EDC Security Requirements

Version 4.1

14 October 2016

Heading
EDC Security Requirements

Document type	Archive-key
Contractual Requirements	<Fill in Archive key>
Domain	Level
Sourcing and IT Security	<Fill in Level>

Version/ status	Date created	Responsible person/ owner
Version 4.1	14 October 2016	Head of IT Security Architecture Jacqueline Johnson

Department/Area	Contact person
IT Security Architecture	Niels T. Andersen

Classification code	Developer
Internal	Niels T. Andersen
Intended for/Target group	Next revision
Business, Group IT, EDC Suppliers, All organizations and individuals in EDCs providing services to Nordea	12 month after date of approval

Approved by	Document replaced	Date of approval
Jacqueline Johnson, Head of IT Security Architecture	2013-05-24_EDC_Security_Requirements_v3.0	2015-09-28

This page contains metadata which are to be used as properties in Documentum. All fields are mandatory. Please use Guidelines for “How to use new templates”, for more detailed information about the different fields.

Revision history

Date	Version	Reason for issue	Author
2012.11.18 - 2012.12.02	0.1 - 0.4	First drafts	Matti Santaniemi
2012.12.02 - 2013.01.23	0.5 – 0.8	Comments from Jacqueline Johnson, Thomas Kristensen, Gustaf Björklund, Christian Kasper, Juha Vaarama, Jacob Øst Hansen	
2013.01.28	0.9	Finalising the proposal for approval	Matti Santaniemi
2013.01.29	1.0	Content and structure approved by Head of IT Security Architecture Jacqueline Johnson	Matti Santaniemi
2013.03.04	1.1	Additions related to email, Internet-access and collaboration	Matti Santaniemi
2013.03.18	1.15	Updates on requirements related to printing	Matti Santaniemi
2013.04.22	1.2	Switch to Nordea template	Matti Santaniemi
2013.04.26	1.3	Comments from Head of IT Security Architecture Jacqueline Johnson	Matti Santaniemi
2013.04.30 - 2013.05.16	1.8 - 1.9	Last comments and updates	Matti Santaniemi
2013.05.16	2.0	Ready for approval	Matti Santaniemi
2015.02.09-2015.03.16	2.1	Draft based on comments from Jan Espersen, Louise Sångberg	Niels T. Andersen
2015.03.16	2.1	Ready for approval	Niels T. Andersen
2015.03.18	3.0	Approved	Niels T. Andersen
2015.09.28	4.0	Changed requirements regarding Security Incidents (section 8)	Niels T. Andersen
2016.10.14	4.1	Specification of background check requirements (section 4, 1st sentence)	Niels T. Andersen

Table on contents

1. Purpose

Extended Delivery Centre (EDC) Suppliers provides IT development, testing and operations/maintenance services to Nordea using environments provided by Nordea.

This document describes detailed specific Information Technology (IT) Security requirements for EDC Suppliers. General information security requirements for Nordea outsourcing arrangements are described in Nordea Outsourcing policies and Nordea Information Security Instructions.

The specific requirements set out in this document together with Nordea information security policy, instructions and IT security standards apply to all employees in EDC providing services to Nordea as well as sub-contractors to EDC. These requirements comprise all premises, equipment, technologies and information used for providing services.

2. The Extended Delivery Centre – EDC

The EDC has a physically separated area, which is solely dedicated to employees working for Nordea inside EDC's premises. Establishment of Nordea dedicated areas must be approved by Nordea before they are put into operation.

Work performed with regards to Nordea must be performed within the Nordea dedicated area.

The EDC Supplier's employees access the Nordea hosted developer environment through a secure communication line from the EDC to a partner portal in Nordea extranet infrastructure[1], which is dedicated to Nordea's vendors and partners.

The secure communication line between Nordea Data Centre and the EDC Supplier network may be terminated in the EDC Supplier's Data Centre. The EDC Supplier must use its internal network for implementing secure encrypted communication from the EDC to the secure communication line entry in the EDC Supplier's Data Centre. Access to Nordea's secure communication line must only be possible from networks in the working area dedicated for Nordea.

