Sanctions for IT Service Abuse

IT service abuse refers to violations of policies and orders issued on the use of information systems or the use of information systems in violation of Finnish laws.

This document outlines the measures applied to members of the higher education community when IT service abuse has been discovered or there are justified reasons to suspect such abuse. The measures range from restricting access rights during the investigation of alleged abuse to implementing sanctions after the abuse has been confirmed. These sanction policies have been approved by the chief information officer and will enter into force on 15 February 2021.

The higher education institution can restrict access to IT services during abuse investigations

When a breach of IT service policies has been discovered or there is reason to suspect one, the institution can restrict the access rights of 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 will be invited to a hearing.

Supervisors, the HR director and chief information officer decide on the restriction of employees' access rights. The director of student services and chief information officer decide on restricting students' access rights. Restricting the access rights of other user groups is the decision of the chief information officer. 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 the chief information officer. When necessary, a user's workstation can be disconnected from the network.

The access restrictions can be removed when the investigation is complete if restoring the user's rights does not pose an evident risk.

Sanctions

Sanctions may be imposed for system abuse.

Sanctions for students

Sanctions applicable to students include a temporary loss or restriction of access rights, administrative actions by the institution (written notice, temporary suspension), or reporting the case to the police (if the act is punishable by law).
A suitable staff member may caution a student. Measures related to access rights are determined by the chief information officer and director of student services. The term of restricted authorisation does not include the time spent investigating the case. Written notices are issued based on a decision by the rector/president and suspension decisions are made by the board of directors. If a student is suspended, his/her IT system access rights are revoked for the duration of the suspension.

Sanctions for staff members

Sanctions applicable to 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 by law).
A user's access to certain systems can be temporarily or permanently denied due to system abuse. Measures regarding access rights are determined by the employee’s supervisor, HR director or chief information officer

Sanctions for other users

Sanctions for users other than degree students or staff members include the cancellation or restriction of access rights or reporting the case to the police (if the act is punishable by law).
A user's access to certain systems can be temporarily or permanently denied due to system abuse. Sanctions concerning access rights are determined by the chief information officer.

Examples of IT service abuse

- Possession and distribution of material punishable under the Criminal Code of Finland
- Unlawful possession and distribution of material protected by copyright legislation.

- Disclosing your user ID refers to, for example
  - 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 refers to, for example
  - disclosing confidential information to a person not authorised to receive it

- failing to observe data processing guidelines of your higher education institution

– Compromising information security at your higher education institution refers to, for example
  - negligent use of your personal password
  - failing to observe your higher education institution's information security guidelines

Lappeenranta

Antti Sirviö, Chief Information Officer

Tämä dokumentti on allekirjoitettu sähköisesti LUT Sign-järjestelmällä
This document has been electronically signed with the LUT Sign system

Päiväys / Date: 10.02.2021 10:20:41

Antti Sirviö

LUT University
Antti Sirviö
Tietohallintojohtaja

Organisaation varmentama (LUT käyttäjätunnus)
Certified by organization (LUT user account)