	Edition No: 1.1	Approved date: 06/01/2021	Page 1 of 6	Approved by: CIO Nortura Owner: CISO Nortura
	Title: Corporate Information Security Instructions			Factory/Area: Nortura

# Corporate Information Security Instructions

## Information Security Management System

1	Purpose.....	1
2	Start of employment and training.....	2
3	Use of ICT equipment and software.....	2
4	Identity and password management .....	2
5	Information handling.....	3
6	Security and order at your own workstation .....	3
7	Private use .....	4
8	Work in premises that do not belong to Nortura .....	4
9	Control of compliance and sanctions in case of violation.....	5
10	Reporting of nonconformities and security incidents.....	5
11	Intellectual Property Rights (IPR) .....	5
12	Termination of employment .....	6
13	Confirmation.....	6

## 1 Purpose


This document is anchored in the Nortura Information Security Policy. The instruction describes how all permanent and temporary employees and hired staff of Nortura Group shall process and protect information.

### 1.1 Extent

This instruction applies to everyone in the Nortura Group, both permanent employees, hired and external (e.g. customers/suppliers) with access to the Nortura Group's information and/or information systems.

### 1.2 Responsibilities and duties

You are obliged to avoid actions that may expose Nortura to an increased security risk, e.g. by complying with this instruction. Personnel who experience a conflict between this instruction and other documents in our information security management system shall immediately report this to their manager.

	Edition No: 1.1	Approved date: 06/01/2021	Page 2 of 6	Approved by: CIO Nortura Owner: CISO Nortura
	Title: Corporate Information Security Instructions			Factory/Area: Nortura

## 2 Start of employment and training

Everyone who uses our ICT systems must complete the training program for information security. As an employee or hired employee, you are obliged, together with your manager, to familiarize yourself with relevant governing documents for information security, and any local regulations that apply to your unit or business area.

## 3 Use of ICT equipment and software

In order to ensure adequate information security in Nortura, for our customers, as well as for you and your colleagues, it is important that only approved ICT equipment and software are used on our computer networks.

- a. It is not permitted to connect private devices to Nortura's computer network. Only equipment approved by Nortura can be used. For private devices, the guest network can be used.
- b. It is not allowed to change the configuration of Nortura's equipment (e.a. the operating system, anti-virus and personal firewall).
- c. It is not permitted to install software or use cloud solutions that are not pre-approved in Nortura.
- d. It is not permitted to use Nortura's equipment or infrastructure for deliberate actions that may compromise the safety or reputation of the group, our customers or our partners.

### 3.1 Approval of ICT equipment, cloud solutions and software

Only ICT equipment, software and cloud solutions approved by Nortura can be used on our infrastructure.

### 3.2 Loss of equipment

If you lose or are robbed of ICT equipment that contains information belonging to Nortura, you are obliged to report this as soon as possible to the nearest manager and Matiq customer center on telephone 55555 (955 18 100). Examples of such ICT equipment are: Laptop, tablet, smart phone, external hard drives and memory stick.

### 3.3 Equipment replacement

When replacing equipment owned by Nortura, the old equipment must be returned to Nortura so that stored information can be deleted securely.

## 4 Identity and password management

Your username and password is used to verify for identity in Nortura's IT solutions. It is therefore important that you handle them safely. It is not allowed to lend your personal username and password to others, such as your manager, support, colleague or family member.

	Edition No: 1.1	Approved date: 06/01/2021	Page 3 of 6	Approved by: CIO Nortura Owner: CISO Nortura
	Title: Corporate Information Security Instructions			Factory/Area: Nortura

## 5 Information handling

To reduce the risk of information being lost or get in the hands of third parties, it is important that it is stored in systems with good access control and where backups are taken regularly.

Business information and personal data must be stored in the relevant subject system, SharePoint can be used where there are routines for this.

Business information should not be stored locally on a PC. It should be stored in professional systems, approved cloud-based services, such as Microsoft OneDrive for business, or in "My Documents".

