University of Stavanger ICT Regulations

Administrator	Head of Section, Support			**Name**	Nils-Arne Midtun
Owner/approved	Director of IT	30/08/2021		**Name**	SM Bjerke
Valid from	01/09/2021	**Valid to**	Next revision	**Classification**	Open (green)

1 Objective

The purpose of the regulations is to describe the rights and obligations of individuals when using the University's information and communication resources ("ICT resources"). These regulations shall also contribute towards ensuring compliance with the University of Stavanger's Data Security and Protection of Personal Information Regulations.
All users shall have a duty to notify the University of Stavanger IT department if they become aware of a breach of these regulations.

2 Scope

These regulations shall apply to all physical persons ("users") that use the University's ICT resources, whether they are employees, students, visitors or others. These regulations shall cover all use of ICT resources, regardless of whether such use occurs using university equipment or not. These regulations shall also apply to the use of third-party ICT resources (such as cloud services) when such use occurs in connection with the user's affiliation with the University of Stavanger.

3 Target group

Students, employees, visitors and anyone else using the University of Stavanger's ICT resources.

4 Description

4.1 User obligations

4.1.1 Identity

Anonymous use of University of Stavanger ICT resources is not permitted. All users shall use their personal University of Stavanger user account for login, identification and authentication. Details of the user account shall not be shared with anyone.

This means

- that users must always identify themselves using a valid personal University of Stavanger user account
- that it is not permitted to circumvent or attempt to circumvent the requirement set out by the University of Stavanger in relation to identification and authentication.

- that the use of ICT resources under the names of others is strictly prohibited. No attempts should be made to gain access to passwords, etc. belonging to others, nor should attempts be made to obtain unauthorised access to data/information belonging to the University of Stavanger or other users. This applies regardless of whether the data and information is protected or not.
- that user accounts must be linked to individuals, so that the University of Stavanger has control of who the University's ICT resources are used by.
- non-personal accounts may be required in certain cases. The creation and configuration of such accounts is managed by the University of Stavanger's IT department in accordance with separate guidelines. The use of such accounts shall be in accordance with established rules and shall always be subject to these regulations.
- Anonymous use of certain services can also be configured (e.g. "Let Us Know *(Si fra)*").

4.1.2 Password management

All users shall comply with the University of Stavanger IT department's conditions for creating and managing passwords for University of Stavanger ICT resources.

This means

- that the password must meet the password requirements published in the portal for creating and changing passwords
- that the password for your University of Stavanger user account cannot be used for other services, including personal ones
- that the password or other security elements cannot be disclosed to others

4.2 Permitted use

4.2.1 Appropriate

Users shall use their access solely for lawful, appropriate purposes.

This means

- that users shall not acquire information for which they have no appropriate work requirements
- that users shall not use the services for purposes other than what the services are intended for or exploit any weaknesses in order to obtain access they are not supposed to have
- that users shall exercise particular diligence in relation to confidential data and information
- that commercial use is not permitted without written approval from the senior director of the department in question
- the production and "mining" of cryptocurrency is considered commercial use and is therefore not permitted
- users shall have a duty to document that the software they install on University of Stavanger ICT equipment has the correct license for the intended use. The University of Stavanger IT department shall be entitled to verify this and to uninstall any software that is found not be properly licensed.

4.2.2 Private use

Private use of the network, e-mail and personal file areas is permitted to a limited extent. Such information shall be placed in folders labelled “Private” so that they are kept separate from University of Stavanger data. This shall apply to both e-mail and files stored locally or in cloud services.

This means

- that personal use shall not occupy large amounts of resources
- that personal use shall not be carried out as part of business activities
- that personal use shall not infringe upon duties that are part of research, teaching, dissemination or administration
- personal use of ICT resources other than what is listed above must be agreed separately with the head of unit. Such decisions may be overruled by the Director of IT

4.2.2.1 The relationship between personal and University of Stavanger use

- Your University of Stavanger e-mail address should normally be used for all work-related tasks. This means, for example, that your University of Stavanger e-mail address must be used as your username for apps, logins to online resources, etc. that relate to work or studies.
- Your personal e-mail address must not normally be used for purposes relating to work or studies.

