



IT Security Requirements for JN Data

Version:	13.04
Classification:	Restricted/Internal
Date of approval:	Danish version approved on 02.07.2025
Valid from:	01.09.2025



Contents

1. Introduction..... 6

 1.1 Structure of the document 6

 1.2 Responsibility..... 7

2 Security Requirement Owner 7

3 Terms and definitions 7

 3.1 Definitions 8

4 IT Risk Management 9

5 Organisational controls..... 10

 5.1 Policies for information security 10

 5.2 Information security roles and responsibilities 11

 5.3 Segregation of duties 12

 5.4 Management responsibilities 12

 5.5 Contact with authorities 12

 5.6 Contact with special interest groups 13

 5.7 Threat intelligence 13

 5.8 Information security in project management..... 13

 5.9 Inventory of information and other associated assets 14

 5.10 Acceptable use of information and other associated assets 14

 5.11 Return of assets 15

 5.12 Classification of information 15

 5.13 Labelling of information..... 15

 5.14 Information transfer 16

 5.15 Access control 16

 5.16 Identity management 17

 5.17 Authentication information 17

 5.18 Access rights..... 18

 5.19 Information security in supplier relationships 18

 5.20 Addressing information security within supplier agreements 19

 5.21 Managing information security in the ICT supply chain 20



5.22 Monitoring, review and change management of supplier services 20

5.23 Information security for use of cloud services 21

5.24 Information security incident management planning and preparation 24

 5.24.1 Planning and preparation of security incidents 24

 5.24.2 Planning and preparation of incidents and major incidents 24

5.25 Assessment and decision on information security events 25

5.26 Response to information security incidents 25

5.27 Learning from information security incidents 26

5.28 Collection of evidence 26

5.29 Information security during disruption 27

5.30 ICT readiness for business continuity 27

5.31 Legal, statutory, regulatory and contractual requirements 28

 5.31.1 Legal, statutory and regulatory requirements 28

 5.31.2 Contractual requirements 28

5.32 Intellectual property rights 29

5.33 Protection of records 29

5.34 Privacy and protection of PII 30

5.35 Independent review of information security 30

5.36 Compliance with policies, rules and standards for information security 30

5.37 Documented operation procedures 30

6 People controls 31

 6.1 Screening 31

 6.2 Terms and conditions of employment 31

 6.3 Information security awareness, education and training 32

 6.4 Disciplinary process 32

 6.5 Responsibilities after termination or change of employment 33

 6.6 Confidentiality or non-disclosure agreements 33

 6.7 Remote working 33

 6.8 Information security event reporting 34

7 Physical controls 34



- 7.1 Physical security perimeters 34
- 7.2 Physical entry 34
- 7.3 Securing offices, rooms and facilities..... 35
- 7.4 Physical security monitoring..... 35
- 7.5 Protection against physical and environmental threats..... 36
- 7.6 Working in secure areas..... 36
- 7.7 Clear desk and clear screen 36
- 7.8 Equipment siting and protection 37
- 7.9 Security of assets off-premises 37
- 7.10 Storage media 37
- 7.11 Supporting utilities..... 38
- 7.12 Cabling security..... 38
- 7.13 Equipment maintenance..... 39
- 7.14 Secure disposal or re-use of equipment..... 39
- 8 Technical controls..... 40
 - 8.1 User endpoint devices 40
 - 8.2 Privileged access rights 40
 - 8.3 Information access restriction 41
 - 8.4 Access to source code..... 41
 - 8.5 Secure authentication..... 41
 - 8.6 Capacity management 42
 - 8.7 Protection against malware..... 42
 - 8.8 Management of technical vulnerabilities 43
 - 8.9 Configuration management..... 44
 - 8.10 Information deletion..... 45
 - 8.11 Data masking..... 45
 - 8.12 Data leakage prevention 45
 - 8.13 Information backup..... 46
 - 8.14 Redundancy of information processing facilities..... 46
 - 8.15 Logging 47



8.16 Monitoring activities 48

8.17 Clock synchronisation 48

8.18 Use of privileged utility programs..... 49

8.19 Installation of software on operational systems 49

8.20 Network security..... 50

8.21 Security of network services 50

8.22 Segregation of networks 51

8.23 Web filtering 51

8.24 Use of cryptography..... 52

8.25 Secure development life cycle 52

8.26 Application security requirements 53

8.27 Secure system architecture and engineering principles..... 53

8.28 Secure coding..... 54

8.29 Security testing in development and acceptance..... 54

8.30 Outsourced development 54

8.31 Separation of development, test and production environments..... 55

8.32 Change Management..... 55

8.33 Test information..... 56

8.34 Protection of information systems during audit testing 56

Appendix A..... 58



1. Introduction

The IT Security Requirements describes the requirements for IT security at JN Data and supports the compliance with JN Data's IT Security Policy. The IT Security Requirements set out the overall scope to ensure protections of the confidentiality, integrity, and confidentiality of JN Data's information and IT assets.