- a. Information should not be synchronized or copied to equipment not approved by Nortura. For example, it is not permitted to synchronize e-mail or business information to private devices that are not subject to additional security measures by Nortura.
- b. When using Office 365, a browser can be used from private devices.

### 5.1 Storage on external storage units

To prevent information from getting in the hands of third parties if the storage device is lost or stolen, only information that is considered public, and that do not encompass personal data, should be stored on external storage devices such as a memory stick or external hard drive.

- a. If the use of an external storage device is necessary for the efficient transmission of data that does not fall into the categories above, the content shall be encrypted using approved encryption mechanisms. More information can be found at <https://sikkerhet.nortura.no/portal>

External storage devices, and especially memory sticks, are often a source of malicious software and should be used with caution. For the same reason, there may be equipment where the ability to use external storage devices has been turned off or is subject to additional security checks.

- b. External storage devices should be checked by up-to-date anti-virus software before connecting to a Nortura machine. This also applies to devices received from other Nortura employees and third parties.
- c. External storage devices whose origin you do not know should not be connected to Nortura equipment. For example, do not connect a memory stick that you have found or that you receive from a third party during a meeting.


### 5.2 Access to information

Access to information in Nortura shall be granted on the basis of business needs and authorization. You should therefore always make sure that the person you provide access to or send information to has a legitimate business need and has the required authorization.

## 6 Security and order at your own workstation

In addition to securing ICT systems, a good security culture at the workplace is important for safeguarding information security at Nortura.

- a. Always carry your access card easily visible. Also remember that the access card is personal and should not be shared with others.

	Edition No: 1.1	Approved date: 06/01/2021	Page 4 of 6	Approved by: CIO Nortura Owner: CISO Nortura
	Title: Corporate Information Security Instructions			Factory/Area: Nortura

- a. Separate rules for the use and carrying of access cards may apply to special areas, such as factory and production premises. Check with your immediate manager for what is applicable where you are staying.
- b. When you receive visitors, remember that they must be registered in the visitor system and that you must escort the visitor while they are on our premises.
- c. Make sure you have a tidy office, clean the desk and place documents in a lockable drawer or cabinet. If you have documents you no longer need, they should be shredded.
- d. When printing or copying documents, make sure you are present while the job is in progress and that you have all the documents with you when you leave the printer.
- e. Always lock your PC when leaving the desk, even if only for a short time. Use the shortcut "Windows key + L"

## 7 Private use

- a. Private use of Nortura's ICT solutions shall be kept to a minimum. All assigned IT equipment and software is the property of the employer and should only be used by personnel authorized for use.
- b. You are responsible for ensuring that any private use does not cause Nortura increased risk, increased costs or damage Nortura's reputation.
- c. It is not permitted to use Nortura's infrastructure for activities that violate Nortura's guidelines, Norwegian law or that may have negative consequences for our brand and trust in the market.
- d. Remember that when you use the employer's equipment and IT solutions, such as e-mail, you operate under your employer's brand, what you write, and your actions can therefore be related to your employer.

### 7.1 Private use of smartphone

Smartphones provided by employers are not subject to restrictions on private use (section 7.a.)

Smartphones may contain information belonging to Nortura, such as e-mail and documents. You should therefore exercise caution when using, restrict lending and do not make changes that weaken the smartphone's built-in security mechanisms.


### 7.2 Private e-mails and documents

- a. Private e-mail or other documents that do not require space can be stored in a folder in e-mail or file structure in your home area. The folder must then be marked "private"
- b. It is not permitted to install software for the use of own private cloud solutions. Examples of such cloud services are Dropbox, iCloud, Box, Google Drive and iDrive. This does not apply to software required for the use of cloud solutions approved and procured by Nortura.

## 8 Work in premises that do not belong to Nortura

It is allowed to connect your Nortura PC to other networks outside of Nortura. If you work from home, from another private premises or from a public place (hotel reception, airport, plane, train, Nortura's partners, etc.), you must be aware of the possibility that unauthorized persons may gain access to or overhear what you are working on.

