ICT Regulations

On this page, you can find NTNU's ICT Regulations, which are in force from 14 June 2018.

About the ICT Regulations

- Type of document: regulations
- Managed by: Director of Organization
- Approved by: The Board of NTNU
- Classification: open
- In force from: 14 June 2018
- In force until: revision date
- Exempt from public disclosure: no
- Legal reference Act/Regulation: Section 14 and Section 20 of Norway's eGovernment regulations (eForvaltningsforskriften); articles 24 and 32 of the General Data Protection Regulation (GDPR)

Purpose

The purpose of the ICT Regulations is to regulate the use of NTNU's information and communication infrastructure (ICT infrastructure).

The regulations also cover personally owned equipment connected to the computer network. When software or information owned by NTNU is installed on personal equipment, this is also covered by the regulations.

Who is subject to NTNU's ICT Regulations?

The ICT Regulations apply to:

- All employees at NTNU
- All students at NTNU
- Everyone who has access to and/or processes and manages information through NTNU's ICT infrastructure.

Definitions

NTNU's ICT infrastructure refers to all equipment, digital information, information systems and services used for information processing and communication.

Overall principles

Access to NTNU's ICT infrastructure

Students and employees must have a user account at NTNU. A user account refers to a unique username, password and an email box. Access to ICT infrastructure may be granted to others based on official needs. Access to the various systems and services is authorized by the system owner.

Use of ICT infrastructure

Anyone who is granted access to NTNU's ICT infrastructure (referred to as a user later in this document) has a duty to familiarize themselves with the ICT Regulations and to comply with them. Users are also obliged to familiarize themselves and comply with the underlying policies, guidelines and procedures, which are available on Innsida.

NTNU's ICT infrastructure is intended for performing tasks related to NTNU's operations. NTNU's ICT infrastructure must be used in a way that does not violate laws, administrative regulations or NTNU's internal regulations.

Each user must take steps to prevent other people from accessing the user's own account. Users must not try to gain access to other people's user accounts.

Users must take steps to prevent unauthorized people from gaining access to NTNU's ICT infrastructure, including access to rooms where ICT equipment is available. Users must not, without permission, change, modify or otherwise cause the ICT infrastructure to function in a way different from what is intended.

Users must not use NTNU's ICT infrastructure in a way that might expose NTNU to loss of reputation.

NTNU's ICT infrastructure must be used only to support activities that help to achieve the university's purposes and tasks related to research, education, including artistic development activities, innovation, dissemination, outreach and administration.

Users must ensure that individual privacy is respected and not violated.

Users are obliged to respect copyright or similar rights to software, services and other digital information such as images, music, video, etc.

Licensed software, services, intellectual property or other data subject to rights must be used only in accordance with the agreement for use, and users have a duty to familiarize themselves with the rules applicable to use. Users may be held responsible for breach of the terms and conditions.

Publishing of other people's work, information or data must only take place by agreement with the rights holder.

During long periods of absence, users must set up automatic ("out of office") replies so that work-related email is not left unmanaged in the email box.

Users must immediately report any circumstances that may affect the security or integrity of the ICT infrastructure (nonconformities) to the IT Division, through the Digital Security Section.

Termination of employment relationship or studies, etc.#

In good time before ending their employment or studies at NTNU, users must clear up their account. Files belonging to cases that an employee has been dealing with must be submitted to the manager of the user/employee for consideration. The files must not be deleted before the user's faculty or unit has approved this. The employee must ensure that files that do not belong to specific cases are submitted to his or her manager, who decides whether the files are to be deleted or archived.

Termination of user name and email box, etc.:

When the employment relationship, admission to study or other form of connection to NTNU ends, user access to NTNU's ICT infrastructure will be terminated. Warning about this is given by email one month in advance.

The contents of the email box and personal storage areas will be permanently deleted within six months after access is terminated. For students, personal storage areas are deleted two months after the right of admission to study ended.

In the event of death, the user account will be blocked. The email box as well as the personal home directory and its contents will be deleted after six months unless public authorities have required access and can present a written petition, or the deceased person's estate through a certificate of probate has claimed a right to the material.

Return of property and equipment to NTNU:

Property and equipment belonging to NTNU must be returned. All copies of software, documentation and data owned by or borrowed from NTNU must be deleted on personal equipment.

The right to connect personal devices to NTNU's network expires at the end of the employment relationship or studies.

Identification and access control

Access to NTNU's ICT infrastructure must be related to a role and with the consequent rights.

A person who wants access to NTNU's ICT infrastructure must identify himself or herself using an approved digital identity or identities linked with the role.

Change in role or termination of the relationship with NTNU

If there is a change of role in relation to NTNU, rights in the ICT infrastructure will be changed accordingly. When the relationship to NTNU ends (students graduate, employees leave), access and rights must be revoked. After a waiting period, personal data will be deleted.

The person who uses the digital identity is responsible for taking care of personal data and for handing over NTNU's data in accordance with these ICT Regulations and the applicable agreement that grants access to NTNU's ICT infrastructure.

Control of the use of NTNU's ICT infrastructure

All use of NTNU's ICT infrastructure leaves an electronic trail. NTNU collects, analyses and keeps electronic trails to manage the ICT infrastructure, to ensure effective operations and cost management, and to protect NTNU's ICT infrastructure against threats and abuse. Collection, storage and use of electronic trails must comply with the legislation in force.

NTNU's ICT infrastructure includes logging and backup solutions for purposes that include enabling documentation of breaches of the law or non-conformance with internal rules and procedures, but also to make it possible to detect/discover security breaches in the ICT infrastructure.

