Group Information Security Instructions

Document Title	**Group Information Security Instructions (v.3.0)**	**2015-12-15**	Date
Entry into force	Group Operational Risk (GOR) has issued these instructions on 15 December 2015. These instructions supersede the previous instructions issued 2 July 2014.	**Page 1 of 53**	

Purpose and scope

The Group Information Security Instructions set out and gather high level mandatory requirements for all specific information security areas and forms part of the internal control framework.

The Group Information Security Instructions are based on a risk assessment and the controls are selected from legislative requirements or considered to be common practice controls for information security.

The Group Information Security Instructions shall be read and adhered to in full or in parts by the whole Nordea Group/unit, and by managers, employees, consultants, suppliers and third parties with responsibilities within one or more information security areas.

Parts of the Group Information Security Instructions also apply to suppliers when a Nordea organization has sourced activities and functions.

Group Operational Risk (GOR) may grant exceptions from the provisions of these Information Security Instructions.

Contents / information security areas

1 INTRODUCTION 3

2 ORGANIZATION OF INFORMATION SECURITY 5

3 HUMAN RESOURCE SECURITY 8

4 ASSET MANAGEMENT 11

5 ACCESS CONTROL 16

6 CRYPTOGRAPHY 19

7 PHYSICAL AND ENVIRONMENTAL SECURITY 20

8 OPERATIONS SECURITY 23

9 COMMUNICATIONS SECURITY 29

10 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE 35

11 SUPPLIER RELATIONSHIPS 38

12 INFORMATION SECURITY INCIDENT MANAGEMENT 40

13 BUSINESS CONTINUITY MANAGEMENT 42

14 COMPLIANCE 45

15 TERMS, DEFINITIONS AND REFERENCES 47

1 Introduction

Group Information Security Instructions provide detailed instructions to support the implementation of the Nordea Group Directive Information Security Policy. The Group Information Security Instructions describe the information security requirements for Nordea Group and reflect the information's value to Nordea, and regulatory, legislative and contractual obligations. The objective of these instructions is to protect information against accidental or malicious disclosure, modification, or destruction and to support the continuity of Nordea's operations.

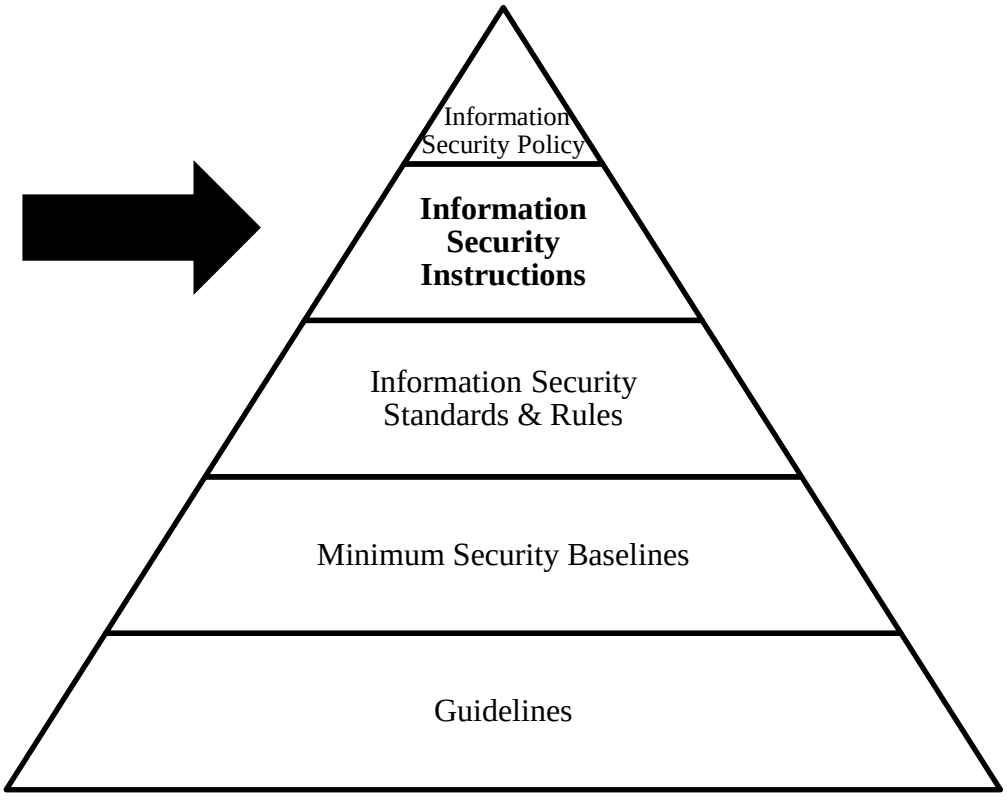
These Group Information Security Instructions are based on ISO27002:2013 Code of Practice for Information Security and 2013 Standard of Good Practice by Information Security Forum. References to the two information security standards of Good Practice have been written below every section of the document if applicable.

Underlying documents, i.e. information security standards, minimum baselines or guidelines details how the stakeholders are to implement the necessary information security requirements under the information security instructions.

Nordea operates in many different jurisdictions. In case of conflict, local laws and other mandatory regulations may override the Group Information Security Instructionsand Information Security Standards.

1.1 Structure of information security in Nordea

These Instructions constitute the middle layer of the information security pyramid.



Nordea information security structure consists of five levels;

Information Security Policy: Describes high level requirements for information security.

Information Security Instructions: High level mandatory rules for each specific information security area

Information Security Standards & Rules: mandatory and approved specific requirements detailing the information security instructions

Minimum Information Security Baselines: minimum implementation requirements for a specific technique regarding network, computing platforms, applications, program products and security configuration applicable to specific products or services.

Guidelines: Supporting recommendations to information security standards and rules.

All requirements in the information security structure and guidelines shall be consistent with the higher levels in the information security pyramid above.

1.2 Risk assessment

Risk assessments shall be performed for critical business environments, business processes, business applications, computer systems and networks on a regular basis by the application owner or application provider. Risks related to information security shall be analyzed once a year as well as in the event of changes that can affect the information security. The purpose is to identify, quantify, and prioritize key information security risks against criteria for risk acceptance and objectives relevant to Nordea and Nordea's suppliers. Risk analyses and decisions on measures shall be documented. The results shall guide and determine the appropriate management action and priorities for managing information security risks and for implementing selected controls.

The scope of a risk assessment can be either the entire Nordea Group, parts of the organization, business processes, individual applications, specific system components, or services where this is practicable, realistic, and helpful. The scope must be clearly described in order to be effective and include relationships with risk assessments in other areas, if appropriate.

Nordea Operational Risk Policy
SR1 ISF Good Practice

2 Organization of Information Security

Organization of information security must describe necessary measures to ensure that responsibilities and duties are clearly defined, allocated and carried out by skilled professionals in a safe organized manner. In every organisation a person, Chief Information Security Officer, responsible for leading and coordinating the information security work shall be appointed.

Responsibilities necessary to ensure a strong fundament for information security are further described in chapter 3 Human resource security.

Security roles and responsibilities must be documented (for example in a job description). In Nordea, this description must include any general responsibility to comply with the Group Information Security Instructions or security standards as well as any responsibility to protect special values or to execute specific security processes or activities.

Conflicting duties and areas of responsibility shall be adequately segregated to reduce the risk of accidental or deliberate misuse of Assets.

Information security shall be addressed in all projects and responsibilities for information security shall be defined and allocated to specified roles.

6. ISO 27002:2013
CF1.2 ISF Good Practice

2.1 Internal organisation

Information security responsibilities in Nordea are mainly allocated within the functions and roles described below.

2.1.1 Group Operational Risk (GOR) and CISO Office

GOR is a centralised staff unit within Group Risk Management, responsible for developing and maintaining the framework for managing operational and compliance risks and for supporting the line organisation in their implementation of the framework. GOR also holds the competence, and support responsibility, for overall general security and information security in Nordea.

The unit establishes and maintains adequate policies, rules and procedures for operational and compliance risk management. The unit also monitors, assesses and reports the risks on Group level as well as the adequacy and effectiveness of the risk management framework on a regular basis and at least once a year. The reporting is sent to the Group Executive Management and the Group Board.

CISO office is part of GOR and responsible for establishing and maintaining information security instructions and standards, including supporting the implementation of these instructions. IT Security Infrastructure is responsible for establishing minimum security baselines for significant infrastructure technologies.

Information Security Policy
6.1 ISO 27002:2013
CF1.2 ISF Good Practice

2.1.2 Group IT

Group IT is a central Group function which provides processes, services and competences to administrate and operate IT systems.

Only IT-systems or equipment approved by and following standards issued by Group IT may be used when processing, storing or transferring information within the Group.

Information Security Policy

2.1.3 Nordea Information Security Committee (NISC)

The NISC comprises of senior representatives from the security functions with representatives from business senior management. The Committee coordinates information security activities across the Group and monitor and set directions for information security initiatives. The Committee has the mandate to take high level decisions on target setting for information security governance, review enterprise information security strategy, Information Security Policy and information security instructions. Compliance issues related to information security and target setting for monitoring external compliance may be dealt by the NISC.

Further NISC approves the information security plan which provides advice on financial allocation for security maintenance and investments.

Charter for the Nordea Information Security Committee
Information Security Policy
ISO27003:2010
SG1.2 ISF Good Practice

2.1.4 Managers

Each manager is responsible for protecting information and IT Assets within their management area for compliance with the Nordea Group Information Security Policy, Information Security Instructions, standards and rules.

Managers shall require that employees adhere to the Nordea Group Information Security Policy, Information Security rules for all employees, and to relevant parts of the Group Information Security Instructions, and ensure that they receive a level of awareness training on information security, relevant to their roles and responsibilities.

Managers that engage in sourcing arrangements with consultants and suppliers shall through the contract ensure compliance with the relevant parts of the Nordea Group Information Security Policy and the Group Information Security Instructions. If the consultants or suppliers are going to handle Nordea confidential information, they shall sign a sufficient non-disclosure agreement for the access provided.

6.11 & 7.2.1 ISO 27002:2013
CF2.2.1 ISF Good Practice

2.1.5 Information owner

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. The information owner shall categorise and classify information and will be treated in accordance with this classification. If the information owner does not classify information, it is assumed to have the classification of confidential (confidentiality), not be significant for the integrity of financial reporting (integrity) and only have a standard need for availability protection (availability), The information owner may allocate access rights to his/her information.

Information Security Responsibilities Standard
8.1.2 ISO 27002:2013

2.1.6 Application owner

The Application Owner shall be nominated for all IT systems, including IT infrastructure and network, and when it is decided to develop or acquire an IT system.
The Application Owner has the overall responsibility that the information security in and around the application (whether sourced or not) is compliant with Group Information Security Instructions and standards.
The Application Owner shall ensure that:

- legal requirements are complied with
- IT systems comply with security standards issued by Group IT
- IT systems are classified according to their criticality for business
- information used in the IT systems is categorised and classified (see 4.2, 4.3)
- controls are implemented in accordance with the classification of the IT system
- periodic risk assessments are performed during the IT system's lifecycle
- access control policies (see 10.1) are defined showing which users (or normally which user groups/roles/job-functions) that may be given authorisation to the different system functions.
- determine which roles should not be combined (segregation of duties)
- decide for whom (if anyone) and for what purpose remote access is permitted
- responsibilities and procedures for the operations and maintenance of the IT system are established in accordance with these Instructions
- recovery procedures are aligned with business continuity plans of units/processes.

Information Security Responsibilities Standard
8.1.2 ISO 27002:2013
CF2.5 ISF Good Practice

2.1.7 Employees

Every employee shall know and adhere to the Information Security Policy, Information Security Rules for employees and information security requirements in standards and procedures that apply to their daily work. All employees shall report information security weaknesses, actual and suspected security breaches to immediate manager or Operational Risk Officer – ORO.

Information Security rules for all employees
6.1.1 ISO 27002:2013
CF2.1.2. ISF Good Practice

2.1.8 Information security in project management

Information security shall in any project be addressed by project initiation and maintained through the project life cycle and transition to operation.

Information security must generally be integrated into Nordea project management method(s) in order to identify and address information security risks as part of a project. This includes an information security risk assessment in an early stage of the project to identify necessary controls.

Responsibilities for information security shall be defined and allocated to specified roles defined in Nordea project management methods.

Information Security Checklist for Projects
6.1.5 ISO 27002:2013
CF1.2.4 ISF Good Practice

2.1.9 Contact with special interest groups

To have appropriate contact with external groups and receiving information and advices of good practices within information security, Nordea shall be a member of adequate interest groups within the area information security.

