Consequences of IT service abuse in brief

The University's IT service rules bind and obligate all users of IT services and systems. Including you.

The term 'IT service abuse' refers to service use in a manner that is against the IT service rules or applicable laws. All detected cases of abuse must be reported to TUT security specialist, system administrator or according to other given instructions.

In case of suspected abuse, the University can restrict the user's access to services for the duration of the related investigation. Depending on the severity and intentionality of the act, service abuse can lead to consequences within the University or be reported to the police.

Further specifications to these rules are provided below.

Consequences of IT service abuse

IT service abuse means activities that are against the University's IT service rules or Finnish laws.

This document outlines the measures applied to the suspected party when a case of IT service abuse has been detected or there is justified reason to suspect such abuse. The measures range from restricting access rights during the investigation of a suspected abuse case to implementing actual consequences after the abuse has been confirmed.

The University can restrict access to IT services during abuse investigation

When a breach of IT service rules has been detected or there is reason to suspect one, the University can decide to set access rights restrictions to the user in question. Access rights are restricted whenever there is justified reason to suspect that a user has abused the services and that the continued use of his/her rights would harm the investigation of the case or hinder damage control. When necessary, the user is invited to a hearing.

The decision to restrict access rights is made by the IT service owner, unit head or another authorised person. The restrictions are implemented by the service's system administrator.

In urgent cases, the system administrator can independently set access restrictions for a maximum of three days, and this must be immediately reported to TUT security specialist and head of information management.

When necessary, a user's workstation can be disconnected from the network.

The access restrictions can be removed once the investigation is completed, if the restoration of the user's rights does not pose an evident risk.

Consequences

In minor cases of abuse, the user receives a notice of improper activity. A user found guilty of IT system abuse can be deemed liable to pay compensation for the abused resources (e.g. servers or network), direct damages and the costs of investigating the abuse.

Consequences to students

Consequences applicable to students include a temporary loss or restriction of usage authorisation, administrative actions by the University (written notice, temporary suspension), or reporting the case to the police (if the act is punishable under a law).

Consequences concerning usage authorisation are determined by head of information management. The term of restricted authorisation does not include the time spent investigating the case. Written notices are issued upon the decision of [the University Rector], and suspension decisions are made by [the University Board]. If a student is suspended, his/her IT system usage authorisation is revoked for the duration of the expulsion.

The minimum period of usage authorisation restriction applied in such cases is outlined in the abuse penalty table.

Consequences to staff members

Consequences applicable to university staff members include labour-law actions (written notice, dismissal, termination of employment contract) or reporting the case to the police (if the act is punishable under a law).
The user's access to certain systems can be temporarily or permanently denied due to the lack of confidence caused by the abuse. Consequences concerning usage authorisation are determined by head of information management, owner of the system or head of the unit.

Consequences to other users

Consequences applicable to users with roles other than degree student or staff member include the cancellation or restriction of usage authorisation or reporting the case to the police (if the act is punishable under a law).
The user's access to certain systems can be temporarily or permanently denied due to the lack of confidence caused by the abuse. Consequences concerning usage authorisation are determined by head of information management, owner of the system or head of the unit.

Penalty Tables

The tables attached to this document outline the recommended penalties for breaches of IT service rules applicable to university students, staff members and other users.

The tables contain examples of typical IT system abuse cases classified by severity. In addition to the severity of the act, the level of intention is taken into account when determining the consequences. In case of users who are both students and staff members, the staff members' table shall apply.

Examples of IT service abuse

Unauthorised handling of material subject to the Criminal Code and Copyright Act.

- *Material subject to the Criminal Code* includes, for example, child porn, zoophilia, extreme violence, racist material and agitation
- *handling* includes the possession and distribution of such material.

Material subject to the Copyright act includes music, videos, comic strips, movies, games and software.
Handing over user IDs includes

- revealing your password to another user
- leaving the workstation session open so that another user can continue using it under your ID.

Compromising the confidentiality of information includes

- disclosing information that is classified as secret or otherwise protected by law to an unauthorised person (for example, handing over server user data)
- neglecting the information security of confidential information (passive negligence)
- intentional breaches of confidentiality (active offense)
- breaching the Personal Data Act.

Negligence of personal information security includes

- Leaving your password on sight
- neglecting to use the university's back-up copy procedures.

Service is a function that can be used from outside of the server, e.g.

- e-mail service (smtp, imap, …)
- file transfer service (ftp, http, scp, Bittorrent, DC++, …)
- peer to peer network service intendend solely on file sharing (Bittorrent, DC++, eDonkey, …)