Regulations
for users of ICT resources at UiT The Arctic University of Norway

Adopted by: The University Board Date: 7.9.2018
Unit responsible: Department of Information Technology ID: UiT.ITA.infosec.reg01
Last amended by: - Date: -
Replaces: Guidelines for use of the university’s IT resources Archive ref.: 2017/5560-3

Contents
1. Purpose ................................................................................................................................. 2
2. Scope .................................................................................................................................... 2
3. Identity .................................................................................................................................. 2
4. Permitted use ........................................................................................................................ 3
   4.1. Decent use ....................................................................................................................... 3
5. Information security ............................................................................................................. 4
   5.1. Logging .......................................................................................................................... 4
6. Right of access to employees’ e-mail and files .................................................................... 5
7. Disclosure of information and data ..................................................................................... 5
8. E-mail and digital collaboration .......................................................................................... 5
9. Processing of personal data ............................................................................................... 5
10. Termination or change of user relationship ...................................................................... 6
   10.1. Preservation, disclosure and erasure of data ................................................................. 6
   10.2. Return of equipment ..................................................................................................... 6
11. Accessibility and safeguarding of day-to-day operations .................................................... 7
12. Duty of confidentiality .......................................................................................................... 7
13. Liability for damages ........................................................................................................... 7
14. Criminal acts ....................................................................................................................... 7
1. Purpose
The purpose of these regulations is to clarify the rights and obligations of the users so the university’s information and communication technology infrastructure (ICT infrastructure) can be utilised in the best possible manner, while also safeguarding information security.

2. Scope
These regulations apply to any natural person (user) who uses the university’s ICT resources, including employees, students, guests and other users, and cover all use of the ICT resources, regardless of whether the use involves university-owned equipment or not. These regulations also apply to the use of third-party ICT resources when such use occurs through the user’s affiliation with UiT The Arctic University of Norway (UiT).

3. Identity
Within the framework of these regulations, the term user account means the personal account that UiT allocates to named individuals.

Users must identify themselves by name, user identity, password or another accepted way when using networks, systems and services. Users are not permitted to circumvent, or attempt to circumvent, the requirements UiT sets concerning identity. Furthermore, users are not permitted to lend their user account to others, even in isolated cases. The use of ICT resources in someone else’s name is strictly prohibited, and a user must not attempt to gain access to other users’ passwords, etc. or apply to obtain unauthorised access to data/information belonging to UiT or other users. This applies regardless of whether the data/information in question is protected or not. Moreover, the use of UiT’s ICT resources without prior approval is prohibited. See also Section 15 Sanctions.

An important principle is that user accounts must be attached to individuals to ensure that UiT has control over the use of the university’s networks, systems and services. However, in certain cases, there is a need for accounts that are not personal, e.g. joint accounts. The use by natural persons of such accounts must occur in line with stipulated instructions and, when using such accounts, the person(s) concerned are covered by these regulations. Access to set up and use such accounts is regulated by separate guidelines (document under preparation).
4. Permitted use

Access to UiT’s ICT infrastructure is given for appropriate use only. Users must only use their access for lawful, appropriate use, and must not acquire information they do not need in an official capacity, use the services for purposes other than what they are intended for, or exploit any weaknesses to obtain access they should not have. Refer also to Section 5 Information Security. Users should exercise special care with confidential information. See also Section 12 Confidentiality requirements.

Before ending their period of employment or study at UiT, users are responsible for ensuring that information owned/used by UiT is secured for UiT. See also Section 10.1.

UiT’s ICT resources are designed to strengthen and support our core activities. Users have a joint responsibility for ensuring that the resources are used in the best manner possible and that all use is justified in UiT’s objective. Private use of networks, e-mail and personal file areas is permitted to a limited extent, provided such use does not take up large resources, form part of business activities or is at the expense of tasks associated with research, teaching, dissemination and administration. Furthermore, users are obliged to store such information in folders marked “private” to ensure they are kept separate from UiT’s data. This applies to e-mail as well as files.

Private use of ICT resources other than the abovementioned requires special approval from the unit manager. Such decisions may be reviewed by the IT Director.

The ICT resources must be used in accordance with the objective of UiT. This excludes commercial use, unless special permission is given for a specific case. Such permission must be in writing and explicit, and given by the faculty director. Cases involving significant use of resources must first be clarified with the IT Director.

