Guidelines on the usage of IT-systems at the University of Southern Denmark July 2006

This document is a brief summary of the guidelines for good IT-behaviour, as the University expects from all its users, together with information on the sanctions in case of misuse.
The detailed guidelines and rules are found in

- *IT-sikkerhedshåndbog for SDU;*
- *Personalepolitiske retningslinier;*
- *Regler om disciplinære foranstaltninger overfor de studerende ved Syddansk Universitet;*
- *Regelsættet for SDU's web-system;*

(unfortunately the above mentioned documents are only available in Danish for the moment) and in national and international provisions and regulations. Furthermore might administrators of local systems connected to the SDU network issue supplemental guidelines.
The user confirms, by signing this document, agreement in abiding the guidelines and be familiar with the fact, that the above mentioned supplementary guidance must be complied with as well.

Any attempt on abuse, whether successful or not, will result in disciplinary actions, e.g. exclusion from network and system access for a shorter or longer period. Disciplinary actions should in all cases be sanctioned by Rector.

1. General guidelines for usage of IT-systems

When a user has received a *user-id*, providing access to the network and servers, the user is responsible for all actions carried out by this *user-id*. Loan or sharing of *user-id* with others is not allowed. Should it happen anyway, the owner of the *user-id* is personally responsible for all actions carried out by the borrower. Acquisition or retaining of *user-id* under false conditions is a violation causing disciplinary actions.

Usage of IT-systems at SDU should be carried out with due prudence and for solving tasks in connection with work and study at SDU. It is not allowed to use the IT-systems in a way that might harm the reputation of SDU. It is permitted to use the IT-systems for reasonable private use, e.g. informations search and electronic mail (e-mail).

The following activities are not allowed:

- Deletion, examination, copying or modification of other peoples files and/or data without their preceding acknowledgement.
- Attempts to cheat or modify allocated resources on IT-systems.
- IT-systems is a limited and valuable resource and should be handled with the same care as other resources, e.g. equipment and furniture. Continued unrestrained usage of system ressources, causing inconvenience for other users, should cease as soon as it is brought to the attention of the person involved.
- Any usage of the University's systems or services for commercial purposes or purposes irrelevant for the university. However, the students are allowed to offer their used educational books for sale via the university's IT-systems.
- The IT-systems must not contain any advertisements.
- Personal websites must not have any content not applying to the rules stated in "IT-sikkerhedshåndbogen" or "Regelsættet for SDU's websystem".
- Any kind of unauthorized, premeditated action, which might destroy or interrupt the normal function of a system, change the normal function or provoke other errors on the system, is a violation, no matter where the system is placed and for how long the action is taking place.

2. Guidelines for usage of electronic mail

Any time a user is sending electronic mail is the users *user-id*, as well as the university's mail-address included. For this reason, the user has the responsibility for all mails, sent from the *user-id* of the involved person.
As a result are the following actions not allowed:

- Falsification (or attempts for falsification) of electronic mail.
- Any attempt to read, delete or copy other users electronic mails.
- Any attempt to send annoying, obscene or threatening mails.
- Any attempt to send *junk mail*, chain letters, spam or similar kind of mails.

3. Network security

Users of SDU-net have access to other networks and the systems connected to those networks. As a result, the following actions are not allowed:

- Use of networks and/or the connected systems with the purpose of getting unauthorized access to other connected systems.
- Use of networks and/or the connected systems with the purpose of avoiding or circumventing restrictions, normally attached to the use of a system.
- Decryption of system- or user-passwords.
- Copying attempts of normally inaccessible systemfiles.
- Copying of copyrighted material, e.g. thirdparty programs, without the consent of the owner or a valid license.
- Attempts to stop the network, destroy its functionality or gain unauthorized privileges.
- Deliberate actions, which might destroy or interrupt the operation of the university's network or systems, as well as any external system.
- Establishment of access to the network by any nonofficial VPN, FTP or wireless service, e.g. setting up an unauthorized wireless accesspoint.
- Scanning the network for IP-addresses, ports and services.

4. Usage of licensed electronic resources

The library subscribes to a number of electronic resources (e-magazines, bibliographical databases etc.). According to the licence agreements, these resources must only be used for personal study- and/or research purposes. As a result, the following actions are not allowed:

- Commercial use of materials from these resources, also not in connection with practical training in industri.
- Handover of personal passwords to others.

5. Other items

The users should be aware of the fact, that any activity on SDU's IT-systems is logged. These logs are used for error solving, assuring of operational reliability, as well as protection against virus, spam etc.. A further description of these logging activities can be found in ""IT-sikkerhedshåndbogen", chapters 7.6.4, 8.6.2 and 8.7.2.

Electronic mail is subject to the same confidentiality rules as ordinary mail (secrecy of the mails). Electronic mail users should be aware, that other might be familiarized with the content of e-mail due to system errors, misdirected addresses or if a system administrator has to conduct a comprehensive review of a system due to technical problems.
System administrators and other technical staff are subjected to duty of professional secrecy, but the same does not apply to potential receivers of misdirected e-mails.