AVICENNA

Batumi Medical University

„Approved"

Annex N3 of the Protocol N01-03/02 of the general meeting of partners of Avicenna -Batumi Medical University LLC. dated July 29,, 2022

Information Technology management Policy of Avicenna - Batumi Medical University

Contents

Article 1. Scope of Regulation

1.1. This policy defines the requirements for information technologies and the processes of collecting, processing and transmitting information, specific technologies and the circle of people who have access to information, the necessary requirements for safe and efficient use of information technologies of Avicenna-Batumi Medical University LLC (hereinafter – "Avicenna" or the "University"), determines the responsibilities of structural units, academic/visiting/ support staff (hereinafter -the staff) and studetns in terms of access to information technologies and information resourses of the University.

1.2. The purpose of this policy is to promote an uninterrupted progress of the educational, administrative and business processes of the University, the proper functioning of information technologies and information resourses of the University, to ensure information security, the introduction of the necessary procedures for the efficient and safe operation of the University activities with information technologies.

1.3. Information technology management policy is aimed at protecting the privacy and personal data of persons (employees and students) associated with the university.

1.4. Compliance with the requirements of the policy is mandatory for each user (employees and students) who has access to information technologies of the university.

1.5. Failure to comply with the requirements of the policy leads to the responsibility defined by this document, internal regulation of the university and other legal acts.

Article 2. Information technology acquisition and installation policy

2.1. The acquisition of information technologies and appropriate software (hardware, software) is made based on the specifics of the University and the established targets.

2.2. The need to purchase information technology and software may arise due to an increase in the staff of a structural unit and/or the amount of work, depreciation /breakdown/ imcompatibility of existing resourses with new tasks or other reason specified in the report of the head of the respective structural unit.

2.3. An application for the acquisition of information technologies or software necessary to fulfill the task provided for by the strategic development plan of the University shall be submitted by the structural unit/person responsible for strategic development of the University.

2.4. The needs of the specific structural unit of the University in terms of the aqusition of information technologies and software are presented by the head of the relevant structural unit to the Deputy Rector for administrative and financial direction.

2.5. The Deputy Rector for administrative and financial direction considers the application; he has the right to reject an application for the acquisition of information technologies or software if:

a) The structural unit of the University does not justify the need for appropriate information technologies or software;

b) There is better alternative of information technologies or software;

c) The acquisition of information technologies or software is not possible due to the lack of an appropriate budget.

2.6. The refusal of the Deputy Rector to purchase information technologies or software may be appealed to the Rector of the University. The Rector is authorized to decide on the allocation of additional budget.

2.7. In case of confirmation of purchase application, the Deputy Rector for administrative and financial direction submits the application to the Information Technology Service which, in turn, is obliged to provide the Deputy Rector with the following information within the prescribed period:

a) Conclusion on the compliance of the required information technologies or software with the task, the possibility of integration with the current technologies of the University, the availability on the market and the absence of a better alternative;

b) Information about technologies or software suplliers (at least 3 suppliers) ;

c) Information about the cost of information technologies or software from each supplier;

d) Information about additional services- transportation, customs clearance, installation and other needs.

2.8. Information Technology Service is authorized to present less than 3 suppliers, if:

a) The cost of the required Information technologies or software does not exceed 30 GEL.

b) The required information technologies or software is purchased from their manufacturer (licensed operative system or software package, application, service, etc.

2.9. Based on the information from the Information Technology Service, the Deputy Rector for administrative and financial direction takes decision on the choice of a supplier and concludes an agreement for the purchase of good/services.

2.10. Installation of the purchased information technology or software is carried out by the Information Technology Service if, on the basis of its conclusion, there is no need to additionally purchase installation services.

2.11. Checking the suitability of the acquired information technology or software, signing the acceptance certificate and, if necessary, organizing warranty service or damage recovery (Bugfixing) processes is the responsibility of the Information Technology Service.

2.12. The receipt of the purchased information technologies or software is confirmed by the head of the respective unit to whom the respective product was delivered.

Article 3. Device Policy

3.1. Each employee of the University is equipped with information technologies necessary for the performance of official duties.

3.2. The University provides an employee holding administrative/management position at the University with a personal computer with the software necessary for the effective performance of his/her official duties.