For the time being Nordea is a member of the Information Security Forum, an independent and non-profit organisation.

6.1.4 ISO 27002:2013
CF1.2.6 ISF Good Practice

2.1.10 Consultants, suppliers and third parties

All consultants, suppliers and third parties handling information on behalf of Nordea are obliged to know relevant part of the Nordea Group Information Security Policy, Group Information Security Instructions and how they apply to their work.

Information Security Policy
15.1.1 & 13.2.4 ISO 27002:2013
CF16.1 ISF Good Practice

2.2 Segregation of duties

Key IT roles, duties and areas of responsibility shall be adequately segregated to prevent any single individual being able to design, develop and implement a change to any system without the involvement of others and thereby reduce opportunities for unauthorized or unintentional modification or misuse of Nordea Information Assets.

The initiation of a change shall not be carried out by the same employee as the authorizer. Where adequate segregation cannot be established, compensating controls shall be implemented and shall include for example review controls and close supervision.

System development, operations and business use shall be separated.

Segregation of duties shall be used as a method in cases where it may involve too great a risk that different business functions may be mixed. The same person shall not be able to initiate and authorize an event, or handle all the steps in a process chain. This shall be reflected in the allocation of access rights. Segregation of duties shall be implemented when assigning roles for access control, e.g. access request, access authorisation, access administration.

An administrator is not allowed to grant any authorisation to him- or herself. Effective controls, monitoring or review procedures to this respect shall be established.

Guideline for SOD
Authorisation of internal users standard
Information Security Policy
CF2.5.7, 6.1.2, 7.7.4 ISF Good Practice
6.1.2 ISO 27002:2013

3 Human resource security

Human resource security describes rules and controls to reduce risks caused by human mistake, abuse and fraud.

7. ISO 27002:2013
CF2 ISF Good Practice

3.1 Prior to employment

Before an employment, it is the responsibility of the manager in cooperation with HR to perform adequate background verification checks on candidates for employment, consultants, and external users in accordance with relevant laws and regulations.

Potential information security functions and responsibilities associated with the actual position shall be clearly communicated to job candidates during the pre-employment process, and documented in adequate job descriptions or in terms and conditions of employment.

Employees, consultants and suppliers shall understand the possible consequences of any theft, frauds or misuse of Nordea information and facilities.

All employees and external parties with access to Nordea confidential and strictly confidential information shall sign a non-disclosure agreement, and be made aware of the need to protect Nordea's information and data of common threats and vulnerabilities.

7.1 ISO27002:2013
CF2.1 ISF Good Practice

3.2 During employment

Each manager shall ensure that all employees are informed of common threats and vulnerabilities related to information security, and that they are made aware of their responsibility to handle and protect information in accordance with Group Information Security Instructions, the Information Security Rules for all employees and other complementing handling guidelines within the relevant business area.

When an employee, a consultant or an employee of a supplier changes job responsibilities, the former manager has the responsibility to inform Nordea and ensure that access rights are removed. New access rights shall be approved by manager in the new position.

7.2 ISO27002:2013
CF2.2 ISF Good Practice

3.2.1 Job descriptions

Information security roles and responsibilities should be clearly documented and included in job description. This description shall include any general responsibility to comply with the Information Security policy, relevant parts of the Group Information Security Instructions, rules or security standards as well as any responsibility to protect special values or to execute specific security processes or activities.

7.1.2 & 6.1.1 ISO27002:2013
CF2.1 ISF Good Practice

3.2.2 Awareness training

All employees and consultants shall receive initial and regular awareness training to the Information Security Policy, relevant parts of the Information security instructions, the Information Security Rules for all employees and relevant information security standards. The objective with this awareness training is to ensure that Nordea employees and consultants who have access to Nordea classified information are aware of security threats and concerns and comply with the Information Security Policy and correct use of IT systems in their daily work.

Information and training shall be appropriate and relevant to employees' tasks, area of responsibility and skill.

7.2.2 ISO 27002:2013
CF2.2 ISF Good Practice

3.2.3 Working outside Nordea premises

Working outside Nordea premises shall be authorized by the manager. The approval shall depend on the tasks, the classification of information and the systems that the employee is authorized to access. Further there shall be appropriate security controls against loss and theft of equipment and information, supported by security awareness material. Additional security controls must be employed when travelling to high-risk countries or regions[1]. Steps must be taken to revoke access rights, and assure the return of equipment when the need for remote activities ends.

Arrangements regarding working from home which is conducted in a permanent manner and reaches a significant amount of time must be stipulated in a formal agreement with the manager, employee and HR defining the work permitted. The arrangements shall consider the hours of work, provision of insurance and local regulations.

Remote Access Standard
Information Security rules - Handling outside Nordea premises
6.2.2 ISO 27002:2013
CF14.1 ISF Good Practice

3.2.4 Disciplinary process

Violation of the Information Security Instructions will be investigated and may result in disciplinary actions including dismissal and possible legal actions. Nordea HR has the responsibility for formal disciplinary processes which must ensure correct and fair treatment for employees who are suspected of committing breaches of information security. Individuals should be made aware that disciplinary actions may be taken against them if they violate the information security instructions or supporting acceptable usage rules.

7.2.3 ISO27002:2013
CF1.1.9 ISF Good Practice

3.3 Termination of employment or contract

When an employee leaves the Nordea Group, it must be ensured that the employee is aware of information security responsibilities and duties that remain valid after the termination of employment.

Upon termination of employment all logical and physical access rights to information and Assets associated with information processing facilities and services shall be removed or suspended promptly. The employee's manager shall verify that Information Assets are returned no later than the termination day. Nordea information on Bring Your Own Devices (BYOD) must be verified wiped.

As a main rule the manager responsible for a consultant or supplier contract shall, upon the termination of partnership/ contract, ensure that all relevant IT and Information Assets in the possession of or under the control of a supplier, are promptly returned to the Nordea Group and that all the logical and physical access rights given to the supplier's employees or the consultants are removed.

7.3 ISO27002:2013
CF2.1.7 ISF Good Practice

[1] Refer to Nordea Travel security and insurance policy

4 Asset Management

Assets consists of Information Assets and IT Assets.

Information Assets are defined as electronic documents, information in databases, paper-based documents or images thereof containing Nordea information.

IT Assets are defined as assets associated with information processing facilities, i.e. applications, end user equipment, hardware and software Assets containing Nordea information. IT Assets are owned by Nordea or by suppliers.

To be able to protect Information Assets adequately, all IT Assets shall be identified, registered, and allocated the necessary protection. The objective of IT Asset management is to clarify and document responsibilities for all involved parties at the operational level and to increase data quality, create efficiencies, reduce overall logistics cost, support safe and secure storage of Assets and thereby reduce disruption of services.

Employees shall be aware of and comply with acceptable use of Nordea's Assets associated with information and information processing facilities. These are described in Information Security rules. When relevant the same shall apply to consultants and suppliers.

Information Assets in business critical processes shall be classified regarding its confidentiality, integrity and availability as the protection level may be higher than the default level, depending on the classification levels.

The classification given to Information Assets is a shorthand way of determining how this information is to be handled and protected, e.g. when copying, labelling, storing, transmitting, distributing, verbally communicating, and disposing of the Information Assets.

Document management aims to protect Information Assets in accordance with legal requirements, ensure availability as required and preserve the integrity and confidentiality of critical information.

Information Security rules - Confidentiality
8.1, 8.2 ISO27002:2013
CF3.1, 3.2 & 3.4 ISF Good Practice

4.1 Responsibility for assets

4.1.1 IT Asset inventory

All IT Assets shall be registered in an IT Asset inventory with important information about each IT Asset, including:

- ownership
- description
- versions in use
- location
- licensing details (e.g. license keys and proof of ownership).
- age and possibly end of life estimate

The IT Asset inventory shall include all IT Assets installed in the end user environment and IT Assets in data centres or at a supplier. The IT Asset management supplier shall have an obligation to maintain the IT Asset inventory and track all Nordea property defined as end user equipment.

The IT Asset inventory shall be kept up-to-date and updated when Nordea is acquiring or scrapping IT Assets. It must be ensured that any changes to IT Assets are implemented through a structured process. The inventory shall be reviewed independently, signed off by an appropriate business representative and protected against unauthorised change. The IT Asset inventory shall be reviewed yearly to identify any discrepancy with physical IT Assets or software licenses. Any discrepancies identified, should be investigated and resolved by for instance purchasing new licenses, removing unlicensed software, locating missing hardware or securely destroying equipment.

8.1.1 ISO27002:2013
CF3.4 ISF Good Practice

4.1.2 IT Asset labelling

To unambiguously identify physical Nordea owned or leased IT Assets in data centres or at a supplier, servers, computer and network equipment shall be physically labelled with a barcode label.

8.2.2 ISO27002:2013
CF3.1.6 ISF Good Practice

4.1.3 Ownership of Assets

All IT Assets associated with the information systems or services shall be "owned" by a designated individual or business unit within the Nordea Group.

Ownership of Assets shall be assigned and communicated to individuals or business units. The responsibilities of Information and Application Owners, such as registration, controlling the production, development, maintenance, use and security of the Assets, shall be documented. These owners should also define and periodically review access restrictions.

8.1.2 ISO27002:2013
CF2.5 ISF Good Practice

4.1.4 Acceptable use of Assets

The Group Information Security Instructions are supported by detailed acceptable usage rules that define how employees, and when relevant consultants and suppliers are expected to use Nordea's IT Assets, and securely handle Nordea's information.

This includes:

- the ownership and purpose of technology provided to individuals
- expected security-related behaviour of individuals
- rules for electronic mail and Internet usages
- guidelines for the use of mobile devices

These usage rules shall, when relevant, be made part of the contract with consultants.

Use of unapproved cloud storage of Nordea information; e.g. Dropbox or other similar file hosted services, is not allowed. Approval shall follow standard cloud sourcing process.

Assets are provided to Nordea employees, consultants and suppliers for business purposes. Where personal use of IT Assets is permitted, such use should be reasonable and not include excessive use of resources, impede Nordea business activities, or compromise the reputation of Nordea. The Assets remain the property of Nordea, which reserves the right to monitor and review the use of any of its Information Assets in accordance with applicable local legislation.

Information security rules for equipment and systems

Information security rules for e-mails
Information security rules for internet
Mobile Devices Standard
8.1.3 ISO27002:2013
CF1.1.5 ISF Good Practice

4.1.5 Procurement of IT Assets

Only IT-equipment, i.e. hardware and software, approved by or following standards issued by Group IT may be acquired and used within the Nordea Group.

Information Security Policy

4.1.6 Return of Assets

As a main rule, all employees, consultants and suppliers shall return all Nordea Assets in their possession upon termination of their employment or contract.

8.2.2 ISO27002:2013
CF3.1.6 ISF Good Practice

4.1.7 Securing IT assets before disposal

Disposal of IT Assets, such as storage media like hard disks on PCs and network printers, including licensed software, shall be handled according to a defined process. Worn out physical IT Assets shall neither be stored freely accessible nor be sold or disposed of, before the data stored on the IT Assets has been deleted and cannot be recreated. Any identification mark indicating that Nordea has owned the IT Asset shall be removed.

11.2.6 & 8.3 ISO27002:2013
CF 3.3.6/7 & 12.3.8/10/11 ISF Good Practice

4.1.8 Security of end user equipment off-premises

Technical controls to protect mobile computing shall be in place and can include physical locks, alarms, privacy filter or equivalent security devices. Nordea information stored on mobile devices shall be encrypted.

Information Security Rules - Handling outside Nordea premises
11.2.6 ISO27002:2013
CF14 ISF Good Practice

4.1.9 Lost or stolen IT- and Information Assets

The end user is required to inform Nordea Group of stolen or lost IT- and Information Assets through the IT Service Desk and their manager.

4.2 Information classification

In order to determine the level of protection that should be applied to particular types of information, classification of data is applied. The object is to identify a relevant control level to reduce the likelihood of unauthorised disclosure, modification and loss.

Data is classified after the different principles described below.

Confidentiality - Data is classified according to its confidentiality into following classes:

- Open
- Internal
- Confidential
- Strictly Confidential

Integrity – Data is classified according to the importance of integrity for financial reporting.

- Data critical for financial reporting (CF)
- Data non critical for financial reporting (NCF)

Availability classification is related to the time business owners can accept downtime when the data is not accessible.

- Business Critical system
- High Available system
- Non-Critical system

The Nordea procedure for classification of data describes in detail the different information classification classes.