4.2.3 Rights

All users shall respect the applicable laws relating to copyrights, licenses and terms and conditions in connection with the agreements entered into by the University of Stavanger. This applies both to software and other privileged information such as text, images and audio.

This means

- that the user shall have a duty to investigate whether the data made available by the user to others using University of Stavanger ICT resources constitutes protected works
- that the user shall have a duty to obtain the necessary permissions from rightsholders before privileged content is made available to others
- that it is not permitted to make data, music or media files available on or via University of Stavanger ICT resources without permission from the rightsholder. The user shall have a responsibility to document such permission from rightsholders.
- that the user shall not be permitted to post links to illegal materials or use file-sharing software on University of Stavanger ICT resources.

4.2.4 Etiquette/proper use

University of Stavanger ICT resources shall not be used to:

- infringe on privacy
- make defamatory or discriminatory statements
- distribute and/or record screenshots without consent
- acquire, view or disseminate materials that are prohibited by law
- distribute confidential information
- carry out, incite or abet criminal acts.

Furthermore, all users are expected to use proper language when communicating internally and online in cases where they represent the University of Stavanger.

4.2.5 Confidentiality requirements

Anyone who performs services or work on behalf of the University of Stavanger is subject to confidentiality requirements.
(cf. Section 7-6(1) of the Norwegian Universities and University Colleges Act and Sections 13 to 13(e) of the Norwegian Public Administration Act).

Students are subject to confidentiality requirements pursuant to Section 4-6 of the Norwegian Universities and University Colleges Act.

This means

- that system owners and administrators shall maintain confidentiality concerning users and their activities in the University of Stavanger's ICT systems
- that system owners and administrators shall still have a duty to report matters that are or could constitute a breach of these regulations and other regulations and guidelines
- such reports shall be submitted to the head of data security (Director of IT), who shall, in turn, determine further management of the matter

4.3 Data security and protection of privacy

Anyone using University of Stavanger ICT resources has a duty to familiarise themselves with the applicable rules and guidelines relating to the resources prior to use.

This means

- that everyone shall be familiar with and comply with the University of Stavanger Data Security and Protection of Privacy Regulations
- that everyone shall be familiar with and comply with the University of Stavanger ICT Regulations
- that everyone shall record all processing of personal data
- that everyone shall properly follow up on established guidelines and procedures to safeguard data security and shall not attempt to circumvent these
- that all users shall have a duty to adhere to the specified instructions for the use of ICT resources, including instructions issued by the University of Stavanger IT department.
- that the use of systems shall be in accordance with requirements set out by the system owner.

Each user shall be responsible for ensuring that all data is managed properly and within the frameworks established by the University of Stavanger and for preventing unauthorised persons from gaining access to ICT resources.

Users' personal files are generally considered to be personal and the University of Stavanger shall not be responsible for such files. Users shall be independently responsible for the protection of personal data.

All users shall have a duty to report matters that could be of significance to data security. Such matters shall be reported to the University of Stavanger IT department.

4.3.1 Logging

All use of University of Stavanger ICT resources may be logged. Logs are used to maintain data security and safeguard the operation of University of Stavanger ICT systems. This has been endorsed through the University of

Stavanger Data Security and Protection of Privacy Regulations. The University of Stavanger IT department's Incident Response Team (IRT) manages the above, preventively and reactively, in the event of security incidents.

4.3.2 Disclosure of personal data

Such data shall generally not be disclosed but there are certain exemptions. In the event that such disclosure is to take place, disclosure shall be based on a ruling from a Norwegian court.

This means

- that the police or prosecuting authorities may require access to the identification of a user of an IP address pursuant to Section 2-9 of the Norwegian Electronic Communications Act. In the event that other data is to be disclosed, the request shall reference a ruling from a court.
- that anyone else who requests the disclosure of personal data must have a ruling from a Norwegian court.
- that users may request disclose of data relating to themselves only.
- in the event that a request relates to the disclosure of data concerning employees, the matter shall be determined by the Director of Human Resources.
- in the event that a request relates to the disclosure of data concerning students, the matter shall be determined the Director of Academic Affairs.
- in the event that the request relates to disclosure of more general data, the matter shall be determined by the Director of IT.
- the Director of Organisation and Infrastructure shall always be informed in the event of disclosure of personal data and shall be directly involved in decision-making if dictated by the circumstances

4.3.3 Users' requests for access to their own personal data recorded in University of Stavanger records

This is governed through Article 15 of the Norwegian Personal Data Act (GDPR). In certain cases, users shall be entitled to access to, as well as correction and deletion of data.