EDC Supplier's employees will develop and maintain Nordea applications in Nordea hosted developer environments with Nordea developer tools. The employees are not allowed to transfer or download data from Nordea's hosted developer environment to EDC environment, or in any other way transfer data related to Nordea outside the dedicated network for Nordea.

No customer related data will be handled or stored outside the Nordea network.

Nordea will use authentication tools and log EDC Supplier's employees' access to platforms, servers and applications with security solutions. These control mechanisms shall be applied in Nordea extranet

[1] A demilitarized zone (DMZ) separated by firewalls

infrastructure (DMZ) dedicated for vendor and partner access, in internal network infrastructure as well as in target platforms, servers and applications.

With reference to the audit clause, Nordea will audit EDC Supplier to verify that security arrangements and corresponding procedures are in place according to the requirements in this document and in the Nordea Information Security Instructions.

3. Information security responsibilities

The EDC Supplier must appoint a manager (later "EDC Security Responsible") who is responsible for implementing and maintaining security in the EDC Supplier's services and environments with regards to the requirements stated in this document and the provisions in Nordea's information security policy, instructions and standards.

Thus the EDC Supplier must develop, deploy, and manage services in accordance with the mentioned requirements. Auditable records demonstrating compliance with the information security policies and instructions must be maintained by EDC.

The EDC Supplier must have clearly defined and documented information security responsibilities and duties. These responsibilities and duties must be carried out by skilled professionals in a safely organized manner.

4. Human resources security

The Supplier shall perform background checks on all new employees taking part in delivering the Services to Nordea. Purpose of such checks is to ensure that the new employees' backgrounds are not likely to be conflicting with the responsibilities and tasks to be undertaken by such employees, and shall include checks of e.g. the employees' criminal records, creditworthiness, past employments, relevant educations, etc. Background checks are performed preferably before the employees are joining the Supplier's organization or immediately thereafter, and within 1 month after employment.

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 shall be informed of the possible consequences of any theft, frauds or misuse of Nordea information and facilities.

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

EDC Supplier must have formal security awareness program for all employees. Security awareness sessions must be run regularly according to a schedule and include Nordea security requirements.

5. Physical and environmental security

The EDC Supplier must implement physical security perimeters to protect premises, buildings, rooms and areas, from loss, theft, damage, interference, interruption of, or unauthorised physical access.

5.1. The area dedicated to working for Nordea

The EDC Supplier's employees working for Nordea and their IT equipment must be sited physically separated, access controlled and in a protected area in the EDC premises.

Access to this dedicated area must be allowed only to employees working for services provided to Nordea. Access to the area must be granted by EDC Security Responsible.

5.2. Secure communications

The equipment used for secure communications in the EDC Supplier's premises and in the EDC Supplier's internal network must be protected according to Nordea's policies and information security instructions.

5.3. Physical access control

All employees accessing the Nordea dedicated area must wear personal identity card or access card visible.

Access cards or keys are for personal use and must not be shared with others.

When passing the outer perimeter to a Nordea dedicated area the user shall be forced to authenticate with a personal access card and entering the corresponding PIN code.

The Nordea dedicated area must be placed so that public access is prohibited and external disturbance (noise, tail-gating, etc.) is being avoided.

Only authorised employees who work in the EDC to provide services for Nordea may be permanently equipped with access cards to the dedicated area.

Visitors must be authorized by EDC Security Responsible and supervised during the visit. The authorization of visitors may be delegated to a limited number of people by EDC Security Responsible.

All physical accesses (including visitors) to the Nordea dedicated area must be logged. The EDC physical access control system must be able to provide a list of who individually has accessed the area in a given time period. Physical keys may not be used, except for emergencies for a very limited number of employees. When the key is used an alarm shall be triggered and the use investigated and recorded in a log.

Logs for use of access cards and keys must be kept at least for 1 year. Nordea shall have access to this log information upon request.

