Policy on Consequences for IT Offences

1) General Information about IT Offences and security breaches

Acting against the rules and regulations concerning university's information systems and other IT services as well as acting against Finnish laws, governing information security, data privacy and cybersecurity, will be treated as IT offences or violations at Metropolia University of Applied Science.

This document outlines the actions taken against an individual when an IT offense has been discovered or there is reason to believe that an offense has occurred. The sanction practices vary from minor user permission restrictions to more severe penalties, depending on the nature of the action, whether the offense results from negligence, deliberate actions, or criminal intent.

> **The definition on security breach.**
>
> Security breach is prohibited by law because it involves attempting unauthorized intrusion into a computer system, service, or device, or unauthorized use of an application with obtained credentials.

The guideline concerns primarily on the university's degree students and personnel.

User credentials and permissions to access university systems may also be given to:

- Interest groups and stakeholders.
- students in further education and open university studies.

Due to the group's heterogeneity, decisions regarding IT violations will require more individual considerations. Instead of providing general one-size-fits-all solutions for IT offenses, the principle of discretion applies to the case at hand.

All occurred IT offences and actions must be reported to the Chief Information Security Officer.

2) Restricting user permissions on pending investigations

User permissions may be restricted by either disabling some or all of a person's user accounts or by employing other methods to prevent access to an information system (e.g., removing modify permissions) during the investigation:

- As a standard procedure, a student's user account is disabled, and the student will be contacted to meet with either the Chief Information Security Officer or the person responsible for the system.
- User permissions for staff members will be restricted as necessary. In the event of a network violation incident, user permission restriction may also include disconnecting the user's workstation from the network.

User permissions will be restricted in cases where there are reasonable grounds to suspect misuse of university IT resources, when access rights hinder the investigation of an offense, or to prevent potential further harm.

The decision to restrict user permissions is made by the owner of the information system in question, the unit leader, or an appointed individual. The implementation of these restrictions falls under the responsibility of the administrator. In urgent situations, the administrator may autonomously restrict user permissions for a maximum of three days and will promptly report this action to the designated authority.

3) Consequences

In minor offences the user is verbally reprimanded for improper action.

The person committing an IT offence is liable for the costs incurred from the use of resources (e.g. computer time) as well as for the costs incurred from the investigation.

3.1 To the students

A student may be subject to the following consequences: restriction of user permissions (disabling of user accounts) (General Policy of the Use of Information Systems), the university's internal administrative actions (a written warning, a temporary dismissal) (Polytechnics Act 14.11.2014/932), and reporting a crime (actions punishable by law).

The university teachers or the other representative of the university, such as the staff, the teacher's supervisor or the Board of Examiners, are standardly responsible for handling a student's IT offence at Metropolia. In minor cases and due to negligence, the student is simply addressed verbally.

The decision to disable a user account is made by the university's President or someone else appointed by the President. The restriction time does not include the time that the account is disabled pending investigation.

The decision to give a written warning is made by the university's President, while the temporary suspension of the student decides the Board of Directors. Access rights into the university's IT services will be withdrawn during the suspension period.

The IT Services do not serve as a disciplinary measure. Instead, instances of IT violations by students will be addressed according to the university's disciplinary guidelines.

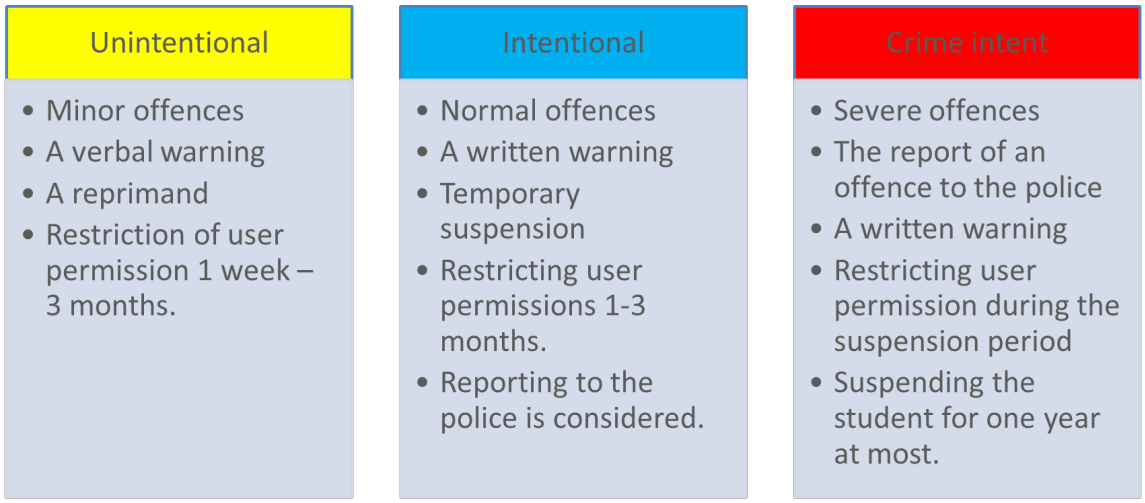
The definition on the minor IT violation of the students