Information classification Standard
Information Security Rules - Classification of data
8.2 ISO27002:2013
CF3.1 ISF Good Practice

4.2.1 Handling of Assets

Appropriate precautions shall be taken to secure information against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. These precautions should include technical, physical and organizational security measures that are commensurate with the sensitivity of the information and the level of risk associated with the processing of the classified information. Documentation of the classification and secure handling of classified information is a key requirement for information sharing arrangements.

Information on all classification levels should be protected according to Group Information Security Instructions. Information that has a higher level than the default level in any of the classification levels, will be protected according to specific requirements; described below. Data on those level also must be labelled to indicate its classification. Where it is not possible to use physical marking, other labeling techniques shall be used, for example, as a text on the screen. Data that is public data must be labeled as such.

Strictly confidential information shall be handled with the greatest care, and can only be shared with individuals with a direct individual work-related need, with explicit approval by the information owner. Access to strictly confidential information shall never be given as a consequence of belonging to a group or unit, but on named basis.

Data related to critical financial reporting have an increased control level regarding use of end user computing (excel); see 8.8 and maintenance of systems; see 10.4. Further effectiveness of controls related to change management, segregation of duties, access control incl. passwords, scheduling of jobs and backup controls are yearly assessed by application owners and independently tested on a periodic basis.

Business critical data/system has explicitly increased availability control levels. This is described in 5.2.5, 8.3, 8.4.1, 8.6, 10.2.1 and chapter 13.

8.2.3 ISO27002:2013
CF3.1.4 ISF Good Practice

4.2.2 Media handling

Handling of removable media shall be in accordance with rules for classified information.

Media with classified information shall be physically protected and appropriate handling procedures shall be complied with to protect information on removable media from unauthorized disclosure, modification, removal, and destruction.

USB flash drives used to store internal, confidential or strictly confidential information shall be encrypted. Nordea employees may only use memory sticks, ordered through Nordea's ordinary purchasing process.

Removable media includes but is not limited to tapes, disks and printed media.

Information Security rules for all employees
Information Security Rules - Handling outside Nordea premises
8.3.1 ISO27002:2013
CF3.1.4 ISF Good Practice

4.3 Document management

Documents, electronically stored or paper-based, shall by Nordea be categorized into types

- Information for financial regulatory reporting or related to stock exchange
- Personal data,
- Other customer information
- Other regulatory or contractual information
- Operational procedures
- Other information

The documents etc. shall be handled in accordance with its categorization throughout the document lifecycle (creation, storage, destruction).

The handling must be supported by applicable Nordea procedures regarding retention and document management. The procedures shall as a minimum include:

- Guidelines for identifying the type of record
- Retention schedule for the type of record
- Methods for handling conflicting retention requirements
- Specifications of employee obligations
- Archiving guidelines

When no longer needed documents shall be disposed using the official Nordea disposal process. If disposal services for papers or other media are used, an agreement with the supplier shall specify adequate controls and experience.

8.3, 18.1.3 ISO 27002:2013
CF3.2 ISF Good Practice

5 ACCESS CONTROL

Access to Assets; e.g. information, business applications, systems, networks and computing devices shall be granted only to authenticated and authorized users on a need-to-know basis.

There must be a formal process for user registration, de-registration and granting of authorisations to multi-user IT-systems and shared files.

Authorisation of internal users standard
9. ISO27002:2013
CF6 ISF Good Practice

5.1 Access control policy

Access control policies approved by Application Owners or Information Owners, shall regulate users' access to information in IT systems and must be reviewed at least yearly. These policies shall be based on users' roles, responsibilities and job function using role based access control. Assigning access rights to users shall be in line with these policies to ensure segregation of duties.

Business users shall only have access to data via business applications and not to resources below "application level".

Technical personnel including supplier employees may only access data through management tools providing traceability and not bypassing authorisation controls.

Customer access control systems shall be clearly separated from access control systems for internal users.

In the event of a system failure or if the access control mechanism is malfunctioning, access must be denied by default.

Authorisation of internal users standard
9.1.1 ISO27002:2013
CF6.1 ISF Good Practice

5.2 Access management

5.2.1 User administration

The registration of all users shall follow a formal procedure covering the whole life-cycle of user access, from the first registration of a new user to the final de-registration of the user leaving the Nordea Group or no longer needing access to the IT-systems.

A user administrator is responsible for creating, modifying, deleting or revoking user IDs, and changes user authorisations according to authorisation approval from the responsible Nordea manager or the Information Owner. User administration verifies that authorizations are according to the access policy before adding or changing access rights.

All users, including operations personnel, network administrators, system engineers, database administrators, consultants etc. shall be given a unique user ID, which they are personally responsible for.

IT systems interacting with other IT systems shall have a unique identifier to ensure traceability.

If the password vault is not used for gaining privileged administrative access rights, another unique user ID shall be created, reflecting the original user ID. Shared user IDs is not allowed.

A user ID shall not be activated before correct authorizations are documented.

The user IDs in Nordea shall follow a Nordea Group wide naming standard.

Authorisation of internal users standard
Workstation Security standard
9.2.1 ISO 27002:2013
CF6.7 ISF Good Practice

5.2.2 Password management

Before access is given to Nordea IT resources the user shall be authenticated. For logon to internal systems from the internal network a password shall be used to verify the user's identity and thereby his/hers rights to access information and use a system. Additional authentication mechanisms, such as two factor authentication should be used when stronger authentication is required based on external requirements or a risk assessment.

Technical measures shall be implemented to support that users change the initial password at first logon. System default passwords shall be changed prior to being installed into production. Passwords shall hereafter be changed on a regular basis and shall be of an adequate length and complexity, in accordance to password standard/rules. Requirements for locking-out an account after a defined number of failed password attempts shall be included.

A password belonging to a personal user ID shall never be shared. Passwords may not be transmitted in clear text across unsecure networks and stored passwords shall be encrypted.

Password Standard
Information security rules - Passwords and PINs
9.2.4 ISO 27002:2013
CF6.4 ISF Good Practice

5.2.3 Privilege management

Users shall be allocated access rights after "least privilege" principle, meaning only enough rights for the execution of the user's tasks. . The owner of the privileged authority and the manager of the individual must approve all requests prior to assigning privileged authorities. Approval may be done explicitly or through demonstration that the criteria for business need has been satisfied. Approval of administrative, or privileged, access must not be automated or machine generated.. All administrative/privileged access rights are temporary and shall be reviewed on a regular basis but at least quarterly. User IDs with privileged access rights shall not be used for ordinary office work, but only for the approved purpose

Privileges implemented by giving group access, also known as role based access, shall only be applied when all members of the group have a valid business need and the privilege is approved.

System ids, also known as technical user IDs, with privileges in support of the operating system (service machines, started tasks, agents, installed system user IDs, etc.) shall be owned by a unit manager and shall not be possible to use interactively.

Use of system utilities that can be used to override system and application controls shall be approved, logged and adhere to the access control policy.

,

9.2.3 ISO 27002:2013
CF6.4.4 ISF Good Practice

5.2.4 Review of user access rights

User access rights shall be reviewed at least annually (re-certification) by the manager and always in connection with change of duties and when employees move to other units or leave the Group. Persons with access to investment management systems or foreign exchange trading must have their accesses reviewed quarterly. Changes to a user's role within the Nordea Group shall immediately be reflected in the users' access rights. All consultants and supplier employees shall have a review date reflecting the users' affiliation with the Nordea Group, as a minimum once a year.

Authorisation of internal users standard
9.2.5 ISO 27002:2013
CF6.1.10 ISF Good Practice

5.2.5 Clear desk and clear screen policy

Information classified as confidential or strictly confidential information, on paper or on electronic storage media, shall be locked away when not required, inclusive-when the office is vacated. Other customer information and critical business information shall be placed in a way that unauthorised access is restricted.

Users shall be instructed to log off or lock systems/work stations when leaving the computer. Time-out facilities shall be used for both users and for remote assistance, which automatically terminates the session if there is no activity.

Workstation Security standard
11.2.9 ISO 27002:2013
CF2.4, ISF Good Practice

5.3 Mobile devices

Mobile devices such as smartphones, tablets and laptops shall have a sufficient security if giving access to or storing to Nordea information.-Special restrictions shall be applied to mobile devices not managed by Nordea. Mobile devices managed, but not owned by Nordea will hereon be referred to as a BYOD, Bring Your Own Device. These devices can only be allowed limited access to Nordea information and collaboration tools. For BYOD there shall be a documented, signed agreement with the employee regarding Nordea's management of the device.

Only approved solutions from Group IT shall be used for giving mobile devices access to Nordea information. An employee may have remote access via a mobile device, but this shall be authorised by the responsible manager.

Access to internal business systems or technical systems must only take place with Nordea authorised equipment complying with Nordea defined standards for workstation security and remote access. The mobile device shall be able to accept wipe requests when initiated by Nordea.

To access Nordea information the mobile device shall use a 'vault', which is Nordea provided software that must be installed on the device. The 'vault' protects Nordea information and creates an encrypted connection to Nordea. Access to the vault shall be protected by authentication. Nordea information on mobile devices shall always be encrypted. A specific standard for mobile devices shall stipulate the specific requirements.

Mobile Devices
6.2 ISO 27002:2013
CF14.5 ISF Good Practice

6 Cryptography

Cryptographic controls shall be used to protect the confidentiality, authenticity and integrity of information classified as, confidential and strictly confidential when stored externally or transferred outside Nordea controlled networks Communication and storage within Nordea shall always apply encryption for Strictly Confidential information.

Provisions regarding emails are stated in section 9.7.2.

Cryptographic techniques shall be used to provide evidence of the occurrence or non-occurrence of an event or action, when the identity of the originator of transactions or communications is required to be confirmed.

6.1 Cryptographic solutions

Approved cryptographic solutions shall be used across the organisation to protect the confidentiality of sensitive information or information that is subject to legal and regulatory-related encryption requirements.

Confidential and strictly confidential information shall be encrypted at all times when data is sent over Nordea networks going through a public area (i.e. area not controlled by Nordea physical controls).

Information transported by mobile device or removable media shall be encrypted.

Integrity of transaction data must be ensured for all financial (update) transactions in Nordea by cryptographic protection.

Passwords, PINs and other means of authentication, by which users can logon and get access to perform transactions, shall be protected from eavesdropping through encryption - also in the Nordea internal network.

Nordea is a member of international payment schemes where encryption is mandatory. For systems handling card-based transactions the Payment Card Industry, PCI, security requirements apply.

Cryptographic Protection of internal transaction standard
Encryption Key Management Standard
10.1.1 ISO27001:2013
CF8.4 ISF Good Practice

6.1.1 Responsibilities

The Application Owner shall ensure that the information processing in their system complies with the following requirements:

a) Authenticity and integrity of data in financial transactions transmitted to/received from a supplier shall be protected by a cryptographic solution.

b) Confidential and strictly confidential information shall be encrypted at all times when data is sent through non-internal network, such as internet, telephone networks, wireless networks and leased lines.

c) Cryptographic solutions shall only use cryptographic standards, key lengths and algorithms approved by Nordea

Cryptographic Protection of internal transaction standard
Encryption Key Management Standard
10.1.1 ISO27001:2013
CF8.4 ISF Good Practice

6.2 Key Management

Cryptographic keys shall be safeguarded against unauthorised modification, loss and destruction. Secret and private keys shall further be protected against unauthorized disclosure. No single person is allowed to know a full crypto key in clear-text used to protect Nordea Assets. If secure key storage and computing cannot be used, segregation of duties shall be employed to ensure the non-disclosure of the crypto keys.

There shall be documented procedures which include generation, distribution, certification, installation, usage, storage, destruction and location of all cryptographic keys handled by Nordea. The requirements shall include instructions for continuous renewal of keys and how to manage the key lifecycle, which shall be defined for each key type and implementation.

There shall be defined procedures for handling of situations where key(s) have been compromised.

Ownership of cryptographic keys shall be assigned to individuals, who shall formally confirm that they have understood their responsibilities for protecting keys assigned to them.

Encryption Key Management Standard
10.1.2 ISO27001:2013
CF8.5 ISF Good Practice

6.2.1 Public Key Infrastructure

Public Key Infrastructure (PKI) used by Nordea shall be supported by procedures documented in certificate policies (CP) and certification practice statements (CPS).

The use of PKI with business applications and integration with technical infrastructure shall be documented.

Documented procedures shall describe actions to be taken in the event of loss or compromise of the PKI.