The purpose of the IT Security Requirements is to establish the overall requirements for the IT Security in JN Data, and connect the IT Security Policy with formalised documents, which describes the operational and in-depth requirements within the specific areas in JN Data based on best practice in relation to security. All IT Security Requirements are supported by documentation to ensure operationalisations, implementation, and compliance.

The IT Security Requirements at JN Data are structured after the ISO/IEC 27001:2022 standard and based on the actual threat landscape with the aim of meet and comply with standards, laws, and regulations, as well as sector, internal and customer specific requirements.

The IT Security Requirements covers several areas in JN Data, and therefore the requirements need to be known by all employees, consultants, and suppliers, with access to JN Data's information and IT assets.

Any deviation from the IT Security Requirements described in this document must be approved by Security Governance through the dispensation process.

1.1 Structure of the document

The IT Security Requirements are structured after the ISO/IEC 27001:2022 standard as a reference framework, which is reflected in numbering and naming of the sections starting with section 5 and up to section 8:

- Organisational controls (section 5)
- People controls (section 6)
- Physical controls (section 7)
- Technological controls (section 8).

Distributed across the four themes are 93 safeguards, named and structured according to the standard, each containing ID and title of the safeguard. The IT Security Requirements are described under each of the 93 safeguards. The 93 safeguards are distributed into 30 areas in JN Data and assigned to a Security Requirement Owner. A description of the role can be found in section 2, and the overview of the Security Requirement Owners can be found in Appendix A in this document.



JN Data identify and manage IT risks in according to the policy for IT Risk Management to ensure, that IT risks are identified, analysed, managed, monitored, and reported to the management. The IT security requirements related to IT Risk Management are described in section 4.

In section 3, a description and definition of some of the terms used in JN Data's IT Security Requirements. The definitions are based on inspiration from the ISO/IEC 27002:2022 standard, JN Data's Concept Dictionary and from the Security Requirement Owners.

1.2 Responsibility

JN Data's IT security function is responsible for updating and maintaining the IT security requirements in collaboration with the IT security requirements owner. All relevant stakeholders, affected by the IT Security Requirements, are more than welcome to suggest improvements, additions and feedback by contacting Compliance Governance on mail: comgov@jndata.dk.

2 Security Requirement Owner

For all IT Security Requirements, a Security Requirement Owner has been appointed, assessed to have the necessary knowledge and expertise in the area. In collaboration with the Security Requirement Owner, Compliance Governance has designed and formulated the overall IT Security Requirements, while the operational requirements are specified and centralised in formalised documents within the specific area. The purpose is to ensure that the operational requirements are described by the areas that have the expertise and knowledge of best practice within the specific area in relation to IT security.

The Security Requirement Owner is responsible for the implementation and maintenance of the formalised documents, security safeguards and verification controls, relevant to ensure compliance with the IT Security Requirements, PCI DSS, PCI PIN, SWIFT and Clearing. All employees are responsible for ensuring that the IT Security requirements, PCI DSS, PCI PIN, SWIFT and Clearing are followed.

An overview has been prepared showing the relations between the IT Security Requirements and the Security Requirement Owner. The overview is attached as Appendix A in this document.

3 Terms and definitions

In the following section, there is a definition and description of selected terms used in JN Data's IT Security Requirements. Definitions are based on inspiration from the ISO/IEC 27002:2022 standard and input from the Security Requirement Owner. The list is not complete and will be continuous updated as deemed necessary. For further definitions of terms, see JN Data's Concept Dictionary available on JN Data Insite.

3.1 Definitions

Formalised documents

Formalised documents serve as an umbrella term and encompasses policies, procedures, processes, concept descriptions, work instructions and other documents designed to describe guidelines and requirements to ensure compliance with the IT Security Requirements, adherence to best practices, and consistency in task execution in JN Data.

Security Safeguards

Security Safeguard are initiatives aimed at reducing the risk of vulnerabilities. A Security Safeguard can be either preventive, detective, corrective, or a combination of all. Security Safeguards can be technical such as access control at the entrance to JN Data or be organisational such as a procedure for periodic review of access right. Technical and organisational security safeguards both aim to ensure a security level that protects JN Data's information and IT assets.

