August 2011

rules.

FOR THE USE OF THE IT INFRASTRUCTURE AT THE MCI:

(1) Scope of the Rules:

These Rules for the Use of the IT Infrastructure (hereinafter referred to as the "Rules") govern the use all IT services made available by Management Center Innsbruck - Internationale Hochschule GmbH (hereinafter called "MCI"), and in particular the use of the IT infrastructure (including all hardware and software) by students of the MCI (hereinafter called "users").

(2) Authorized use: Use of the IT services at the MCI is only permitted for purposes relating to the study programs and scientific working, and in particular for purposes of research and teaching. Such use includes computer-aided teaching, project and class work, and organizational procedures relating to the study programs. The user is aware of the fact that scientific working has priority over all other purposes.

(3) Rights and duties of the user:

To the extent that resources are available, the user is entitled to make careful, considerate and responsible use of the IT infrastructure and other facilities and services made available by the MCI as necessary for the purposes defined in Section 2. Any malfunction or defect that occurs and any damage caused must be reported by the user without delay.

- The user undertakes not to perform any actions that are contrary to authorized use and in particular not to misuse the IT infrastructure in any of the ways listed in the annex.
- The user must maintain secrecy with regard to passwords and/or codes required for access to the IT infrastructure and must change them regularly. In the case of any misuse or damage resulting from the disclosure of any such passwords or codes to any unauthorized persons or any other unauthorized use by third parties resulting from the acts of the user, the user shall be responsible to the MCI for all consequential damage in accordance with the provisions of the law of tort.
- In the case of all messages sent or forwarded by the user via local, national or international networks (e.g. Web pages, FTP, e-mail, Usenet News, etc.), the identity of the person responsible for the content must be clearly indicated. The user must not send or forward any communications that could endanger public order, security or morals or infringe any laws or these Rules.
- The user is not authorized to install any software nor to make any changes to software already installed.
- All misuse of the IT infrastructure, including the unauthorized copying, storage, provision or publication of software or information made available via MCI's IT services is forbidden. The user shall indemnify the MCI in full and hold it harmless for all claims relating to any such misuse lodged by a licensor, proprietor or other authorized party.
- The user undertakes to assist the MCI and any organization collaborating with the MCI in any investigations relating to misuse of or damage to the IT infrastructure. All instructions issued by authorized personnel relating to the use of the IT services must be followed without delay.

MCI®
MANAGEMENT CENTER
INNSBRUCK

(4) Exclusion of users:

MCI is entitled to exclude individual users or groups of users from using its IT services in whole or in part should that be necessary to maintain or restore normal operations with said services. The use of MCI's IT services can also be refused in whole or in part for reasons of capacity and data protection. Use of said services can be refused in particular where the use involved is incompatible with the work and objectives of the MCI. The MCI can accept no responsibility for loss or damage arising out of the user's exclusion from its IT services in whole or in part.

(5) Data storage:

Through the act of depositing data in an area of an IT system in which data storage is performed, the user explicitly consents to storage of said data. That also includes cases where the data continue to be stored even after the user has taken steps to delete them. Ultimate responsibility for data security rests with the user him/herself. The MCI can accept no responsibility for the uninterrupted and errorfree functioning of its IT services including any data storage facilities offered and/or operated. The MCI accordingly excludes all liability for direct or indirect loss of or damage to any data processed and/or stored in the framework of its IT services. The MCI also reserves the right to make changes with or without prior notice to the parameters of its data storage facilities, including temporary data storage on its "T:\" network drive, for which there is no back-up and from which data are actively deleted once a week.

(6) Content of data and messages:

The MCI can accept no responsibility for the content of data stored by users or of messages generated, sent and/or received by them (e.g. mails, news). The MCI accordingly can accept no liability for any criminal or illegal content found on data carriers or in memory areas put at the disposal of users. Nor can the MCI accept any responsibility for unauthorized access to confidential data.

- Should the MCI discover or learn about data with illegal content in the process of its monitoring procedures or by any other means, access to the content concerned will be denied and/or the data deleted where deletion is reasonable and technically and legally possible.

(7) Records and evaluation:

The MCI is entitled to keep records of the use of its IT services by individual users where that is necessary in the interest of normal system operation and administration, resource planning, protection of the personal data of other users, or the detection and prevention of illegal or abusive use as long as the keeping of such records is not contrary to any mandatory legal provisions. Where necessary to eliminate a fault or to investigate and terminate any illegal or abusive use, the MCI is entitled to inspect user data.

(8) Liability of the MCI:

The MCI can accept no responsibility for the uninterrupted and errorfree functioning of its IT services. In particular no liability on the part of the MCI and/or its employees can be entertained for any kind of loss or damage suffered by the user as a result of any fault or defect in the IT infrastructure including any software or hardware supplied by third parties. Nor can the MCI accept any liability for the correctness, completeness or up-to-dateness of any information to which it merely provides access.

(9) Users are kindly requested to keep themselves informed with regard to new developments and changes, including changes to these Rules, by regularly visiting http://www.mci.edu/terms.

ANNEX: MISUSE OF THE IT INFRASTRUCTURE INCLUDES THE FOLLOWING

(A) Use of electronic communications for attacks on individual persons or groups of persons (Netiquette)

1. Dissemination or circulation of information that is demeaning or insulting to persons for reasons of race, nationality, faith, gender, political leanings or sexual orientation
2. Sourcing and dissemination of personal or other privileged information about an individual person or group of persons
3. Repeated and unwanted dispatch of information

(B) Use of electronic communications with the intention to hinder others in their work

4. Occupying resources beyond the authorized extent
5. Electronic mass mailing (spam)
6. Sending or forwarding electronic chain letters
7. Manipulation of electronic data
8. Accessing third-party data without explicit consent

(C) Infringement of intellectual property rights and disclosure of access codes

1. Illegal use, copying and dissemination of material protected by copyright. This includes the use of file-sharing services/clients (e.g. LimeWire, RapidShare, eMule, Azureus, BearShare, BitTorrent, etc.) and also applies to data imported via third-party devices.
2. Disclosure of access codes to third parties, whether for payment or not, unless the MCI has given explicit written consent

(D) Use of electronic communications for attacks on computers, the network or services offered via the network

1. Port scans (automated network scanning for servers and services) except for security checks in consultation with the system administrator
2. Unauthorized control over resources or the attempt to gain unauthorized control (hacking) except for security checks in consultation with the system administrator
3. Damage to or interference with electronic services (denial of service attacks)
4. Dissemination or circulation of virus programmes, computer worms, Trojan horses and any other malware
5. Phishing or attempted phishing for passwords (e.g. using password sniffers)
6. Manipulation or falsification of mail headers, electronic directories or other forms of electronic information, and the assumption of a false identity (including IP spoofing etc.)
7. Any form of manipulation of electronic data

These Rules were drawn up in the framework of a project for the Management and Law study program. We are grateful to the students of the 2002 year group and to Prof. (FH) Ralf Geymayer as program director. IT-Services: Prof.(FH) Peter Mirski.

MCI®
MANAGEMENT CENTER
INNSBRUCK