Encryption Key Management Standard
10.1.2 ISO27001:2013
CF8.6 ISF Good Practice

7 PHYSICAL AND ENVIRONMENTAL SECURITY

Physical and environmental security cover all physical security related to information and IT equipment used in Nordea or producing IT service to Nordea. This includes computer systems operated or hosted by suppliers containing Nordea information.

Physical Security for IT equipment standard
11. ISO27002:2013
CF19 ISF Good Practice

7.1 Secure areas

7.1.1 Responsibilities

For “secure areas” such as data centres, computer rooms, technical rooms or even cabinets hosting IT equipment an IT area owner shall be appointed. As a rule-of-thumb, in Nordea, the manager responsible for IT premises or the branch manager is the IT area owner.

Physical Security for IT equipment standard
11.1 ISO27002:2013
CF19.1 ISF Good Practice

7.1.2 Physical security perimeters

Nordea uses security perimeters to protect information and information processing facilities in secure areas from loss, theft, damage, interference, interruption, or unauthorised physical access.

The physical security perimeters to secure areas shall include a combination of solid construction walls, alarmed fire doors, armoured windows and entry gates with physical access control. In the perimeter there shall be alarms that warn about any kind of physical intrusion attempts on external doors and accessible windows, ensuring swift reaction.

Photographing, video or tape recording or other kinds of "recording" in the secure areas are not allowed unless a special permission is granted by the IT area owner.

Physical Security for IT equipment standard
11.1 ISO27002:2013
CF19.1 ISF Good Practice

7.1.3 Physical entry controls

To protect areas that contain Nordea information and Nordea information processing facilities, all individuals shall wear a visible personal identity card / access card or guest card in Nordea secure areas and open landscape Nordea premises. Access card or keys are personal and may not be lent to others. Use of access cards and keys shall be logged and reviewed.

When passing the outer perimeter to an office area or an entry to a secure area the authorised user shall be forced to authenticate with the access card - by entering a belonging PIN.

Secure areas shall be placed so that public access or disturbing sources is avoided. These areas shall be secured by electronic access control and alarms shall be activated if the door only is opened by a key. Only personnel who regularly have tasks to perform in the area and are authorised access by the IT area owner may be permanently granted access to a secure area. Technical suppliers with tasks to perform may have temporary access cards. Visitors in secure areas shall be supervised at all times. Secure areas within data centre shall only have as few entrance points as possible, which shall be kept under constant surveillance using closed-circuit television (CCTV).

Suspicion of a security breach at any premises, shall be reported to Helpdesk and the IT area owner as security incidents. This includes, but is not limited to unauthorised access, doors left open, locks that do not work, keys or security codes passed on to unauthorised persons, unescorted visitors, a key or access card lost.

Physical Security for IT equipment standard
11.1.2 ISO27002:2013
CF19.1 ISF Good Practice

7.1.4 Securing offices

Offices with workstations shall be guarded by sufficient perimeter access control as well as intrusion and fire detection. All premises or buildings shall have an audible alarm system as well as a connection to an emergency service centre.

Windows and doors, which can be forced from the ground floor, shall be equipped with sufficient physical security controls. Appropriate precautions shall be taken to secure Nordea information against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.

In Nordea offices, though not branches, only visitors with guest card or visitors accompanied by a Nordea employee are allowed access.

Physical Security for IT equipment standard 11.1.3 ISO27002:2013
CF19 ISF Good Practice

7.1.5 Hazard protection

Critical IT facilities shall be located in a safe environment protected from natural and man-made hazards, i.e. as flooding, fire or damage from neighbouring activities. The main data centre shall not have the same risk profile and shall be located at a sufficient geographical distance from the location where the backup is stored. If there is an alternative data centre, it must not be dependent on the same physical infrastructure as the main data centre

Data centres and computer rooms shall be protected with alarm mechanisms, which consist of smoke and heat detectors connected to the building's fire alarm. When activating the alarm, it shall be audible. Data centre premises shall have an automatic fire extinguisher system. All other IT premises with equipment in operation shall as a minimum contain portable fire extinguisher at the entrance to the room. All IT premises shall have a well-marked escape route to emergency exits.

Protection against lightning shall be applied to all buildings and external communications lines.

Water detection/humidity alarm devices shall be installed in data centres.

Water detection devices, fire detection and fire extinguishing equipment shall be tested regularly, at least on a yearly basis.

Good housekeeping shall be maintained in data centres and computer rooms, i.e. tidy and free from unnecessary material that can burn. There shall be no eating, drinking or smoking in any secure area. Cleaning shall regularly be carried out in data centres and computer rooms.

Physical Security for IT equipment standard 11.1.4 ISO27002:2013
CF19.3 ISF Good Practice

7.2 Equipment security

7.2.1 Supporting utilities

All supporting utilities, such as electricity and air conditioning shall be adequate for the systems they are supporting. Support utilities shall regularly be tested in accordance with the manufacturer’s recommendations and the adequacy of the capacity evaluated, at least yearly.

An uninterruptible power supply (UPS) shall be installed to supply all of the equipment in the data centre with power. The capacity shall be approved by the IT area owner and aligned with business requirements from application owners.

For data centres a back-up generator with an adequate supply of fuel, is required to continue in case of a prolonged power failure. Large data centre shall use multiple power sources or a separate power substation. The capacity shall be approved by the IT area owner and aligned with business requirements from application owners.

Data centres shall be equipped with humidification equipment and redundant air-conditioning which operates 24 hours a day 7 days a week. The water supply should be stable and adequate to supply air conditioning and humidification equipment in a 24/7/365 operations.

Physical Security for IT equipment standard 11.2 ISO27002:2013
CF19.2 ISF Good Practice

7.2.2 Cabling security

Power and telecommunications cables/lines in the data centre shall be placed underground, where possible, or subject to adequate alternative protection. Further network cabling shall be

protected from unauthorized interception or damage. Power cables shall be segregated from communications cables to prevent interference and relevant cables shall be labelled to reduce the risk of erroneous connections.

Multiple feeds to the data centre shall be established for networks, servers and telecommunication to avoid a single point of failure in the communication.

Physical Security for IT equipment standard
11.2.3 ISO27002:2013
CF8.3.1, 9.2.1, 19.2.1 ISF Good Practice

7.2.3 Securing equipment before repair

If IT equipment is to be repaired at a supplier, a non-disclosure agreement shall be signed with the supplier. All data on the equipment must be encrypted or scrubbed, i.e. deleted and overwritten on the hardware before they are sent for repair. Hard drives with data on Nordea work stations are encrypted.

IT Security in Operational Environments standard
11.2.6 & 8.3 ISO27002:2013
CF 3.3.6/7 & 12.3.8/10/11 ISF Good Practice

8 Operations Security

Operations security describes requirements for stability, monitoring and security related to the daily operations of systems.

CF2.5.7, 6.1.2, 7.7.4 ISF Good Practice
12. ISO 27002:2013

8.1 Separation of development, test and operational facilities

There shall be a clear logical separation of all development, test and production environments in order to prevent unauthorized access or changes in the production environment. Development and test systems shall be hosted on network segments separated from production network, using a virtual local area network and firewalls. Strict use of change management process must support the implementation of segregation of duties.

Separation of environments shall be supported by a clear naming standard, logical access control and logical separation.

System development security standard
12.1.4 ISO 27002:2013
17.2.2 ISF Good Practice

8.2 Operating procedures

The application owner shall ensure that there is an up-to-date documentation with all relevant information relating to the operation and inter-dependencies with other systems.

Standard operating procedures (SOP) shall be documented, up-to-date and at a minimum address:

- back-up procedure and handling
- system restart and recovery procedures for use in the event of system failure
- instructions for handling errors and exceptional conditions

- scheduled tasks and job scheduling requirements where applicable
- contact information for technical support and relevant stakeholders

12.1.1 ISO 27002:2013
CF7 ISF Good Practice

8.3 Change Management

All changes to business applications, computer systems and networks shall be performed according to a documented change management process, which comprise the process from the recording of a change to the review after implementation into production.

A change manager shall be appointed as responsible for the change process. The change manager is responsible for informing relevant stakeholders about the change and may abort any unsuccessful changes and launch the fall-back plan.

The change management procedure shall require that the following tasks are performed prior to a change being applied to the operational environment:

- Identification and recording of the change in a change register to ensure tracking of the change from its approval through to closure.
- Assessment of the potential impacts of such changes
- Approval of the change by Nordea (the application owner)
- Adequate testing of the change
- Accurate version control.
- Fall-back plan for aborting and recovering from unsuccessful changes.

The change manager shall evaluate the flow of planned changes to secure necessary availability.

Changes shall always involve a Request for Change. For changes that are repeated at intervals, standard procedures may be agreed upon that do not require change management approval on a case-by-case basis.

For business critical infrastructure and applications there can be a fast track/emergency change procedure, which only can be used for emergency purposes. Fast track/emergency changes shall be approved by the Application Owner prior to deployment. It shall be ensured that all necessary system documentation is updated as it would be in the case of a normal change.

All changes, including fast track/emergency changes shall be documented according to the above and logged to change register.

The implementation of changes, also called release management, shall be documented and controlled to minimise any negative effects on the production environment.

The specific requirements stated in a contract with a supplier shall be supplemented by this section (8.3).

Change Management Standard
12.1.2 ISO 27002:2013
CF7.6 ISF Good Practice

8.4 System planning and acceptance

8.4.1 Capacity management

Capacity management shall be used to identify potential bottlenecks which might present a threat to system security or services, and plan appropriate action.

For all business critical activities, both new and on-going, capacity requirements shall be identified, monitored and tuned to ensure the required system performance. Detective controls shall be implemented to indicate problems in due time. Particular attention needs to be paid to any resources with long procurement lead times or high costs.

Capacity management on critical systems shall as minimum include the following:

- disk use and size
- network traffic load
- load balancing
- processing power
- memory requirements

12.1.3 ISO27002:2013
CF4.1.5, 7.1.4, 10.5.3, 18.1.2, 18.2.2, 18.4.7, 20.3.2 ISF Good Practice

8.4.2 System acceptance

A formal approval (system acceptance) from the Application Owner shall be given to ensure that acceptance criteria for new or significantly-changed applications are established and that suitable tests of the systems are performed during development and prior to implementation. These acceptance criteria include but are not limited to:

a) Agreed security controls in place, including contingency plans

b) Evidence that installation of a new system does not affect existing systems in production adversely

c) Compliance with performance and capacity requirements

d) Training in the operation or use of new systems

The Application Owner is responsible for documenting that the system acceptance criteria are in place.

14.2.9 ISO27002:2013
CF18.6.1 ISF Good Practice

8.5 System management

System management refers to design and administration of infrastructure, applications and network management.

8.5.1 Computer and network installations and design

There shall be up-to-date documentation for computer system, network, firewall and telecommunication installation designs. The design shall incorporate Nordea's approved technical architecture principles as well as the business and security requirements.

The design shall minimize manual intervention by incorporating high-reliability systems designed around the concepts of fault tolerance, patch management, automated back-up that can be remotely configured, and automatically monitored against predefined thresholds.

Administrative access to computer systems, network devices, firewalls and telecommunications equipment shall be built with security by design and use strong security controls and surveillance, intrusion detection sensors and continuous review.

CF7.1 ISF Good Practice

8.5.2 Server Configuration

Both physical and virtual servers shall be configured in accordance with approved minimum baselines, documentation and procedures, which shall contain standard configurations including descriptions of disabling/restricting of unnecessary functions or services.

Each server shall also be protected by applying standard security management practices (including restricting physical access, system hardening, applying change management and malware protection, monitoring and performing regular reviews, and applying network-based security controls, such as firewalls, intrusion detection).

Access to powerful system utilities and server parameter settings shall be authorized and restricted to a limited number of individuals.

CF7.2, 7.3 ISF Good Practice

8.5.3 Virtual Servers

Virtual servers shall be subject to approval, deployed on robust, secure physical servers and configured to protect information. Physical servers that are used to host virtual servers shall be protected against

- unmanaged and ad hoc deployment of virtual servers
- resource overload (e.g. excessive use of the CPU, memory, hard disk and network) by restricting the maximum number of virtual servers that can be created on each physical server.

The central management console or hypervisor allocating the physical server's resources to each virtual server shall be configured to

- logically separate each virtual server to prevent information being transferred between discrete environments
- restrict access to a limited number of authorised administrators.
- encrypt communications between virtual servers

Administrators of individual virtual servers may not be hypervisor administrator or administrators of the operating system of the physical server hosting the virtual machines.