3.3. It is allowed for an employee to use his/her own information technologies (laptop, tablet, smartphone, etc.) with the consent of the head of his/her structural unit or, in the absence the latter, the head of a higer structural unit. In order to give consent, the authorized person must make sure that such consent does not lead to damage, loss of University information as well as the risk of unauthorized access or the breach of cybersecurity.

3.4.) It is allowed for an employee to use information technologies of the University outside the campus (premises) of the university with the consent of the head of his/her structural unit and Debuty Rector for administrative and financial direction. Before giving consent, authorized persons must ensure that such consent does not lead to damage, loss of University hardware and or/information on them as well as the risk of unauthorized access or the breach of cyber security.

3.5. A University employee works on the computer hardware of the University under a user account. When using own information technologies, a University employee is required to create a user account; it is not allowed to work with University resources with device administrator rights.

3.6. Using information technologies that do not restrict administrator rights (tablets, smartphones), the employee undertakes not to install any software bypassing the official application stores (Play store, App store) and /or not to obtain device superuser rights (Root, Jailbreak).

3.7. When working with computer resources as well as on the Internet network of the University, a University employee is prohibited from:

a) Installing of any software;

b) Working with administrator rights;

c) Misusing of the computer hardware;

d) Violating the rules for operating the equipment.

3.8. An University employee has the right to apply to the Information Technology Service with the request to check the information technologies used for the activities of the University for malware. In turn, the Information Technology Service has the right to require the employee to install a working anti-virus program on the equipment used for work.

3.9. Installation of software purchased by the University on personal information technologies is allowed with the permission of the Deputy Rector for Administrative and Financial Direction and for a period specified by him/her. It is not allowed to use the software purchased by the university for any other purpose.

3.10. The use of portable momory cards and disks (USB, Flash, HDD, SDD) is allowed provided that the anti-virus program is working and functioning on the information–issueing and information-receiving device on the computer. In the absence of the relevant information, the portable media is subject to anti-virus scanning by the Information Technology Service.

3.11. For public information technology (printer, scanner, server, etc.), an employee is identified who is responsible for its efficient operation.

3.12. By handing over the computer equipment of the University, the employee confirms that he/she is familiar with the rules for using the relevant device at the usual, consumer level and is responsible for compliance with the established rules in the process of using this device.

3.13. The use of computer equipment of another employee of the University is possible with the permission of the employee using it, or in his/her absence - with the permission of the head of this employee.

3.14. The user of the corresponding equipment is responsible for the damage caused by the incorrect use of the equipment, intentionally or by failure to comply with the requirements established by this policy. This does not include natural amortization of the equipment or failure due to other reasons as well as cases of damages to peripheral devices and wiring during normal operation.

3.15. In case of the damage, the specified device must be transferred to the Information Technology Service where the causes of damage are determined and its repair is ensured in the manner prescribed by Article 2 of this regulation or applies to the Deputy Rector for Administrative and Financial Direction to write off the equipment.

3.16. In case of damage to the device belonging to an employee which contained information valuable to the University, the employee is obliged to report this information to his/her superviser and the Information Technology Service and transfer the device to retreive information of the University. If there is a risk of losing information valuable to the University, the employee does not have the right to repair or dispose of the device without the permission of the head.

3.17. In agreement with the Deputy Rector for the Administrative and Financial Direction, an inventory of computer equipment and other information devices of the university is carried out and their technical serviceability is checked.

3.18. In case of termination of labor relations with an employee, the employee is obliged to hand over the equipment to the Information Technology Service, as well as to remove information from his/her device regarding the activities of the University, and transfer the information to the Information Technology Service.

Article 4. Email Policy

4.1. Employees of the University in the course of their professional activities are required to use the e-mail created on the domain name (**...@avicenna.ge**) of the University .

4.2. **e** Students of the University provide communication with the university, as well as authorization in the learning process management system, using an e-mail address created on the domain name of the University (...@avicenna.ge).

4.3. (The e-mail address on the University domain is created by the Information Technology Service and provided to the employee/student of the University with temporary login data, which is subject to mandatory change by the user-employee/student. The password of the user must be at least 8 characters long, contain Latin letters, Arabic numerals and additional characters. It is not allowed to use the name, surname, year of birth of the user and the name of the University in the password (it is recommended to use a multi-factor, at least two-step authentication system).

