Based on Article 5, paragraph 1 and Article 23, paragraph 2 and 3 of the Law on Personal Data Protection (Official Gazette of R. of Macedonia, number 07/05, 103/08 and 124/10), Article 27, paragraph 1 of the Law on Electronic Communications (Official Gazette number 13/05, 98/08, and
83/10) and Article 14, paragraph 1, item 8.3 of the Statute of South East European University, the

University Board, at its meeting held on 07.06.2011 approved the following:

# RULE ON COMPUTER AND NETWORK USE

*Article 1*

When members of the University are granted access to a shared computer system or computer network, they become part of a community of users. This Rule applies to all users of University computers and network resources. Additional policies may also apply to specific systems.

**Computer and Network Use**

*Article 2*

User accounts and network connections (be it via the Computer Centre or a University office) are for individual, work related use. A computer account is to be used only by the person to whom it has been issued. All members are responsible for all actions originating through their accounts or network connections. They must not impersonate others or misrepresent or conceal their identity in electronic messages and actions.

*Article 3*

While the University's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the systems remains the property of the University.

*Article 4*

Unless information is specifically made public or accessible to a member, that member should assume that anything on the network is confidential. Just because members may have the ability, through a loophole, someone's carelessness, etc., to access files, directories, or information that does not belong to them, they do not have the right to do so. Any attempt to circumvent computer, network or file security or to take advantage of security lapses is prohibited.

*Article 5*

E-mail communication is an official communication within the University. Everyone is obliged to read and check their e-mail regularly.

Postings by employees from a University email address to external media should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the University.

Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

*Article 6*

Disruptive and/or invasive actions using computer systems and networks are strictly prohibited. Examples of this include, but are not limited to, viruses, threatening or harassing messages, "spamming", packet sniffing, self-perpetuating programs, excessive volume of file transfers, network traffic or printing, and other programs, files, hardware, software, or actions that deliberately or unintentionally degrade or disrupt system or network performance, compromise or circumvent system or network security, or interfere with the work of others. Due to its adverse impact on the University's systems and networks, the sending of chain letters and similar "pass- along" e-mail messages is explicitly prohibited.

Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.

Port scanning or security scanning is expressly prohibited without authorization from the Director of IT.

Executing any form of network monitoring which will intercept data not intended for the user's host is expressly prohibited, unless this activity is a part of their normal job/duty or if it is used for academic purposes under controlled conditions and with approval of the Director of the IT Department.

Interfering with or denying service to anyone (for example, making a denial-of-service attack) is expressly prohibited, unless this is for academic purposes under controlled conditions and with the approval of the Director of the IT Department.

Using any program/script/command, or sending messages of any kind, with the intention of

interfering with, or disabling a user's session, via any means, locally or via the internet is expressly prohibited, unless this is for academic purposes under controlled conditions and with the approval of the Director of the IT Department.

*Article 7*

Respect for intellectual labour and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement, right to privacy, and right to determine the form, manner and terms of publication and distribution. Because electronic information is easily erased or reproduced, respect for the work and personal expression of others is especially critical in computer environments. The burden of proof of ownership or obtaining permission from the copyright owner is upon the account holder. Upon receiving proper notification, as defined by law, of a

potential infringing activity, the IT Department will where possible remove or block access to the material in question. Verified reports of repeated copyright infringements will lead to termination of computer/network services and/or other University/legal actions.

*Article 8*

The University is obliged to have its computer systems and networks available at all times. However, availability may be affected as part of regular maintenance and other planned and unforeseen activities; or actions taken by providers beyond the control of the University where systems and networks may be unavailable at any particular time. The University reserves the right to restrict or terminate access to its computer and network resources as necessary. The University computer systems and networks are for non-commercial individual use, related to the educational mission of the University, by its faculty, staff and students, and for approved University business activities. The academic staff will be allowed access to lab equipment (servers, computers etc) using remote connections or other methods such as VPN.

The University provides wireless network connection on its campuses, and the IT Department is responsible for promoting the ease of access to this network to clients with user accounts (students, faculty and staff) and others (not affiliated to the university) with guest accounts.

The University provides wired Internet connection in the dormitories. This type of service is for connecting computers for individual use, and cannot be used for installation of rogue devices like access points, routers that may violate the security and privacy of other users.

The IT department will routinely monitor the quality of the Internet connection in the dormitories, and respond to reported problems in a timely manner (within 24hrs of receipt of the report).

For security and network maintenance purposes, authorized individuals within University may monitor equipment, systems and network traffic at any time.

The University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly and user level passwords every six months.

*Article 9*

All users are required to familiarize themselves with the provisions of the relevant Laws of the Republic of Macedonia relating to the use of computers, telecommunications, intellectual property rights, data protection and other relevant issues. These Laws must be respected by all users. Ignorance of such Laws will not be accepted as an excuse for any illegal activity. All users must also abide by all University rules and policies.

*Article 10*

The University will take reasonable steps to ensure that user files and e-mail messages remain private, and does not routinely monitor the contents of user files or messages. However, given the

nature of computers and electronic communications, the University cannot guarantee the absolute privacy of user files and information. Users must take reasonable precautions and understand that there is a risk that in some circumstances others can, either intentionally or unintentionally, gain access to files and messages. Where it appears that the integrity, security or functionality of the University's computer or network resources are at risk, or in instances of abuse of University policies, codes, or the Laws and regulations of the Republic of Macedonia, the University reserves the right to take whatever actions it deems necessary such as monitoring activity to investigate and resolve the situation.

*Article 11*

The University may impose restrictions on the use of its computer and network systems and/or take additional actions in response to verified complaints of violations of this Rule or other University policies, or codes, or the Laws or Regulations of the Republic of Macedonia.

**Content**

*Article 12*

The University reserves the right to remove any material from the system with prior notification. Information sponsors and providers are responsible for ensuring that their information complies with the following standards:

- Any information placed on the University's intranet or web-page must be suitable for distribution to both the campus community and, potentially, the rest of the world.

· Some examples of suitable material are: calendars or announcements of upcoming events; descriptions of services offered; course descriptions and schedules;
· Some examples of material that would be considered inappropriate are: commercial advertisements, endorsements or logos except when used to recognize sponsorship, further the academic mission of the University, or promote a University business service offering; material that is illegal; confidential information

- Material should be checked for accuracy and updated regularly;

- Copyrighted material may only be posted with the permission of the copyright holder.

- The format of material must conform to the University standard page layout and design.

- Every document must contain the following information:

· The provider's name, organization, and e-mail address
· The author of the document (if different from the provider)
· The document's last revision date
· Any known problems with the information

**Reporting Violations**
*Article 13*

If a user believes that a violation of this Rule has occurred, that user should notify the Director of the IT Department in writing.

**Concluding Provisions**
*Article 14*

This Rule comes into force from 01.09.2011