The EDC Supplier must review and immediately revoke employees' physical access rights to the dedicated area for Nordea when the employee discontinues working for Nordea. To support this, formal procedures must be established and a centrally managed system implemented.

5.4. Equipment security

Security devices (e.g. tokens enabling strong authentication to Nordea) provided by Nordea for accessing Nordea hosted developer environments must only be used in the area dedicated for employees working for Nordea. This area must be equipped with locked cabinets where EDC Supplier's employees must store their security devices when they are not in use. Nordea will arrange additional security tokens for EDC employees for temporary use when they are visiting and working in Nordea offices.

All EDC workstations and laptops used for providing services to Nordea must be security enabled and protected with a user login process to verify that only authenticated EDC employees can open and access them.

EDC workstations and laptops must be equipped with hard disk encryption and a firewall. The firewall shall prevent that the equipment can be used directly on the open Internet. The firewall may allow the equipment to connect to the Supplier's Data Centre and from there, through a controlled proxy, to Internet.

5.5. Secure disposal of equipment

All items of equipment containing storage media must be disposed in a way that all data has been securely overwritten prior to disposal or handover to third party for disposal.
All storage media must not be reused by third parties or for services to other customers.

EDC Supplier must have a formal disposal process complying with industry best practices and recognized overwriting standards for erasing the data from hard disks.

6. Communications and operations management

The EDC Supplier must maintain documented operating procedures and technological controls to secure the information systems, infrastructure and data.

6.1. Network security

The network used for Nordea services and the IT equipment attached to that network must be separated with firewall from rest of the EDC Supplier's network.

EDC Supplier's employees must use workstations in the EDC to establish a secured and encrypted SSL connection to virtual developer workstations hosted by Nordea. In order to implement this secure SSL connection, the EDC Supplier must install root certificates issued by Nordea Certificate Authority (CA) to workstations physically located in Nordea dedicated area.

EDC Supplier must verify that the connection from EDC workstation to Nordea developer's environment is only available for the employees working for Nordea. EDC workstations used for accessing Nordea hosted developer environments must not have any other network connections than internal LAN installed.

6.2. System patching

The EDC Supplier must implement an effective software update management process to verify that all relevant, up-to-date, approved patches are installed on all applications, operating systems and BIOS on IT equipment in scope.

All equipment in the EDC must regularly be scanned for relevant software and security updates. Security updates and patches for vulnerabilities must be applied as soon as possible, but at the latest 10 business days after they have been made generally available from the suppliers.

Test of the update must be carried out on a reference group before deployed generally. There must be rollback procedures in case any problems occur during or after the installation of the security patches.

6.3. Malware protection

The EDC Supplier must install and run an antivirus system on all servers, gateways and workstations in the EDC. The antivirus system must be based on an internationally recognised product that is continuously updated with respect to signatures and scanning concepts.

All local hard disks must be scanned at least once a week. All files must be scanned in real time when received, opened, stored or accessed by a service or external user.

EDC employees must be able to initiate the update of the latest signature file in case of automatic updates are not working. EDC employees must be able to scan the local hard disk whenever needed. EDC employees must not be able to change antivirus settings.

EDC Supplier must generate monthly statistics on malicious code activity in the EDC. Nordea shall have access to these statistics by request.

6.4. Email gateway security

All inbound and outbound emails in email gateways used by EDC employees must be scanned to detect and to block malware, links to hostile sites and unwanted file types.

The email gateway used by EDC employees must be equipped with one or more well-acknowledged spam-filter products capable of handling mails in relevant languages. These filters must be able to recognize and prohibit inbound and outbound spam.

Only approved file types (based of control of file extension) must be allowed to pass through the email gateway used by EDC employees. Executable code must be blocked in a way that it cannot pass. Links leading to hostile sites must be removed.

The email gateway must be equipped with a different antivirus system product than the one on EDC workstations.

The email gateway used by EDC must be part of Sender Policy Framework (SPF) and must reject all emails in conflict with SPF records.

Transport Layer Security (TLS) must be enabled in the email gateways in EDC. TLS-encryption must be enforced (Forced TLS) between Nordea email gateways and EDC email gateways.

