NTNU's ICT regulations

Type of document	Regulations
Managed by	Director of Organization and Infrastructure
Endorsed by	Director of Organization and Infrastructure
Classification	Open
Valid from	12.06.2023
Next revision within	12.06.2025
Reference ISO	ISO 27002:2022; 5.4, 6.2, 6.4
Reference NSM's principles for ICT security	
Reference LAW/Rule	Legal reference Act/Regulation: Section 20 of Norway's eGovernment regulations (eForvaltningsforskriften); articles 24 and 32 of the General Data Protection Regulation (GDPR), Act concerning public employees (lov om statsansatte), Act relating to Universities and University Colleges (universitets- og høyskoleloven)
Reference internal documents	Policy for information security, underlying topic specific policies for information security and privacy

1. Purpose

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

2. Who NTNU's ICT regulations apply to

The ICT regulations apply to:

a. All employees at NTNU
b. All students at NTNU
c. Anyone who has access to, and/or processes and manages information through NTNU's ICT infrastructure.

2.1. Scope

NTNU's ICT infrastructure refers to all equipment, digital information, information systems and services used for information processing and communication.
Privately owned equipment is covered by the regulations when it is connected to the computer network, or when software or information owned by NTNU is installed on private equipment.

3. General principles

3.1. Access to NTNU's ICT infrastructure

Students and employees must have a user account at NTNU. User account means unique username, password, and an e-mail address. Others may be given access to ICT infrastructure as service needed. Access to the various systems and services is authorized by the system owner.

3.2. Use of ICT infrastructure

a. Anyone who is granted access to NTNU's ICT infrastructure (hereinafter referred to as a user) is obliged to familiarize themselves with the ICT regulations and to comply with them. The user is also obliged to familiarize themselves with and follow the underlying policies, guidelines and procedures available on Innsida.
b. NTNU's ICT infrastructure is intended for performing tasks related to NTNU's operations[1][2].
   NTNU's ICT infrastructure must be used in a way that does not conflict with laws, regulations or NTNU's internal rules.
c. Users shall prevent others from gaining access to their own user account. Users shall also not seek to gain access to someone else's user account.
d. Users shall prevent unwanted persons from gaining access to NTNU's ICT infrastructure, including access to rooms where ICT equipment is available. Users shall not, without permission, change, modify or otherwise cause the ICT infrastructure to function in a different way than intended.
e. Users must not use NTNU's ICT infrastructure in a way that may expose NTNU to loss of reputation.
f. NTNU's ICT infrastructure shall only be used to support activities that contribute to achieving the university's objectives and tasks related to research, education, including artistic research, innovation, dissemination, and administration.
g. Users shall ensure that the individual's privacy is complied with and not violated.
h. Users are obliged to respect copyright or similar rights to software, services, and other digital information such as pictures, music, and films etc.
i. Licensed software, services, intellectual property, or other copyrighted data may only be used in accordance with the user agreement, and the user is obliged to familiarize himself with the rules that apply to the use. User may be held liable for violation of the Terms.
j. Publication of other people's works, information or data must only be done by agreement with the copyright holder.
k. In the event of a longer absence, the user must submit an absence notification so that business-related e-mail is not left unhandled in the e-mail box.
l. Users are obliged to immediately report matters that may affect the security or integrity of the ICT infrastructure (non-conformities) to the IT Division, at the Section for Cyber Security.

3.3. Termination of employment or studies, etc.

In reasonable time before termination of employment and termination of studies at NTNU, the user must clear his/her account. Files belonging to cases that an employee has managed shall be submitted to the user's/employee's superior for evaluation. The files should not be deleted until the user's faculty or unit has approved this. The employee shall ensure that files that do not belong to specific cases are submitted to their immediate superior, who decides whether the files should be deleted, or archived.

3.4. Termination of user and mailbox etc.

[1] https://i.ntnu.no/wiki/-/wiki/Norsk/Politikk+for+informasjonssikkerhet
[2] https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+retningslinjer

a. When employment, study rights or other forms of affiliation to NTNU cease, user access to NTNU's ICT infrastructure is closed. Notification of this is given by e-mail one month in advance.
b. In the event of dismissal or suspension, access to ICT infrastructure shall be withdrawn with immediate effect. If there is a need to retrieve personal information or other relevant information, this must be done by agreement with the immediate superior and be supervised.
c. Contents of mailboxes and personal storage areas are permanently deleted no later than six months after access is closed. For students, the personal storage areas are deleted two months after the termination of the right to study.
d. In the event of death, the user account will be blocked. The mailbox and the private home directory and its contents are deleted after six months unless public authorities have requested access and can submit a written request, or the estate of the deceased has asserted the right to the material by certificate of probate.

3.5. Return of materials to NTNU

a. Materials belonging to NTNU must be returned. All copies of software, documentation and data owned by, or loaned from NTNU, must be deleted on private equipment.
b. The right to connect private machines to NTNU's network ceases upon termination of employment or studies.

3.6. Identification and access management

a. Access to NTNU's ICT infrastructure must be linked to a role and with subsequent rights.
b. Anyone who will have access to NTNU's ICT infrastructure must identify themselves using an approved digital identity(s) associated with the role.

3.7. Change of role or termination of the relationship with NTNU

a. In the event of a change of role in the connection to NTNU, changes of rights in the ICT infrastructure shall be changed accordingly. When the relationship with NTNU ends (students graduate, employees leave), access and rights must be withdrawn. After a quarantine period, personal data must be deleted.
b. The person who uses the digital identity is responsible for taking care of personal data, as well as handing over NTNU's data in accordance with these ICT regulations and the applicable agreement that provides access to NTNU's ICT infrastructure.

