IT Regulations at NTNU

Approved June 14th 2005.

(Note: this English translation is for information only.
For all legal purposes the original document in Norwegian is the authoritative version "Vedtatt av rector på fullmakt 14.06.2005")

1 Area covered by these regulations:

These regulations cover all use of NTNU's computer system.

1.1 Definition of NTNU's computer system:

- All physical components (computer networks consisting of cabling and network electronics as well as general or specific computers), software and other IT-based resources provided, or used by NTNU.

The regulations also cover private equipment when connected to NTNU's computer system as well as licensed software at NTNU which is installed on private equipment. (See Section 5.2)

1.2 These regulations cover all use of the Internet (including the World Wide Web and e-mail).

1.3 The operational administrator at the faculty/unit at NTNU or other groups that manage parts of the computer system are obliged to make sure that these regulations are followed.

2 Definitions:

User: A person who has obtained permission to use a computer system at NTNU.

User-account: A user's defined access to one or more computers with additional personal storage space, and rights to read and write data and use programs.

User-name/User-ID: A unique symbolic name that identifies a user of a computer or a computer system.

System-user (System-user's ID, System-user's account): User-names that are used for administration purposes such as *root* and *admin*. These users appear in the computer system with non-personal User-ID's and non-personal User-accounts.

Password: A personal key. The password must be used in addition to the User-ID to access a User-account or another area of limited access.

Operational administrator: A person responsible for the operation of a computer or a computer network. The operational administrator will also be a user, but with special rights and duties.

The network: NTNU's computer network and all other networks that are directly or indirectly connected to NTNU's network. Where the regulations only apply to NTNU's computer network, this will be specified.

Defined parts of the network: (expression used in Section 7.1). A part of the network that can be separated from the remainder of NTNU's computer network and treated individually. Examples of such are a computer workshop,

a subnet, a single room/apartment in a student village, a student village or a group-room at a department.

User-administered parts of the network: Parts of NTNU's computer system managed by users who are not IT staff employed by NTNU. Examples of such equipment are workstations and servers in offices, group-rooms, student villages or private computers connected to the network.

3. User-account, User-name and user's password

3.1 Users of NTNU's computer system must be registered users with User-names allotted by NTNU. Other users can be given access if this is explicitly stated in the connection agreement between the given unit and NTNU. From computers located on the user's premises, family members have permission to use NTNU's network as a transit network to outside networks. For these other users, separate authentication is required. Family members cannot use the NTNU user's User-ID, see Sections 3.2 and 3.4. Also see Sections 4.1 and 4.3.

3.2 User-accounts are strictly personal accounts. Logging on or attempting to log on with other users' User-name and/or password is forbidden. It is also forbidden to identify oneself as somebody else in all use of the computer system.

3.3 When opening a User-account, the operational administrator is to make sure that other users do not have access to the user's personal storage space.

3.4 The user is obliged to keep the password secret from others. System-users are obliged to insure that their passwords are only familiar to those who are entitled access to them.

It is forbidden to loan passwords to others or help other users to gain access NTNU's computer system by any other means. If the user knows of, or suspects that an unauthorized user has learned the user's password, the user is obliged to immediately change the password.

4 Information and following the regulations

4.1 To get a User-name in NTNU's computer system, the IT Regulations at NTNU must be read and accepted.

4.2 Users of NTNU's computer system are obliged to keep themselves updated with changes in all parts of the IT Regulations. The IT Regulations are published on NTNU's web site.

4.3 The operational administrator of the user-accessed parts of the network, which gives users access to use the network, must inform users about the IT Regulations and ensure that the users follow the regulations. The operational administrator also has to make sure the users have legal access in accordance with Section 3.1 in the IT Regulations.

If there is violation of the IT Regulations from the user-accessed parts of the network, this part can be partly or totally disconnected from NTNU's computer network. The operational administrator can be reported to NTNU for violating the IT Regulations. The administrator's access to NTNU's computer system can be disconnected in accordance with Section 7.

5. Use of NTNU's computer system

5.1 NTNU's computer system is only to be used for academic, administrative, research and teaching purposes. It is not be used for advertising or commercial purposes without obtaining written permission from the University Director in advance. Exceptions are student organizations which are allowed to publish links to sponsors (if any), in accordance with specified guidelines.

Users must follow the guidance from the operational administrator when using the computer system during times of resource shortage.

5.2 The user is not to use NTNU's computer system to commit an action that is illegal according to Norwegian law. Examples of this are writing libellous or discriminatory statements, the invasion of privacy, the distribution of pornography or the dissemination of classified information.

Classified information is to be handled in accordance with NTNU's Information security policies and NTNU's regulations for handling personal information.

