UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH

Guarant: CICT UPJŠ

Košice, 25/05/2018
Č. j: REK000239/2018-ÚPA/

Rector’s Decree No. 12/2018

issuing the Operational Regulations of the SAUNET Computer Network at Pavol Jozef Šafárik University in Košice and its units

Article 1
Introductory Provisions

1.1. The Operational Regulations of the Computer Network of Pavol Jozef Šafárik University in Košice, hereinafter referred to as "UPJŠ in Košice" - **SAUNET** (Šafárik University NETwork) (hereinafter the "**Operating Regulations**") set out the operational regulations of the computer network, the rights and obligations of the computer network administrators, the rights of access of the authorized users to the computer network services, the rights and obligations of these users and regulates the rules for network services and specific computer networks.

1.2. The Operational Regulations are based on the following documents:

- Law Act No. 351/2011 Coll. on Electronic Communications
- General rules for the SAUNET network use

1.3. The computer network is built and operated to support the activities carried out at UPJŠ in Košice in accordance with its main role and mission in the provision of higher education, scientific and research activities, economic and administrative operation, and may only be used for these purposes.

1.4. The Operational Regulations are binding for all the users of the SAUNET computer network.

1.5. The Operational Regulations are divided into # parts:

a) administration of the computer network,

b) using the computer network

c) special computer networks.

Article 2
Definitions of Basic Terms

2.1. For the purposes of these Regulations, the following terms shall have the following meanings:

a) **the SANET computer network** shall mean the Slovak Academic Network managed by the SANET civic association in order to provide academic and commercial institutions with access to the Internet World Wide Web in accordance with the approved statute and rules for the use of this computer network.

b) **the local computer network** shall mean the part of the computer network for which the corresponding part of the University is responsible.

c) **the wireless network** shall mean the electronic communication network made by electromagnetic means.

d) **the electronic service** shall mean the service provided in the electronic form by means of information and communication means.

e) **the electronic communications network** shall mean the functionally interconnected system of transmission systems and, where appropriate, interconnection and routing devices, as well as other means of transmitting signals by line, radio, optical or other electromagnetic means, including satellite networks, fixed circuit interconnection and packet switches including the Internet and mobile terrestrial networks, power distribution networks to the extent that they are used for the transmission of signals, radio and television networks and cable distribution systems, regardless of the type of information transmitted.

f) **The IP address** shall mean the identifier for the TCP/IP network entity that allows multiple parties to communicate across the network.

g) **IP address of the SAUNET network** shall mean the IP address from the 158.197.0.0 - 158.197.255.255 IP address range or the IP address from the 193.87.218.0-193.87.218.255 address range.

h) **the end-user** shall mean a person who uses or requests a publicly available service and does not provide or further provide any such service.

i) **the end-user equipment** shall mean the electronic communication device or a technical part thereof which allows communication and is intended for direct or indirect connection to the connection points of the computer network. For the purposes of these Operational Regulations, the end-user equipment shall also include server, switch, router, AP Wifi.

j) **localization data** shall mean the data processed on a computer network or through a network service that indicate the geographic location of the end user device.

k) **MAC address** shall mean the hardware address, the unique identifier of the end-user equipment assigned by the manufacturer.

l) **the computer network** shall mean an electronic communications network in which data are transmitted by fixed or wireless communication connections.

m) **the operating data** shall mean the data relating to the end-user and the particular transmission of information in the computer network and the data generated by such transmission, which are processed for the purposes of transmission of the message in the computer network.

n) **the point of connection** shall mean the active network element in which the end-user device accesses the local computer network.

o) **server** shall mean a computer or a programme that is running network applications or network services for end-users.

p) **the network application** shall mean a computer programme that provides end-user groups with predefined network services.

q) **the network service** shall mean the capability by means of network resources to satisfy predefined user requirements.

r) **the security incident** shall mean any event that has a negative impact on information security due to a security breach of the network and the information system or a violation of the UPJŠ security policy in Košice - accessibility, confidentiality or integrity of the information systems and the data stored in these

Part 1
Computer network administration

Article 3
SAUNET Computer Network Organizational Structure

3.1. **SAUNET** is a computer network spread over the territory of the Slovak Republic, the communication core of which is the SANET network. The SAUNET network serves as the communication infrastructure of the UPJŠ Information Infrastructure in Košice for the needs of the basic, applied research and for the needs of the educational process at UPJŠ in Košice and for the needs of the employees of UPJŠ in Košice access to information.