The users are obliged to respect the rights of others, including terms and conditions of agreements UiT has entered into. Furthermore, users have an obligation to check whether material they publish on websites, or otherwise make available using UiT’s ICT resources, are protected works. If so, the user is obliged to obtain the necessary permission from the rightsholder in advance. UiT makes it explicitly clear that users are not permitted to share data files, including music and media files, on or via UiT’s network without the permission of the author/originator. Furthermore, users are not permitted to post links to illegal material, including via file sharing programs, on UiT’s computer network. See also Sections 14 Criminal Acts and 15 Sanctions.

4.1. Decent use

UiT’s ICT resources must not be used to violate the peace of private life, advance slanderous or discriminatory remarks, distribute, watch or possess pornography, spread confidential information, or execute, encourage or contribute to criminal acts. Furthermore, users must refrain from indecent communication on the internet.
5. Information security

Before using UiT’s ICT resources, users must familiarise themselves with the Information Security Management System at UiT, including the ICT regulations and other relevant regulations, and is obliged to comply with these. Users must faithfully follow the guidelines and procedures that have been established to safeguard information security and should not seek to circumvent these. Furthermore, users are obliged to follow instructions relating to the use of ICT resources, including instructions given by the operations personnel. Users must also adequately familiarize themselves with instructions, documentation, etc. for the systems they use to prevent damage and loss.

Users are responsible for ensuring that files and documents are handled in an appropriate manner, within the framework set by UiT, as well as preventing unauthorized persons from accessing UiT’s ICT resources.

As a starting point, users’ private files are considered personal, UiT has no responsibility for these and users should protect these to prevent unauthorized access. See also Sections 4 Permitted use and 6 Right of access to employees’ e-mail and files.

When selecting and using passwords for UiT’s ICT resources, the user must follow the Retningslinje for bruk av passord ved UiT (Guidelines for use of passwords at UiT) (document under preparation). The user is obliged to avoid using the password for their UiT account for other services, including for private use, and sharing their password or other security elements with others.

The use of UiT’s ICT resources with privately-owned equipment (e.g. privately-owned computers, mobile phones, etc.) must be limited. In cases where privately owned equipment is used, users are obliged to ensure that the equipment in question complies with the security requirements set by UiT (e.g. antivirus programs, firewall, system for regular updates, the password/PIN of the device, etc.). Some of UiT’s ICT resources must only be used with equipment owned by UiT. If this is the case, this will be stipulated in the guidelines for use of the service in question. This may also apply to certain types of data, such as confidential data, regardless of the system or service used to process these data. If such cases, special regulations will apply.

Users are required to report matters that may affect IT security to UiT’s Computer Security Incident Response Team (CSIRT), see uit.no/csirt. Discrepancies related to information security must be reported in accordance with the prescribed procedure, see uit.no/sikkerhet. This includes any weaknesses or breaches that the users discover in systems or services.

5.1. Logging

All use of UiT’s ICT resources can be logged. These logs are used to support the operation of UiT’s ICT systems, as well as safeguarding information security.

Logging at UiT, including what is logged and how the logs are used, is regulated by the Retningslinje for logging og bruk av logger i IT-systemer (Guidelines for logging and use of logs in IT systems) (document under preparation).
6. Right of access to employees’ e-mail and files
Under certain circumstances, UiT can access employees’ e-mail and personal areas in UiT’s computer network, or on other electronic equipment belonging to UiT and that is at the disposal of the employee to use in his/her work. This is regulated in Retningslinjer for gjennomføring av innsyn i ansattes e-post og filer (Regulations for implementation of access to employees’ e-mail and files).

7. Disclosure of information and data
User data, information, logs and/or traffic data are only disclosed to external sources, including the Police and the prosecuting authority, if legal grounds for such disclosure exist. Decisions relating to disclosure are made by the IT Director. The University Director shall always be informed about such disclosure and involved directly before a decision is made if the circumstances so indicate. See also Section 10.1 Preservation, disclosure and erasure of data concerning the disclosure of content in the “private” folder in the event of a user’s death.

8. E-mail and digital collaboration
E-mail must only be used for communication and not for prolonged storage and/or filing of information. The use of e-mail is regulated in the Retningslinjer for bruk av e-post ved UiT Norges arktiske universitet (Guidelines for use of e-mail at UiT The Arctic University of Norway) (document under preparation).