IT Security Event

An IT security event is a single or series of events that from a security perspective has the potential to negatively impact confidentiality, integrity and/or availability for JN Data or JN Data's customers, if relevant and timely measures are not taken to address the threat. An IT security event is defined as confidentiality, integrity and/or availability is at risk, but not yet compromised.

IT Security Incident

An IT security incident is an event that indicates that systems or data could be compromised, and the established safeguards failed to protect the systems. An IT security incident is defined as confidentiality, integrity and/or availability is compromised but has not yet been defined as a breach.

IT security breach

An IT security breach is a single or series of events that from a security perspective has/have had a negative impact on confidentiality, integrity and/or availability for JN Data or JN Data's customers. An IT security breach is defined by confidentiality, integrity and/or availability is compromised and has had a consequence.

Source Code

Source code is well-structured, human-readable text describing the behaviour of or desired state to a machine.



Artifact

Artifacts are self-developed software used for configuring purchased products. JN Data own the source code for the artifacts, but not the product itself.

Removable storage medias

Removable storage medias are devices that are not permanently connected to an IT asset and do not have any processing capacity such as a USB drive and external hard drives.

User endpoint devices

User endpoint devices are devices used by users to access information and data such as tablets, PCs and mobile phones issued by JN Data.

4 IT Risk Management

There must be a formalised document that describes requirements and guidelines for IT risk management, including identification, analysis, assessment, handling, monitoring and reporting. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

A policy for IT risk management must be in place, which must be approved by the Board of Directors at least annually.

There must be an inventory of the IT assets subject to the IT risk management guidelines.

There must be an annual cycle to ensure that risk assessments are carried out on the identified IT assets subject to IT risk management.

If the identified IT risk is outside of JN Data's risk appetite, the risk must be managed in accordance with the IT risk management policy.

Identified IT risks must be reported at least annually to the Board of Directors and the VP Group of JN Data.

5 Organisational controls

5.1 Policies for information security

There must be a formalised document that describes requirements and guidelines for the preparation and maintenance of the IT security policy and the underlying IT security requirements. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to ensure that relevant employees and consultants are familiar with the applicable IT security policy and IT security requirements.

The IT security policy and the IT security requirements take effect after an agreed period, which must be used to update documents in the affected areas. The length of the agreed period is determined by Security Governance based on the scope of the update.

There must be an annual cycle describing the activities relating to maintenance of and compliance with JN Data's IT security policy and IT security requirements.

There must be a formalised document that describes requirements and guidelines for registering, managing and maintaining deviations from applicable IT security requirements. Responsibilities must be defined and delegated for all identified activities.

Deviations from IT security requirements, the IT security policy or defined safeguards must be registered as an exemption and approved by Security Governance.

There must be a formalised document that describes requirements and guidelines for execution, documentation and follow-up of IT security test in JN Data for relevant IT assets.

IT security testing must be defined using a risk-based approach, on the basis of criticality, and be carried out in accordance with legal and regulatory requirements.

For PCI DSS, it is required that documentation is created that considers whether an it-asset processes confidential information.

For PCI DSS, there must be a formalised document for penetration test which considers the requirements for using recognised methods for the performance of penetration tests and an assessment of the test results.

Penetration tests must be carried out at least on internet-facing IT assets, multi-tenant solutions or where deemed necessary to maintain a high level of IT security.



For PCI DSS, it is required that penetration tests of Cardholder Data Environment (CDE) is performed at least every 6 month, to ensure that safeguards implemented to isolate the CDE are reassuring and effective.

For PCI DSS, it is required that a penetration tests is conducted to ensure a logical separation of the customers environments at least once every 6 month.

For PCI DSS, it is required that a penetration test of the entire CDE perimeter are conducted at least once a year.

For PCI DSS, it is required that a penetration test is conducted from both internal and external networks at least once a year.

For PCI DSS, it is required that network tests, which include all network components and operating systems are conducted at least once a year.

For PCI DSS, it is required that a penetration test for significant changes in the infrastructure or application updates are conducted.

For PCI DSS; it is required that penetration tests are conducted by an internal or external qualified party.

For PCI DSS, it is required that application tests which identify known vulnerabilities, are conducted at least once a year. Supporting systems are exempted from this requirement.

For PCI DSS, it is required that a comprehensive assessment of the threats and vulnerabilities relevant to JN Data are conducted at least once a year.

Threat-Led Penetration Testing (TLPT) must be carried out at least every three years.

5.2 Information security roles and responsibilities

There must be a formalised document that describes relevant IT security activities. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a formal description of key roles related to IT security in JN Data. Tasks and responsibilities must be clearly defined and described for each role.

There must be a formalised document that describes how IT security initiatives are coordinated and processed internally in JN Data.

