



Norges miljø- og
biovitenskapelige
universitet

ICT regulations for NMBU

Adopted by the Joint Board for the Norwegian School of Veterinary Science (NVH) and the University of Life Sciences (UMB)

Table of contents

- 1 The scope of NMBU's ICT regulations..... 3
 - 1.1 Scope..... 3
 - 1.2 Information and requirement that users are familiar with the regulations 3
 - 1.3 Definitions and terms..... 3
- 2 The purpose of NMBU's ICT system and acceptable use..... 3
- 3 Loyal use and the responsibilities of the users (requirements of users) 4
 - 3.1 Identification..... 4
 - 3.2 Loyal use of the ICT system and resource awareness..... 4
 - 3.3 Data security..... 4
 - 3.4 Use of personal equipment 5
 - 3.5 Unacceptable activity..... 5
- 4 Respect for other users and protection of privacy..... 5
- 5 Respect for copyright..... 5
- 6 Ownership of data and access..... 6
 - 6.1 Ownership and integrity..... 6
 - 6.2 Handling data when a user role is terminated 6
 - 6.3 Access..... 6
 - 6.4 Interventions 6
 - 6.5 Monitoring of equipment..... 6
- 7 Duty of confidentiality 7
- 8 Service quality and liability in damages 7
- 9 Sanctions..... 7

1 The scope of NMBU's ICT regulations

1.1 Scope

These regulations apply to the use of the university's ICT system. By ICT system is meant common computers and IT systems, end user equipment, networks, programs, data etc. that are provided by the university. The regulations apply to employees, students and others who are granted access to the ICT system.

The regulations also apply to the use of private equipment or other equipment that is not provided by NMBU, when it is connected to NMBU's ICT system and used to process NMBU's information.

1.2 Information and requirement that users are familiar with the regulations

The regulations are given to people who register as users for the first time, or are made known to the users in another way. The regulations are available in electronic form in NMBU's internal control system and can be obtained by contacting the IT department.

Users are obliged to keep up-to-date about the applicable ICT regulations and any supplementary provisions at all times.

1.3 Definitions and terms

User	Person who has been granted access to and uses the ICT system
ICT system	Computers, IT systems and specialist systems, end user equipment, networks, programs, data etc. that are provided by the university.
Data	Information stored in the university's ICT system
Personal areas	Data storage areas to which users have exclusive access and can store their own data. NMBU defines the following areas as personal: the local area, email account and local computer.
Authentication key	A combination of username and password, PIN code card or other secret combination of device and code known only to the user and used to grant access to the ICT system.
Disruptions to operations	Disruptions of IT services can be caused by technical failures (hardware errors, software errors or configuration errors), external disruptions (online attacks) and user-initiated error situations.

2 The purpose of NMBU's ICT system and acceptable use

The university's ICT system shall be used to meet NMBU's objective.

The ICT system shall not be used for purposes which are incompatible with NMBU's objective, fundamental values and regulations. The use of NMBU's ICT system for purposes that are unlawful in Norway may result in NMBU imposing independent sanctions.

3 Loyal use and the responsibilities of the users (requirements of users)

3.1 Identification

Users are obliged to identify themselves with their own authentication key when using the ICT system.

Users are obliged to keep their authentication key secret. Users are not permitted to hand over or lend their authentication key to other users.

If a user's personal authentication key is lost or becomes known to others, the user is obliged to change the key as soon as possible.

Users are responsible for all activity in NMBU's ICT system that takes place via user accounts to which access has been granted using the user's authentication key.

3.2 Loyal use of the ICT system and resource awareness

Users are obliged to comply with instructions from operating personnel concerning use of the ICT system.

Users are obliged to familiarise themselves with guidelines and documentation to a sufficient and satisfactory extent, so that the risk of disruptions to operations as a result of ignorance is reduced.

Users are responsible for ensuring that their own activities do not take up more of NMBU's ICT system's resources than necessary.

Users shall only use NMBU's ICT system in accordance with the ICT system's purpose.

Use that is unnecessary in relation to NMBU's objective is only accepted if the resource use is insignificant. NMBU's IT manager decides whether such use can be considered insignificant or not.

3.3 Data security

Users must not contribute to disruptions arising in any part of the system or in other ways cause inconvenience to others.

Users are obliged to take the necessary measures to reduce the risk of any loss of own data, programs etc. by taking backups, storing media in a satisfactory manner, complying with recommended procedures for use of NMBU's network infrastructure and using the available protective mechanisms.

