DIRECTIVE OF VICE-RECTOR FOR DEVELOPMENT AND IT REF. 1/2012

OPERATIONAL RULES OF INFORMATION AND COMMUNICATION NETWORK OF J. E. PURKYNĚ UNIVERSITY IN ÚSTÍ N. L.

DIRECTIVE FOR UJEP

Valid from:	25. 1. 2012
Prepared by:	Mgr. Palíková
Cancels.	Directive of vice-rector for development and IT No 1/2006

doc. ak. mal. Vladimír Švec

I.

Definition of basic terms

1. For the purposes of this directive **the information and communication (hereafter "computer") network** of the Jan Evangelist Purkyně University in Ústí nad Labem (hereafter "UJEP") means the totality of technical hardware and software of the university computer and information systems, the IT resources connected to them and all resources for the mutual linkage of these systems.

2. For the purposes of this directive UJEP **computer network user** means everyone who directly or indirectly uses the UJEP computer network or equipment connected to it.

3. For the purposes of this directive **user account** means access right to computer network and to UJEP information systems. Access to a user account is performed via a suitable authentication mechanism, usually it consists of the user name and user password.

4. For the purposes of this directive **network account** means type of user account serving for the use of centralised services and applications of the network environment. The central administration of network accounts is ensured by the UJEP IT Centre (hereafter "ITC").

5. The ITC, with contact email address sit@rt.ujep.cz, is the **operator of the UJEP computer network.**

6. **The operator and administrator of an individual part of the computer network, server or computer classroom** (laboratory) is the UJEP unit which administers the part of the network, server or computer classroom. Should the nature of the unit require it, for this unit the operator will issue operating rules which comply with this directive. The operator of an individual part of the network (server, classroom etc.) works closely with the ITC. The creation of an individual part of the computer network (faculty server, classroom etc.) must be discussed in advance with the ITC, with the central administrator.

7. **The ITC is the administrator of the domain names *.ujep.cz and address space (IP addresses).**

8. The UJEP employee who the head of the unit has entrusted with the performance of activities associated with systems administration and maintenance of the operating system is the **administrator** (administrator of computer network, administrator of information system).

9. **The administrator of a user computer** is its owner, and in the case of computers owned by UJEP, the responsible person given in the property records of UJEP. The administrator of a user computer is responsible for the software installed on the given computer and for the activity associated with the operation of the computer.

10. **A network incident** is any harmful behaviour in the UJEP computer network, including breach of this directive. The ITC monitors and resolves network incidents. Reports are accepted at the address abuse@ujep.cz.

II.

Fundamentals for use of computer network

1. Access to other computer networks which is mediated via the UJEP computer network is possible only for administrative, educational, research and development or artistic purposes and for other creative activity. When accessing information sources it is necessary to adhere strictly to the rules of behaviour valid in the target network. The university computer network is connected to the academic network of the Czech Republic.

2. Duties of users when working in the computer network:

a) To ensure the security of their user account. If through negligence they allow abuse of their identity in the network, they are fully responsible for any damages caused.

b) To keep their password secret. The password must not even be divulged to the network administrator during the resolution of problems.

c) To look after the state of hardware which they use for their connection, to protect it from abuse and keep the relevant software (in particular the operating system and protective programs) up to date.

d) To ensure that they do not infect the UJEP computer network with viruses or other malware.

e) When using computer network services to behave in such a way as does not overly inconvenience the other network users.

f) To inform the network administrator of discovered network security flaws.

g) Only to connect computers, notebooks and other mobile equipment to the UJEP computer network at reserved places.

h) During work to adhere to safety regulations for work with electrical equipment.