There must be a formalised document that describes how IT security is communicated between JN Data and JN Data's customers.

5.3 Segregation of duties

There must be a formalised document that describes requirements and guidelines for the segregation of duties to ensure that conflicting tasks and responsibilities are segregated. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

An overview of conflicting roles in JN Data must be in place.

Safeguards must be implemented to ensure that conflicting functional areas, tasks and responsibilities cannot be assigned to the same employee. Deviations must be approved, documented and reassessed every six months in accordance with JN Data's exemption document, cf. 5.1.

Where conflicting roles are necessary, compensatory safeguards must be implemented to mitigate the risk of compromising JN Data's IT security.

5.4 Management responsibilities

There must be a formalised document that describes requirements and guidelines for the IT security responsibilities of the Executive Leadership Team (ELT). Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

The ELT must ensure that employees are informed about roles and responsibilities relating to IT security.

There must be a formalised document that ensures activities conducted by the board of directors, which are in the nature of IT and cyber risks education, are documented to the relevant extent in accordance with FIL 333b, section 7.

5.5 Contact with authorities

There must be a formalised document that describes requirements and guidelines for contact with identified authorities with relevance for JN Data. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

5.6 Contact with special interest groups

There must be a formalised document that describes requirements and guidelines for JN Data's involvement in relevant external professional and security organisations, specialist forums and interest groups. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

JN Data must be a member of IT security forums with relevance for the sector and the industry.

For all relevant external organisations, specialist forums and interest groups, the following must be documented:

- Contact details
- Purpose of cooperation
- What communication channels are used
- How data and information are exchanged.

A cooperation organisation must be established between JN Data and JN Data's customers, ensuring that IT security is coordinated and planned across the community. Each organisation in the community must be represented by an IT security responsible.

5.7 Threat intelligence

There must be a formalised document that describes requirements and guidelines for the collection, monitoring, analysis and reporting of IT threats. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Situational awareness must be maintained, including online underground environments. A threat profile must be in place, as well as a threat landscape that is monitored and maintained on an ongoing basis.

Safeguards must be implemented to ensure that threats are monitored and classified.

Risk scenarios that may affect business functions, processes and IT assets must be identified, documented, reported and maintained.

5.8 Information security in project management

There must be a formalised document that describes requirements and guidelines to integrate IT security into project management, ensuring that IT security requirements are built into all IT projects.

Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

For all IT projects, an impact assessment must be in place to identify risks during project development, as well as which risks are realised when the project is put into production.

The establishment and progress of IT projects that involve critical or important solutions must be documented. Reporting must be carried out either individually or in a consolidated form, depending on the importance and scope of the projects.

There must be a formalised document that ensures ongoing assessment and handling of IT security risks throughout the project life cycle.

IT solutions must be registered in the inventory of IT assets, cf. 5.9, and maintained throughout the project life cycle. The IT solutions must reflect the Business Impact analysis (BIA) for the business processes the solutions are designed to support.

Safeguards must be implemented to prevent unauthorised access to projects and information about them. Access must be managed in accordance with the relevant guidelines, cf. 5.15 and 8.3.

5.9 Inventory of information and other associated assets

There must be a formalised document that describes requirements and guidelines for managing and maintaining the IT asset during its life cycle. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be an inventory of all IT assets in JN Data, which must be updated and maintained on an ongoing basis. IT assets must be classified in accordance with the relevant guidelines, cf. 5.12.

Ownership must be defined for all IT assets. The owner of the IT asset is responsible for ensuring that there is appropriate protection for the IT asset throughout the life cycle.

There must be a documented decision as to whether an IT asset is used for processing personal data.

For PCI DSS, it is required that documentation is created which considers whether an IT asset is within the scope of PCI DSS. The continuously, and at least semi-annually, be reviewed and approved.

5.10 Acceptable use of information and other associated assets

There must be a formalised document that describes requirements and guidelines for acceptable use of IT assets. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.



There must be a formalised document to ensure that an assessment takes place as to whether safeguards can be implemented that prevent the unacceptable use and handling of IT assets.

5.11 Return of assets

There must be a formalised document that describes requirements and guidelines for returning IT assets upon termination or cancellation of the contract. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to ensure that all employees and consultants return JN Data's IT assets upon termination or cancellation of the contract.

The return of IT assets must comply with the classification guidelines for the particular IT asset, cf. 5.12, and the secure disposal requirements, cf. 7.14.

5.12 Classification of information

There must be a formalised document that describes requirements and guidelines for classifying all IT assets. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

A classification model must be in place which is applicable to all types of IT assets.