CF7.3.5 ISF Good Practice

8.5.4 Network Storage Systems

Network storage systems, such as Storage Area Network (SAN) and Network-Attached Storage (NAS) shall be designed, deployed and maintained according to standard security management practices in 8.5.2 above. The network storage systems shall use standardised components and be managed from a single point (e.g. an operations centre), using a minimum number of management consoles.

Network storage systems shall be configured to restrict logical access to storage areas and be subject to system 'hardening', monitoring, change management and malware protection.

CF7.4 ISF Good Practice

8.6 Monitoring and logging

Standards or procedures for monitoring the use of Business Critical System shall be established and the results of the monitoring activities reviewed regularly.

A log standard shall set the minimum requirements for contents, type of records, log management and retention periods for logs. Based on that, the Application Owner decides which user activities, exceptions and information security events to log. The requirements in the standard shall include that:

- User activities, exceptions, faults and information security events shall be logged
- Significant updates to technical data or code are logged.
- All transaction information, including transaction queries and updates to customer information and contracts/agreements shall be logged. It shall be possible to trace business transactions from the source to the target system and back.
- System administrator and system operator activities shall be logged.

Computer clocks needs to be synchronised and reviewed on a regular basis to ensure the accuracy of the logs. Logging facilities and log information shall be protected against tampering and unauthorized access by an access control system. Access to any logs in order to investigate a person's use of a system shall follow an approved procedure and be approved by the appropriate Operational Risk Officer – ORO. All users of IT systems shall be informed that their actions in the systems are logged, and that the log might be used in future investigations.

Network Security Standard
IT Security Log standard
12.4 ISO 27002:2013
CF10.4 & CF10.5 ISF Good Practice

8.7 Technical Vulnerability Management

Roles and responsibilities for technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, vulnerability scanning and security patching responsibilities shall be defined.

Nordea shall have a unit responsible for vulnerability management, which gathers information about and assessing software vulnerabilities, by utilizing all available sources like mailing lists, websites, suppliers and other contacts/networks. Information about technical vulnerabilities of information systems shall be obtained in a timely fashion.

The gathered information about software and other components are registered in Asset Inventory. Relevant vulnerabilities for these shall be published to relevant Application Owners who are responsible for that the latest security patches are installed on their system or otherwise mitigated, and that identified vulnerabilities are remediated. Vulnerability management comprises all platforms in Nordea, thereby including servers, workstations, laptops, mobile devices, network devices, firewalls and any other components with embedded software connected to the Nordea network.

Vulnerability and patch management standard
12.6 ISO 27002:2013
CF10 ISF Good Practice

8.7.1 Vulnerability scanning and security patch management

All IT systems connected to the Nordea network shall regularly be scanned for vulnerabilities. Identified vulnerabilities shall be mitigated by installing relevant security patches or performing other mitigating actions. All security patches shall be evaluated, on their relevance

and urgency. Test of the security patch shall be carried out on a reference group before deployment. The risks posed by the vulnerability should be compared with the risk of installing the security patch. Security patches shall be implemented in accordance with set timeframes and based on the severity of the vulnerability.

Vulnerable software or applications shall be reported to the relevant Application Owner. Detection of vulnerable software without appointed Application Owner shall result in removal of the software or appointment of an Application Owner, who shall ensure that relevant security patches are applied regularly.

Vulnerability and patch management standard
12.6 ISO 27002:2013
CF10.1 ISF Good Practice

8.7.2 Protection from malware

The provider of the platform is responsible for installing, configuring, and maintaining the server/system with effective protection against malware, such as viruses, worms, Trojan horses, logic bombs. This shall be complemented with awareness advice for users. There shall be documented procedures for handling attacks of malware.

Malicious Code Defence standard
12.2 ISO27002:2013
CF10.3 ISF Good Practice

8.7.3 Restrictions on software installation

An ordinary user shall only be allowed to install software on Nordea workstations from Nordea Software Distribution.

Local administrator rights are approved by a manager and may be given to a user (or group of users mainly within Group IT) only when strictly necessary. Local administrator authorisations are always limited in time to maximum six months.

Workstation security standard
Nordea Information Security rules - equipment and systems
12.6.2 ISO27002:2013

8.8 End User Computing

Critical end user applications such as spreadsheets (e.g. Microsoft Excel) and database programs that support or feed data to Nordea Business Critical Systems, or otherwise support business critical processes shall be approved and registered in an inventory/list related to the business unit. The list should include:

- a description of the intended purpose with the end user application
- the primary responsible for maintaining the end user application
- a description of any changes made to parameters or calculations and by whom.
- classification and categorisation of the information
- a description of users (names or unit)
- backup and continuity

Critical end user applications and data shall be stored on Nordea managed server, which shall be included in the business continuity plans for the critical application/process they support or feed data to. Access privileges, such as open, read and modify, shall be limited to authorised individuals only. These applications shall be designed in a secure manner to prevent users from accidently or intentionally changing the logic or the design of the application. The

primary responsible for maintaining the end user application shall yearly verify the above and that the database or spreadsheet is of a supported version. Before critical end user applications are made available to users they shall be tested to verify that they function as required. Version control shall be used when changes are made

Workstation security standard
CF 13.1.2, CF 13.2.5, CF 13.4.7 ISF Good Practice

8.9 Backup

All information of value to Nordea shall be backed up, including operating system, system software, system documentation, data, software and licenses. The Application Owner is responsible to have an overview of what is backed up and have established a backup procedure, which meets business, operational, legal and contractual requirements.

The backup procedure shall consider the bookkeeping requirements for accounting data as specified in local legislation. Backup of sensitive privacy information shall be deleted and stored according to the Personal Data Act's requirements.

Documented backup procedures shall describe how back-ups are performed, backup cycle, labelling, methods for restore and for verifying that the backup was successful. Back-up shall also be regularly tested to ensure that it can be read and restored when needed.

There shall be at least two generations of backups. Backup media shall be stored under environmental conditions, so that it is very unlikely that all generations of data can be destroyed by the same person or physical event, such as heat, humidity, flooding, fire etc. simultaneously.

Access to the backup media shall be restricted to only authorised personnel.

Segregation of duties shall be in place to restrict anyone from having access to all generations of data, i.e. both access to production environment and backups.

Backup standard
Disaster Recovery in Data Centres standard
12.3 ISO 27002:2013
CF 7.5 ISF Good Practice

9 Communications Security

Information in networks and its supporting information processing facilities shall be protected against the compromise of confidentiality, integrity and availability of the information they process.

9.1 Network Security Management

Network and telecommunication installations shall be designed to cope with current and predicted load, quality and availability requirements, and be protected against internal and external threats using a range of security controls. The networks shall protect the confidentiality and integrity of the information that flows through them.

Network Security Standard
13.1 ISO27002:2013
CF9 ISF Good Practice

9.2 Network Device Configuration

Network infrastructure devices, including but not limited to routers, switches and firewalls, shall be configured to function as required and to prevent unauthorised or incorrect updates.

Network documentation shall be kept up-to-date and readily accessible to authorised individuals.

Network devices shall be subject to standard security management practices, which include the following:

- restricting physical access to network devices by locating them in secure or dedicated, locked storage rooms
- 'hardening' the operating system(s) that support them i.e. disabling unnecessary services and changing suppliers' default parameters
- keeping network devices up-to-date, i.e. by applying security and software updates
- continuously monitoring network devices
- reviewing network devices on a regular basis to verify configuration integrity, evaluate password strengths and continuously monitor logs to detect unauthorized activities

Networks shall be protected using access control providing differentiated access to networks depending on level of authentication of user and device. An example is authenticated Nordea managed devices can be provided full access, unmanaged devices and non-Nordea users shall be provided only limited levels of access.

Unauthorised devices shall be prevented from connecting to or interfering with authorised devices on the internal networks. This could be achieved by device authentication at the network level combined with network segmentation.

Vulnerability and patch management standard
13.1.1 ISO27002:2013
CF9.1 ISF Good Practice

9.2.1 Segregation in networks

Nordea networks shall be segmented into separate network domains (including 'Demilitarised Zones'). The domains shall be separated by firewalls, configured to only allow necessary traffic between the domains. Dedicated networks shall be used to isolate particular types of network traffic to prevent impact on other network traffic.

Data Exchange between internal and external systems standard
13.1.3 ISO27002:2013
CF9.2 ISF Good Practice

9.3 External Network Connections

There shall be documented procedures for managing external network access to Nordea computer systems and networks. All external network connections to computer systems and networks shall be individually identified, verified, documented, and approved by the unit responsible for the network.

All external network connections to (or from) Nordea IT systems shall go through a firewall environment consisting of at least an outer firewall, a gateway and an inner firewall. The firewalls shall only allow necessary traffic. The gateway shall be designed and thoroughly tested to reject unauthorized access attempts.

External access to computer systems and networks shall be configured to restrict access by using strong authentication. Any other setup needs to be approved by approved by an IT

security unit in Group IT. For interactive user access two-factor authentication such as challenge/response devices featuring one-time passwords, smartcards, tokens or biometrics, shall be used.

All banking transactions, customer-related data and personal data that are transferred outside Nordea network shall be encrypted to ensure the integrity and confidentiality of the data.

External connections shall be deactivated when no longer required, i.e. by physically removing the network connection or modifying firewall rules.

Network Security Standard
Data Exchange between internal and external systems standard
13.1.2 ISO27002:2013
CF9.3 ISF Good Practice

9.4 Firewall

Employees, suppliers and consultants' access to information via external networks shall be routed through a securely configured firewall prior to being allowed access to internal networks, or before leaving internal networks.

There shall be documented standards / procedures for managing firewalls. The documentation shall include rules for filtering networking traffic. All traffic to and from the firewall shall be blocked unless specifically authorised.

Firewall configurations shall be reviewed on a regular basis, to ensure that

- Each firewall rule is formally approved.
- Expired or unnecessary rules are removed.
- Conflicting rules are resolved.
- Unused / duplicate objects are removed.

Information about and documentation with networks and firewalls configuration shall at least be handled as confidential information.

Strong security controls in Internet proxy and e-mail gateway shall also be established and documented

Network Security Standard
13.1.2 ISO27002:2013
CF9.4 ISF Good Practice

9.5 Remote access

Remote access for employees, consultants and suppliers shall be specifically approved by the line manager or manager responsible for the contract. Access rights for remote access to Nordea information processing facilities and Nordea information shall be based on a work-related need and a risk assessment. This shall be performed prior to the approval of remote access.

Remote access shall always be established with a cryptographically safe tunnel, such as VPN.

Administration of user access rights shall not be done via remote access.

Dealing and trading is not allowed via remote access. Access to customer or transaction information and execution of financial transactions shall be limited to an absolute minimum. Such transactions shall be of a reasonable size limit, and shall always be subject to the four-eye-principle (i.e. two employees of the bank verify the transaction, where one part always has to be in Nordea premises).

Remote access standard

6.2 ISO27002:2013
CF6.1 /9.3 ISF Good Practice

9.5.1 Remote access for employees

The employee's manager shall assess and approve the risk for each individual user before granting remote access. Remote access rights outside Nordea premises shall only be granted to Nordea information and Nordea information facilities needed to perform approved remote tasks.

Developers may have remote access, providing that they cannot execute business transactions or that they do not have administrator access to production servers.

Handling outside Nordea premises
Remote access standard
9.1.1 & 9.1.2 ISO27002:2013
CF9.3, 14.1 ISF Good Practice

9.5.2 Remote access suppliers and consultants

Any remote access set-up between a supplier/consultant and Nordea shall be regulated by a written agreement approved by Group Legal describing the reason for the access to Nordea and how and when the supplier/consultant can connect to Nordea. Consultants using Nordea managed devices shall comply with the same requirements as for employees, including signing a non-disclosure agreement.

Supplier connections shall not be directly connected to computers in the internal network but shall use a dedicated vendor gateway when accessing Nordea resources. Only a limited number of predefined sites or equipment at the supplier, are allowed to access the vendor gateway at Nordea. The communication shall be encrypted.

Remote access from outside supplier's office to business applications with customer data is not permitted.

Supplier employees shall not be provided with remote access to business application functions or have permanent access to Nordea information facilities. These users shall only have very restricted access to production environment. Suppliers' remote activities shall be logged and both the log and remote access rights for suppliers shall be reviewed at least quarterly.

Remote access standard
6.2 ISO 27002:2013
CF14 ISF Good Practice

9.6 Wireless Access

Wireless access to the network should be subject to an information risk assessment and approved by premise and network owners, prior to its implementation.

Wireless access shall be authorised, users and computing devices authenticated, and wireless traffic encrypted.

