NHH	**MANAGEMENT SYSTEM FOR INFORMATION SECURITY** Governing documents		Classification: Open
	Version: 1.1	**Date of approval:** 19 June 2020	**Document ref.:**
Title: IT Regulations			
Applies to: NHH		**Responsible for the document** Office of IT Services	

1 Purpose

The purpose of the IT Regulations is to regulate the use of IT systems and equipment at the Norwegian School of Economics (NHH).

2 Scope of application

By IT systems is meant all software, computer systems, infrastructure and equipment used in connection with digital information and data processing, and the information and data stored in them. Digital communication linked to the above is also included, as are IT systems included in other infrastructure and equipment.

By IT systems at NHH is meant IT systems that are available at NHH, that are owned by or at the disposal of NHH, or that are made available to NHH's users by external parties, suppliers or others on assignment for or by agreement or understanding with NHH, and that are used by NHH's users or partners for purposes linked to NHH's activities.
The regulations apply to:

- Employees, students, guests and others who are given access to IT systems at NHH, hereinafter called users.
- All use of NHH's IT systems.

The regulations also apply to:

- The users' and other third parties' IT systems, insofar as they are used to perform tasks linked to NHH's activities, irrespective of whether the system is located on NHH's grounds or not.
- Private and other third parties' IT equipment that is connected to NHH's IT infrastructure (e.g. network), irrespective of the purpose it is being used for.

3 Access to NHH's IT services and systems

As a student or employee at NHH, you will have a user account at NHH that gives you access to its IT systems.

Access to NHH's IT systems can also be given to others with an official need. Access to the different systems and services is authorised by the system owner.

4 Termination of employment relationship or studies etc.

You must clear up your accounts well before the termination of an employment relationship or studies at NHH. Files linked to cases that you have processed shall be presented to your superior for assessment. Such files must not be deleted before this is approved by the relevant entity. As an employee you must ensure that files that may be of importance to NHH's activities, but that are not linked to specific cases, are presented to your immediate superior who will decide whether the files are to be deleted or, if relevant, filed.

4.1 Termination of user accounts and email accounts etc.

Students' user accounts are closed three months after their admission to study is terminated.

Employees' user accounts are closed on termination of the employment relationship. Employees' electronic mailboxes are closed on termination of the employment relationship, unless they must be kept open for a short period due to the presence of special circumstances.

As a retired NHH employee you can apply to keep your user account with changed account access. This must be approved in advance by the head of the entity where you last worked.

Other users' user accounts at NHH are closed when their affiliation to NHH ends, or when the approved access period expires.

Data linked to a user account is automatically deleted six months after the user account is closed. Data can be stored in back-up systems for a longer period, but no longer than one year.

In the event of a user's death, the user account will be closed immediately. The user account is deleted after six months unless there is a demand for access, or a right to the material is exercised as described in these regulations.

4.2 Return of equipment, software and licences

IT equipment and licences belonging to NHH must be returned. All copies of software, documentation and data owned by or borrowed from NHH must be deleted from private equipment.

5 Use of NHH's IT services and systems

NHH's IT systems shall be used to perform tasks linked to NHH's activities. Your use of NHH's IT services and systems must not violate laws, regulations or NHH's internal rules.

You must prevent others from gaining access to your user account. Nor must you attempt to gain access to other user accounts.

You must take steps to prevent unauthorised persons from gaining access to NHH's IT systems.

You must not, without permission, amend or modify NHH's IT systems or otherwise alter them to work in a different manner than intended.

You are obliged to respect copyright and similar rights to software, data and other digital information such as publications, images, music, films etc.

You must ensure that individuals' data protection is safeguarded and not violated.

You must avoid any use of IT systems that may entail a risk of significant loss of reputation for NHH.

You are obliged to immediately report any circumstances that may affect IT security and data protection at NHH to the Office of IT Services (hjelp@nhh.no).

6 Activity log and control

NHH's IT systems include logging and backup solutions for purposes that include enabling documentation of breaches of the law or non-conformance with internal rules and procedures, but also make it possible to uncover/detect security breaches in the IT infrastructure..

The Office of IT Services, represented by the IT manager, has the main responsibility for access control to NHH's network and general IT systems, and for mobile devices and equipment used outside NHH, and has the authority to exercise this control in accordance with NHH's management system for information security and data protection.