6.5. Configurations management

EDC Supplier's employees must not be able to alter any hardware or software settings, which are related to security on IT equipment. Thus the employees are not allowed to be local administrators on the VDI, local Nordea laptops or workstations.

Nordea may verify that appropriate security policies, patches, configurations and antivirus products are implemented, updated and enforced in the connecting equipment (i.e. workstation).

6.6. Wireless networks and technologies

Use of wireless LAN, Bluetooth and other wireless technologies are not allowed in IT equipment in EDC used for accessing Nordea developer environment. All radio buttons enabling use of such technologies must be set "OFF".

6.7. Removable media

No removable media devices (USB sticks, etc.) are allowed in the dedicated Nordea area in EDC. Nordea may verify that USB receptacle and DVD/CD drive are disabled.

6.8. Printing and print-outs

The EDC Supplier must implement explicit written procedures regarding handling of print-outs from Nordea's systems. The EDC Supplier must upon request provide Nordea with a copy of the applicable written procedures and describe how they are implemented.

Printers must be sited inside the Nordea dedicated area where only employees working for Nordea can access them.

Printing must be limited to print-outs strictly necessary for delivering services to Nordea. Print-outs must immediately be removed from the printers after printing. The printed materials must not be taken out from the dedicated area. They must be stored in a locked cabinet or safe.

Printed materials must be shredded with a cross-cut (confetti) shredder or disposed immediately after the relevant employee has finalised the work for which the print was produced, unless it is necessary for the proper documentation of the performed task.

Printing, print screen and other screen capture functionalities must be disabled in EDC workstations.

7. Access control

The EDC Supplier must implement sufficient authorization controls regarding access to information processing systems and facilities. These controls must comply with industry best practices, supplier's internal policies and Nordea instructions and standards.

7.1. Identity and access management in the EDC equipment

EDC must implement user identity and authorisation management processes. When accessing EDC workstations and servers employees must use user credentials provided according to this process. User credentials are for personal use only. Sharing of user credentials is not allowed.

The EDC Supplier must use formal user registration and approval procedure for granting access to systems and environments. Formal procedures must be in place to manage the allocation of logical access rights to systems.

The EDC Supplier must review and immediately revoke user access rights in all systems for terminated employees, terminated consultants and employees that no longer need access. Their security device (token) must be withdrawn and Nordea must immediately be informed.

The EDC Supplier must inform the relevant Nordea manager of terminated employees well in advance to ensure Nordea can fulfil responsibilities regarding revocation of logical access rights in the Nordea systems.

Formal procedures must be in place to centrally manage revocation of logical access rights to systems used for providing services to Nordea.

7.2. Password controls

The EDC Supplier must verify that its password rules meet Nordea requirements.

The password shall be chosen by the user and kept as a secret.

An initial password must always be changed at the first login.

Password must not be written down or stored in clear text.

Passwords that need to be stored must be stored in encrypted form.

Passwords must not show on screen when keyed in.

Passwords must be blanked out in log files.

After 5 attempts to sign-on with a wrong password the user-id is revoked.

Passwords must be changed regularly - at least after 45 days.

The last 15 passwords must not be reused.

Passwords must have at least 8 characters.

Passwords must contain at least 1 number, 1 letter and one special character.

The user must choose passwords that are hard to guess. No user IDs, names, words, popular phrases, birth dates or similar as part of the passwords are allowed.

7.3. Inactive accounts

The EDC Supplier must implement formal procedures and technical mechanisms to verify that only active users have system access. In addition to formal de-registration procedure, EDC Security Responsible must monitor and remove user logical access rights of inactive components at regular and predefined intervals.

7.4. Controls for unattended systems

When equipment or session in the equipment has not been used for 15 minutes it must be automatically locked. Unlocking can only be performed with corresponding user's password.

7.5. Logging in EDC environment

EDC Supplier must be able to provide consistent log report from the whole access chain in EDC Supplier's employee's access to Nordea developer's environment.