Documented information for controlling wireless access to the network shall cover

- placement and configuration of wireless access points
- approved methods of authenticating and limiting access for users and devices
- approved use of encryption for protecting information in transit

- methods for granting ad-hoc access to non-Nordea users
- detection and removal of unauthorised wireless access points on internal network.

Wireless Security Strategy
CF9.6 ISF Good Practice
6.2 ISO27002:2013

9.7 Information transfer

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities. Information which is classified as confidential or strictly confidential shall be encrypted before transfer outside Nordea, unless otherwise specified in information security standards. Transfer of information in e-mails is specified below.

File transfers between Nordea and external parties shall be based on a formal exchange agreement. This shall include requirements for minimum technical formats for transmission, back-up of transmitted information, fall-back procedure, traceability and non-repudiation for transmitted data. The supplier shall be authenticated and authorisations checked before up- or download is performed.

For each application, the application owner shall set rules for how to move confidential or strictly confidential information to and from other systems. The rules must be described in the individual system security documentation.

The administration of access privileges given for transmission products or message-oriented middleware shall comply with the principle of segregation of duties. Integrity violations shall be recorded and proper actions shall be taken and documented.

Financial transactions and other confidential data shall be encrypted when communicated over open networks or internal networks using non-internal cabling. The communication shall be protected against manipulation, either by message authentication or by applying encrypted tunnels. Data used for authentication shall be encrypted during any transfer and storage.

Data Exchange between internal and external systems standard
Information Security rules – E-mail
CF15 ISF Good Practice
13.2 ISO 27002:2013

9.7.1 Information leakage protection

Information leakage protection mechanisms shall be considered for systems and networks that process store and transmit strictly confidential or confidential information, for instance information that is subject to regulatory requirements such as data privacy legislation, Payment Card Industry Data Security Standard (PCI DSS), etc. Information leakage protection mechanisms shall be supported by documented procedures covering:

- Types of information that should be monitored
- Regular monitoring of system activities (see 8.6)
- Techniques for alerting, detecting and blocking user actions or network transmission that expose confidential information
- Reporting of confidentiality breaches

CF8.7 ISF Good Practice

9.7.2 E-mail

Nordea's e-mail system may be used for exchanging confidential information internally, but confidential information or private customer information shall not be sent by unprotected e-mail outside Nordea, unless otherwise specified in information security standards or rules.

E-mail systems shall be protected by a combination of policy, awareness and technical security controls; including scanning e-mail messages for malware, chain letters and offensive content, and blocking e-mails with attached files with particular data types or with certain extensions, e.g. exe.

Only the official Nordea e-mail service is permitted to be used. Limited private use of Nordea e-mail service may be allowed. Automatic forwarding of e-mail from internal Nordea mailboxes to external e-mail addresses is not allowed.

All e-mails are considered Nordea property and shall be treated as such. The use of e-mail is automatically logged and may be monitored. The use of e-mail will be reviewed in certain situations and always in accordance with local legislation.

Information Security rules - e-mail
13.2.3 ISO 27002:2013
CF 15.1 ISF Good Practice

9.7.3 Instant messaging

Instant messaging or text-based communication that involves immediate correspondence between two or more users real-time may be used for communication with suppliers and other external partners if controlled channels are used. Insecure instant messaging shall not be used for communication of confidential information to customers.

Information Security rules - Internet
CF 15.2 ISF Good Practice

9.7.4 Telephony and Conferencing

To protect telephony and conferencing facilities, such as tele-, video- and online web-based conferencing, there shall be documented rules, which cover physical and logical controls, recording, regular monitoring and restriction of access to the facilities.

Online conferencing facility shall be initiated from the internal Nordea network and requires presenter confirmation, before external users are granted access to a conference. If external servers are used for the conference, the communication shall be encrypted.

After a conference has ended, any network connections shall be closed and conferencing hardware (e.g. screens and cameras) and software (e.g. presentation, screen sharing and remote takeover applications) disabled.

Direct external connections, i.e. by modem or 3G, from equipment, which is connected to the Nordea Internal Network, are not allowed.

CF9.8, 9.7 ISF Good Practice
13.1.3 ISO27002:2013

9.8 **E-banking**

All information of a confidential nature sent in public networks between a customer and Nordea, shall be sufficiently protected to prevent incomplete transmissions, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. Secure protocols or data encryption between all involved parties shall be applied.

All financial transactions from the customer to Nordea passing over public networks shall be protected against fraudulent activity and unauthorized disclosure and alteration. User credentials for all parties shall be valid, verified and secured. Customers shall only have access to services especially designed for customer use, with specifically designed access control mechanisms.

For internet systems that solely provide customer read access to customers own data, but no access to perform any kind of committing transaction, a one factor authentication (e.g. password) is sufficient, provided that an encrypted tunnel is used between customer and bank and that requirements from local authorities are met. For systems that allow access to execute financially committing transactions, strong authentication is required, unless preauthorisation is used or transfers are made between own accounts.

Data Exchange between internal and external systems standard
13.2, ISO27002:2013
CF 8.6 ISF Good Practice

10 Information Systems Acquisition, Development and Maintenance

Necessary security requirements shall be specified for IT systems at the time of purchase, development, operations and decommissioning. The security requirements shall both be part of the system development at an early stage and considered during the entire system development lifecycle. The requirements can be implemented as automated controls incorporated in the system or as supporting manual controls.

System Development Security standard
14.1 ISO27002:2013
CF 17 ISF Good Practice

10.1 Responsibilities

The Application Owner has the overall responsibility that the security in and around the application (whether sourced or not) is compliant with Group Information Security Instructions and standards.

System Development Security standard
Information Security Responsibilities Standard
14.1 ISO27002:2013
CF18.1 ISF Good Practice

10.2 System development security requirements and design

There shall be approved and documented system development methodologies. These shall include standards and procedures for developing systems or integrating other systems. The methodologies shall cover specification of requirements, system design, development, testing and deployment.

Specification of security requirements shall be documented before the design commences, but can be updated during the development. Business requirements shall include the need for system performance, capacity, continuity, scalability, connectivity and compatibility. The system design shall include integration of a security architecture that supports the above mentioned requirements as well as the confidentiality, integrity and availability of information.

The design shall contain a visual overview showing the whereabouts and sequence of security controls and other security measures protecting the data in the system.

If the four-eye principle (dual confirmation) is a business requirement, it shall be enforced by the system design, and not just rely on manual procedures.

Validation checks shall be incorporated into the design of applications to detect any corruption of information through processing errors, human mistakes or deliberate acts.

All systems shall be designed to verify that the requestor is authorised to get a request served. When designing externally facing systems, these shall always include controls to verify that received requests are within the expected range of values.

System Development Security standard
14.1 ISO27002:2013
CF17.1, 18.2 ISF Good Practice

10.2.1 Resilience

All business critical systems and applications must be designed and build in a scalable, robust and fault-tolerant manner, considering multiple sites. Resilience requirements against attacks shall also be considered. Applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, or disclosure of information to the public. Therefore proper selection of controls shall be based on risk assessments. Controls required often include cryptographic methods for authentication and securing data transfer.

14.1 ISO27002:2013
CF17 ISF Good Practice

10.2.2 System Testing and security review

There shall be a process for testing systems under development, which is supported by documented standards. This shall require that all key components of new systems are tested before deployment to production environment, including application software packages, system software, hardware and communications. No system is allowed to achieve production status, before it has been thoroughly tested. Systems having external connections shall also pass penetration tests, carried out by Nordea. Test results shall be documented.

Vulnerability scan shall be performed for all systems in all environments.

Application security test is mandatory for all externally reachable applications and interfaces as well as for all systems handling strictly confidential information.

Risks and vulnerabilities identified during these tests shall be documented and managed. Identified risks shall be addressed as soon as possible and any residual risks shall be tracked and followed up.

Access to data used in test environments shall be restricted to individuals with work related need; e.g. testers and not developers. Confidential information, e.g. personal data, customer data, card data and other sensitive information shall not be used for testing purposes. Personal identifiable information shall be desensitised beyond recognition before use. Equally, demo users or fake customer data shall not be placed in production systems.

Prior to deployment, a review shall be performed to assess the fulfilment of the information security requirements, the quality of security controls and any incidents during system development. The review shall be signed off by the appropriate internal security function.

System Development Security standard
The Nordea Test Strategy
14.2 ISO27002:2013
CF18.4 ISF Good Practice

10.2.3 Security of source code, system files, and operational software

Access to version control system; e.g. system files, source code, designs and specifications shall be restricted, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

Program source code should not be held in operational systems. Program source code shall be stored centrally in a version control system, which shall be managed according to established procedures. Technical system users shall not have access to program source code.

Changes or upgrades to system files shall only be carried out when there is a documented need to do so and according to change management procedures. Regression testing shall be performed after the change to verify that hosted applications provide same services as before upgrade. Previous versions of application software shall be retained as a contingency measure.

Development code, compilers or system tools shall not be present on operational environment.

Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier.

System Development Security standard
14.2 ISO27002:2013
CF18.3 ISF Good Practice

10.2.4 Secure development environment

System development activities shall be performed in appropriately protected secure development environments, which are isolated from the live and testing environments, and protected against unauthorised access.

Changes to business applications (including those under development) shall be performed in accordance with a formal, documented change management process and reviewed to ensure that they do not adversely affect intended functionality or compromise security controls. Development staff shall be prevented from making unauthorised changes to live environments.

Application source code should be protected by removing unnecessary sensitive information from programs and malware detection / protection mechanisms shall be employed prior to deploying them in the live environment.

Backup copies of program development shall be taken and in accordance with an agreed backup policy.

System Development Security standard
14.2 ISO27002:2013
CF17.2 ISF Good Practice

10.3 Outsourced development

When system development is outsourced the Application Owner shall verify,

- contractual requirements for secure design, coding and testing practices
- licensing arrangements, code ownership and intellectual property rights related to the outsourced content
- provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities
- compliance with applicable laws and control efficiency verification
- contractual right to audit development processes and controls

- escrow arrangements for Business Critical Applications or if relevant, e.g. if source code is no longer available.

14.2.7 ISO27002:2013
CF17 ISF Good Practice

10.4 Acquisition of Hardware and Software

Only IT-systems or equipment approved by or following standards issued by Group IT may be acquired and used within the Group.

There shall be documented standards for acquiring (e.g. purchasing or leasing) hardware and software, which address security requirements and specify the methods for identification of any security deficiencies. Software licensing requirements shall be met by obtaining adequate licenses for planned use and by providing proof of ownership of software.

Hardware and software shall be acquired from approved suppliers with a proven record of providing robust and resilient products which shall be tested prior to use. The maintenance of hardware and software belonging to business critical systems shall be regulated in a contract to ensure that the version currently in use is always supported.

14.1.1 ISO27002:2013
CF16.2 ISF Good Practice

11 Supplier relationships

The adherence to the security requirements for suppliers delivering services to Nordea shall be at least the same as if the services are delivered from the internal organization in Nordea.

When considering Outsourcing there are three main aspects which shall be considered:

- The type of service; i.e. what is supposed to be sourced.
- The proposed location of Nordea Information Assets
- The type of information the Outsourcing concerns, e.g. accounting or personal data.

This indicates both the risk level and what laws and regulations are relevant, whether the Outsourcing is possible and the statutory requirements the supplier shall adhere to when handling Nordea Information Assets.

15. ISO27002:2013
CF16 ISF Good Practice

11.1 Risk assessment

Before contracting a service from a supplier, a risk assessment of the proposed arrangement and the supplier shall be performed. This shall comprise, but is not limited to evaluation of compliance with regulatory requirements, what kind of information that will be processed, where the information will be handled/stored, controls regarding information in transit, back-up, restore, business continuity plans, logical and physical access controls.

Contingency plans shall be considered should the supplier no longer be able to provide the agreed services. These plans should include escrow of information, applications, licenses, encryption keys and an alternative supplier.

Nordea shall include the supplier in the Group’s control and risk assessments. The supplier shall be obliged to provide any information necessary for arranging effective risk management and internal control; such as information about significant organizational changes.

15 ISO27002:2013
CF16.1-3 ISF Good Practice

11.2 Addressing security within supplier agreements

The supplier agreements shall set forth that Nordea's and the service provider's rights and obligations are written in a sourcing agreement.