3.8. Control of the use of NTNU's ICT infrastructure

a. All use of NTNU's ICT infrastructure leaves electronic traces. NTNU collects, analyses and stores electronic traces to manage the ICT infrastructure, ensure efficient and cost-bearing operations, and to protect NTNU's ICT infrastructure against threats and abuse. The collection, storage and use of electronic traces shall be done in accordance with applicable law.
b. NTNU's ICT infrastructure is facilitated with solutions for registration of activities (logging) and backup, among other things to be able to document breaches of law or deviations from internal rules and routines, but also to be able to uncover/detect breaches of security in the ICT infrastructure.
c. The IT department has the main responsibility for control of access to NTNU's network and general ICT services.

3.9. Access to information

a. As an employer, NTNU has the right to access the employee's e-mail box and user account, etc. within the framework of the regulations. Employees shall, as far as possible, be notified and given the opportunity to express their views before access is carried out, and the employee shall, as a general rule, have the right to be present during the inspection. Employees have the right to be assisted by a union representative or other representative.
b. If access has been made without prior notice, the employee must subsequently receive written notification of the access. The decision and implementation of access must be documented in NTNU's case management and archive system.
c. Access must be carried out in such a way that the data are not changed as far as possible, and that the information generated can be verified.
d. NTNU only has the right to search, open or read e-mails in the employee's e-mail box or home directory, etc. in the following cases:
    i. When necessary to safeguard day-to-day operations or other legitimate interests of the business.
    ii. When there is a reasonable suspicion that the employee's use of the mailbox constitutes a serious breach of the duties arising from the employment relationship or may give grounds for dismissal[3].
e. If access to the mailbox shows that there is no documentation that the employer is entitled to access, the mailbox and documents in it must be closed immediately. Any copies should be deleted.
f. The decision to access the employee's mailbox is made by the head of the unit (dean or department director). The same applies to deaths where access is necessary to find business-related e-mail and other things related to user accounts.
g. NTNU can provide access to information, logs, and backup copies to public authorities when this is authorized by law or regulations, as well as when submitting a court decision.

3.10. Reactions and sanctions for breaches of ICT regulations

a. Violations of ICT regulations and/or underlying policy documents, guidelines, procedures, and routines may lead to reactions or sanctions against the user.
b. The user is responsible for familiarizing himself with the governing documents and instructions that apply to his/her use of the ICT infrastructure. An overview of relevant documents is available on NTNU's website[4].
c. Equipment or software that causes damage to NTNU's ICT infrastructure, to NTNU's information/data, other users' information/data, that in any other way creates disturbances in the ICT infrastructure or is an obstacle to achieving NTNU's purpose with the ICT infrastructure, may be removed from the ICT infrastructure immediately and without prior notice.
d. Employees who commit violations of the ICT regulations may face employment law sanctions in the form of a warning or sanctions in the form of suspension pursuant to "Act concerning public employee, section 29".
e. Students who commit violations of the ICT regulations may be excluded completely or partly from NTNU's ICT infrastructure pursuant to the Universities and University

[3] https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/innsyn-epost-filer/?print=true
[4] https://i.ntnu.no/informasjonssikkerhet

Colleges Act. Exclusion exceeding 14 working days is considered an individual decision for a student and must follow the procedural rules in the Public Administration Act.

f. The decision on reactions and sanctions against employees is decided by the chief executive of the basic unit, or the dean if the user is a student. The decision shall be made in consultation with the system owner.
g. Appeals about decisions made pursuant to the Act on public employees or the Act relating to Universities and University Colleges comply with the provisions of the act relating to appeals.
h. Guest users who commit violations of the ICT regulations are followed up by the responsible client. The consequences of breaches are governed by the Assignment Agreement or Service Agreement, or by rules of contract law.

4. Roles and responsibilities

Responsibility for the ICT regulations has been delegated from the Board to the Director of Organization and Infrastructure through the Headmaster[5].

4.1. Director of Organization and Infrastructure

a. Revises the ICT regulations every other year.
b. Shall submit the ICT regulations to the rector for determination in the event of revisions or changes that may affect users' rights and obligations.

4.2. IT Director

a. The IT Director implements the exclusion of access to NTNU's ICT infrastructure.

4.3. Appointing Authority

a. Decides on sanctions against employees pursuant to the Act relating to State Employees and the Personnel Regulations for Academic and Technical-Administrative Staff respectively.

4.4. Dean/Museum Director/Department Director

a. Is responsible for ensuring that students are made aware of the ICT regulations, and that this is accepted in writing (electronically) before they gain access to NTNU's ICT infrastructure.
b. Makes a decision to exclude up to 14 days of NTNU's ICT infrastructure as a sanction against students in the event of a breach of the ICT regulations.
c. Makes a formal decision to exclude NTNU's ICT infrastructure beyond 14 days as a sanction against students for violations of ICT regulations.
d. Makes a formal decision on access to the user's mailbox, etc.

4.5. Line manager

a. Is responsible for ensuring that employees are made aware of the ICT regulations, and that this is accepted in writing (electronically) before they gain access to NTNU's ICT infrastructure.
b. Follows up that nonconformities within information security and privacy are reported in the nonconformity system in accordance with. The topic specific policy for “discrepancy reporting and discrepancy processing within information security and privacy".

4.6. User

[5] https://i.ntnu.no/wiki/-/wiki/English/Regulations+on+delegation

a. Users are responsible for familiarizing themselves with the ICT regulations and other rules for the use of NTNU's ICT infrastructure and complying with this.
b. Users shall ensure that breaches of policies within information security and privacy are reported without undue delay to their immediate manager and/or in NTNU's deviation system.