7 Employers' access

7.1 The regulations on employers' access – area of application

NHH is entitled on certain terms to access employees' electronic mailboxes etc., cf. Section 9-5 of the Working Environment Act and the regulations on employers' access to electronic e-mail inboxes and other electronically stored material. The regulations apply to both current and former employees.

By electronic e-mail inbox is meant the electronic mailbox that the employer has placed at the employee's disposal for use in the course of their work. The regulations also apply to the employer's right to search through and access an employee's personal area in the organisation's computer network, IT systems or other electronic equipment that the employer has placed at the employee's disposal for use in the course of their work. The provisions apply correspondingly to access to information that has been deleted from the aforementioned areas, but that exists as back-up or similar.

7.2 Conditions for access

NHH is only entitled to access information stored in the areas mentioned in section 7.1

a) when this is necessary to safeguard day-to-day operations or other legitimate interests of the organisation, or
b) when there are reasons to suspect that the employee's use of the electronic mailbox or other electronic equipment constitutes a serious violation of the duties arising from the employment relationship, or may provide grounds for dismissal with or without notice.

NHH is not entitled to monitor employees' use of electronic equipment, including the use of internet, unless the purpose of the monitoring is

a) to administer the organisation's computer network, or
b) to detect or solve security breaches in the network

7.3 Procedures for access

As an employee, you shall as far as possible be notified and given an opportunity to make a statement before NHH accesses the data. In the notification, NHH must explain why the conditions for access are deemed to be met and inform you about your rights.

As an employee you have the right to object under Article 21 of the General Data Protection Regulation.

You shall, as far as possible, be given an opportunity to be present during the access and have a right to be assisted by a union representative or other representative.

If access takes place without prior notification or without you being present, you must be informed of this in writing as soon as the access has been carried out. This information shall, in addition to information about why NHH deemed the conditions for access to be met, include information about the method of access used, which emails or other documents were opened, and the result of the inspection.

The exemptions from the right to information are regulated in Section 16 of the Personal Data Act.

The access must be exercised in such a way that, as far as possible, the data are not changed and the data obtained can be verified.

Opened emails, documents or similar that do not turn out to be necessary or relevant to the purpose of the access, must be closed immediately. Any copies must be deleted.

Petitions for access shall be submitted by the head of the entity in consultation with the HR department and system owner. Decisions on access are made by the rector.

The rector can decide to carry out access in the event of a death

- when this is necessary to safeguard day-to-day operations or other legitimate interests of the organisation, or
- when the deceased's estate has exercised a right to the material

Petitions for access shall be submitted by the head of the entity in consultation with the HR department and system owner.

Requests or petitions for access to information, logs and security copies from the public authorities, when provided for in laws or regulations, or court decisions, are handled by the rector.

8 Sanctions

Breaches of the IT Regulations and/or underlying policy documents, guidelines and procedures can lead to disciplinary measures being taken against you as a user of NHH's systems and services.

NHH can without delay remove equipment or software that:

- causes damage to NHH's IT infrastructure, or
- causes damage to NHH's or other users' information/data, or
- creates disruption in NHH's IT infrastructure, or
- in any other way prevents NHH from attaining the purpose of its IT infrastructure

Violation of the regulations' provisions may lead to you being refused access to the whole or parts of NHH's IT systems. It may also lead to sanctions under other regulations, such as disciplinary sanctions under the Civil Servants Act, a warning or exclusion from studies and exams under the Act relating to Universities and University Colleges, liability for damages, criminal liability etc.

The head of the entity (department, faculty or department in the central administration) can impose temporary exclusion for up to 14 working days following consultation with the system owner. The HR department must be notified immediately if the exclusion concerns an employee. Exclusions of more than 14 working days are decided by the rector.

Temporary exclusions may be used in response to a reasonable suspicion that

- you are guilty of serious violations, or that
- you or your IT equipment constitute a significant threat to information security

In the assessment, emphasis shall be placed on the seriousness of the violation, whether you have previously violated the regulations, the consequences of the exclusion for you as a user and circumstances otherwise.

Appeals against decisions made under the authority of the Civil Service Act, University and University Colleges Act and the Public Administration Act follow the rules on appeals set out in these acts.