UNIS IT Policy

Policy number:	
Applies to:	All UNIS employees, students, guest lectures and others using the UNIS computer system
Effective Date:	Current

Document content:

1 Policy overview and scope

1.1 The UNIS computer system definition and policy impact

This policy covers all use of the UNIS computer system. The UNIS computer system is defined as:

> All UNIS owned recourses or resources employed by UNIS - including physical data network cables and electronics, servers, e-mail and Internet access, applications, data, as well as workstations and laptops (computers).

This policy covers personal computer resources as long as connected to the UNIS computer system. It further covers software licensed by UNIS installed on personal computers (ref. 2.5 Copying software).

This policy covers anyone not using UNIS resources, but who affiliate themselves with UNIS. (e.g., by using their UNIS mail signature or UNIS logo while using their private e-mail account). Whenever an individual is identified as being affiliated with UNIS, their use of computing resources would be subject to the requirements in this policy, even if the computing resources do not belong to UNIS.

1.2 Supplements

For specific parts of the UNIS computer system it may be worked out more detailed and supplementary rules/points within the scope of this policy/document.

1.3 Policy distribution and revision

All who this policy applies to should be given a copy of this policy document before using the UNIS computer system. The policy is considered read, understood and accepted when the computer system is used by the individual for the first time.

All who this policy applies to are expected to be, at all times, acquainted with the current version of this policy, including any supplementary rules as stated in point 1.2 Supplements.

2 Acceptable use of the UNIS computer system

2.1 Definitions and terms

User:	Anyone granted access to the computer system.
User Name:	A unique, symbolic name identifying a user of the computer system.
User Password:	A personal “key”. The password has to be entered in addition to the user name when being authorized on the computer system.
User Account:	A user’s defined and granted access rights to one or more computers, e-mail and/or data. The user account is made available to the user through the combination of User Name & User Password.

2.2 User accounts and passwords

A user account is strictly private. Use or intention to use other users’ user accounts and/or passwords is forbidden.
It is the users’ duty to ensure own passwords are not known to others. If a user knows or suspects own password is in hand of others, it is his or her duty to immediately change this password.

2.3 Purpose of use

The UNIS computer system is to be used for administrative, science and educational purposes only. It should not be used for any commercial activities without written approval from UNIS. It is each user's duty to ensure the system is used as correct as possible according to this.

UNIS has a wireless network (wlan) both in the Science Centre and the student houses. It is forbidden to set up other wireless routers/access points because this is detrimental to the performance of the wlan that's already in place.

2.4 Copyright and intellectual property regulations

In their use of the UNIS computer system, users must comply with all software licenses, copyrights, and all other local laws and regulations governing intellectual property and online activities.
By definition, anything posted on the Internet that is an original work (including e-mail, pictures, jokes, artwork, music, etc.) is protected by copyright law(s), whether or not it is explicitly indicated that the work is copyrighted, or the copyright (©) symbol is included. Therefore, users may not use such original works of authorship (e.g., by using "cut and paste" or "copy and paste"), or download music or videos without the author's (or artist's) express permission. In a text-based document, merely changing a few words is not enough to avoid copyright infringement issues. If a copyright law is violated using UNIS resources, UNIS can be implicated as a distributor.

2.5 Copying software

The software on the UNIS network was purchased under license agreements with the manufacturers, and is protected by copyright laws. These licenses and copyrights limit each user's right to copy, distribute, and use the software. Unless otherwise documented in the license agreement, users may not copy or distribute software from the UNIS network or media available at UNIS without prior written approval from the software's manufacturer. The user is personally responsible for any claim for indemnification set by the software manufacturer for use without permission.

If license allows installing the software on private computers when a user is associated with UNIS (as a student or employed), it is the user's duty to completely remove this software when this association discontinues.

2.6 Hacking / unauthorized access

It is strictly forbidden to actively try to gain unauthorized access to any part of the computer system as outlined in the UNIS computer system definition section. It is also forbidden in every respect to listen or tap network traffic.
If a user unintentionally should get access to data created or owned by another user, he or she is expected to notify the system administrator and the owner of the data.

2.7 A user's duty to report

Each user of the UNIS computer system is required to report to UNIS technical support personnel or UNIS leadership about any circumstances that may have an impact on the system's security or operational stability.

2.8 Electronic communication of inappropriate materials

Material that is unlawful according to Norwegian laws, i.e. defamatory statements or pornographic material, may not be sent by e-mail or other form for electronic communication (such as bulletin board systems, chat groups, newsgroups, or instant messaging services) using UNIS resources. Nor may it be displayed or stored on the UNIS's network.

2.9 Forwarding sensitive e-mail

Sensitive e-mail is defined as e-mail containing data that cannot be classified as unrestricted. Prior to sending a sensitive e-mail, the user must ensure that the recipients of the e-mail are authorized to view such information and that the e-mail is appropriately protected (e.g., via encryption, labeling, and disclaimers), in accordance with its classification level. If sensitive information is inappropriately distributed, it could lead to loss of reputation for UNIS.
UNIS e-mail must not be automatically forwarded outside of UNIS's control, such as to the Internet.

2.10 Chain e-mails

A chain e-mail is a message sent to a number of people asking each person to send the message to a specified number of other people to receive some benefit or avoid a negative occurrence. The number of chain e-mail recipients increases exponentially each time the e-mail is sent. This is very taxing to UNIS network resources, as well as to other external network resources, degrading performance and consuming unwarranted amounts of disk space. Therefore, UNIS users are prohibited from initiating or forwarding chain e-mails using their UNIS account or from a UNIS computer. Users must immediately delete any chain e-mails that they receive from others.

2.11 Spam

Spam is any unsolicited, non-business related e-mail, including chain e-mails, or offensive or harassing material. Sending spam intentionally from any UNIS account or computer is expressly prohibited.

2.12 Impersonation and anonymous e-mails

UNIS users may not, under any circumstances, use any techniques to modify the *From:* line or other sender or origin information in e-mails, messages, or postings to change, hide, or disguise their identity. Sending anonymous or pseudonymous electronic communications is strictly forbidden.

Sending e-mails on behalf of someone, when this is indicated in the e-mail, is acceptable.

3 Privacy

3.1 Expectation of privacy

The workstations, laptops, and user accounts given to UNIS users are to enable them to perform their jobs and studies in the most efficient and effective way possible. However, users should not have an expectation of absolute privacy in the materials that are created, sent, or received by them on UNIS systems. To the extent permitted by laws and regulations, UNIS authorized personnel (such as technology support personnel) may examine all material stored on UNIS systems without prior notice, (some examples of situations may include investigation for a suspected breach of security, or for the prevention or detection of crime, and other legally permissible situations).

3.2 Monitoring and computer usage

Subject to laws and regulations, UNIS may monitor any and all aspects of its computerized resources, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded from or uploaded to the Internet by UNIS users, and reviewing e-mail sent and received by UNIS users.
Wherever possible, monitoring will be carried out by methods which prevent misuse, such as automated monitoring software.

4 Means of reactions when not complying to this policy

4.1 Discontinue access to UNIS computer resources

A user who does not comply with this policy can partly or completely lose access to the UNIS computer system (UNIS computer system definition). In the process of investigating any incidents regarding breach of this policy, the UNIS technical support personnel can discontinue a user's access privileges up to one week. This should be done in a way that has as little impact for the user's work or studies as possible.