3. Forbidden activities of users in the computer network:

a) to connect communication equipment (routers, switches, wireless access points etc.) or an entire network to the UJEP computer network without the consent of ITC,

b) to broker access to the UJEP computer network and other information services to other legal or natural persons,

c) to utilise the services of the UJEP computer network in order to disseminate non-university commercial information or for advertising purposes or for dissemination of information in conflict with legal regulations, internal regulations and the internal standards of UJEP, ethical or moral standards or which could harm the name of UJEP,

d) to work under someone else's identity or abuse the negligence of other users (for example, forgetting to logout, unsuitable protection of files) to access not own data or information,

e) to use or create such software as could lead to the gaining of someone else's identity,

f) to use software with the aim of gaining unjustifiable anonymity (for example, sending anonymous mail etc.),

g) to attempt to gain access rights which had not been granted by the administrator (for example, unauthorised access to any non-public information sources of the university or third parties); if a user gains such rights through a software or hardware error, they are obliged to inform the ITC of this fact without delay (contact email: sit@ujep.cz),

h) to eavesdrop on traffic and create copies of messages passing through the individual nodes of the network, unless this involves the performance of such activity in the context of teaching of specialised subjects of an expert department, and this activity must be performed only in the laboratories of this department under the conditions designated by the operator of this laboratory and with the consent of the affected users,

i) to install without the approval of the ITC software which excessively increases the load on the UJEP computer network and servers,

j) without authorisation to install, reproduce or announce to the public via the computer network UJEP works, computer programs, databases and other results of intellectual creative activity protected by intellectual property right (in particular the copyright act, personal data protection act and classified information act),

k) to modify or allow without authorisation the modification of programs, data or technical equipment owned or used by UJEP (for example such change in configuration of the computer or terminal as has an impact on the operation of the network),

l) to intervene in any way in the cabling and connecting elements of the UJEP computer network, including its switching off without serious reasons,

m) to harass other users with unsolicited email.

III.
Creation of network accounts

1. A UJEP employee gains the right to create a network account on the day when his/her employment begins at UJEP, and he/she loses this right on the day when employment ends. The data kept in the UJEP personnel information system is decisive for the evaluation of a right.

2. A UJEP student gains the right to create a network account on the date of enrolment for study (the first enrolment or enrolment after end of study interruption), and he/she loses this right on the day of ending or interruption of study. The data kept in the UJEP study information system is decisive for the evaluation of a right.

3. A third party gains a right to the creation of a network account in exceptional cases on the basis of a written request approved by the rector or vice-rector for UJEP development and IT. A request contains the declaration of a user concerning familiarisation with this directive, on the request the relevant manager confirms the justification of the scope and time period for the user network account, documents the facts with contractual relationship (contract of employment, contract for work, contract for provision of services etc.). The manager immediately informs the ITC when the reason for the use of an account by a third party no longer exists.

4. The network accounts of students and employees come into being and expire automatically on the basis of information in the source information systems.

5. Each user proves his/her identity at the study department or personnel department by the presentation of a valid civic ID card or passport.

6. When personal data changes, a student contacts the study department, and an employee contacts the personnel department. Workers enter the verified changes in relevant information systems.

7. A user with verified identity gains the user account of the federation of identities eduID.cz. **The Czech academic federation of identities eduID.cz** provides its members with a framework for mutual utilisation of user identities during the management of access to network services whilst respecting the protection of personal data. The operator of the federation is CESNET, z.s.p.o.

8. Each account may be terminated on the basis of a written request of a superior worker or in the case of grave breach of this directive.

9. The validity of a network account is suspended in the case of a breach of this directive or in the case of suspicion that the account has been compromised (abuse). The suspension of a network account does not block students' access to the study system.

10. In cooperation with the head of the ITC computer network administration department, the head of ITC designates the periods of the stages of the user account life cycle.

IV.

Basic rights and duties of ICT employees

1. Depending on their competencies, ICT employees are responsible for the operation of the UJEP computer network and functionality of connection of the individual units.

2. Depending on their competencies ICT employees are responsible for the operation of central network services, they process and publish information, guides and methodological instructions at the address http://ci.ujep.cz.

3. The head of ICT designates the security policy for network operation, administration of user accounts and passwords.

4. Depending on their competencies ICT employees represent UJEP in the administration of processes for the electronic confirmation of UJEP user's identity for the Czech Academic Federation of identities eduID.cz.