3.2. SAUNET is part of the **SANET** computer network, administered by the SANET Civil Association (hereinafter referred to as '**SANET CA**') through its member organizations operating the nodes of the SANET computer network. UPJŠ in Košice is also a member of the SANET CA.

3.3. **The Centre of the UPJŠ Information and Communication Technologies (hereinafter referred to as "CICT")**, Šrobárova 2, 041 80 Košice, is responsible for the administration of the SANET CA network node.

3.4. SAUNET has **upjs.sk** as its assigned domain.

3.5. The central node of the SAUNET network is located in the CICT's premises, where the SAUNET spine network and the primary domain server **ns.upjs.sk** with IP address **158.197.16.31** are located.

3.6. **The SAUNET computer network** has a hierarchical structure. It is divided into the following:

(a) the SAUNET spine network with the SANET university node; and

(b) the SAUNET local computer networks.

3.7. The SAUNET computer network consists of the following local computer networks:

a) The local computer network of the Faculty of Medicine

b) The local computer network of the Faculty of Science

c) The local computer network of the Faculty of Law

d) The local computer network of the Faculty of Public Administration

e) The local computer network of the Faculty of Arts

f) The local computer network of the CICT UPJŠ in Košice

g) The local computer networks of the UPJŠ in Košice Rectorate

h) The local computer network of the UPJŠ in Košice University Library

i) The local computer network of the UPJŠ in Košice Student Dormitories and Canteens (SDC)

j) The local computer network of the Institute of Physical Education and Sport

k) The local computer network of the Botanic Garden

l) The local computer network of the teaching and training Centre in Danišovce

m) The local computer network of the UNIPOC counselling centre

n) The local computer network of the Life-Long Education Centre and Project Preparation

o) The local computer network of the TIP

p) The local computer network of the Medipark

q) The experimental computer network of Institute of Computer Science (ICS) and the Institute of Physics (IoP) of Faculty of Science UPJŠ in Košice

Article 4
Connection to the SAUNET Computer Network and the Green Border

4.1. Each UPJŠ in Košice unit shall have the right to be connected to the SAUNET computer network by at least one line to the switch or to the router in the nearest information cabinet located either in the SAUNET network or in the SANET network.

4.2. Only the CICT shall have the right to provide free-of-charge or for money the access for third parties to the SAUNET computer network.

4.3. Organizations outside UPJŠ in Košice may connect through the SAUNET computer network to the SANET network only if they are members of the CA SANET and at the same time meet the conditions set out by this civil association.

4.4. The connection point between the SAUNET backbone network and the local computer network is referred to as the **green border**. It divides the administraiton responsibility of the SAUNET network among the UPJŠ in Košice units.

4.5. The green border includes a manageable network active element (network switch or network router) managed by the appropriate local computer network administrator.

4.6. The Local Area Network Administrator is required to provide the CICT access to the green border in cases necessary to ensure the integrity and security of the SAUNET computer network.

Article 5
Computer Network Administrator

5.1. The SAUNET computer network administrator (hereinafter referred to as the "**Computer Network Administrator**") is the UPJŠ employee in Košice in charge of operating the backbone of the SAUNET network (the "**Central Administrator**") or for operating the local computer network (the "**Local Administrator**").

5.2. Each UPJŠ in Košice unit must have its local computer network administrator, whose qualification or practice in the field corresponds to the content of this work.

5.3. The Local Area Network Administrator is the first consultant for all eligible users of the respective local computer network in the area of network functionality and subsequent failure troubleshooting.

5.4. The computer administrator is a member of the Virtual Information Centre (VIC) and a contact person for the CICT for the local computer network to troubleshoot the SAUNET computer network.