Users are obliged to prevent unauthorised persons from gaining access to NMBU's ICT system.

Users are obliged to bear in mind that programs or data can contain undesirable elements, and must take appropriate quality control and protection measures.

Users are obliged to report any matters that could affect the security or integrity of the ICT systems to their immediate superior or the IT department.

3.4 Use of personal equipment

Users may use their own equipment and connect it to NMBU's ICT system. The level of access depends on the certification of the equipment.

NMBU's ICT regulations and information security policy apply when users connect their own equipment to NMBU's ICT system. Users are obliged to familiarise themselves with the applicable information security policy and pertaining procedural documents before connecting their own equipment to the system.

When downloading NMBU's information from NMBU's ICT system onto users' own equipment, NMBU's ICT regulations and information security policy apply.

3.5 Unacceptable activity

Users must not use the ICT system to carry out, aid or abet, or incite actions that are in violation of Norwegian law or NMBU's regulations.

It is prohibited for users to use NMBU's ICT system for their own private and/or commercial purposes.

4 Respect for other users and protection of privacy

Users must not attempt to gain unauthorised access to other people's data, programs etc. or to obtain other people's passwords or other security elements.

By accepting these regulations, users undertake a duty of confidentiality in relation to personal information about others that they become aware of through using the ICT system.

5 Respect for copyright

Users are obliged to respect copyrights, i.e. other people's rights to copyrighted material. It is not permitted to use NMBU's ICT system to distribute or store copyrighted material in violation of the copyright holder's interests.

When the university makes programs or data etc. available, users are obliged to respect the limitations on use that follow from the licence agreement. The agreement will be available from the IT department.

Users are not permitted to copy programs using the university's equipment over and above what follows from agreements concerning right of use (licence agreements).

It is not permitted to copy licensed programs for private use, unless this is permitted under the licence agreement with the university.

6 Ownership of data and access

6.1 Ownership and integrity

Data stored in a user's personal areas are in principle considered personal.

All users are entitled to having their privacy and integrity protected against infringement

6.2 Handling data when a user role is terminated

Users are responsible for emptying their personal data storage areas upon termination of their user role.

Users are responsible for handing over any data of importance to NMBU's activities to their immediate superior.

The personal areas will be deleted by the IT department without further inspection three months after termination.

In cases where the user role is terminated because a user dies or otherwise becomes incapable of fulfilling his/her commitments, special procedures in NMBU's internal control system apply.

6.3 Access

According to the Personal Data Regulations Chapter 9, an employer has right of access to personal areas under certain circumstances. Right of access applies under the following circumstances:

- When necessary to protect other legitimate interests in the organisation.
- When there is reason to suspect that the use of the ICT system involves gross breaches of the obligations that follow from the employment relationship.
- When there is reason to suspect that the employee's use of the ICT system could give grounds for dismissal with or without notice.

Power of decision regarding access rests with the Rector.

6.4 Interventions

An intervention is an act that is carried out by the IT department's personnel in NMBU's ICT system and that can involve access to personal areas, including unintentional access.

If the IT department seeks such access, permission must be obtained in advance from the Rector, unless particularly weighty reasons exist that warrant immediate intervention. Such weighty reasons must be documented to the Rector after the intervention has taken place.

6.5 Monitoring of equipment

If a workstation or other end user equipment is monitored on grounds of operational security or for other reasons, information about this shall be provided by labelling the unit or in some other expedient manner.

7 Duty of confidentiality

The IT department's personnel have a duty of confidentiality concerning information about users or the activities of users of which they become aware in the performance of their work. The duty of confidentiality does not apply to circumstances that could represent a breach of regulations and which must be reported to the appropriate bodies.

8 Service quality and liability in damages

Users are responsible for their use of information, programs, etc. made available through the ICT system. The university accepts no liability for financial loss resulting from errors or defects in programs, data, the use of information from available databases or other information obtained through NMBU's network infrastructure etc.

9 Sanctions

Violation of these regulations can lead to users being denied access to the university's ICT system.

Violations of provisions relating to protection of privacy, the duty of confidentiality etc. can lead to liability in damages and/or criminal liability. Employees who misuse the ICT system may be subject to the normal sanctions concerning dismissal with or without notice, and disciplinary measures may be imposed on students who misuse the system.