4.4. The name of the e-mail user in the case of administrative and academic,visiting and scientific personnel is created by combining first letter of his/her name and his/her surname in Latin transcription: N.Surname@avicenna.ge and in the case of a student - by combining the name and surname in Latin transcription Name.Surname@avicenna.ge. If name and surname match, additional Arabic numerals may be used in the username: N.Surname@avicenna.ge / Name.Surname1@avicenna.ge

4.5. The e-mail accounts of the administration, teaching and visiting staff must be filled in the signature form provided by the Public Relations and Marketing Service, indicating the University logo, staff position and contact information.

4.6. The use of the e-mail for non-official correspondence is not allowed.

4.7. It is not allowed to register an e-mail address for non-official purposes on various resourses including e-commerce sites except structural units responsible for procurement and the Public Relations and Marketing Service and others on social networks.

4.8. It is not allowed to leave an e-mail account unprotected without logging out or locking user's account on a computer.

4.9. When using an e-mail on other devices, it is necessary to enable "Incognito" mode in the brouser and sign out after the end of the session.

4.10. The security rules for using e-mail equally applies to the use of other web applications (sheets, froms, docs, etc) included in the GSuite package along with e-mail.

4.11. A user of corporate e-mail must comply with the service terms of the provider (google).

4.12. The University has the right to monitor a use of corporate e-mail by the user and access, modify and terminate a user's account without further permission.

4.13. Each operation performed from a user account is considered to be performed by the user.

4.14. In case of loss of access to e-mail account or other obstacle to use the account, the user is obliged to immediately notify the Information Technology Service.

Article 5. Social Media Policy

5.1. Use of Social Media is allowed for:

a) Official purposes –as a platform for searching, displaying and disseminating information.

b) Personal correspondence – within the functionality of messengers available on other platforms of Social networks.

c) Other personal purposes-if this does not jeopardize the performance of official functions by the employee.

5.2. Access and monitoring of Social Media is carried out by the Public Relations and Marketing Service of the University.

5.3. It is forbidden to create an account in the name of the University and/or verify it in any social network or other platforms of social media (blog, vlog,microblog, etc) in the name of of the university as well as to communicate on the own social networks in the name of the University.

5.4. A University employee has the right to post relevant information about an employer, position and work experience on his/her personal Social Media page.

5.5. Information about the University, its employees, students, partners and persons associated with the university must be disseminated in social networks objectively and collegially in compliance with the requirements established by the legislation of Georgia on the protection of personal data and the Code of Ethics of the University.

5.6. Spam (providing information that does not correspond to the content), open or hidden advertising, political propaganda, expression of hateful and discriminatory speech are prohibited on the University's Social Media Pages.

5.7. The Univeristy has the right to assess the opinion of an employee about the University or collegue, expreseed in social media for its compliance with the charter of the university and the Code of Ethics, recognizing the freedom of expression.

Article 6. Internet Policy

6.1. Internet use on campus is permitted through the wired or wireless network of the University.

6.2. Each employee of the University administration is provided with a password to enter the network.

6.3. A guest network (no password required) is available for students.

6.4. It is not allowed to connect to the Guest networks for official purposes.

6.5. When connecting to the Internet outside the university, an employee must follow the following network security procedures:

a) Have an anti-virus program recommended by the Information Technology Service of the University, updated to latest version;

b) Do not go to unverified, suspicious (phishing) links;

c) Do not work with financial and personal data and information related to the intellectual property of the University on sites that do not have proper protection (https-certificate).

6.6. Use of the Internet at the University in the course of work is allowed taking into account restrictions established by this Artile.

6.7. It is forbidden to use VPN and P2P connections, to change IP address as well as use a brouser (Internet Explorer, ToR, etc) that is not recommended by the Information technology Service.

6.8. The user's brouser must be updated to the latest up-to-date version.

6.9. The use of Internet for personal purposes, including sources of information, social networks, and personal e-mail is allowed within reasonable limits, if this does not prevent the employee from performing official functions. The direct supervisor of the employee has the right to demand that the employee stop using Internet resources for personal purposes.

6.10. It is prohibited to use pornographic, violant and hate speech resources on the Internet as well as computer games with a web interface.