Article 6
Responsibilities and Obligations of Computer Network Administrators

6.1. Responsibility for managing the SAUNET computer network shall be with the CICT.

6.2. Responsibility for managing the local computer network SAUNET shall be with the following UPJŠ units:

Local computer network	**Local computer network administration**
FM network	ULI FM
FS network	CAI FS
FL network	FL
FPA network	FPA

FA network	FA
Rectorate network	CICT
Institute of Physical Education network	CICT
Botanic Garden network	CICT
University Library network	CICT
CICT network	CICT
Student Dorms network	SDC
TTC in Danišovce network	CICT
UNIPOC network	CICT
CCVaPP network	CCVaPP
TIP network	TIP
Medipark network	CICT
FS UPJŠ experimental network	ICS FS UPJŠ

6.3. The central computer network administrator shall be responsible for the following:

a) building the SAUNET network,

b) development, technical and system administration of the SAUNET network backbone, local computer networks of the UPJŠ Rectorate and the entire University information systems (except for the library information system).

6.4. The central computer network administrator shall be required to do the following:

a) ensuring coordination of network services, consultancy and advisory services in the areas covered by these Operational Regulations,

b) ensuring the integrity and availability of the SAUNET computer network.

6.5. The local computer network administrator shall be responsible for the following:

a) technical and system administration of the local computer network of the individual UPJŠ in Košice units from the green border to the connected user equipment,

b) correctly setting the communication parameters of end user devices connected to the local computer network,

c) compliance with the conditions for connection to the SAUNET computer network pursuant to Article 9 of these Regulations,

d) immediate disconnection from the local computer network of such end-user equipment whose operation is contrary to these Operational Regulations,

e) investigating the causes of, and removing the rules of, these Operational Regulations,

f) local computer network security.

6.6. The local computer network administrator shall be responsible for the following:

a) allocating IP addresses from the range assigned to CICT for the given local computer network,

b) keeping records of end user devices, including details of authorized users, keepinmg it up to date and providing it in order to maintain the CICT central register of end user devices,

c) monitoring and receiving information from the CICT on the state of the SAUNET computer network and informing the authorized users in the relevant UPJŠ in Košice units,

d) using the monitoring and diagnostic devices,

e) providing the training for eligible users in the appropriate UPJŠ in Košice units so that their computer literacy meets the requirements of these Operational Regulations,

f) increasing their qualification by studying and participating in courses and professional ventures,

g) familiarizing themselves with the new features of the SAUNET network under the VIC guidelines,

h) consulting the failure situations and communication problems of authorized users of the relevant UPJŠ in Košice units in the local computer network,

i) in cases where the problem or failure exceeds the green border, reporting this status to the CICT,

j) in identifying and subsequently eliminating the causes of the failure status cooperate with the administrator of the local computer network concerned or with the CICT staff,

k) maintaining and updating the local computer network documentation.

Article 7
Authorizations of the Network Administrators

7.1. The central computer network administrator shall be authorized to do the following:

a) ensuring integrity or security of the SAUNET computer network, disconnecting the particular end-user device or a specific segment of the SAUNET computer network for the time necessary for eliminating the deficiency or restoring the SAUNET network integrity and safety.

7.2. The local administrator of the computer network shall be authorized to do the following:

a) ensuring the integrity or security of the local computer network to restricting or prohibiting the use of network services of the local computer network, its part or end user equipment for the time necessary to removing the defect or restoring the integrity and security of the local network or its part.

b) ensuring the integrity or security of the local computer network to restricting or prohibiting the use of end-user equipment or parts thereof for the time necessary to removing the defect or restoring the integrity and security of the local network or its part.

c) deleting, copying, or archiving the end-user data or parts of the end-user equipment, in order to ensure the integrity, security and retention of data, on the basis of an order issued by the University, Faculty, or University site.

d) modifying the settings, applying security patches, or removing harmful content on end-user facilities of the University, without the consent of the authorized user, ensuring the integrity, security and data retention, provided the technical means and security level allows this being performed.

e) changing the settings, applying the security patches, or removing malicious content on end user devices that are not owned by the University, with the sole consent of the authorized person, to ensuring the integrity, security and retention of data, and, if the technical means, licensing conditions and security level allow this be performed.