This means

- if the request relates to access to or correction or deletion of data relating to employees, the Director of Human Resources shall coordinate and determine the matter in consultation with the Director of IT.
- if the request relates to access to or correction or deletion of data relating to students, the Director of Academic Affairs shall coordinate and determine the matter in consultation with the Director of IT.

4.3.4 Access to e-mail and file areas

The University of Stavanger may access employees' e-mail and personal areas in University of Stavanger systems, subject to certain conditions being met.

This means

- that the Norwegian Working Environment Act shall govern how and when such access can be made.
- that the University of Stavanger may only access e-mail accounts that the University has made available to the user
- that the University of Stavanger may access file storage areas in the University's own infrastructure or cloud services for which the University of Stavanger has granted the user access to.
- that the University of Stavanger may access physical devices that are owned by the University and made available for the user to use

4.4 Use of ICT resources

All use of ICT resources shall be in accordance with the principles set down in 4.2 concerning Permitted use.

This means

- that the University of Stavanger IT department shall be entitled, without notice, to audit, inspect, modify or remove all ICT resources linked to University of Stavanger ICT infrastructure and that are not in accordance with these regulations.
- that attempts to prevent the University of Stavanger IT department from gaining access to ICT resources shall be deemed unauthorised use.
- that the University disclaims any liability for any losses arising as a result of necessary work to safeguard the confidentiality, integrity and availability of the ICT infrastructure

4.4.1 ICT resources managed by the University of Stavanger IT department

ICT resources that have been configured by the University of Stavanger IT department shall not be modified by others without approval from the University of Stavanger IT department.

This means

- that computers and other ICT equipment shall not be modified in such a way that could compromise ICT and data security. This shall apply to hardware, software and configuration settings alike
- Fixed ICT resources shall not be removed from the locations in which they have been placed
- ICT equipment shall be stored in such a way that it is protected against theft and unauthorised access
- that it is not permitted to connect or remove any form of networking equipment to the University of Stavanger ICT infrastructure

4.4.2 ICT resources not managed by the University of Stavanger IT department

In certain cases, there may be scientific or educational reasons for employees, students or groups at the University of Stavanger being permitted to establish their own ICT resources. This can take place only by agreement with the University of Stavanger IT department.

This means

- that the University of Stavanger's IT department and the University itself shall not be responsible for such ICT resources or data managed therein. Those responsible for the operation of the ICT resources in question shall be liable for any damages or losses arising as a result of use or misuse.
- The University of Stavanger IT department cannot be expected to provide equipment and software for the purpose of connecting ICT resources that are not managed by the University of Stavanger's IT department to University of Stavanger ICT infrastructure.
- the following must be clarified with the University of Stavanger IT department before ICT resources are established at university premises:
    - who is responsible for the ICT resources (an individual)
    - what kind of information will be processed
    - physical location of the ICT solution
    - ICT resources shall be configured in accordance with the instructions provided by the University of Stavanger IT department
    - Under no circumstances may ICT resources be used for the storage and distribution of unlawful software or information

- ICT resources shall be accessible to the University of Stavanger IT department's operational staff at all times
- If necessary, the University of Stavanger IT department may disconnect the ICT resources from the network at any time and without prior notice if necessary to safeguard the confidentiality, integrity or security of the University of Stavanger

4.4.3 Domain management

Domains registered using the University of Stavanger organisation number must be approved and governed by the Department of Communication and Public Affairs and the University of Stavanger IT department.

This means

- that the University of Stavanger IT department shall have an overview of all domains registered using the University of Stavanger's organisation number
- that the University of Stavanger IT department shall assess the security of the solutions prior to creation
- that the Department of Communication and Public Affairs shall approve the creation of domains based on the University of Stavanger communication strategy.
- that anyone asking for the creation of a domain shall be responsible for the content published on the domain and for safeguarding data security and the protection of privacy.
- The Department of Communication and Public Affairs shall have overall editorial responsibility for the content published on such domains and may remove undesired content.
- The Department of Communication and Public Affairs and the University of Stavanger IT department will collaborate to perform regular domain audits and may decide to discontinue domains.