- a. Do not leave IT equipment unattended and choose a workplace that provides the least possible access for others.
- b. Do not use networks that require you to install software on your PC in order to connect.

	Edition No: 1.1	Approved date: 06/01/2021	Page 5 of 6	Approved by: CIO Nortura Owner: CISO Nortura
	Title: Corporate Information Security Instructions			Factory/Area: Nortura

- c. Use Nortura's established solutions for remote work. Examples of such solutions are Citrix, Office 365 and VPN.

## 9 Control of compliance and sanctions in case of violation

In order to protect your personal data, safeguard our customers' and owners' data and secure the company's goals and values, it will be a follow-up that the requirements set out in Nortura's Information Security Policy and in this document are complied with.

- a. All activity performed in Nortura's computer systems can be logged and the information can be reconstructed. This information can be used to detect and resolve technical error situations as well as investigate whether there is fraud, including breaches of regulations and routines, provided there is a legitimate suspicion of such matters. The logs can also be used to remove unjustified suspicions of breaches of adopted regulations and routines within information security.
- b. Access to the e-mail box or other electronic equipment will be done in accordance with regulations on access to email and electronically stored material.
- c. If you violate adopted regulations and routines for information security in Nortura, it may have consequences for your employment relationship and access to our ICT Systems. Serious or repeated violations of the regulations are handled in accordance with current HR processes and may result in dismissal.
- d. Actions that are considered a violation of Norwegian law will be reported to the police for further investigation and prosecution.

## 10 Reporting of nonconformities and security incidents


You are obliged to report deviations and security incidents that have or may have an impact on information security. IT Helpdesk has routines for the handling of security incidents, so all deviations must be reported to the helpdesk:

- a. If the incident includes loss or exposure of sensitive data or personal data, the incident must be reported as soon as possible by telephone to Matic customer center, tel. 55555 (955 18 100).

## 11 Intellectual Property Rights (IPR)

All rights to and disposal of intellectual property rights such as patents, designs, trademarks, patterns and copyrights as well as methods, concepts, know-how, etc., which arise as a result of or in connection with an employment or an assignment, shall remain with Nortura unless otherwise agreed in writing.

- a. The same applies to information and data, which is created by employees or contractors during their performance of the employment or an assignment, or otherwise according to Nortura's instructions.
- b. Nortura shall have the right to process and make changes to any such product, physical as well as intangible.
- c. Nortura shall have the right to transfer all rights in whole or in part to third parties.

	Edition No: 1.1	Approved date: 06/01/2021	Page 6 of 6	Approved by: CIO Nortura Owner: CISO Nortura
	Title: Corporate Information Security Instructions			Factory/Area: Nortura

This provision does not prevent the individual, even after the end of the employment or assignment, from utilizing acquired general knowledge, skills and experience, as set out in the employment contract.

## 12 Termination of employment

Your e-mail and any information stored in your home area will as a general rule be deleted upon your resignation from Nortura. You should confer with your manager to ensure

- a. Transfer work-related information from home areas and local disks to agreed storage areas
- b. Disseminate relevant business-related e-mails and attachments to the person concerned.

Upon termination, all ICT equipment belonging to Nortura must be returned. Please note that it is not permitted to bring physically or electronically stored information and material belonging to Nortura when you resign.

Please remember that the duty of confidentiality still applies, also after the end of the employment.

### 12.1 Mailbox deactivation

The employee's mailbox is deactivated as soon as the employment ends. E-mails sent to someone who has left Nortura will be automatically deleted, and an e-mail will be sent back to the sender with information about a new contact person in the Nortura Group.

## 13 Confirmation

I confirm having read and understood these Instructions for Information Security. Further, I am aware that any breaches of adopted regulations and routines for information security in Nortura, may have consequences for my employment and my access to Nortura's ICT Systems:

Date/Location: \_\_\_\_\_

Signature: \_\_\_\_\_

Change log:

Given	Change	Initials
16.10.20	Ver 1.0: Document approved in version no. 1.0	KL
06.01.21	Ver 1.1: forwarding of emails chapter 12.1 removed   English version established	SGS