Other communication and collaboration solutions must be used in line with the guidelines and premises set for the solution in question.

During communication, all users must act objectively, constructively and respectfully. For employees, UiT has compiled a joint kjørreregler for bruk av sosiale medier og digital samhandling (rules for use of social media and digital collaboration).

9. Processing of personal data
Users who processes/shall process personal data, whether administrative, in connection with teaching, in research or student projects or in other contexts, are obliged to familiarise themselves with the current regulations concerning data protection and UiT’s own guidelines for processing of personal data. UiT shall have full overview of, and control with, all processing of personal data. How these shall be notified internally depends on the nature and area of the processing, so refer to the guidelines for the respective activities and processes (research, education, administration and dissemination).
10. Termination or change of user relationship

10.1. Preservation, disclosure and erasure of data

Termination of user account

When the user’s relationship with UiT ends, e.g. on completion of their studies or term of employment, the user must ensure his/her private data is removed from UiT’s ICT resources. Users are responsible for ensuring that any data stored in their private area, and which is necessary for UiT’s future activities, is transferred to a specified system and/or storage area. This should be done in consultation with the employee’s immediate supervisor. Access to the user account will be closed when the user’s affiliation with UiT ends. The data will be erased no later than three months after closure of the user account.

In event of a user’s death, the user account will be closed immediately after UiT has received the necessary confirmation of the death. E-mail and files that are necessary to maintain day-to-day operations or other legitimate interests will be retrieved in line with Retningslinjer for gjennomføring av innsyn i ansattes e-post og filer (Regulations for implementation of access to employees’ e-mail and files). Content in folders marked “private” will be erased after three months, and disclosure of content in private folders can only occur if adequate legal grounds exist. Decisions concerning the disclosure of content in private folders are made by the University Director.

Change of position internally at UiT

If the user changes position internally, especially if this is to another unit, the user must ensure that files, etc. belonging to the unit/position he/she is leaving, are transferred and secured. An assessment must be undertaken in consultation with the unit about whether there are files and documents the employee concerned shall not have access to in his/her new position. If such files, etc. are stored in the user’s personal area, these must be erased from there. Such erasure shall be taken care of by the user, who must confirm to the unit that this has been done.

The unit the employee is leaving must review the accesses the user has to file areas, individual files, specialist systems, services, etc., and take care of withdrawing the accesses (including access level) that are no longer necessary.

10.2. Return of equipment

When the user’s relationship with UiT ends, all ICT equipment (laptop computers, mobile phones, tablets, external memory sticks, etc.) that UiT has made available to the user must be returned in accordance with an agreement with the user’s immediate supervisor.

If the user changes their terms of employment internally, i.e. transfers from one unit to another, clarification must be sought from the Department of Information Technology about whether standard equipment (office computer and related equipment, i.e. computer, screen, docking station, keyboard, mouse and camera) shall accompany the employee to the new unit. However, for equipment that was purchased directly (e.g. tablets, mobile phones, external memory sticks and external hard disks, etc.), the unit manager shall decide whether such equipment should be returned to the unit that issued it or whether it may be taken to the new unit. Such clarification must occur before the employee changes their place of work.
11. **Accessibility and safeguarding of day-to-day operations**

UiT can temporarily close user accounts or access to systems and/or services when this is necessary prevent or resolve operational disruptions or incidents concerning information security. Systems and/or services may be inaccessible to many or all users when it is necessary to carry out necessary operational tasks to safeguard the stability and security of the systems and/or services. To the extent possible, advance notification will be provided in service announcements to users via uit.no and/or UiT’s intranet.

12. **Duty of confidentiality**

Everyone who performs services or work for UiT is subject to the duty of confidentiality, cf. Section 7-6 (1) of the Act relating to universities and university colleges, cf. Sections 13 to 13e of the Public Administration Act. Students are subject to the duty of confidentiality, pursuant to Section 4-6 of the Act relating to universities and university colleges.

Attention is drawn to the fact that the systems administrator and operations manager have a duty of confidentiality concerning information about the user or the user’s activities, but this does not prevent them from notifying higher levels of authority at UiT of any matters that may constitute violations of the regulations. See also Section 15 Sanctions.

