed in case of system outage;

4.2. An updated list of all necessary human and technical resources to restore the continuity of teaching activities;

4.3. Information for responsible persons and their substitutes who will be responsible for the recovery of the operation in case of the unpredicted events, including their defined duties and responsibilities, also the plan of internal and external communications lines;

4.4. An alternative location in case of the interruption of teaching activities and recovery in function of educational activity processes in the primary location. This location must have the appropriate distance from the primary center, in order to avoid the impact of the same threats on both locations.

5. To implement the plans according to paragraph 4 of this article, the University will make sure that all employees will be familiar with their roles and responsibilities in case of emergencies.

6. University will harmonize the plans with the plans the changes of IT services, including product change, activities, processes and systems, with the environmental changes, as well as with the policies and IT services strategy.

7. University will test the plans, at least once a year and after the occurrence of significant changes, and it will document the results of those tests.

8. In managing the continuity of IT services, University will consider the activities that have been trusted to third parties and the dependence on the services of those parties.

Article 18
Documentation of IT activities

University keeps the complete and up to date documentation of the organization, equipment, systems, access and of other important factors related with the IT activity. Such documentation, will prove that compliance with the requirements of this regulation is constant.

Article 19

Improving measures

Any violation of provisions of this regulation will be subject to improving and penal measures as is defined in the regulation for procedures and the processing and security measures of the personal data.

Article 20

Entry into force

This regulation enters into force on the day of approval by the Governing Council of the University “Ukshin Hoti” Prizren.

Prof. Asoc. Dr. Arif Murrja

_____

Chairman of Governing Council