Nordea

Internal

Document Title	**Information Security Guidelines for individuals working for the Nordea Group**	**2016-08-30**	Date
Entry into force	Group Operational Risk (GOR) has approved these guidelines 30. August 2016. They supersede the instructions last updated on 9 December 2011.	**1 (9)**	Page
Purpose and scope	These Information Security Guidelines set out the information security requirements for all employees, including non-permanent staff and third parties, working for Nordea.		

1 Introduction

Banking is about trust. To retain this trust, you are required to handle electronic, printed, written or verbal information with due care and in accordance with the rules in these guidelines.

When working at Nordea, you have an important responsibility to ensure that information is handled in compliance with internal instructions and external regulations governing e.g. banking secrecy, personal data and insider regulations.

These guidelines are for all individuals who work for Nordea and specify, with a set of rules, what is set out in the Group Information Security Instructions (GISI).

Violations of these rules may lead to disciplinary actions.

2 The 8 information security rules – brief overview

1. Confidentiality
   You must handle all information in accordance with Nordea's confidentiality classes: open, internal, confidential and strictly confidential.

2. Access on a need-to-know basis
   You must only request, access or use information, systems or networks that you need for your assigned work. Remember that just because something is possible does not mean that it's permitted.

3. Handling of information outside of Nordea
   You must take extra care when handling information outside of Nordea. This includes e.g. physical and virtual services, conversations, paper and electronic devices.

4. E-mails
   Always take great care when communicating with e-mail externally, since Nordea e-mails are unencrypted by default when leaving the Nordea network. Always assume that someone might be reading the content unless you encrypt the e-mail. Nordea provides different solutions for use when forwarding e-mails encrypted.

5. Internet
   Minimise private use of the internet and consider that you expose Nordea's brand. It is not permitted to visit sites with pornographic, racist or other extreme content. Don't put your "fingerprints" on any website that could jeopardise Nordea's brand or reputation. Be aware that when you use the internet, your access can be easily traced back to Nordea and yourself.

6. Passwords and PINs
   You must keep your password or PIN code strictly personal in order to protect the information and your own integrity. Don't lend or disclose your password or PIN code to anyone, and don't borrow such information from anyone else. Log off or lock (Win+L) your workstation (PC, mobile phone) whenever you leave it.

7. Equipment and systems
   You must only use IT systems or equipment approved by or that follow the standards issued by Group IT. Never connect unapproved equipment (e.g. private devices) to workstations or networks, and only install or download software if you are authorised to do so.

8. Privacy and monitoring
   When you use Nordea's IT systems and equipment, your activities will be logged and might be used for internal monitoring and investigations. This includes traffic from the Nordea network to the internet. Nordea respects the privacy of the individual but may, in special situations, need to access a user's e-mail box or other information generated and stored by an employee.

3 The 8 information security rules – full text

3.1 Rule 1: Confidentiality

You must handle all information in accordance with Nordea's confidentiality classes:

- Open
- Internal
- Confidential
- Strictly confidential

The classes are based on the sensitivity of the information and regulatory requirements.

The information owner, who is overall responsible for ensuring the security of the information, is the originator of the information or the receiver of information from outside of Nordea, unless a specific owner is defined. Specific owners are to be defined for e.g. customer information. The information owner must classify the information with respect to confidentiality, thereby requiring that the information is treated in accordance with the selected class.

3.1.1 General handling guidelines

Since most information handled at Nordea is confidential, you shall, when in any doubt of information classification, treat it as confidential.

- You must store information protected from unauthorised access.
- Never store business-critical information only on your workstation's hard disk or on a memory stick, as there wouldn't be any backup if the equipment is damaged or lost.
- Always remove confidential information in physical form (e.g. paper) before leaving your desk and make sure that your workstation is locked (Win+L) so that confidential information is never exposed to unauthorised persons.
- Social engineering in the context of information security refers to psychological manipulation of people into performing actions or disclosing information. You should always be aware that you may be exposed to manipulative actions intended to harm Nordea by accessing, compromising, stealing or destroying information.
- Business needs and regulatory demands determine how long information should be archived in Nordea. This shall be documented in the archiving plans for your unit.
- When the information is no longer needed at Nordea, you shall make sure it is destroyed or disposed of securely. Always put printed documents that are no longer needed in disposal containers or shredders within Nordea's premises. Used IT equipment shall be disposed of according to procedures set by Group IT.

