Disciplinary procedure for IT violations

The university's IT service terms of use are binding and they must be observed by all users, including you.

IT violation refers to a use of IT services in a way that violates rules, regulations or Finnish law. All suspected violations must be reported to the IT manager.

If a violation is suspected, the university may restrict the user's privileges to the service during the investigation. Depending on the severity of the violation and whether it was premeditated, the university can impose internal disciplinary action and/or report the incident to the police.

Disciplinary procedure for IT violations

IT violations are actions which violate the university's rules or regulations on the use of its information systems or the use of information systems in a way that violates Finnish law.

This procedure describes the disciplinary measures which may be taken in the event of an IT violation or when there are grounds to suspect a violation. The procedures include restriction of user privileges during the investigation and possible disciplinary consequences.

The university can restrict the user's privileges to IT services for the duration of the investigation

Possible restrictions will be determined when an IT violation is found or suspected to have taken place. Restrictions will be imposed if there are grounds to suspect that the user has committed a violation and when it is possible that the user privileges could hinder the investigation or the minimisation of losses. The user may be invited to be heard if necessary.

Restriction of user privileges will be decided by the owner of the IT service, the IT manager, or another designated person. The restriction will be implemented by the service administrator.

In urgent cases, the administrator may restrict the user's privileges at its discretion for a maximum period of three days. In this case, the person responsible for restrictions must be notified immediately.

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

Restrictions can be removed after the investigation has been completed, provided that restoring the privileges does not present an obvious risk.

Consequences

In cases of minor violations, a warning is issued to the user on inappropriate behaviour.

As a result of an IT violation, the user could be liable for compensation for the improper use of resources (e.g. servers or network), direct losses and the costs of the investigation.

Consequences to students

Possible consequences to students include the temporary loss or restriction of user privileges, administrative measures by the university (written warning, temporary suspension) and reporting to the police (for an act punishable by law).

Measures affecting user privileges are decided by the IT manager or the owner of the service. The period of restriction does not include the time spent investigating the matter. The decision to issue a written warning to a student shall be made by the rector of the university and the decision on a suspension by the board of the university. All user privileges will be suspended for the duration of the suspension.

Consequences to staff members

Possible consequences to staff members include labour disciplinary measures (a written warning, dismissal, termination of employment) and reporting to the police (for acts punishable by law).

User privileges to individual systems may be suspended temporarily or permanently due to a lack of trust as a result of a violation. Measures affecting user privileges are decided by the IT manager or the owner of the service.

Consequences to other users

Possible consequences to users other than staff members or degree students include the suspension or restriction of user privileges and reporting to the police (for acts punishable by law).

User privileges to individual systems may be suspended temporarily or permanently due to a lack of trust as a result of a violation. Measures affecting user privileges are decided by the IT manager or the owner of the service.

Examples of IT violations

- Unauthorised handling of material under the Criminal Code or the Copyright Act
  - Material regulated by the Criminal Code includes child pornography, bestiality, excessive violence, racist materials and incitement materials
  - handling includes e.g. the distribution and possession of regulated material.
- Material regulated by the Copyright Act includes music, video clips, comic strips, films, games and software.
- The disclosure of user ID to another party includes e.g.
  - giving a personal password to another user.
  - leaving a computer on in such a way that the user ID can be used by another person.
- Jeopardising confidentiality includes e.g.
  - disclosing information that is secret or otherwise protected by law to another person who does not have the right to receive the information in question (e.g. user data from servers).
  - negligence related to the security of confidential information (passive inaction).
  - wilful offences related to secret information (active action).
  - violation of the Personal Data Act.
- Negligence of personal data security includes e.g.
  - leaving a personal password visible.
- use of IT services for communications containing obscene material or for inappropriate promotion.