6.11. It is prohibited to download files with extension and install them.

6.12. The University is authorized to establish a list of prohibited websites and restrict users' access to them.

6.13. The Information Technology Service of the University is authorized to monitor the user's traffic and provide information about the user's web history to the Deputy Rector for Administrative and Financial direction.

Article 7. Account Management

7.1. The University has the following groups of Information Technology users accounts:

a) Administrator and operator –Information Technology Management Service

b) User with specific rights - defined by the Deputy Rector for Administrative and Financial direction;

c) Ordinary user- all employees of the University unless he/she is granted special rights by the decision of the Deputy Rector;

d) Student-student-user;

7.2. Groups of users use physical or electronic equipment and services provided to them. Based on the specifics, there are internal additional access levels in the group.

7.3. Groups and levels of users are determined/modified in advance by the Information Technology Service in agreement with the Deputy Rector for Administrative and Financial direction.

7.4. The authority to create, modify, monitor activity and cancel accounts is assigned to the system administrator .

7.5. Inappropriate behavior of user groups and levels will lead to:

a) Limited access to devices and electronic service;

b) Seperation and/or isolation from the University network.

7.6. An administrator or user with special rights is authorized to obtain remote access to the account to perform a specific task or resolve a problem, with the user's consent.

7.7. Functional groups and management of access points:

7.7.1. Depending in the internal structure of the University, an independent internal network (physical or/and virtual) is allocated for all groups and meets the requirements of a particular group for security and availability;

7.7.2. The group is designed to manage the internal network, devices and services of the University. It has access to all other groups as well as to services and devices. Only the network/system administrator and operators have access to the group and operators have limited rights (only access without the right to modify).

a) Group of employees - the group is intended for University employees and the exchange of information between devices is allowed. Communication with other groups is limited;

b) Group of guests and students – the group is intended for guests and students and has access only to certain Internet services for a limited time;

c) Group of Security and telephone - The group is intended for surveillance cameras, telephones and their control devices. Arbitrary access of third parties and devices to the group is restricted. Only registered devices can access this network. Access to other groups and individual services is also limited.

d) Examination and laboratory group - the group is intended for electronic exams and laboratory work. It has access to exam and lab resources only. Access to other groups and individual services is limited.

e) Access to telecommunications nodes – Only the administrator and the operator have the right to access the telecommunications nodes. For security reasons, it is closed as a telecommunications shaft. To access the equipment it is necesssary:

e.1) to inform the administration in writing about the purpose and necessity of the access (sending a message / appeal);

e.2) to notify the security service for access to the telecommunications shaft;

e.3) to notify the operator and security service after completion a work.

Article 8. Information Security

8.1. Information security policy at the University is implemented at physical, network and cybersecurity levels :

a) Physical security includes password protection of accounts, web applications and software as well as the restriction of system administration functions to ordinary users.

b) Network security refers to the use of hardware and software (Switch, Firewell) to protect physical and wireless networks of the University from unauthorized access.

c) Cybersecurity includes media restrictions, data backup, application installation restrictions, account and password management and multi-factor authentication methods which reduces the rist of cyber attack using software and social engineering, as defined in this policy.

8.2. No one, except for the person(s)(administrator and operator)specified in the relevant order of the Rector has the right to arbitrary connect the device to the University network, artificially extend its coverage area or implement any other actions that violate the reliability, security, integrity and availability of the University network, services and devices.

Article 9. Policy on the use of Educational process management system

9.1. The educational process management system of the University is provided by the outsourcing company.

9.2. Outsourcing company is responsible for the security of electronic educational management process which is governed by the service contract concluded with the company.

9.3. The educational process management system of the University (hereinafter the System)- staff.avicenna.ge and students.avicenna.ge – provides affective management of the educational and administrative activities of the University, support existing processes, communication, processing and protection of information.

9.4. General functions of the system (modules are):

a) Automation of the educational process management at the University;

b) Automation of the financial moduel (a module related to the calculation/ accounting wages andtution fees;);

c) Electronic proceedings;

d) Human Resources amagement (HR).;

e) Electronic library;

f) Electronic testing.

g) Interviews;

h) Reporting;

I) SMS Notification;

l) An individual panel of administration/visiting staff;

m) Communication between administration, lecturers and students;

n) determination of user rights;

o) data reservation 3 times a day;

9.5. The system uses cryptography where passwords of users (administration, lecturer, student) are encrypted.

9.6. Users of the system are:

a) Administration;

b) Lecturer;

c) Student.