Article 8
Interoperation in the Computer Network Administration

8.1. Computer network administrators shall be required to cooperate with each other to ensure the operation of the SAUNET computer network and to address possible problems.

2.8 The disputes between the authorized user and the administrator of the computer network shall be resolved by the management of the workplace that administers the relevant network element in the consequence of the use of which the dispute has arisen.

8.3. The UPJŠ in Košice units, together with CICT, shall be involved in resolving any conceptual issues of the construction of the SAUNET network and shall be involved in the preparation of proposals for their solution.

8.4. The individual personnel workplaces of the University units and the Faculty study departments shall be required to report to the CICT in time all the changes that have an impact on the authorization to use the SAUNET network. In the case of employees, these pertain to changes in employment relations, especially the creation, change and termination of the employment relationship or other employment relationship. With students, these changes are in their study, particularly enrolment for study, discontinuation of study, exclusion from study or termination of study.

8.5. Any verification and deployment of new network services in the SAUNET network, which may affect the operation of the backbone of the SAUNET network, shall only be possible with the CICT's consent. In the local computer networks, verification and deployment of new network services shall only be possible with the consent of the appropriate workplace that manages the local computer network.

8.6. For communication, the computer network administrators shall use the mail group saunet-adm@upjs.sk.

7.8 The CICT shall convene a meeting of the SAUNET network administrators at least once a year. The SAUNET Network Administrator shall also convene the CICT in the course of operation, as appropriate, to address the current situation in the computer network or on request by the local administrators.

Article 9
Telecommunication Operation and Protection of Personal Data

9.1. For the purposes of these Operational Regulations, **telecommunication operation** shall mean the following:

- operational data,
- localization data.

9.2. The CICT shall keep the telecommunication data for the purposes and to the extent as specified by Law Act No. 351/2011 Coll.

9.3. Only the CICT may issue the telecommunication traffic data. Any request to issue this data directed to the local administrator of the computer network shall be forwarded to the CICT.

9.4. Local administrators are required to be cooperative in overseeing the traffic data within the local computer network administered by them.

9.5. Network services may not be used for private purposes. Illegal content stored, transmitted, delivered, or operated through the SAUNET network services shall be the responsibility of the authorized user.

9.6. The contents of messages, stored documents, and other contents of the SAUNET network services shall not be monitored, collected, or evaluated. The content may be made available to another authorized user only in exceptional cases to ensure the integrity, security and retention of data, based on the order of the University, Faculty, or a University department.

9.7. The general binding regulations and internal regulations of UPJŠ in Košice governing the protection of personal data shall also apply to the use and administration of the SAUNET computer network.

Part 2
Computer Network Use

Article 10
Authorized User

10.1. It shall be the end user who shall be **the authorized user of the SAUNET computer network** (hereinafter referred to as the „authorized user“) who is:

a) an employee in employment with UPJŠ in Košice (hereinafter "the employee"),

b) student of UPJŠ in Košice in any form and at any level of study (hereinafter referred to as the "student") or

c) another person, guest.

10.2. UPJŠ in Košice employee is an authorized user since the emergence of employment until the termination of employment.

10.3. UPJŠ in Košice student is an authorized user from the date of commencement of study until the date of termination of their study.

10.4. Another natural person is an authorized user if that person has a legitimate interest in gaining access by such a person based on the agreement by the University management, the Faculty management, or the University department management. The agreement shall specify the scope of the authorizations and the access period of time.

10.5. The University guest can only become an authorized user after being provided authentication data, the end-user device information, and after approval by the appropriate central/local administrator of the UPJŠ computer network in Košice, and only for the duration of hosting at UPJŠ in Košice.