13. **Liability for damages**

Users are responsible for the use of data that is made available by using the ICT resources. UiT disclaims liability for any financial loss resulting from faults or shortcomings in UiT’s ICT infrastructure, e.g. faults or shortcomings in data, the use of data from accessible databases or other sources, etc.

UiT is not liable for any damages that occur to the user as a result of insufficient protection of their own personal data.

If UiT becomes liable for damages, or suffers other financial losses, due to wilful misconduct or gross negligence on the part of the user, including misuse of the ICT resources, consideration will be given to whether grounds exist for seeking recourse and/or compensation from the user concerned.

14. **Criminal acts**

If suspicion arises that UiT’s ICT resources are being used in connection with criminal acts or attempts of such, UiT will consider reporting the matter to the Police even if UiT is not the aggrieved party. However, reporting suspicion of serious violations of the law, or attempts of such, to the Police is standard procedure.

15. **Sanctions**

In the event of breaches of the *Regulations for users of ICT resources at UiT The Arctic University of Norway* and associated regulations, UiT will consider imposing a reaction.

UiT cannot withdraw rights from users or hold them responsible for their actions where these are a direct result of failures in UiT’s ICT services and/or resources. However, this does not apply if such failures are intentionally exploited by the user.
The form of the reaction will be assessed based on how serious the violation is, whether the user has previously violated the regulations, the consequences the form of reaction will have for the user and other aspects of the case.

Examples of forms of reaction that may be imposed include temporary exclusion from some or all ICT resources at UiT (services), a warning, disciplinary reactions pursuant to the Civil Servants Act, exclusion from studies and examinations pursuant to the Act relating to universities and university colleges or liability for damages, etc.

Temporary closure of a user account and/or exclusion from services may be imposed in connection with justified suspicion that:

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

Decisions concerning temporary closure of students’ user accounts and/or exclusion from services will be processed pursuant to the provisions concerning individual decisions in the Public Administration Act. Decisions concerning closure are made by the IT Director. The University Director shall always be informed of such decisions and involved directly before a decision is made if the circumstances so indicate.

If the student shall sit an examination during the period his/her user account is closed and/or he/she is excluded from other relevant services, and the examination in question is an electronic examination, UiT shall either provide alternative access to the examination platform or find another appropriate solution so the student can sit the examination. This also applies for compulsory coursework requirements.

If there is reason to assume that someone is abusing access to electronic communications with UiT, the person concerned can be partially or completely denied further use of such communications with UiT, cf. Section 14 of the eGovernment regulations.

16. Appeals

Individual decisions to students, and decisions concerning the temporary closure of students’ user accounts and/or access to services, may be appealed to the university’s appeals committee no later than three weeks after the party concerned has been advised of the decision, cf. Section 5-1 (1) of the Act relating to universities and university colleges.

Decisions concerning disciplinary action, dismissals or suspensions pursuant to the provisions of the Civil Servants Act may be appealed, cf. Section 35 of the Civil Servants Act. The appeals body is regulated by Section 33 of the Civil Servants Act.

Other individual decisions may be appealed within three weeks of the date of the decision. The appeals body is the Ministry of Education and Research.
17. **Delegation of authority**

The University Director has delegated authority to change these regulations. Updates can be undertaken by the Director of the Department of Information Technology.

The Director of the Department of Information Technology has delegated authority to stipulate guidelines and procedures pursuant to these regulations. New guidelines and procedures shall be contained in a list of appendices to these regulations. This list shall be published on a specific web page about these regulations and kept updated.

18. **References**

- Act of 15 June 2018 no. 38 relating to the processing of personal data (The Personal Data Act)
- Act of 10 February 1967 relating to procedure in cases concerning the public administration (The Public Administration Act)
- Act of 1 April 2005 no. 15 relating to universities and university colleges
- Act of 16 June 2017 no. 67 relating to civil servants (The Civil Servants Act)
- *Forskrift av 2. juli 2018 nr 1108 om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale* (Regulations of 2 July 2018 no. 1108 concerning employers’ right of access to employees’ e-mail inboxes and other electronically stored material)
- Regulations of 25 June 2004 no. 988 on electronic communication in public administration (eGovernment)
- Information Security Management System at UiT The Arctic University of Norway
- Local regulations, guidelines and procedures, etc. at UiT The Arctic University of Norway