9.7. Sysem Security:

9.7.1. The system code is written on a dedicated local server where new modules added to the system are tested after which the tested code is uploaded to the main server;

9.7.2. The system works according to GDPR (General Data Protection Regulation) standard, logs of actions are stored on the server with the following data: author of the action, time of the action, performed action, IP address;

9.7.3. To ensure business continuity, in the event of a failure of the main server, a back up server is automatically activated which replicates to the main server;

9.7.4. The system is hosted in Google Cloud;

9.7.5. System data is automatically saved 3 times a day on the University's google drive;

9.8. System Development Mechanisms:

9.8.1. The network infrastructure of the University is equipped according to modern standards. In the event of a change in sdandards, the University constantly takes care to bring its infrastructure in line with the new standards.

9.8.2. The code of the existing educational process management system is written with current standards and the software approach and solutions change as the standards change.

9.8.3. The University provides information resources development, improvement, optimization and monitoring of processes, both with the forces of the program development unit of the administration and with the autsourcing of relevant services.

Article 10. Access points and information technologies

10.1. The planning and installation of information technologies and telecommunications infrastructure of the University was carried out simultaneously with the construction of the University premises and is designed to adopt to the technology development in the next 8-10 years.

10.2. The University network and devices on the territory of the University, as well as services and equipment stored in the cloud and various data centers, are part of the University's infrastructure .

10.3. In all premises on the territory of the University there are physical access points and the use of radio frequency spectrum is possible .

10.4. The University has implemented the latest, wireless, broadband radio frequency network which uses 802.3 a/b/g/n/ac standard and automatic user roaming technology. WPA2 protocol (sdantard: IEEE 802.11i) with AES encryption algorithm is used,

10.5. Wired access points located on the territory of the University use 1000BASE-T technologies (Standard: 802.3ab-1999 (40)) and physical wiring allows the use of 2.5GBASE-T (standard: 802.3bz-2016 (125)) if necessary.

10.6. L2TP/IPSec , IPSec protocols with AES, DES, HMAC-SHA1/SHA2 encrypting algorithms are used for the virtual internal network.

10.7. Network access security levels are defined for access functional groups according to this policy. Groups have access only to the resources (physical and electronic) defined to them.

10.8. In the entire territory of the University, except for classrooms and administrative premises, a video surveillance system has been installed that covers both the interior space of the building and the perimeter.

10.9. The Surveillance network is a closed system, access to what in change/record mode is limited to all and in read mode is available only to the structural unit responsible for security.

10.10. Any action taken in the surveillance system is recorded in an electronic log in the network video recorder.

10.11. A telephone system based on the VolP technology is introduced on the territory of the University which ensures uninterrupted communication between employees as well as with subscribers of various fixed-line telephone operators in Georgia..

10.12. All telephone equipment is pre-registered at the internal telephone station and receives a unique code. Based on the purpose, the access of devices to services is limited. In necessary, SRTP and TLS encryption technologies are used.

10.13. The University has implemented various back up systems (physical and electronic) to ensure business continuity. The University has a storage server. To ensure the security of documents placed on the server, at the end of each day, files are automatically backed up on the google drive.

10.14. the University is served by two Internet providers- Siknet and MagtiCom. Silknet line is used as the main source of Internet. And magticom is used as a back up source.

10.15. For uninterrupted power supply, the University has a Diesel generator with a capacity of 500 Kilowatts which starts automatically in 3 minutes after a power outage; also, the employees of the University are equipped with uninterruptible power supply (UPS).

Article 11. Management of Information Technology Resourses

11.1. The Information Technology Service of the University is responsible for the administration of information systems and services, electronic databases and proper functioning of information technologies.

11.2. The Information Technology Service:

a) Develops university information technology, information security and data protection procedures;

b) Coordinates the operation of the educational process management electronic system of the University;

c) Administers databases;

d) Is responsible for the proper functioning of the university's hardware, network, server;

e) Administers website of the University;

f) Supervises the safe use of information technologies in the University, in accordance with established procedures;

g) Participates in the selection, procurement, maintenance and evaluation processes of information technologies;

h) Instructs staff in the efficient and safe use of information technologies;

i) Within its competence, takes care of the implementation of innovative technologies in the educational and management process of the University;

j) Exercises other powers defined by the legal acts of the University.