3.1.2 Open information

Open information is information that can be published externally. Examples of open information: Published annual reports, press releases.

3.1.3 Handling guidelines for open information:

Open information does not need to be labelled, but it should be clear that such information is meant to be published externally. If you produce information that will be published outside of Nordea, always contact your unit's communication partner in Group Communications (GC) for advice.

3.1.4 Internal information

Internal information is information that can be published on the Nordea Intra. Examples of internal information are: general Nordea news articles, Nordea's Group Directives, Instructions and Guidelines (e.g. this document).

3.1.5 Handling guidelines for internal information

Internal information does not need to be labelled. Access for external parties to internal information can only be granted on a case-by-case basis after appropriate evaluation and authorisation, and according to the relevant legal procedures.

3.1.6 Confidential information

Confidential information is all information that is not open or internal. The confidentiality relates to e.g. banking secrecy regulation, insider regulation, general business considerations or personal data protection. Examples of confidential information are: All information about the business relationship with a customer, HR information, contracts and incident reports. When in doubt or if the information is not classified/labelled, the information shall be treated as confidential.

3.1.7 Handling guidelines for confidential information

Confidential information should always be labelled if the information owner assesses that there is a risk of misunderstanding about the confidentiality.

Confidential information must be protected with access controls, and only employees who have a documented work-related need may have access to and use the information. Heads of units and information owners are responsible for determining such a need.

3.1.8 Strictly confidential information

Strictly confidential information is extremely sensitive information, often of strategic importance to Nordea. This is information which is commercially or otherwise sensitive, and whose disclosure or loss would have a highly significant impact on Nordea. Examples of information that can be considered strictly confidential: Insider information, details of mergers & acquisitions and presentations of the Group result prior to publishing. Any information about Nordea or any other company listed on a stock exchange, which may affect the share price, should be classified as strictly confidential.

3.1.9 Handling guidelines for strictly confidential information:

Employees or departments, who may be in possession of inside information, are separately instructed regarding handling of such information.
Strictly confidential information must be labelled, and distribution lists with named individuals must be established. The owner of the information is responsible for this. If you have received strictly confidential information for which you are not a listed recipient, you must immediately inform the information owner and file an incident report.
Subsequently, strictly confidential information must never be redistributed without the information owner’s consent.

3.2 Rule 2: Access on need-to-know basis

You must only request, access to or use information, systems or networks that you need for your assigned work.

Information available in Nordea’s systems must be used only on a need-to-know basis.

Access to a system does not automatically mean that you are permitted to view or otherwise use all information in the system. You are not permitted to access any customer information for your own personal purposes or for serving relatives, friends and colleagues. This is in order to avoid any conflicts of interest and any legal consequences.

3.3 Rule 3: Handling of information outside of Nordea

You must take extra care when you handle information outside of Nordea. This includes physical and virtual services, conversations, paper and electronic devices.

- Don't talk about or display anything other than open information when others can hear or see it.
- It is also important to protect the information when you talk with a colleague, when travelling, at external meetings or in public places.
- Always use a screen filter on laptops and take other necessary precautions to prevent others from seeing what is on your screen. Precautions should be taken when using devices for which screen filters cannot be used (e.g. mobile phones, tablets, etc.).
- Documents, equipment and memory devices must be protected from unauthorised access and damage. Laptops and other electronic devices should be carried as hand luggage when travelling.
- You must only use encrypted memory sticks, ordered through Nordea's ordinary purchasing process. Always remove information that is no longer needed on the stick. Only connect the memory stick to a Nordea workstation.
- Always report any loss or misuse of information or equipment without delay to your manager, Operational Risk Officer (ORO) and IT Service and Support (ITSS).
- Remote access to information and IT systems i.e. from premises not controlled by Nordea, is restricted and must always be activated through Nordea's processes for approval of remote access.
- Users may not use the internet to
    - Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
    - Download illegal copies of music, films, games or other media content and software, whether through file-sharing services or other technologies.

