



PRIVACY STATEMENT of USING JU NETWORK

General

1. Users must comply with all legislations to access and use of the JU network.
2. Computer Center can ask the user to provide with her/his personal information in order to provide her/him with some services.
3. University is responsible for providing user with Internet Browsing, Anti Virus and JU-specified Applications unconditionally.
4. Each user cannot access JU network restricted services unless via a user code and a password.
5. A user is responsible to obtain his account information via the provided request form.
6. A user is responsible to keep his account information secret. Any sequences upon giving the account information to other users are not the university's responsibilities.
7. The network is a limited resource and users must use it in an equitable manner taking account of the rights and needs of others.
8. A user understands that the university monitors access to, and use of, the network to ensure compliance with legislations and University rules, regulations and policies, and to verify that privacy is approved. Access contents are not monitored. This information can be used to investigate incidents and crimes.
9. A user agrees that the university can keep their actions on JU network services. University has the right to keep the information as long as it decides. This information can be used to prove incidents and crimes.
10. A user understands that JU network performance cannot function with 100% efficiency due to substantial costs spent on administration and security.
11. All university network users are responsible for notifying the university authorities of possible breaches of the conditions documented in this statement. In such case, a member must notify the Internet and Network Security Section by phone or via e-mail.
12. A user cannot use another individual's account, or attempt to capture or guess other users' passwords.



13. To apply for any service of Computer Center, a staff member has to apply for the service by its related form.
14. If a virus file has come from inside the University (i.e. is not caused by a removable disk or file), then you should contact the Computer center immediately and inform the owner of the source PC.
15. Exporting software, technical information, decryption software or technology, in violation of international or regional export control laws, is illegal.
16. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.), is illegal.
17. Any attempts to change Network Connections without permission of Computer Center are illegal. The privilege of connecting and changing network connection is given exclusively to the Computer Center.
18. Violations of the rights of any person or university protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by university.
19. A user understands that Internet use is ethically restricted on research, learning and work-related topics.
20. Using Internet is practically controlled as shown in the following policies; [Staff Policy](#) , [Students Policy](#) , [Dorms Policy](#) , [Graduated Studies Policy](#) .Where some URLs are blocked.
21. A user understands that JU is not responsible for his/her actions on Internet; a user is the only responsible party for what the user browses, downloads, writes or uploads via Internet.
22. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which university or the end user does not have an active license is strictly prohibited

Mail

1. A user understands that has to apply for an e-mail account using the specified form in order to initiate an email account and have a user code.



2. A user understands that System and Mail administrators do not keep passwords as plain texts. Passwords are kept as encrypted texts and they are unreadable. The user has to change the first password given to him by Mail administrators.
3. The mail user is the only responsible party for the user's sent mails via JU mail.
4. A user understands that JU has the right to monitor the mail access including email header and size, e-mail contents are considered highly private and they cannot be viewed.
5. All the following uses are highly restricted; any of the following actions will be officially questionable.
 - a. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
 - b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
 - c. Unauthorized use, or forging, of email header information.
 - d. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
 - e. Use of unsolicited email originating from within university networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by university or connected via university network.
 - f. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).