The contract shall include the following provisions:

- non-disclosure clauses,
- roles and responsibilities
- termination clauses. Termination of a supplier contract shall include, when relevant, revocation of access rights, removal of dedicated network connections, return of IT Assets, deletion of information/data, termination of licenses and securing of intellectual property rights.
- agreement on a process for change management
- description of Nordea access to Nordea information stored at the supplier.
- description of supplier's access to relevant information stored at Nordea. This shall include permitted access, access methods and the authorization process for user access and privileges
- escalation process for incident solving
- procedures to investigate and report without undue delay any security incidents or breaches
- right to audit
- possible requirements of assurance statements

Suppliers of IT services shall comply with Information Security Policy and instructions, and shall maintain auditable records demonstrating compliance with the requirements in these documents. Information Security Policy and instructions shall be attached to the contract. Additional security requirements relevant for the specific sourcing may be added to the contract as an addendum.

The following paragraphs in the Information Security Instructions are not relevant for suppliers. All in 2.1 and 3.1, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 4.2.1, 4.1.3, 4.1.5, 5.3, 6.1.1, 8.4.2, 9.5.1, 9.8, 10.1, 10.2, 10.3, 11, 11.1, 11.3, 11.4, 12.1.1, 14.1, 14.2

Guidelines on Business Continuity and Crisis Management
Incident and Problem Management Standard
Nordea Sourcing Policy
15.1.2 ISO27002:2013
CF7.7, CF16.1, 16.3 ISF Good Practice

11.3 Supplier service delivery management

Supplier service deliveries shall regularly be monitored, reviewed and audited to verify that the agreed level and conditions of service deliveries and information security are maintained. This responsibility lies within the customer area, product area or group function responsible for providing the goods and services to be sourced. Appropriate action should be taken when deficiencies in the service delivery are observed.

Regular monitoring and review of supplier services shall verify that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly. In addition, it shall be verified that the supplier assign responsibilities for reviewing compliance and enforcing the requirements of the agreements.

When the sourced service, includes access to personal data, the sourcing unit shall at least every second year monitor the supplier's compliance with security requirements. To meet this Nordea's obligation, the supplier may be requested to provide a relevant international assurance report (e.g. ISAE or SOC Reports - Service Organisation Control). Nordea shall assess whether the outsourced services are sufficiently covered in such a report (specific report for Nordea, effectiveness tested, inclusive/sub suppliers included, relevant application or infrastructure), or if additional audit activities should be instigated. Incompliances shall be addressed by the supplier and mitigation monitored by the sourcing unit.

15.2.1 ISO27002:2013
16.3 ISF Good Practice

11.4 Cloud Computing

Prior to contracting or using cloud services an information risk assessment shall be performed, which complies with the requirements in 11.1. This risk assessment shall include a description of consequences. In the contract with the supplier it shall be stated that the cloud provider will implement appropriate technical and organisational measures (see risk assessment above) as prescribed by IT Security Architecture. If required, notification to the public authorities shall be performed.

An assessment of the suppliers compliance of the key information security controls stipulated in the contract shall be performed if the sourcing include confidential or strictly confidential data before the sourcing agreement. Lastly the sourcing unit shall verify that the supplier complies to any specific security levels agreed on in the contract.

Additional security requirements shall be documented on the base of an impact analysis made by IT Security Architecture when the sourcing agreement involves personal information or strictly confidential information. The provisions shall take into account if the sourcing agreement involves using public cloud; i.e. computing resources hosted outside Nordea on a shared infrastructure and primarily accessed via the internet.

Regulated- or strict confidential data shall not be sourced using a public cloud service, unless a risk assessment has been made and the supplier has accepted to comply with GISI and the additional controls in the Nordea Cloud Computing Security Requirements.

Sourcing Security Standard
Nordea Technology Strategy
15.1.3 ISO27002:2013
CF16.4 ISF Good Practice

12 Information Security Incident Management

The purpose of Information Security Incident Management is to identify, respond to incidents and to restore normal status of information/IT systems, minimizing the adverse impact and reduce the risk of similar incidents occurring.

Information Security Incident Management consists of incident management and problem management. Criminal offenses using Nordea network or mobile devices are handled as cybercrime attacks.

Incident and Problem Management standard
16. ISO27002:2013
CF11 ISF Good Practice

12.1 Incident management

An incident is a disturbance to an IT system or another event leading to the actual outcome(s) of a business process to differ from the expected outcome(s). It also comprises incorrect configurations that have not yet affected a business process.

All employees, consultants and suppliers when working on Nordea equipment, shall be aware of their responsibility to report identified incidents to IT Service Support (ITSS) or the Nordea line manager. Users affected by the incident shall be given feed-back of the incident handling regularly until the incident is solved.

There must be internal rules to manage incidents arising in its operations.Incidents shall be recorded in an incident handling system and categorised depending on the impact and urgency also losses that have arisen in conjunction with the incident shall be documented. There shall be procedures in place to ensure that this information is correct.. Reported incidents shall be investigated and diagnosed to assess how the incidents best are resolved. Solution or workarounds and other relevant information about the incident handling shall be documented before the incident record is closed.

An incident manager shall be appointed for handling of incidents regarding IT services in a timely manner. Incident management routines shall be coordinated with change management to secure that change procedures are not circumvented.

For technical IT security related incidents, which can compromise the security in infrastructure and production systems, there must be established a dedicated and documented IT security incident management process. This process shall be connected to procedures for forensic investigations. All technical IT security related incidents will be managed by the Nordea IT Security Incident Response Team, NITSIRT.

Incident and Problem Management standard
16. ISO27002:2013
CF11.1 ISF Good Practice

12.1.1 Assessment of and decision on information security events

The incident manager is responsible for that each information security event is assessed to decide whether the event should be classified as a major information security incident.

Should an incident exceed pre-set thresholds or severity level it shall be escalated according to described escalation routines. Incidents classified as major and also threaten the availability of critical business systems, shall be escalated to Head of the relevant unit in Nordea.

All major incidents shall as a minimum be reported to the relevant Operational Risk Officer – ORO who is responsible for further reporting to central risk functions. Incidents with no direct financial loss shall also be reported to the ORO, if there is a reputational, regulatory or other substantial impact for Nordea.

Incident and Problem Management standard
16.1 ISO27002:2013
CF11.1 ISF Good Practice

12.2 Problem Management

A problem is an undiagnosed root cause of one or more incidents. Problem management shall be considered for all severe incidents or incidents with high resource consumption in order to produce corrective or preferably preventative solutions.

A manager shall be appointed as responsible for a problem management process and shall report the status of open problems on a regular basis.

Problems shall be recorded in a searchable log containing actions taken during the solution. This includes a description of workarounds until a permanent solution has been implemented. Before closing a problem, the reporter of the incident shall confirm that it has been solved.

Incident and Problem Management standard
CF11.1.9 ISF Good Practice

12.3 Cyber Attacks

Cyber-attacks are offences with a malicious motive to obtain financial gain or intentionally harm Nordea directly or indirectly, using network or mobile entities.

There shall established specific procedures for formally documenting the attack, the investigations, mitigating actions, reporting to authorities and all decisions during the course of actions. When the attack is on Nordea equipment, these issues are managed by Nordea IT Security Incident Response Team, NITSIRT.

Further there shall be a preventive process for cyber defence, which shall include on-going risk analyses, measuring, prioritizing, monitoring the resilience, mitigating and transferring cyber risks, applying existing best practices or guidelines where possible.

CF 11.2 ISF Good Practice

12.4 Forensic investigation

There shall be established a documented process for dealing with incidents that may require forensic investigation. The process shall include seeking of legal advice, planning the collection, preservation of electronic evidence and maintenance of a log of investigations undertaken. Evidence should be collected and handled in accordance with legal constraints and with respect for individuals' privacy and human rights. Results from a forensic investigation shall be reported to executive management and appropriate legal / regulatory bodies.

16.1.7 ISO27002:2013
CF 11.4 ISF Good Practice

13 Business Continuity Management

Business Continuity Management (BCM) is a holistic management process that provides a framework for building resilience and capability for an effective response that restore business critical information and processes for potential impacts threatening an organisation's continuity of business activities.

Business Continuity Plans (BCP) shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level. These plans describe the procedures to respond, recover, resume, and restore to a pre-defined level of operation for business-critical processes following disruption. The BCP shall be supported by relevant disaster recovery plans, covering technical infrastructure, IT systems and applications.

There shall be specific methods and procedures including contingency, continuity and recovery plans.

Guidelines on Business Continuity and Crisis Management in the Nordea Group
Disaster Recovery in Data Centres
17.1 ISO27002:2013
CF20 ISF Good Practice

13.1 Roles and responsibilities

There shall be three basic levels of BCP; crisis management, infrastructure and application/IT system specific. GOR is responsible for creating, supporting and maintaining the overall organisational business continuity framework for Nordea, including Business Continuity Planning, testing and reporting, Business impact analysis, Business Continuity Management Strategies, Crisis management, Business Continuity Management Awareness and Training. IT Operations are responsible for having up to date BCP for technical infrastructure and operating systems. Application Owners are responsible for that their systems are designed to deliver continuous service and are covered by an applicable and tested BCP. The business area and unit managers are also responsible for informing their organisations

-what information the plans include
-where to find them, physical presence

Internal rules for continuity management shall specify officers responsible (roles and positions) for steering operations and for deciding on measures in the event of an interruption or major operational disruption, and principles for managing and making decisions on measures depending on the type and scope of interruption or major operational disruption. The managing director shall decide on the internal rules.

A supplier is responsible for having an up to date BCP covering technical infrastructure, operating systems and applications used by Nordea and for any system or process supporting critical services for Nordea.

Guidelines on Business Continuity and Crisis Management in the Nordea Group
17.1 ISO27002:2013
CF20 ISF Good Practice

13.2 Planning

An organization shall regularly analyze the impact of possible interruptions or major operational disruptions that may occur in the undertaking's operations, and also in the operations that the undertaking has engaged another party to perform, with the goal of producing suitable contingency, continuity and recovery plans.

13.2.1 Scope

The relevant business unit in Nordea and the supplier shall identify which processes or system that are to be included in the BCP. When defining the scope, the relevant business unit in Nordea or the supplier shall document and explain exclusions; any such exclusion shall not affect the relevant business unit in Nordea's or the supplier's ability and responsibility to provide continuity of business and operations, as determined by a business impact analysis.

17.1 ISO27002:2013
CF20.5 ISF

13.2.2 Business impact analysis

BCP shall be based on a business impact analysis, i.e. a risk assessment of how long business critical systems or processes can be unavailable according to business requirements or, without serious impact in regard to legal requirements, loss of earnings and reputation. This shall be used to set prioritized timeframes for resuming the activities at a specified minimum acceptable level. The Application Owners shall be involved in evaluating the risk of the applications they are responsible for and shall establish and prepare the necessary countermeasures. The business impact analysis shall also include an identification of dependencies and supporting resources, including suppliers, sourcing partners and other relevant interested parties.

A review of the business impact analysis shall be performed every second year or when the criticality of the business process is changing or if there are significant changes in the Nordea processes, applications or suppliers.

Instructions for Business Continuity and Crisis Management in the Nordea Group
17.1 ISO27002:2013
CF20.3, 20.5 ISF Good Practice

13.2.3 Invocation a BCP

There shall be a definition or criteria of when a BCP can be activated, considering Nordea's goals, internal and external obligations, and legal and regulatory responsibilities. This is usually a predefined estimate of how long the business critical processes will be unavailable during an extraordinary event.

Before a BCP is invoked; relevant head of unit, business area or Group function shall be informed as well as the appropriate Operational Risk Officer – ORO and Group Identity and Communication. If the extraordinary event is only affecting one unit, the head of the affected business area or the head of the affected unit, can invoke the BCP, provided the definition or criteria above is satisfied.

In a situation where several critical business areas are affected, or when the disaster situation escalates to the whole group, crisis management shall be instigated. Only the Group CEO or Deputy Group CEO can activate this process. These situations is then handled by a crisis management team, led by a crisis management officer, normally head of business area or group function or member of GEM depending on the extent of the event, these are listed in the BCP.

There shall be procedures for informing all staff and relevant parties potentially impacted or covered by a BCP about their roles, tasks and expectations in case of invocation. These procedures shall be available and suitable for use, as well as adequately protected. Check and contact lists, internally and externally, shall be updated continuously.

There shall be procedures to manage internal and external communications in conjunction with an interruption or major operational disruption. When planning communications, it shall also be considered that an interruption or disruption may have a significant impact on the activity of subsidiaries or branches or affect the financial system in some other way

A supplier supporting Nordea critical processes or services shall have defined a set of criteria's for when the suppliers BCP can be activated.