The IT Division has primary responsibility for controlling access to NTNU's network and general ICT services.

Access to information

As the employer, within the framework of the regulations, NTNU has the right of access to the employee's email box, user account, etc. As far as possible, the employee must be notified and given the opportunity to make a statement before the data is accessed, and the employee will generally have the right to be present during access. The employee has the right to be assisted by a union representative or other representative.

If access takes place without prior notice, the employee must receive written notification of the inspection afterwards. The decision on and implementation of access must be documented in NTNU's administrative and records management system.

Access must take place in such a way that, as far as possible, the data are not changed and that information produced can be verified.

NTNU only has the right to search, open or read email in the employee's e-mail box or home directory, etc., in the following cases:

- When this is necessary in order to perform day-to-day operations or safeguard other legitimate interests of the organization.
- When there is reason to suspect that the employee's use of the email box involves a serious violation of the duties arising from the employment relationship, or may provide grounds for dismissal with or without notice.

If access to the email box shows that there is no documentation that the employer has the right to inspect, the email box and documents in it must be closed immediately. Any copies must be deleted.

An application for access to an employee's email box is submitted by the head of the unit (at a department, faculty or division of the central administration) in consultation with the director of the HR and HSE Division and the system owner.

A decision on access is taken by the Director of Organization.

In the event of death, the director of the HR and HSE Division may decide that the data must be accessed to find email and other data related to the user account. Such access will take place in cooperation between the head of the unit and the director of the HR and HSE Division.

NTNU may provide access to information, logs and backups to public authorities when there is a basis for this in law or regulations, and when a court ruling is presented.

Sanctions for breach of the ICT Regulations

Breach of the ICT Regulations and/or underlying policy documents, guidelines, procedures, and routines may lead to disciplinary measures against the user. Users are responsible for familiarizing themselves with the governing documents and instructions that apply to their use of the ICT infrastructure. An overview of relevant documents will be available at NTNU's website.

Equipment or software that causes damage to NTNU's ICT infrastructure, NTNU's information/data, other users' information/data, that in other ways causes disruption to the ICT infrastructure or impedes fulfilment of NTNU's purpose for the ICT infrastructure, may without delay be removed from the ICT infrastructure.

Anyone who violates the provisions of the regulations, including a user who causes damage to NTNU's ICT infrastructure, to NTNU's information/data, or to other users' information/data, who in

other ways causes disruption to the ICT infrastructure or impedes fulfilment of NTNU's purpose for the ICT infrastructure may cause the user to be denied access to all or part of the institution's ICT infrastructure; see Section 14 of the eGovernment regulations. In addition, it may result in sanctions under other rules, such as disciplinary responses under the Act concerning public employees (lov om statsansatte), a warning or exclusion from studies and examinations under the Act relating to Universities and University Colleges (universitets- og høyskoleloven), liability for damages, or criminal liability.

Temporary exclusion for up to 14 working days, decided by the head of the unit (the dean if the user is a student) in consultation with system owner. The HR and HSE Division must be notified immediately if the exclusion applies to an employee. Exclusion beyond 14 working days will be regarded as an individual decision for a student or employee, and must follow relevant procedural rules.

Temporary exclusion may take place in connection with a legitimate suspicion that:

- The user has committed serious violations, or
- The user or the user's ICT equipment poses a significant threat to information security.

The focus in the assessment must be on how serious the violation is, whether the user has previously violated the regulations, the consequences that an exclusion will have for the user and other aspects of the case.
Appeals against decisions made under the Act concerning public employees, the Act relating to Universities and University Colleges and the Public Administration Act (the eGovernment regulations) follow the rules on appeal set out in these laws.

Roles and responsibility

Rector

- The Rector may make necessary changes to the ICT Regulations by authority of the Board.

Director of Organization

- The Director of Organization revises the ICT Regulations every other year.
- The Director of Organization must submit the ICT Regulations to the Rector for approval in connection with revisions or changes that may affect users' rights and obligations.
- The Director of Organization makes a formal decision on access to the user's email box, etc.

Head of the IT Division

- The head of the IT Division implements exclusion of access to NTNU's ICT infrastructure.

Director of the HR and HSE Division

- The director of the HR and HSE Division will assess the need for temporary exclusion for up to 14 days as a sanction against employees in connection with breach of the ICT Regulations.

Appointments authority

- The appointments authority decides on sanctions against employees in accordance with the Act on public employees and
- Staff regulations for academic personnel and for technical and administrative staff respectively.

Dean/Museum Director

- The Dean/Museum Director is responsible for ensuring that students are informed about the ICT Regulations, and that the regulations are accepted in writing (electronically) before students are granted access to NTNU's ICT infrastructure.
- The Dean/Museum Director decides on exclusion of up to 14 days from NTNU's ICT infrastructure as a sanction against a student for violation of the ICT Regulations.
- The Dean/Museum Director makes a formal decision on exclusion beyond 14 days from NTNU's ICT infrastructure as a sanction against a student for violation of the ICT Regulations.

Line manager

- The line manager is responsible for ensuring that employees are informed about the ICT Regulations, and that the regulations are accepted in writing (electronically) before employees are granted access to NTNU's ICT infrastructure.

User

- Users are responsible for familiarizing themselves with the ICT Regulations and other rules for the use of NTNU's ICT infrastructure, and for following them.
- Users must ensure that breaches of personal data security are reported without undue delay to the line manager and in NTNU's system for reporting incidents and nonconformities.