5. Depending on their competencies ICT employees have the right to monitor traffic of the UJEP computer network with the aim of its optimisation, to ascertain and prevent abnormal states, and to ensure network security. Only verified ICT employees have a right to monitor the network, but they are obliged to preserve the confidentiality of facts discovered. No one else is authorised to monitor or analyse the traffic on the computer network. The purpose of the authorised monitoring of the network is either to discover operational problems or to ensure network security (detection of attack or attempt to discover attackers).

6. Depending on their competencies ICT employees have the right to restrict temporarily access to UJEP computer network services in the case of reasonable suspicion of a breach of this directive.

7. Depending on their competencies ICT employees have a right and a duty to resolve a breach of this directive with a user (network incidents) and to make out a protocol concerning this.

8. Depending on their competencies ICT employees have a right to block a user account immediately if they have a reasonable suspicion of abuse of a user account. The ITC will without delay pass on information about the blocking of a user account to the user and, depending on the gravity of the situation, to the relevant superior worker or relevant study department.

9. With the consent of the vice-rector for development and it, the head of the ITC has the right to issue individual managing and operational documents in order to ensure the rights and duties of the ITC pursuant to this directive.

10. Upon request the ITC user service department provides employees with a basic university IT service, contact email address servis@rt.ujep.cz.

11. Upon request the ITC information system administration department provides UJEP information system users with expert assistance, contact email address is@rt.ujep.cz.

12. Upon request the ITC computer network administration department provides users of the UJEP computer network with expert assistance, contact email address sit@rt.ujep.cz.

V.

Basic duties of operator

1. The operator pursuant to article 1 paragraph 6 is obliged:

a) to secure the used IT equipment using suitable resources. The duty of protection applies to the used hardware, software and all data.

b) to ensure that all the computers used by it in the UJEP computer network use only centrally as-signed addresses and domain names.

c) to ensure that no computers used by it in the computer network use anonymous login for network services. If such a computer offers access to network services, its administrator is responsible for all of its activity.

d) to discuss in advance with the ITC planned changes to the computer network, including prepared intents (preparation of project with IT technician, creation of new computer classroom, connection of IT systems of unit etc.).

e) to provide cooperation to central administration (ITC) during the resolution of network incidents associated with the operated IT equipment (for example, who worked with a technician and if necessary when).

VI.

Rights of computer network users

1. The gaining of a user account is a basic right of a UJEP student and employee.

2. A user is authorised to use the UJEP computer network for commercial purposes only in compliance with Act No 111/1998 Coll., on Higher Education Institutions, and the internal regulations for additional activities.

3. A user is obliged:

a) to familiarise himself/herself with this internal standard for operation of the UJEP computer network before first use,

b) to adhere to the operational code applying to the used resources of the UJEP computer network (operational rules of classrooms, IT systems etc.)

c) to respect the instructions of authorised persons and administrators of resources of the UJEP computer network,

d) to use the UJEP computer network in compliance with Act No 111/1998 Coll., on Higher Education Institutions, as amended, and in compliance with the document "Fundamentals for Access to Network of National Research and Education of New Generation" http://www.cesnet.cz in the section documents.

e) to change the password of all their user accounts in the UJEP computer network after first login and to keep this password secret, to choose a non-trivial password.

f) to ensure the protection of copyright and other rights of intellectual ownership, personal and sensitive data.

VII.

Publication of information on UJEP internet servers

1. A UJEP internet server is a computer with the domain name ujep.cz (for example, www.ujep.cz, pf.ujep.cz) or with IP address of the UJEP university network which affords access to published information.

2. Every UJEP computer network user who publishes information on the UJEP servers is responsible for its content.

3. The published information must be compatible with the activity of its authors at UJEP.

VIII.

Concluding provisions

1. A breach of this directive constitutes a breach of working discipline and may be considered a disciplinary offence. This provision does not impact the right of UJEP to compensation for damage incurred nor the civil or criminal liability of a user.

2. This directive was discussed by the Academic Senate of the UJEP on 25. 1. 2012.

3. This directive cancels the directive of the vice-rector Directive of Vice-Rector for Development and IT No 1/2006 OPERATIONAL RULES of UJEP computer network and information system.