RULES OF OPERATION OF THE COMPUTER NETWORK OF THE INSTITUTE OF BIOPHYSICS OF THE CAS, V.V.I

Article 1

Basic Provisions

1. Computer Network of the Institute of Biophysics CAS, v.v.i. (hereinafter referred to as the IBP) is a part of the Brno Academic Computer Network (BACN) built by universities, institutes of the CAS and other organizations in Brno. It is directly connected to the National Research and Education Network and through it to the Internet.

2. The term "computer network" encompasses all technical and program resources that are used both to interconnect computers and to use this interconnection. The mission of the computer network is the data interconnection of IBP workplaces and their connection to BACN for the purposes of research, teaching and operation of the Institute.

3. The rules set out in this Directive are binding on all computer network users and all computers and similar devices that are connected to the computer network. When specific part of the rules applies only to students, the term student is used. When specific part of the rules applies only to employees, the term employee is used. When the term user is used, the rule applies both to employees and students.

4. The management of the computer network is governed by the IBP Computer Network Administration Rules. These rules define the rights and obligations of network administrators. The corresponding articles of these rules also apply to users who manage their own computer resources connected to the IBP computer network on their own.

5. Rules for access to BACN and other networks (Internet, EDUROAM, ...) are specified by the operating rules of these networks.

6. "Illegal Software" means software that has been obtained in violation of laws, in particular the Copyright Act of the Czech Republic, and international copyright treaties. Any software for which there is no proof of its legal acquisition, i.e., in particular, an invoice or a licensing agreement, is also considered to be illegal.

Article 2

Access Rights and Identity

1. The IBP computer network can only be used by authorized users. Authorized users (hereinafter referred to as the user) are users who are demonstrably acquainted with this directive. The list of users is kept by the respective computer network administrator.

2. The right to become user applies to all IBP employees and students working in IBP and guests (EDUROAM). The use of the IBP computer network by persons of other organizations is only possible on the basis of a written permission issued by the IBP management or by its authorized representative.

3. Each user is required to keep continuously familiar with the rules of the IBP computer

network and with other up-to-date information and instructions that are available in electronic form on the IBP (Rules) pages. The user is also required to keep continuously familiar with the rules of work in all external networks and all external computer resources he/she uses and to observe these rules.

4. In case a user's identity is required to access the computer network, the user is required to use the name assigned to him/her by the administrator of the computer network. The user is required to use a password that is non-trivial to verify the identity, and keep this password secret so as to prevent any misuse thereof.

5. The user must not provide the assigned name and password to another person. Provision of the aforementioned data to a person who is not entitled to access the network or who has been blocked from the network is considered a gross violation of rules.

6. The user must not abuse the negligence of another user (e.g., forgotten logout) to work under a foreign identity.

7. The user's access rights are assigned to him/her by the administrator of the computer network. The user may not attempt to obtain access rights that have not been assigned to him/her. If a user receives access rights that do not belong to him/her by a system failure, he/she is required to report this fact to the administrator immediately and not to use such rights.

8. The user must not abuse the IBP computer network to obtain unauthorized access rights to any information resources available through the IBP computer network.

Article 3

Using the IBP Computer Network

1. The user is allowed use the computing resources and the computer network only for scientific, research, development, and educational purposes, or tasks related to the operation and management of the IBP. Any use of the aforementioned for commercial non-IBP related activities, in particular the dissemination of commercial information; political, religious or racial agitation; promotion of drugs and the dissemination of materials that are against the law is considered to be a violation of the rules.

2. The user has the right to use only legally acquired software. Copying programs can only be done under applicable copyright laws. The user may only use Shareware or freeware acquired through the IBP computer network for the purposes specified in paragraph 1. Any use of the computer network to offer illegally acquired software or data is considered a gross violation of the rules.

3. The user must not interfere with programs, data and technical equipment of the computer network without the administrator's consent. Unauthorized changes to the configuration of computers or other devices that could affect the operation of the computer network are strictly prohibited. The student may not install any programs without the administrator's consent.

4. The user has the right to use allocated disk space, computing resources, and computer network only with respect to the total load. The user may not deliberately interfere with the work of other users, nor with the operation and performance of the network. The user

must immediately obey the administrator's instructions to reduce the load generated by him/her.

5. The size of e-mails and conferences may be limited. The specific limit is given by technical possibilities and determined by the administrator. If the user limit is exceeded, the disk space may be automatically blocked for any further mail receipt of a particular user.

6. If, for any reason, the user cannot work for more than two months on IBP computer resources where he/she has a user account, he/she is obliged to discuss it with the network administration in advance. Otherwise, his/her account and files may be deleted.

7. IBP is not responsible for any loss of user data generated in any way. Users are responsible for making backup copies of user data and programs.

Article 4

Privacy Protection and Information Disclosure

1. For the use of e-mail and conferences, the same rules apply as for regular mail, wherein the mail message has the character of an open correspondence.