A student insults or bullies other students, staff, visitors or other people he or she works with in connection with studies or a work placement, or reveals their personal data to a third party or otherwise acts in violation of data protection rules and guidelines. A student intentionally or through gross negligence damages property at Metropolia or at a work placement or property belonging to a partner.

The definition on the severer IT violation of the students

A student poses a threat to public safety or causes significant damage to Metropolia. A student reveals to a third party the personal data, including sensitive personal data, of other students, staff, visitors or other people he or she works with in connection with studies or a work placement, or otherwise acts in violation of data protection rules and guidelines, and does so repeatedly or in a manner that can be considered deliberate or gross. A student accesses a forbidden domain in an information network, causes an information security threat or causes damage to an information system.

Examples on the scale of the IT offences made by the students



3.2. To the staff

A staff member may face the following consequences: disciplinary actions outlined in labor law (including a written warning, dismissal, or termination of employment contract) as per the Employment Contracts Act (Chapter 7, Section 2; Chapter 8, Section 1), and reporting to law enforcement for criminal actions. Warnings are issued by the head of the unit or the director of administration. Access to specific information systems may be temporarily or permanently disabled based on trust concerns resulting from misuse. When determining consequences, the intent and severity of the offense are considered.

Examples on the scale of the IT offences conducted by the personnel

4. Examples of offences

Distributing material subject to criminal law such as:

- Cruel violence, racist material and incitement of the masses to crime.

Unlawful distribution of material subject to copyright law such as:

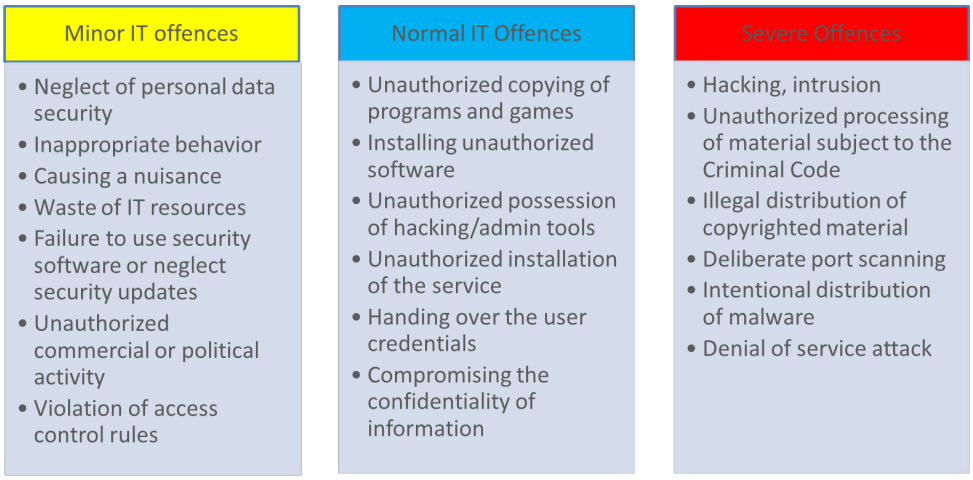
- Music, videos, cartoons, games and software.

Giving one's login credentials to someone else:

- Giving login credentials includes giving one's password to another user or leaving a session open so that someone else can use the credentials unsupervised.

Risking data integrity:

- Disclosing non-public information to unauthorized individuals, such as providing access to server user data
- Neglecting information security for non-public information, such as inadequate protection of an information system
- Breaching confidentiality agreements.
- Violating the Data Protection Act
- Neglecting personal information security, for example, by leaving passwords exposed.



Tietotekniikkarikkomusten seuraamuskäytäntö