3.4 Rule 4: E-mails

Always take great care when communicating with e-mail externally, since Nordea e-mails are unencrypted by default when they leave the Nordea network. Always assume that someone might be reading the content unless you encrypt the e-mail. You must always validate the identity of the information recipient in order to ensure that Nordea is communicating with the right counterparty.

Exchange (transmission/receipt) of information must comply with relevant legislation and be appropriately protected against unauthorised access, misuse or corruption. If you need to communicate with a customer by electronic means, either based on encryption or an agreement with a specific corporate customer, or have any other questions, please contact an Operational Risk Officer in your business area for guidance.

3.4.1 E-mail outside Nordea with confidential information

- All confidential and strictly confidential information must always be protected (encrypted) when communicated through e-mails outside Nordea. There are some specific solutions:
    - E-mail communication with private customers can take place via secure e-mail connected to Nordea's e-banking systems.
    - Secure e-mail system deployed by Nordea
    - One solution for encrypted communication with corporates and authorities is called TLS (Transport Layer Security). Please contact IT Service and Support (ITSS) for more information.
- When transferring confidential information, it is an absolute requirement to identify that Nordea is communicating with the right counterparty.
- Nordea employees are not permitted to
    - accept changes in customer contact details, such as physical addresses, e-mail addresses and telephone numbers by way of e-mail, unless the identity of the information provider and the validity of the data can be verified. Fraud often starts by changing these details!
    - accept instructions to transfer funds out of the client accounts based on unprotected e-mail.
    - send or receive a binding order, a contract, a promise or an undertaking, such as a securities transaction, solely based on unprotected e-mail.
- You are allowed to reply to an unprotected external e-mail from an existing or prospective customer only to inform them how to communicate securely.
- If you are distributing e-mail to several customers at the same time, ensure that one recipient cannot see the other recipient's addresses, e.g. by using the blind carbon copy (bcc) address field.
- In cases where e-mails are part of the customer communication and necessary to document the customer relationship, copies must be securely stored in an easily retrievable way and in accordance with existing regulations.

3.4.2 General e-mail guidelines

- Nordea's e-mail system is considered safe for exchanging confidential information internally.

- Do not click on attached files or links in unexpected e-mails. They may contain malicious code or lead you to a hostile site, resulting in infection of the workstation or the network. If you suspect having received an infected e-mail, contact IT Service and Support (ITSS).
- Be aware that virus-infected e-mails can also come from someone you know well and trust.
- The use of internet links should be avoided when communicating outside of Nordea, since such communications might be mistaken for phishing attacks.
- Only e-mail boxes supplied by Group IT are allowed for your work at Nordea. Minimise private use of Nordea e-mail and consider that you expose Nordea's brand. Never use the Nordea e-mail system for any business purposes not related to Nordea.
- Automatic forwarding of e-mail from internal mailboxes to external e-mail addresses is not permitted since sensitive information may be sent over the open internet and be stored in insecure mailboxes.

3.5 Rule 5: Internet

Minimise private use of the internet and consider that you expose Nordea's brand.

It is not permitted to visit sites with pornographic, racist or other extreme content.

This applies irrespective of whether the internet access takes place at Nordea's premises, while travelling for business or while working from home.

It also applies to use of the internet on any device that is owned or managed by Nordea, or that is connected to the Nordea network.

- You are not permitted to use Cloud services providing the option to enter data, share and or store files hosted outside of Nordea for work-related purposes unless the service has been approved by the Cloud Service Acquisition Review Board (CSAR) as this is not compliant with the Nordea sourcing policy and the sourcing security standard.
- You are not permitted to register for any cloud service with your Nordea credentials, such as Nordea user-id, e-mail address, etc. unless you have such a mandate.
- You are not permitted to use your private credentials to enter into, register for, use or procure, any cloud service agreement with any cloud service provider for work purposes.
- Be aware that internet sites may contain malicious code/malware (such as virus or Trojans), which could attack your workstation and subsequently other computers in the Nordea network. You should therefore be careful before you e.g. click on links. If you suspect that your equipment has been infected, please contact IT Service and Support (ITSS) immediately.
- To protect Nordea's systems against malware you must only download work- related files from trusted sites on the internet.
- Don't put your "fingerprints" on any website that could jeopardise Nordea's brand or reputation. Be aware that when you use the internet your access can be easily traced back to Nordea and yourself. Also familiarise yourself with the "Internal guidelines on social media" on the Nordea intranet.
- Only chat / instant messaging services / collaboration tools supplied or approved by

Group IT are allowed for your work at Nordea.