5.3 The programs installed in NTNU's computer system that according to licence agreements can be installed in private computers, are offered to users on the conditions set by the owner of the program in question and that are stated in the licence agreement. Teaching aids and other electronically distributed material placed at the users disposal by NTNU via the computer system must be used in accordance with specified licences. The user is not permitted to copy any software or any other material without making sure that this is authorized by the "Åndsverkloven" (the Intellectual Property Act), or by prior agreement with the owner holding the copyright.

5.4 The user is obliged to investigate if the material/work that he/she publishes on web pages or otherwise make available to others using NTNU's computer system is copyright material/work. If a copyright licence protects the material/work, the user is obliged to get authorization from the copyright holder prior to any such publication.

With regards to musical material/work, the user is always to investigate whether the owner of the material/work has entered into a copyright agreement that protects the material/work against unauthorized distribution, reproduction etc.

If a copyright agreement exists, the user must get authorization from the copyright holder/representative (TONO) or the record company, before the music is to be distributed via NTNU's computer network.

The logo of NTNU is copyright material and is only be published on NTNU's official web pages on the World Wide Web.

A photograph portraying a person is only to be published if written permission is given by the person in question or if this is covered by the cases stated in "Åndsverkloven" § 45c.

The user is personally responsible for any possible legal action or financial demands against the user for distributing work/material without authorization.

5.5 NTNU has no responsibility for any financial loss caused by errors or deficiencies in programs, data or information found via NTNU's computer system, databases or other sources.

5.6 Reading, writing or copying files in another user's personal storage space is forbidden unless one has explicitly been give permission from the user in question to do so. Breaking in, or attempting to break into others' computers through NTNU's computer network is forbidden.

Monitoring computer activity on the network is illegal except when done by IT-personel working with network security network maintenance.

5.7 It is forbidden to commit actions that illegally block other computers from the network or that intentionally try to stop data transfer to and from other computers.

It is forbidden to distribute programs or other materials, such as a computer virus, that is causing network instability or harming the network, stored material or computers and components that are connected to the network.

5.8 A user is obliged to report to the operational administrator about circumstances that he/she understands or assumes may have signification for the security and operational stability of the computer system.

5.9 The operational administrator can impose routines on the user to insure the functionality of the system and operational reliability.

5.10 The operational administrator only has access to use operational logs to identify a single user or his/her use of the network, or to log into a user account in order to:

1) manage the system and insure the system's functionality
2) assist a user when the user has given permission to do so in a particular case
3) unveil/clarify possible violations of security issues
4) determine the facts when there is reasonable cause to believe that the user has violated the IT Regulations and that this could be of significance for the responsibilities and reputation of NTNU

Regarding items 3) and 4):

The University Director or the University Director's representative must give authorization in advance to taking such action, unless substantial circumstances demand immediate action. These substantial circumstances must be documented for the University Director following the incident.

Regarding item 4)

Authorization must also be given by the user in question.

6. Termination of employment or completion of studies

6.1 When terminating a contract of employment or finishing studies at NTNU, the user must clear his/her account. Files belonging to matters that the employee has handled must be presented to the employee's superior for consideration. The files must not be deleted until the faculty or unit that the employee belongs to has authorized this. Files that do not belong to particular matters must be presented to the employee's immediate superior who will decide if the files should be deleted or not.

6.2 When closing a User-account, the operational administrator will block the account for further use. The remaining contents in the account will be deleted 3 months after the account was closed.

6.3 Material belonging to NTNU must be returned. All copies of software, documentation and data owned by, or rented out by NTNU, must be deleted on private equipment.

6.4 The right to connect private computers to NTNU's network ceases with the termination of a contract of employment or completion of studies.

7. Sanctions in cases of violation of the IT Regulations

7.1 If there is violation of the IT Regulations, the user's access to NTNU’s computer system can be partly or completely disconnected. To clarify whether a user has violated these regulations or not and determine the circumstances surrounding the incident, the administrator can disconnect the user for up to 5 working days.

When violation of the IT Regulations is traced to user-defined parts of the computer system, the connection between this part and the rest of NTNU’s network can be partly or completely disconnected. To clarify if there has been a violation and to insure against future violations, the operational administrator can close the connection completely for up to 5 working days. The University Director or the University Director’s representative will decide if the connection to NTNU’s remaining network also should be partly or completely disconnected.

7.2 Violation of the IT Regulations should be reported to the faculty or unit where the person in question works/studies and this body will decide if the user's access to NTNU’s computer system should be partly or completely disconnected. The faculty or unit must also decide whether the violation should lead to disciplinary action.