2. The user is required to ensure that his/her messages are addressed accurately and that any unwanted spam of other users distributing chain letters or letters addressed to address lists collected without the consent of the addressee is avoided.

3. The user is required to use the assigned username (mailbox name) when sending an e-mail. Sending letters under false identity with the intention of fraud, intimidation and obtaining unauthorized information is considered a gross violation of the rules.

4. Receiving emails from addresses that violate the provisions of Article 4, paragraphs 2 and 3, may be blocked.

5. Rules governing manipulation with electronic mail are described in detail in the document "Rules of operation of electronic mail in the Institute of Biophysics of the CAS, v.v.i.".

6. The User bears full legal responsibility for the content of their own publicly accessible WWW pages and other information sources, in particular for violating the Copyright Act when copying foreign materials.

7. Files in user directories and system mailboxes are considered to be private data of their owners. Users are entitled to privacy protection, even if they do not protect their directories. Making copies of foreign data and intercepting operation on the computer network to obtain content of messages or data is considered a gross violation of the rules.

8. The administrator has the right to disable any files that are in violation of Article 3, paragraph 1, possibly endangering the security of the system and the computer network (malicious programs, operation monitoring tools, obtaining non-rights, etc.) and the user is obliged to remove them without any delay.

9. IBP is not responsible for any possible data misuse in the transmission and storage of information in the computer network.

10. The administrator has the right to perform all the tasks necessary to perform his / her function, including possible data control and monitoring of a user's activity. If a user uses encryption to encrypt information, he/she is required to make the content of the data available to the administrator in case of doubt as to use within the meaning of Article 3, paragraph 1.

Article 5

Rules for Connecting to the Computer Network

1. The user is required to request the consent of the network administrator:

   a. prior to connecting the device to the computer network,

   b. prior to changing the configuration of the device that could affect performance of the network,

   c. prior to permanently disconnecting the device from the computer network.

   The administrator registers the connected devices in accordance with the Rules of Administration of the IBP Computer Network in Brno.

2. The correct installation of the operating system and network software of the computer connected to the computer network is the responsibility of either the authorized employee designated by the network administrator or the user if he/she is allowed to install the operating system on their own.

3. When managing the operating system and network software of a computer connected to a computer network on their own, the user must comply with the relevant provisions of the IBP Computer Network Administration Rules.

4. The user must not use network address other than the one, which has been assigned to him/her (either automatically or statically) for connection to the computer network.

5. Modems and other means for external access to the IBP computer network can only be operated by the user with the consent of the administrator.

6. The use of the IBP computer network in the framework of scientific and pedagogical cooperation with other organizations is possible only on the basis of a written authorization issued by IBP management.

Article 6

Penalizing Students for Failure to Comply with the Rules of Computer Network Operation

1. Any detected minor breach of the rules of the operation of the computer network gives the network administrator or the authorized person the right to admonish the student.

2. In the case of more serious breaches or repeated minor breach of the rules, the administrator or the person authorized by him/her may remove the right to freely use the computer network services for a predetermined period (maximum of two calendar months) from the student. In this case, the student has the right to appeal to the Director of the IBP.

This appeal has no suspensive effect.

3. In case of repeated or particularly serious violation of the rules, the case will be solved as follows:

   a. on the day of detection of a violation of network operation rules, the student loses the right to use the services of the computer network,

   b. the case is handed over to the Disciplinary Board of the IBP,

   c. based on the proceedings, the management of the Disciplinary Board of the IBP will decide to impose a sanction - this may also be a denial of IBP computer network services for a predetermined period of time.

Any criminal liability is not limited or excluded by this procedure.

Article 7

Penalizing Employees for Failure to Comply with the Rules of Computer Network Operation

1. Violation of the provisions of this Directive will be considered to be a violation of the employee's basic duties (§ 73, para. 1, (c) and (d) of the Labour Code) and may result in the relevant employment consequences, including the termination of the employment relationship.

2. When a breach of rules of computer network operation is detected by the network administrator or the person authorized by him/her, this person will notify the employee who violated the rules, in case of gross violation of the rules, relevant head of the department staff will be notified of this fact.

3. In case of repeated violation of the rules, the case will be solved as follows:

   a. on the day of detection of a violation of network operation rules, the employee loses the right to use the services of the IBP computer network,

   b. the case is handed over to IBP management, which decides on labour law measures.

Any criminal liability is not limited or excluded by this procedure.

Article 8

Final Provisions

1. By signing the "Request for User Account Allocation" users agree to comply with the principles set out in these guidelines, thereby taking note of sanctions resulting from non-compliance.

2. These rules take effect on the date of signature. The rules of the operation of the computer network of 3 December 2003 cease to be effective on the same day.

In Brno on 13. 8. 2015

doc. RNDr. Stanislav Kozubek, DrSc.
Director of the Institute of Biophysics CAS, v.v.i.