4.4.4 Users' personal ICT equipment

Users that use their personal equipment for work or studies shall be responsible for ensuring that such use is in keeping with the University of Stavanger's regulations and guidelines. Examples include forwarding or downloading e-mails or documents to personal computers or mobile phones.

This means

- that users must ensure that the equipment complies with the security requirements set out by the University of Stavanger (such as updated operating systems, software and antivirus, etc.)
- that users shall not be permitted to install or connect personal devices to the University of Stavanger's wired networks without approval from the IT department.
- that separate wireless networks have been established for use with personal devices (e.g. Eduroam)
- that users are not permitted to establish their own information servers (WWW, FTP, IRC, etc.) or multi-user systems without the agreement of the University of Stavanger IT department
- that users shall not be permitted to connect networking equipment such as routers, switches or wireless access points to the University of Stavanger's ICT infrastructure. This shall also apply to the establishing of equipment that interferes with or damages the performance and scope of the equipment belonging to the University of Stavanger.

4.5 Termination or modification of user relationships

4.5.1 Termination of user accounts

When the user's relationship with the University of Stavanger ceases, for example at the end of studies or employment, the user shall be responsible for ensuring that any necessary data is retained. This applies both to data required by the University of Stavanger and for personal use.

This means

- that the user shall ensure that they make any copies and delete their personal data from the University of Stavanger's ICT resources
- that the user shall be responsible for ensuring that any data that is required by the University of Stavanger that is stored in personal areas is transferred to the University of Stavanger. This shall be done in consultation with the immediate supervisor
- access to the user account shall be disabled when the affiliation with the University of Stavanger ceases
- the user shall be notified via e-mail of when the account will be disabled. All data will be deleted following a given period after the account has been disabled.

4.5.2 In the event of the user's death

The user account shall be disabled immediately after the University of Stavanger has received necessary confirmation of the death. Any e-mails or data necessary to maintain everyday operations or safeguard other justified interests shall be retrieved.

This means

- that the retrieval of data shall take place in keeping with the guidelines on access to employees' e-mails and files
- that the content of folders labelled "personal" shall be deleted after three months
- that the disclosure of the content of the personal folder may take place only if there is a sufficient legal basis for such disclosure. The decision to disclose the content of personal folders shall be made by a level 2 supervisor in consultation with the Director of Human Resources.

4.5.3 Changes to internal position with the University of Stavanger

The supervisor of the user whose position or unit at the University of Stavanger is changing shall be responsible for ensuring that data and access to data is safeguarded for the position or unit that the user is leaving.

This means

- that the user shall ensure that data belonging to the unit or position they are leaving shall be transferred and made available to the unit/position in question.
- that the supervisor shall consider whether there is any data the individual should no longer have access to in their new position
- that if such data is stored in the user's personal area, the data shall be transferred to the unit and deleted from the user's area. The user shall confirm to the supervisor that this has been done
- the user's supervisor at the unit the user is leaving shall review the user's access to file areas, individual files, systems, services, etc. and shall make sure to disable any access that is no longer required

4.5.4 Return of equipment

When the user's relationship with the University of Stavanger ceases, all ICT equipment (computer, mobile phone, tablets, memory sticks, etc.) that the University has made available to the user shall be returned. How such

returns will take place shall be agreed with the immediate supervisor. This is governed more closely in the regulations for the management of ICT equipment.

4.6 Accessibility and management of everyday operations

The University of Stavanger may disable user accounts or access to systems and services if necessary in order to prevent or resolve data security incidents or operational disruptions.

Systems and services may be periodically unavailable for all or some users, if necessary in order to perform work to ensure security and stability. To the extent possible, such work will be reported in advance using operations notices via the University of Stavanger website and intranet.

4.7 Liability

Users of the University of Stavanger's ICT infrastructure shall be responsible for familiarising themselves with and practising proper use of equipment and data that is processed.

