

March 2002  
JBN/MC

## **RESPONSIBLE USE OF COMPUTERS** (Students and Staff)

### **1. Objective**

The Engineering College of Aarhus (IHA) make computer systems and programs available in connection with work and studies. The means to achieve the necessary security is a combination of rules and a sense of responsibility of the users. This document is therefore a combination of concrete technical instructions and directions, which are not necessarily exhaustive. The rest will be classified as “responsible use of computers”. The document also contains guidelines for supervision and control of activities taking place on the Internet plus information on sanctions if existing rules and norms are broken.

Computer security is, among other things, about avoiding the following:

- unauthorized use of computer systems
- illegal use and copying of software and
- compromising data (meaning that unauthorized persons get unjustified access to data).

Staff will be informed about the rules on direct application.

At the drawing up of their user account, students will sign a document saying that they are familiar with the rules and will obey them.

### **2. Access**

Access to IHA’s computer facilities require a valid user-id. A password is personal and may not be passed on or lent to anybody.

### **3. Equipment**

You may not connect your own equipment (computer or other) to the net without specific permission from the IT Department. You may not change the arrangement or connection of the equipment or the configuration of the net printers.

### **4. Software and data**

Most of the software that can be found on the systems are subjected to license regulations, which forbid copying and use of software on other machines. Thus it is illegal to copy any software without prior approval by the IT Department, not even if it were technically possible to carry out copying without breaking the security system.

The individual user has user rights (unless otherwise decided) to data and programs in his/her own file systems, and it is not legal to obtain access to those of other users without previous arrangement with the person in question.

Staff can for work-related purposes install programs locally, if necessary license has been paid and the programs do not change the functionality of the systems.

## **5. Generally on priorities and use**

Computer equipment and software are available for work-related use, but private use is accepted to a limited extent.

Pause/screen-lock in group rooms and data bars is allowed for a maximum of 10 minutes.

Commercial use of equipment and software is not allowed.

The use of computer equipment in group rooms and data bars is prioritized in the following way:

1. Scheduled activities
2. Other study-related activities
3. Non-study-related activities

When a workplace in a data bar is abandoned, log-off must take place, printouts and notes must be removed and manuals/books must be cleared away (general tidying up).

After 14:15 all equipment must be turned off in group rooms and data bars when workplaces are abandoned. In other respects, the general clearing-away rules of IHA apply.

Back-up of students' user-files is not carried out. It is thus up to the individual student to see to this.

## **6. System administration, access to data**

The institution management does not monitor the use of E-mails and Internet. In required cases, for example in connection with suspicion of misuse, cf. present rules, information of reading of logs will be supplied in advance to the person(s) in question and to the relevant confidential organizations. E-mails which in this connection are marked "Confidential" in the subject field will not be read.

In connection with the system administration of IHA's servers etc., it is necessary for IHA's IT staff to obtain access to user data and programs, including monitoring of mail traffic. This only takes place in case it is required for technical and security reasons, a.o. at illegal or inappropriate use of the systems, and information related to this is covered by professional secrecy.

The registration (logging) makes it possible to trace every activity to a specific workstation on the net. The level of details makes it possible for example to read what web-pages are being visited. There is no time limit to the logging.

## **7. Network connected systems**

Via networks like IHANET (IHA's LAN), Sektornet and Forskningsnettet, NORUnet a.o., the systems are connected to many other systems (the Internet), which are run by other organizations and companies.

Systems and net connections may only be used to communicate with other systems via definitely public net services such as www-browsers, anonymous file transfer and electronic mail. Other systems (such as terminal protocols, remote executions etc.) may not be used without prior permission from the relevant organizations in the form of user registration.

### **8. System protection**

In connection with the use of network, harmful programs (viruses) can occur, which can be spread both intentionally and unintentionally. The security measures in force at the time in question must be observed in this connection.

### **9. Use of resources**

All resources in the form of storage capacity and network traffic etc. are limited and should therefore primarily be used for their purposes, i.e. education, development and administration. Efforts must be made not to use unnecessary resources.

### **10. Web-publication**

To be written.

### **11. Sanctions**

Violation of existing rules and guidelines can lead to oral or written action.

For students it may be a question of temporary or permanent withdrawal of the right to use IHA's computer systems or parts of these.

In serious cases, it may be a question of expulsion from the Engineering College.

Criminal code offence will be handed over to police investigation.

*The present rules were presented to and approved by the Liaison Committee in February/March 2002*