11.3. The Information Technology Service is obliged to:

a) Provide users with resources pre-defined for the group, introduce rules for their operation, in case of violation, temporarily suspend or terminate access to the resource;

b) Develop, implement, and manage new information technology resources as technologies, standards, and services evolve and change. The introduction of a new service, device, network and technology and / or change to an existing one must comply with the strategic development and information technology management policy of the University;

c) Monitor the electronic or physical network, services and devices of the University. If any defect is found, repair it immediately. Disable or isolate devices or services from the network that interfere and / or threaten the reliability, security, integrity and availability of the network, services and devices of the University.

Article 12. Error Elimination

12.1. Any error (any event, which interferes with business continuity and/or restricts user access to local or global resourses intended for them) is immediately eliminated.

12.2. The stepwise structure of the processes is as follows:

a) Damage notification (via phone and/or email);

b) The operator identifies and eliminates damage from the control panel;

c) If necessary, the operator goes to the place of damage;

d) If the operator fails to eliminate the damage, he/she informs the administrator;

e) The administrator performs network diagnostics;

f) Notifies the operator about the work to be performed.

g) The operator informs the customer about the damage and the estimated repair time.

Article 13. Audit of Information technologies and Information Security

13.1. The University periodically audits an information technology and information security in order to search for up-to-date information for the proper functioning information technologies, ensuring information security and improving the operation of information systems.

13.2. Audit is conducted at least once in a year. The terms of audit and the circle of involved persons are determined by the Deputy Rector for Administrative and Financial direction.

13.3. To conduct the audit, an audit committee is formed, which may include the University staff and external invited specialists.

13.4. Based on the results of the audit, the committee will develop a conclusion with a list of identified information security violations and recommendations aimed at improving processes.

13.5. The person responsible for the implementation of the recommendations of the Audit committee is the Deputy Rector for Administrative and Financial direction.

Article 14. Policy implementation and control over its implementation

14.1. The control over fulfillment rules, procedures and obligations specified by this policy is carried out by the Deputy Rector for Administrative and Financial direction on the basis of the information provided by the Information Technology Service

14.2. To study a particular issue, depending on ts complexity, the Deputy Rector has the right to apply to the Rector with a request to create a temporary working group and entrust it with the duty to study the relevant issue.

14.3. Along with control measures, awareness-raising activities of the employees, trainings, information meetings and preparation of information material in the field of effective functioning of information technologies and information security are carried out under the coordination of the Deputy Rector for Administrative and Financial direction.

Article 15. Responsibility for violation of the requirements of Information Technology Management

15.1. Violation of the requirements of information technology management or information security provided for in this policy, which did not cause property or non-property damages, is considered a minor violation of working conditions by the employee.

15.2. In case of a slight violation, the employee may be issued an oral or written remark/warning as well as measures may be taken to develop the information literacy of the employee.

15.3. Violation of the requirements of information technology management or information security provided for in this policy, which caused property or non-property damage, is considered a significant violation of working conditions by the employee and may become the basis for bringing him/her to disciplinary responsibility in accordance with the rules established by the charter of the University.

15.4. The issue of compensation for the damages is resolved in accordance with the Civil Code of Georgia, the Labor Code and the internal rules of the University.

15.5. In the event of a repetition of the violation, as well as in the event of a particularly gross or harmful violation, a question may arise of terminating the employement contract with the employee in the manner prescribed by the legal acts of the University and the employement contract concluded with the employee.

15.6. Violation of the requirements of information technology management or information security provided for in this policy, which may contain signs of an administrative or criminal offence, is subject to investigation in accordance with the the law.

Article 16. Final Provisions

16.1. In_accordance with the charter of the University, the first edition of the policy was adopted and approved by the meeting of partners of the University. .

16.2. The policy enters into force upon its approval by the meeting of partners.

16.3. The modified version of the policy, additions and changes to it are approved by the Rector of the University on the basis of the presentation by the Deputy Rector for Administrative and Financial direction.

16.4. Amendments and additions to the policy come into force after its approval by the Rector of the University unless a different date of entry into force is specified by the order of the Rector.