Logs relevant for such investigations must be kept at least for 2 years. Nordea shall have access to this log information by request.

7.6. Remote access

Remote access to IT equipment used for accessing Nordea services must be disabled except for limited access (e.g. Windows Remote Assistance) to EDC internal Help Desk (HD) provided by the EDC Supplier. This may be used for supporting EDC employees in solving problems regarding EDC workstations. Remote assistance connection must be requested and approved by EDC employee. EDC employee can share his or her screen and EDC internal HD may instruct the employee in solving the problem. EDC internal HD must not perform any changes on the workstation. When EDC HD is connected to EDC workstation or laptop, it must not be connected to Nordea.

7.7. Identity and access management in Nordea hosted developer environment

The EDC Supplier employees will have and use personal Nordea consultant user credentials, including consultant user ID with password and security device with PIN attached to the user ID, for accessing Nordea hosted developer environment and services.

User credentials (user ID, password, security device with PIN-code) are for personal use only. Sharing of user credentials is not allowed.

User credentials including authorisations to Nordea developer's environments is provided with Nordea identity and access management processes and solutions implemented by the Nordea responsible for the EDC Supplier. This includes managing digital identities and managing how these identities can access resources in the Nordea network.

Access to needed services, application and environments must be based on work-related needs and must follow Nordea's instructions and standards for authorizations.

7.7.1. Nordea email

EDC employees must not be able to send email messages out from Nordea or receive email messages from outside Nordea.

Access can be granted to whitelisted domains or mailboxes, through formal approval procedures.

7.7.2. Internet access in Nordea hosted environment

EDC employees must not have access to Internet from their Nordea hosted developer's workstations. EDC employees' Internet access will be blocked in Nordea's Internet proxies.

Access can be granted to whitelisted domains, through formal approval procedures.

7.8. Logging in Nordea hosted environment

Nordea may log the EDC Supplier's activities in Nordea environments. Nordea shall disclose the content of such logs upon request provided that the EDC Supplier gives sufficient information on the reasons for such request.

Nordea's obligation to provide logs is subject to availability of the logs since Nordea will delete the information in relevant logs on a regular basis.

7.9. Access to Nordea operational environments

The EDC Supplier's employee may need access to Nordea production environments, i.e. environment where some Nordea operational data is stored, for error fixing and problem solving purposes. In those cases the EDC Supplier employee must be granted temporary access with read access rights to production systems in scope. This limited access must be revoked after it is not needed anymore. Nordea must monitor and record all accesses and any actions performed in the production environment. In addition Nordea must execute a quarterly review on all EDC employees' access rights to operational environments. All access rights that are not needed must immediately be revoked.

EDC Supplier's employees must not be granted access to business applications or authorisations to perform any business transactions (make money transfers or alike), in order to ensure full segregation of duties.

Segregation of EDC employees’ duties and areas of responsibility in Nordea environments must comply with Nordea’s policies and information security instructions.

System development, operations/maintenance and business use shall be separated.

8. Security incidents and investigations

The Supplier shall report significant security Incidents, which affects the service to Nordea without undue delay after the Incident was first observed and categorized. Reporting shall also include security Incidents at subcontractors. Reporting shall take place to Nordea IT Security Incident Response Team (nitsirt@nordea.com).

9. Business Continuity Management

The EDC Supplier must have a Business Continuity Plan that can support Nordea’s requirements to restore operations and ensure availability. For IT Service Continuity Management (ITSCM) the recovery time shall not exceed 8 hours.

The EDC Supplier must have the technical infrastructures to support full operating secondary sites. No single-point-of-failure may exist for critical components.

Escalation procedures must be in place with the EDC supplier as part of their BCP / ITSCM.

The Business Continuity Plan shall be reviewed, updated and tested annually.

A copy of the approved and tested Business Continuity Plan must be provided upon request to Nordea.

10. Information security audit

Independent security audits shall be performed regularly for EDC Supplier’s environments in order to verify that security arrangements and corresponding procedures are in place. The results of these security audits shall be reported to Nordea. Audit arrangements are described in a separate contract appendix.