Validated: 3.6.2010	Validated by: Tuula Teeri, President
Co-operation procedure: 27.4.2010	Reviewed: 18.4.2012 (version 1.1) Vice president Ilkka Niemelä

POLICY OF SANCTIONS FOR IT OFFENCES AT AALTO UNIVERSITY

Contents:

Contravening the policies and regulations issued for the use of Aalto University information systems, or using the information systems in violation of Finnish law, is considered an IT offence.

This document (hereafter “policy of sanctions”) describes measures that are to be taken against a person after an IT offence has been detected or when there is just cause to suspect an offence. Measures are divided into restricting user rights *during an investigation of* the offence and any *sanctions* determined as punishment for the offence.

The policy of sanctions focuses principally on the university's degree students and employees. The following groups of people may also have user accounts on the university’s information systems:

- Researches and Emeriti working under external financing
- Employees of third-party service providers
- Post-graduates and open university students

Due to the heterogeneity of these user account holders, any IT offences will be dealt with on a case-by-case basis.

Any IT offences detected, and any subsequent measures taken, will be reported to the university's chief information security officer.

1 Restricting user rights for the duration of an investigation

User rights may be restricted either by suspending some or all of the user's accounts or by otherwise preventing the use of an information system (e.g. by removing the right to change data).

During an investigation:

- *A student* will primarily have his or her user account suspended and he or she will be called in for a discussion with the chief information officer/security manager or the person administering the system

- The user rights of an employee will be restricted as needed. In cases involving network disruption, the restriction can also be the disconnection of the work-station from the network.

User rights will always be restricted when

- there is reasonable cause to suspect that the person could be guilty of abuse, AND
- it is possible that the user could hinder the investigation of the offence or the minimization of the damage unless access is restricted

Decisions on restricting user rights during an investigation will be made by the owner of the information system, the head of the unit or other person appointed for the position. Restrictions will be implemented by the administrator. In urgent cases, the administrator can decide to restrict user rights for a maximum of three days, and the restrictions will immediately be reported to the person in charge of the restrictions.

The restriction of user rights for the duration of an investigation may be cancelled when the matter has been investigated and it is evident that returning user rights poses no apparent harm. The user in question can expedite the investigation by actively co-operating with investigators.

2 Sanctions

In minor cases, the user will be reprimanded for inappropriate activity.

As a result of an IT offence, a person can be held liable for the following:

- misused resources (e.g. machine time)
- any direct damage caused by the misuse
- the costs for investigating the misuse

2.1 Students

Sanctions for *a student* may include restricting access to information systems (suspending user accounts), administrative measures within the university (written caution, suspension for a fixed period) [1] and reporting the offence to the relevant authorities (if the offence is punishable by law).

The IT director decides on the suspension of user accounts. The period of suspension does not include any suspension enacted for the duration of an investigation. The student's co-operation in the investigation may, however, be taken into account, and may lead to the suspension period being shorter.

Decisions in regard of a written caution to a student will be made by the rector of the university and in regard of a suspension for a fixed period by the board of the university. User access will be cancelled for the duration of the suspension. The mini-mum total length for the restriction of user rights will, however, be as stated in the appendix (degree students, employees, others).

2.2 Employees

Sanctions for *an employee* include measures governed by labor laws and carried out by the university as an employer (written caution, giving notice, termination of employment) [2], as well as the reporting of the matter to the relevant authorities (if the offence is punishable by law).
Cautions are issued by the schools' dean or director of human resources. In case of termination of employment decision is done by school's dean or director of

1 Universities Act section 45

2 Employment Contracts Act Chapter 7, section 2 of, Chapter 8, section 1

human resources (Aalto shared units). The matter is prepared by the HR lawyer in co-operation with human resources manager. User rights to individual systems may be suspended for a specified term or rescinded altogether if loss of confidence has arisen due to abuse.

3 Tables of sanctions

The tables in the appendix outline recommended sanctions for IT offences for the university's degree students, employees and others.

The tables contain examples of typical offences linked with the use of information systems, grouped by the seriousness of the offence. In addition to the seriousness of the offence, sanctions will be more severe if it can be shown that the offence was premeditated or otherwise intentional.

In the “sanction” cells, the topmost row is reserved for the possibility of reporting the offence, the next row is reserved for general administrative measures and the bottom row for measures concerning the use of information systems and/or sanctions decided upon by the IT director.

If the person is both a student and an employee, the rules for employees will be applied. However, the rules for students may be applied if the offence or the person's type of employment gives specific reason to do so.

3.1. Concepts

Handling of illegal material

- *material subject to criminal law* can include child pornography, material dealing with bestiality or raw violence, racist material and demagogic material
- *handling* can include possession and distribution of material

Material subject to copyright law can include music, videos, comics, movies, games and software.

A service is a function that can be used from outside the machine, such as the following:

- email services (SMTP, IMAP, etc)
- file transfer service (SFTP, HTTP, SCP, etc)
- peer-to-peer network service (Kazaa, eDonkey, etc)

Handing over an ID can include disclosing a password to another user or leaving a session open so that another person can use the user account.

Endangering information confidentiality can include the following:

- handing over information classified as confidential or otherwise protected by law to a third party. This can include disclosing server user information.
- negligence with regard to the security of confidential information. This can include processing information using a system with insufficient protection.
- breaching an obligation of secrecy
- violating the Personal Data Act

Negligence of personal data security can include leaving a password exposed.