- Do not place information related to your work at Nordea on internet sites, if it can directly or indirectly be considered as confidential or otherwise sensitive information. Do not register your Nordea e-mail address on internet websites unless necessary for your work, and do not use Nordea's logotype in connection with your private affairs.
- Using information, photos and programs from the internet must comply with copyright rules, licence restrictions and other relevant laws and regulations, domestic as well as international. Contact Group Legal or Group Communication if you need guidance.
- Based on their considered inappropriate or illegal content, or for information security reasons, access to certain internet sites and services will be blocked by Nordea.

3.6 Rule 6: Passwords and PINs

You must keep your password or PIN code strictly personal in order to protect the information and your own integrity. Don't lend or disclose your password or PIN code to anyone, and don't borrow such information from anyone else.

- Log off or lock (Win+L) your workstation (PC, mobile phone) whenever you leave it.
- Do not keep a record of passwords or PINs written down or stored in clear text.
- An initial password (possibly known by administrator) must always be changed at initial login.
- Don't use userIDs, names, words, popular phrases, birth dates, etc. as part of the passwords. Mix both numbers and letters and change the password regularly.
- If you suspect that your password has been compromised, immediately change your password, contact IT Service and Support (ITSS) and your manager.

3.7 Rule 7: Equipment and systems

You must only use IT systems or equipment approved by or that follow standards issued by Group IT. Never connect unapproved equipment (e.g. private devices) to workstations or networks and only install or download software if you are authorised to do so.

Unauthorised, non-tested software, IT systems or unapproved equipment can cause instability, malware infections or intrusion. This may lead to production disruption and generate considerable costs, and damage Nordea's reputation.

- Information should only be uploaded to and shared via services approved by Group IT (please also be aware of the usage of Cloud services mentioned in rule no. 5).
- All new software, hardware and service upgrades must be tested and approved according to internal Change Management procedures to avoid technical problems and to ensure that the programs function properly. Contact IT Service and Support (ITSS) if it is unclear how to do this.
- You must not establish your own internet connection from Nordea's premises using for example modems, phone cards or an external wireless network. Never change the security settings in the browser or on your PC/laptop.
- For certain equipment (e.g. smartphones) specific conditions might apply and therefore additional instructions, guidelines and/or restrictions are issued and must be followed.
- Never connect mobile phones and tablets (even if bought via Nordea's ordinary

purchasing system) to your laptop or workstation. This includes charging those devices. The risk is that the equipment may be infected or information may be transferred outside Nordea via the connection.

3.8 Rule 8: Privacy and monitoring

When you use Nordea's IT systems and equipment, your activities will be logged and might be subject to internal monitoring and investigations. This includes traffic from the Nordea network to the internet. Nordea respects the privacy of the individual but may, in special situations, need to access a user's e-mailbox or other information generated and stored by an employee.

Nordea should always have a strong reason for accessing the information. It could be in order to proceed in an internal case when for some reason the employee is not present or can't be contacted, or in the event of technical or operational problems, malware attacks, suspected crime or violation of internal rules.

In such situations, the company representative may neither read nor use e-mails that are marked as private, or which are obviously private for other reasons. Access to the user's mailbox or information storage is granted through a local procedure supported by Group HR to ensure compliance with local legislation.

When accessing certain internet sites like facebook.com or your private e-mail account on e.g. google.com, the communication is normally encrypted. Please be aware that Nordea might potentially automatically decrypt this traffic to ensure that malware is not entering the Nordea infrastructure. If malware is detected you will experience a notification page informing you that the site has been blocked due to malware.

Responsible unit and contact
The Chief Information Security Office is responsible for preparing and maintaining these guidelines and for supporting the implementation.
Contact person: Tapio Saarelainen, Chief Information Security Officer