This means

- that users shall have an independent responsibility for the use of data made available via University of Stavanger ICT resources
- that the University of Stavanger disclaims any liability for financial losses arising from errors or shortcomings in the University of Stavanger's ICT infrastructure. This includes errors or shortcomings in data, the use of data from available databases or other sources, etc.
- The University of Stavanger shall not be liable for damages on the part of the user as a result of inadequate protection of personal data in University of Stavanger ICT infrastructure
- that in the event that the University of Stavanger is held liable or suffers other financial losses due to intentional or grossly negligent actions on the part of the user, for example misuse of ICT resources, the University may consider seeking recourse or compensation from the individual in question.

4.8 Criminal acts

In the event of suspicion that the University of Stavanger's ICT resources are being used in connection with criminal acts or attempted criminal acts, the University of Stavanger will consider reporting the matter to the police at its own initiative, even in cases in which the University of Stavanger is not the aggrieved party. Suspicion of serious breaches or attempted serious breaches shall be routinely reported.

4.9 Sanctions

Sanctions will be considered in the event of breach of these regulations, associated regulations and rules.

The type of sanction will be determined based on the severity of the breach, whether there have been any previous breaches and what consequences the sanctions would have for the user and the circumstances in general.

Sanctions may include:

- temporary suspension of access to some or all ICT resources at the University of Stavanger
- disciplinary sanctions pursuant to the Norwegian Civil Servants Act

- suspension from studies and exclusion from examinations pursuant to the Norwegian Universities and University Colleges Act
- claims for compensation

The University of Stavanger cannot withdraw rights from users or hold users liable for their actions if the cause of such actions can be attributed directly to failure in University of Stavanger ICT resources and services. This shall not apply if the user intentionally exploits such a failure.

This means

- that a decision to temporarily suspend a user account and/or access to services for employees shall be determined by the Director of IT in consultation with the Director of Human Resources. The Director of Organisation and Infrastructure shall always be informed of such decisions and shall be directly involved in decision-making if dictated by the circumstances. The line manager shall be informed.
- that a decision to temporarily suspend a user account and/or access to services for students shall be determined by the Director of IT in consultation with the Director of Academic Affairs.
- that if a student is due to digitally sit an examination during the period in which the user account and/or relevant access is suspended, the University of Stavanger IT department shall provide alternative access to the examination platform or find an appropriate different solution so that the student can take the examination. The same shall apply to mandatory coursework requirements
- that if there is reason to believe that someone is misusing their access to electronic communications with the University of Stavanger, the individual may be fully or partially denied further use of such communications with the University of Stavanger, cf. Section 14 of the Norwegian Public Administrative Regulations.
- The University of Stavanger IT department may remove or block unlawful software and hardware running on University of Stavanger systems without prior warning

4.10 Appeals

4.10.1 Students

Decisions taken against students may be appealed to the University's Appeals Committee within three weeks of the decision having been received by the individual, cf. Section 5-1(1) of the Norwegian Universities and University Colleges Act.

4.10.2 Employees

Decisions relating to disciplinary action, suspension or dismissal taken pursuant to the Norwegian Civil Servants Act may be appealed, cf. Section 35 of the Norwegian Civil Servants Act. The appeals body is governed by Section 33 of the Norwegian Civil Servants Act.

4.11 Reporting incidents and breaches

Incidents and breaches of the regulations must be reported via e-mail to it-hjelp@uis.no

5 Glossary

5.1.1 University of Stavanger ICT resources

All hardware, software, networks and cloud services that the University of Stavanger makes available to employees, students, visitors and other users.

5.1.2 System owner

The system owner is a manager responsible for purchasing, developing, managing and operating an information system or IT service.

6 Document references

University of Stavanger Data Security and Protection of Privacy Policy

University of Stavanger Data Security and Protection of Privacy Regulations

Regulations for the management of ICT equipment

7 Appendices

N/A

8 Version history

Ver.	Date	Author(s)	Reason
0.9	14/12/2020	Midtun/Lie/Auning/Bryne	Created
0.9.1	03/03/2021	Midtun	Changes following consultation and input from the team working on the regulations.
0.9.2	25/08/2021	Midtun	Item 4.4.2 relating to the management of domains has been added
1.0	30/08/2021	Midtun	Approved and published