Graubner, Pettinen, Valjakka

17 February 2021

Sanctions policy for the misuse of IT services at Laurea

Discussed at the codetermination advisory board of Laurea University of Applied Sciences on 17 February 2021

AMMATTIKORKEAKOULU
University of Applied Sciences

Sanctions Policy

Graubner, Pettinen, Valjakka

17 February 2021

Table of contents

Graubner, Pettinen, Valjakka 17 February 2021

1 Introduction

Every user is bound and obligated by the regulations of Laurea's IT services. Misuse of IT services refers to contravening the regulations or legislation issued for the use of IT services. All misuse detected shall be reported by means of an electronic form intended for this purpose.

In case of suspected misuse, the user's access to Laurea's IT services may be restricted for the duration of the investigation. Based on the seriousness and intentional nature of the act, the misuse may lead to consequences within Laurea. The most blatant cases of misuse may be reported to the police.

2 Sanctions for misuse of IT services

This sanctions policy describes the measures that a person will be subjected to when the misuse of IT resources has been detected or there are reasonable grounds to suspect it has taken place. The measures are divided into restrictions on access rights for the duration of the investigation of the offence, and possible consequences specified for it.

As a result of IT misuse, the user may be liable for any resources misused (such as computers, servers or a data network), for direct damage, and for the costs arising from investigating the offence.

In minor cases, the user is notified of their inappropriate behaviour. In the most serious cases, and if the user continues to act in breach of the rules, the following measures can be taken.

2.1 Restricting user rights for the duration of the investigation

Decisions are made on the restrictions when the misuse has been detected, or when, for justified reasons, the user is suspected of being guilty of misuse and it is possible that the access rights may obstruct the investigation or harm the damage limitation. If necessary, the user is summoned and heard to clarify the matter.

Decisions on restricting user rights are made by an information security specialist or the Director of ICT.

In urgent cases, the service administrator may, by autonomous decision, restrict the user rights. Such cases are to be reported to the Director of ICT and information security specialist without delay.

Restrictions may be lifted after the investigation has been completed, as long as restoring the user rights would not apparently lead to adverse consequences.

For the duration of the investigation, the user's device can be disconnected from the network and/or the user ID locked. If necessary, a device owned by Laurea can be taken over.

2.2 Consequences for students

Consequences for students may include temporary loss or restriction of user rights, Laurea's administrative measures (written caution, temporary dismissal) or reporting the offence to the police (acts defined as punishable by law).

Decisions on actions concerning user rights are made by the Director of ICT. The time spent on the investigation shall not count towards the duration of the user rights restriction. The decision to issue a written caution to a student is made by the President of Laurea, and the decision of temporary dismissal is made by the Board of Directors of Laurea. The person's access rights shall be revoked for the duration of the dismissal.

2.3 Consequences for staff members

Consequences for staff may include Laurea's labour law measures (written caution, dismissal, termination of employment) or reporting the offence to the police (acts defined as punishable by law).

Access rights to individual systems may be suspended or permanently denied for reasons of misconduct. Decisions on actions concerning user rights are made by the Director of ICT together with the supplier of the service that has been subjected to misuse.

If the situation so requires, equipment owned by Laurea and handed over to staff for work duties may be claimed back to Laurea for the duration of the investigation.

2.4 Consequences for other users

Consequences for users who are not degree students or members of Laurea's staff may include the removal or restriction of user rights, and reporting the offence to the police (acts defined as punishable by law).

Access rights to individual systems may be suspended or permanently denied for reasons of misconduct. Decisions on actions concerning user rights are made by the Director of ICT together with the supplier of the service that has been subjected to misuse.

3 Examples of misuse of IT services

- Unlawful processing, distribution and possession of material under The Criminal Code of Finland and Copyright Act, such as
    - child pornography, brutal violence, racist material and demagogic material

- illicit distribution or sale of music, videos, comics, films, games and software.

- Misuse of a user ID
    - sharing a password with another user
    - unauthorised use of another person's device.
      As a rule, the use of another person's device is prohibited with the exception of presentations or similar. In such cases, the use may be temporarily permitted under the supervision of the user.
    - using another person's ID to access information systems, files or other material.
- Compromising the confidentiality of information
    - disclosing confidential information or information otherwise protected by law to a person who is not entitled to access it (such as disclosure of data on server users)
    - collecting confidential or personal data from Laurea's services without an acceptable reason
    - leaving documents that are confidential or contain personal data at the workstation when absent from the workstation
    - storing a document containing confidential or personal information in a location that does not fulfil the information security requirements (see classification of data)
    - disclosing information to third parties in public spaces or means of public transport
    - neglecting the appropriate settings for file sharing (file sharing instructions for the O365 environment)