Article 11
Rules for Connecting to the Computer Network

11.1. The uthorized user will gain access to the SAUNET network by registering with the appropriate local administrator of the computer network. Upon registration, the authorized user is obligated to comply with these rules in writing or in any other appropriate manner. Registry details will modify the operational regulations of local computer networks or methodical instructions from local computer administrators.

11.2. The authorized user shall have the **right to connect the end-user device** to the SAUNET computer network.

11.3. The connection of each authorized user end user device is subject to the registration obligation with the local computer network administrator responsible for the relevant part of the SAUNET computer network that has a connection point for that device.

11.4. The end-user device must not be connected directly to the router or to the SANET computer network switch.

11.5. Only an end-user device may be connected to the SAUNET network that:

a) contains application equipment and application settings to ensure adequate security protection (e.g. antivirus protection, use of secure passwords);

b) contains a legal operating system for which there is official support from the manufacturer of that operating system.

11.6. For details on end-user equipment conditions, please refer to the methodological guideline issued by the CICT.

11.7. The local computer network administrator is also required to keep records of end user devices in the central database of user equipment of the information system managed by the CICT (hereinafter referred to as the "**central database**"). This does not apply if the end user is connected to the SAUNET network wirelessly after verifying the user's identification data.

11.8. End user devices are defined in the SAUNET computer network by the following identifying data:

a) IP address in the SAUNET,
b) MAC address,
c) the name of the authorized user who is responsible for the end-user device,
d) UPJŠ in Košice unit, which has end user device registered in its register.

11.9. An end-user device that lacks any of the identifying data listed in the previous paragraph of these Operational Regulations may not be connected to the SAUNET computer network.

11.10. An exception to the previous rule is an IP address from the following ranges:

a) 10.0.0.0 – 10.255.255.255,
b) 172.16.0.0 – 172.31.255.255,
c) 192.168.0.0. – 192.168.255.255.

11.11. Each server must have an administrator responsible for the activity of this server and all the servers must be registered at the CICT UPJŠ in Košice. The connection of the server to the SAUNET network is subject to the approval by the CICT UPJŠ in Košice or by the local computer network administrator with regard to the location of the connection point of this server.

Article 12
Authorizations and responsibilities of the computer network users

12.1. The authorized user of the SAUNET computer network shall have the following rights:

a) to use the SAUNET computer network and the network services provided within it,
b) to inform about the reasons for unavailability of the SAUNET computer network,
c) to inform about the way of operation of the computer network SAUNET.

12.2. The authorized user of the SAUNET computer network is required:

a) to protect their user authorizations and not provide them to other persons,
b) to follow the instructions of the central or local administrator of the computer network,
c) when working on other computer networks, to comply with the rules that apply to such networks,
d) to behave in the SAUNET computer network in accordance with these Operating Regulations,
e) to take adequate care of their end-user devices so that during the whole time of their connection to the SAUNET computer network they meet the conditions imposed on the end-user in accordance with Articles 10.6 and 10.7 hereof,
f) to make the end-user device available for setting up, prophylactics or checking compliance with the Operational Regulations,
g) to report a security incident to the email address **incident@upjs.sk**.

Article 13
Sanctions for violation of the Operational Regulations

13.1. It is forbidden to use the SAUNET computer network for activities that are inconsistent with the law applicable in the territory of the Slovak Republic or with good morals.

13.2. In addition to the above activities, the activities are forbidden which:

a) harass other users,
b) create or transmit illegal content, or allow such activities,
c) enable or effect the transfer of unsolicited commercial and advertising material,
d) enable or make intentional unauthorized access to the devices and services available over the computer network,

e) lead to network congestion, server overloading and reduced availability of services,

f) provide authentication data to third parties.

g) modify, encrypt, or otherwise modify the unauthorized content of other end-user devices.

13.3. In the event that an end-user device that does not meet the requirements of these Operational Regulations or an authorized user using this device performs an activity under Articles 13.1 or 13.2 of these Regulations, the local computer administrator or the central computer administrator shall have the right to disconnect the user device from the SAUNET computer network. If the end user is disconnected by the central administrator of the computer network, this status is reported to the local administrator of the computer network in whose local network the user device was identified.

