

# IT Policy

## Date 17.09.2009

To guarantee the computer network's security, every student is obligated to abide following *user regulations*:

Students are allowed to use computers which are *assigned to the students*.

It is interdicted to download and/or install *programmes while* using the University's computer.

The students are responsible for the confidentiality of the *user ID*.

The data *saving* of local data is incumbent upon individual responsibility.

Students are liable for the abidance of the *statutory provisions*, especially concerning the copyright while using the University's computer.

It is illegitimate to use *peer-to-peer file sharing* for all kinds of data.

Furthermore, students have to verifiably take notice of the declaration which contains the abidance of the *data secrecy* (according to § 15 Data Protection Act 2000).

The students are obligated to refuse external people the *access* to the computer and lecture rooms, to treat the *equipment* extremely carefully and to keep the password given from the degree program a secret.

Moreover, students are not allowed to *drink* and *eat* in the computer and lecture rooms.

Following *limitations* are valid for the *electronic resources*, which are provided to the students:

### **a. Memory capacity limitations:**

- Z:\drive – max. 425MB
- Total e-mail account volume – max. 500 MB
- Saving time of alumni e-mails – 150 days
- No data on LAB-PCs

### **b. Following points are obligatory for every student**

- care of the Z:\drive
- care of the e-mail account
- acceptance of the memory capacity limitations
- immediate announcement of possible security vulnerability to [support@imc-krems.ac.at](mailto:support@imc-krems.ac.at)

### **c. The points below are strictly interdicted for every student:**

- changes of provided hardware (Lab-PCs, surf stations...)

- sending spam mails (e-mails to more than 5 recipients without direct relation to the course)
- transmission of all kinds of passwords
- use of passwords under 6 signs
- saving excessive private data on the Z:\drive
- any kind of trying to avoid the security mechanisms
- saving foreign software on the Lab-PCs

**d. Besides, following is to consider:**

- broadly manners on the eDesktop

In case of *contempt* against the user regulations, the *user ID* of the particular student gets locked for at least 3 working days.