Instructions for Business Continuity and Crisis Management in the Nordea Group
17.1 ISO27002:2013
CF20.4 ISF Good Practice

13.2.4 Redundancies

Business requirements for the availability of information systems shall be identified. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures shall be considered. This includes also underlying services such as power, cooling, storage and communications. No single-point-of-failure may exist for these systems.

Redundant information systems shall be tested to ensure the failover from one component to another component works as intended.

Disaster Recovery in Data Centres standard
17.2 ISO27002:2013
CF20.3 ISF Good Practice

13.2.5 Information security continuity in adverse situation

BCPs shall describe processes, procedures and controls to verify the required level of continuity for information security during an adverse situation, e.g. during a crisis or disaster.

Information security controls that have been implemented should continue to operate during an adverse situation. If this is not the case, other controls shall be established, implemented and maintained to a predetermined level, based on management-approved information security continuity objectives.

Disaster Recovery in Data Centres standard
17.2 ISO27002:2013
CF20 ISF Good Practice

13.3 Test and verification

BCPs, procedures and contact information for business critical processes shall be tested and verified at least yearly according to a documented and approved schedule, or after major changes to critical processes, their usage or organisational changes. Test shall be performed on crises management and technical parts of business continuity plans, such as BCP of a business service. There shall be a test plan with goals and assumption. The activities during the test and the result of the test shall be recorded in a report, which shall be signed off by the Business process owner.

Testing of the BCP shall, as a minimum, include verification of that all contact information is correct, exercise of communication procedures to reach relevant parties when needed, that the service chain approach works and that evacuation plans are up to date.

Results from tests of the contingency, continuity and recovery plans shall be reported to the board of directors at least once a year.

Guidelines for Business Continuity and Crisis Management
17.1.3 ISO27002:2013
CF20 ISF Good Practice

14 Compliance

Legal and regulatory areas stating requirements for information security shall be recognised by Application Owner and representatives of security-related functions. The manager of a Business Unit/process is responsible that the handling of information in the Business Unit complies with Nordea's Information Security Policy and related instructions, standards and rules as well as external requirements, and that employees and temporary staff are aware of how information should be handled.

14.1 Legal and contractual compliance

A Business unit should establish a process to identify relevant legal, regulatory and contractual requirements affecting information security, which covers:

- Information security specific legislation (e.g. data privacy, computer crimes, encryption export)
- General legislation which has security implications (e.g. book keeping act and intellectual property rights)

- Relevant regulations (e.g. financial regulation, bank secrecy related regulations, insider regulations, anti-money laundering, corporate governance, industry specific regulations such as the Payment Card Industry Data Security Standard).

The Business Unit shall review the identified requirements at least once a year. An approach to meet the identified requirements shall be documented. This may include support from relevant group functions. The approach shall also consider protection of the information throughout its lifecycle, i.e. through creation, processing, transmission, storage and destruction.

There shall be contractual requirements to protect any material that may be considered Nordea intellectual property which is used outside of Nordea. Intellectual property rights include software or document copyright, design rights, trademarks, patents, and source code licenses. Use of installed proprietary software products in Nordea shall be reviewed regularly and non-compliance reported.

The Business Unit should in order to protect Nordea organizational records, such as accounting records, transaction logs and IT system documentation issue guidelines on the retention, storage and disposal of records and information in accordance with statutory, regulatory, contractual, and business requirements. Appropriate logical and physical controls shall be implemented to protect important records and information from loss, destruction, and falsification.

Information security rules - Privacy and monitoring
18.1.1 ISO27002:2013
SR2.1 ISF Good Practice

14.2 Compliance review

A compliance review or a self-assessment that includes information security shall be performed regularly by managers or the Compliance Officers. Managers shall also review the compliance of information processing within their area of responsibility with the appropriate Nordea information security requirements.

If any non-compliance is found as a result of the review, managers shall evaluate the need for corrective actions and document the result.

Information systems shall regularly be checked for technical compliance with approved security standards and minimum baselines. The results of penetration tests or vulnerability assessments shall be kept confidential.

18.1 ISO27002:2013
SR2.1.5 ISF Good Practice

14.3 Information security audit

Independent information security audits shall be performed regularly for selected environments that are critical to Nordea. The results of information security audits shall be documented and reported to the board of directors. The information security audit report shall describe business risks, significant audit findings and provides a set of recommendations relating to each audit finding.

18.2, ISO27002:2013
SI2.3, SI1 ISF Good Practice

15 Terms, definitions and references

15.1 Terms and definitions

Application owner: is the business manager responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system, and may rely on the assistance and advice of the IT staff in the implementation of the responsibilities. Application Owner decides the content of the application, who is allowed to use it, how quickly it should be possible to recover from an IT disaster etc. See also 2.1.6

Asset: anything that has value to Nordea and consists of Information and IT Assets.

Back-up: refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.

Availability: the ability to use information to the expected extent and within the desired period.

Biometrics: Refers to the identification of humans by their characteristics or traits.

Business Critical Systems: A system is considered "Business Critical" if a 'long' duration outage would:
- Result in a significant loss of assets, revenue flow, market share or goodwill.
- Make the business unable to meet regulatory and statutory requirements.

Confidentiality: the fact that information is not made available or disclosed to unauthorised persons

Compilers: Is a computer program (or set of programs) that transforms source code written in a programming language (the source language) into another computer language to create an executable program.

Computing Devices: Is a general purpose device that can be programmed to carry out a set of arithmetic or logical operations.

Contingency plan: a plan describing the measures that an undertaking is to take to deal with serious and extensive interruptions, disruptions or crises

Continuity plan: a plan describing how operations are to be maintained in the event of an interruption or a major operational disruption,

Control: means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature

Cryptographic: Is effectively synonymous with encryption and is the practice and study of techniques for secure communication in the presence of external parties.

Demilitarised Zones (DMZ): In computer security, a DMZ (sometimes referred to as a perimeter networking) is a physical or logical sub-network that contains and exposes an organization's external-facing services to a larger untrusted network, usually the Internet.

Firewalls: Is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analysing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set.

FSA: Regulator of all providers of financial services in the local country.

Incident: an event that has or is at risk of having an adverse effect on the organisations operations, assets or reputation,

Information Assets: are defined as electronic documents, information in databases, paper-based documents or images thereof containing Nordea information.

Information Processing Facilities: any information processing system, service or infrastructure, or the physical locations housing them

Information Security Forum (ISF): is one of the world's leading independent authorities on information security.

Information Owner: 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.
IT Assets comprises hardware, software and infrastructure

integrity: property of information entailing that the information has not been amended without authorisation, by mistake or due to a malfunction

IT System: covers applications, operating systems, computer system (server) and networks.

Logic Bombs: Is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Malware: Short for malicious software, is software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer systems

NAS: Network-Attached Storage is file-level computer data storage connected to a computer network providing data access to a heterogeneous group of clients.

Need-to-know Principle: access to certain information is restricted. Access is only allowed when it is necessary for the conduct of one's official duties

Non-disclosure Agreement (NDA): is a legal contract between at least two parties that outlines rules for sharing confidential material, knowledge or information.

Outsourcing: is a form of sourcing that refers to when activities are performed by a supplier that would otherwise be undertaken in house.

Penetration Test: Is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders and malicious insiders.

Personal Data: means any information relating to an individual, which can be reasonably linked to that private person. Information on a representative (private person) of a company is regarded as Personal Data as well.

Recovery plan: a plan describing the priorities and procedures according to which an undertaking shall revert to normal operations following an interruption or major operational disruption.

Regression Testing: Is any type of software testing that seeks to uncover new software weaknesses. The intent of regression testing is to ensure that a change, such as a bug-fix, did not introduce new faults.

Remote Access Gateway: Is the termination and verification point of connections from outside where authorized users or clients are validated and forwarded inside the network.

Risk appetite: The broad-based amount of risk a company or other entity is willing to accept.

SAN: Storage Area Network is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers.

Shell: Is software that provides an interface for users of an operating system which provides access to the services of a kernel.

Sourcing Unit: The unit in Nordea (e.g. Division) who own the outsourcing agreement with the supplier. Typically the Sourcing Unit has the direct cost in the units' RFF.

Supplier: is a company that provides Nordea with consulting, legal, education, communications, processing or other services.

System 'hardening': is usually the process of securing a system by configuring it securely, removing unnecessary functionality, limiting outside access to the system, etc.

Tokens: Are used to prove one's identity electronically they can be hardware or software.

Traceability: is the ability to unequivocally trace activities and the individuals or systems that have carried them out.

Trojan Horses: Is a type of malware that masquerades as a legitimate file or helpful program but whose real purpose is malicious; i.e. to grant a hacker unauthorized access to a computer.

Two-factor Authentication: is an approach to authentication which requires the presentation of two or more of the three authentication factors: a knowledge factor ("something the user knows"), a possession factor ("something the user has"), and an inherence factor ("something the user is").

Two-way SSL: The Secure Sockets Layer is a commonly-used protocol that provides confirmation of identity and encryption for transactions over the Internet. Two-way SSL refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity.

VPN: Virtual private network is a technology that enables a predefined group of computers to establish secure connections over an open network (e.g. the Internet) while not allowing any other parties to connect.

Virus: Is a malicious code that can replicate itself. It attaches to files and when a user executes or opens a file the code is activated and tries to spread to other computers.

Worms: Is a standalone malicious computer program that can replicate itself in order to spread to other computers. It may travel by infecting another program, but it often spreads directly over a network abusing vulnerabilities in the infected computers.

15.2 References

Document name	Ver.	Date
ISO 27002:2013 Information Technology – Security techniques – Code of practice for information security management		2013-06-15
ISF - The 2013 Standard of Good Practice for Information Security		June 2013
Nordea Operational Risk Policy	3.2	2011-10-18
Information Security Instructions for the Nordea Group		2011-05-09
Security for Smartphones and Tablets with access to Nordea	1.0	2012-04-12
Wireless Security Strategy		2011-12-30
Network Security Standard	4.0	2011-07-11
00_Inf_Se_rules for all employee's_MAIN - GORC		
01_Inf_sec_rules_Confidentiality - GORC		
02_Inf_sec_rules_Access on need - GORC		
03_Inf_sec_rules_Handling outside Nordea premises - GORC		
04_Inf_sec_rules_e-mail – GORC		
05_Inf_sec_rules_Internet – GORC		
06_Inf_sec_rules_Passwords and PINs - GORC		
07_Inf_sec_rules_Equipment and systems - GORC		
08_Inf_sec_rules_Privacy and monitoring - GORC		
2013_04_05_Backup	1.0	2013-04-05
2013_12_09_Business Application Security	1.1	2013-12-09
2013_04_05_Change Management	1.0	2013-04-05
2013_04_05_Data Exchange between internal and external systems	1.0	2013-04-05
2011_01_07_Disaster_Recovery_in_Data_Centres_ver_20	2.0	2011-01-07
Vulnerability and patch management	3.0	2013-12-09
2013_04_05_Incident and Problem Management	1.0	2013-04-05
2014_02_31_ Information Security Checklist for Projects	1.0	2014-02-31
2013_05_30_ Information Security Exception standard	1.0	2013-05-30
2009_08_27_IT_Security_in_Operational_Environments_ver_10_Final_2	2.0	2009-08-27
2013_12_09_ Password Standard	1.0	2013-12-09
2013_04_05_ Physical Protection For IT Equipment	1.0	2013-04-05
Remote Access		
Mobile Devices	2.0	2014-02-25
2013_12_09_ System Development Security	1.1	2013-12-09
Authorisation of internal users - IT Security Standard	4.0	2013-06-26
2009_03_31_Cryptographic_Protection_of_internal_transaction_10	1.0	2009-03-31
2009_03_31_Encryption_Key_Management_Standard_10	1.0	2009-03-31
2008_10_06_Workstation_Security_Version_10_n	1.0	2008-10-06
2007_06_29_Malicious_Code_Defence_ver_20	2.0	2007-06-29
IT_Security_Log_standard	1.0	2007-03-22
2004_04_01_Intrusion_Control_Systems_ver1_0	1.0	2004-04-01
Instructions for Business Continuity and Crisis Management Procedures		2012-06-11
Guidelines on Business Continuity and Crisis Management	2011-10-31	2011-10-31
Information Security Responsibilities Standard	1.0	2014-04-10

15.3 Responsible unit and contact

Head of IT Security Architecture, Jacqueline Johnson +45 3333 6185

Contact: IT Security Architecture, Christian Kasper +45 33 700 724
IT Security Architecture, Pierre Schwartz +45 4040 1215