13.4. The end user equipment disconnected within the meaning of Article 13.3 of these Operational Regulations may be re-connected to the SAUNET computer network only after proven removal of the reasons for disconnection of that device.

13.5. The local administrator of the computer network shall be responsible for removing the reason for disconnection of the end user device with whom the device in question has its connection point.

13.6. In the case of extremely serious threats to the SAUNET computer network, the central administrator of the computer network may disconnect the local computer network that has the source of the threat to the SAUNET computer network for the time necessary to remove the serious threat to the SAUNET computer network. The central administrator of the computer network shall inform the appropriate local administrator of the computer network about this disconnection.

13.7 In case of repeated violations of these Regulations, the local computer network administrator or the central computer network administrator shall have the right to disconnect all the user terminal devices of the authorized user of the computer network temporarily or permanently with regard to the scope and intensity of the activities that do not comply with these Regulations.

13.8 In the event of a serious breach of these Regulations, in particular in the activities where there is reasonable suspicion that a crime has occurred, the local computer network administrator or the central computer network administrator shall have the right to pursue disciplinary action against the authorized user performing such an activity.

Part 3
Special Computer Networks

Article 14
Wireless Computer Network of UPJŠ in Košice

14.1. The wireless computer network of UPJŠ in Košice (hereinafter referred to as the "**wireless computer network**") means part of the SAUNET backbone network, which meets the set of standards for wireless network (IEEE 802.1).

14.2. The foregoing parts of these Regulations shall be appropriately applied to the wireless computer network.

14.3. The authorized users shall access the wireless network through access points ("AP Devices").

14.4. The requirements for the technical and operational properties of the AP devices are governed by the CICT methodological guidance.

14.5. Before using the wireless computer network, the authentication of the authorized user is required by his/her identification (e.g. by name and surname, by e-mail) and the password assigned to him/her.

14.6 It is also possible to use one-time keys to connect to the local network administrator or another authorized person to temporarily connect to the wireless network. The person issuing the temporary key shall be responsible for the access keys issued, security, protection and record keeping referred to in Article 9. Temporary keys may be issued for a maximum of 5 days.

14.7. The wireless EDUROAM UPJŠ in Košice computer network (hereinafter referred to as the "**EDUROAM computer network**"), which is part of the Eduroam (education roaming) project and provides access to computer networks for the users of institutions involved in this project, is part of the wireless computer network. By connecting to the EDUROAM computer network these users become authorized users while they are being connected.

14.8. Authorized users of the EDUROAM computer network shall follow, in addition to these Operational Regulations, the roaming policy set by the coordinator for this OZ SANET computer network.

14.9 Creating and using one's own local wireless computer networks is prohibited.

Article 15
Virtual Private Network

15.1. The Virtual Private Network (**VPN**) is part of the SAUNET computer network, which aims to making the SAUNET computer network and its network services accessible to authorized users for the purpose of Article 1.3 of these Operational Regulations.

15.2. For the VPN, the other parts of these Operational Regulations will be applied appropriately.

Article 16
Cloud Services

16.1. Cloud services (Internet-based computing services) shall use the SAUNET computer network to make their services available to authorized users for the purpose of Article 1.3 of these Operational Regulations.

16.2. For cloud services, the other parts of these Operational Regulations will be used appropriately.

Article 17
Common and Final Provisions

17.1. The Operational Regulations of local computer networks shall comply with these Operational Regulations. These Operational Regulations detail the administration of the local computer network, in particular, they will regulate the end user devices access to the local computer network, the rights and obligations of the local computer network administrator and the rights and obligations of authorized computer network users.

17.2. These Operational Regulations repeal the Decree of the Rector No. 16/2014, which issued the Operational Regulations of the SAUNET computer network at UPJŠ in Košice dated 17 September 2014.

17.3. These Operational Regulations shall become valid on 25 May 2018 and shall be binding on all the users of the SAUNET computer network.

UPJŠ in Košice

Prof. RNDr. Pavol Sovák, CSc.
UPJŠ Rector