All IT assets must be classified in accordance with the guidelines and protected using a risk-based approach.

The classification of IT assets must be reviewed and updated periodically (at least annually).

IT assets must have at least the same or a higher level of classification than the classification of the data that can be processed in the IT asset. Deviations from this must be in accordance with the exemption document, cf. 5.1.

Safeguards must be implemented to ensure that all employees are familiar with the document for classifying IT assets and the classification model.

5.13 Labelling of information

There must be a formalised document that describes requirements and guidelines for labelling information and documents. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a description of how information and documents are labelled.

Safeguards must be implemented to prevent the existing labelling of information and documents from being changed without approval.

Safeguards must be implemented to ensure that all employees are familiar with the document for labelling.

5.14 Information transfer

There must be a formalised document that describes requirements and guidelines for internal and external transfer of information and documents, including electronic, physical and verbal transfer. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

The transfer of information and documents must only take place in accordance with the classification guidelines and labelling of information, cf. 5.12 and cf. 5.13.

5.15 Access control

There must be a formalised document that describes requirements and guidelines for managing physical and logical access to information and other associated IT assets. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

The control and management of access to information and IT assets in JN Data must be centralised in Identity and Access Management (IAM). Deviations from centralised access management must be approved, documented and reassessed in accordance with JN Data's exemption document, cf. 5.1.

Safeguards aimed at ensuring adequate access control, including alerting and logging, cf. 8.15, must be implemented.

Accesses must be granted in accordance with the guidelines for the segregation of duties in order to prevent conflicting roles, cf. 5.3.

Physical and logical accesses must be reassessed periodically (at least every six months) in accordance with applicable procedures, standards and executive orders.

5.16 Identity management

There must be a formalised document that describes requirements and guidelines for managing the entire life cycle of identities. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Identities must be personal and unique. If there are deviations, the use of generic identities must be approved, documented and made subject to adequate protection and monitoring in terms of criticality.

Technical identities, e.g. service accounts, must be subject to approval and the purpose of using the account must be documented and reassessed annually.

Safeguards must be implemented that prevent interactive login with technical identities.

Safeguards must be implemented to prevent previously used identities from being re-used to identify another user.

5.17 Authentication information

There must be a formalised document that describes requirements and guidelines for managing and assigning authentication information. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Authentication information must be assigned to users in a secure way and must not be stored in unprotected plain text.

Default passwords for IT assets must be changed during setup and before migration to operating environments.

Guidelines must be implemented to ensure that compromised authentication information is changed if there are any suspicions.

When passwords are used as authentication, they must comply with the applicable password policy. Deviations must be approved, documented and reassessed every six months in accordance with JN Data's exemption document, cf. 5.1.

Safeguards must be implemented to ensure that automatically generated passwords for personal accounts must be changed after the first login.

5.18 Access rights

There must be a formalised document that describes requirements and guidelines for managing access rights to information and other associated IT assets, including the granting and withdrawal of access rights. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Access rights to IT assets must be managed according to a role-based approach. Roles must be assigned on the basis of work-related needs, following the principles of managing privileged accesses, cf. 8.2 and according to the guidelines for the segregation of duties, cf. 5.3.

All roles and access packages must be risk-assessed.

Safeguards must be implemented to ensure that access rights are withdrawn and amended promptly according to the guidelines on responsibility after termination or change of employment, cf. 6.5.

All roles and access packages must be reassessed periodically (at least annually) in accordance with applicable procedures, standards and executive orders.

5.19 Information security in supplier relationships

There must be a formalised document that describes requirements and guidelines for managing and maintaining supplier relationships. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a list of all concluded supplier agreements which is maintained on an ongoing basis. The list must include information about which suppliers have access to IT assets that handle confidential information.

All solutions must be screened prior to entering into agreements to ensure that the solution meets JN Data's determined security level and risk appetite.

A comprehensive list of IT security requirements and safeguards, which can be included in the agreement with the individual supplier as part of the contractual obligations, must be in place. The scope of IT security requirements for each supplier must be defined taking proper account of risk.

5.20 Addressing information security within supplier agreements

There must be a formalised document that describes requirements and guidelines for managing and maintaining concluded supplier agreements. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

When new supplier agreements are concluded, there must be a document that ensures that the supplier is made aware of the IT security requirements and safeguards that the supplier must comply with. Relevant IT security requirements must be defined and documented taking proper account of risk, highlighting key factors that may have an impact on the IT security of JN Data.

When new supplier agreements are concluded, the parties must make it compulsory that relevant regulatory and sector-specific requirements are complied with.

When new supplier agreements are concluded, the parties must ensure that significant IT security events on the supplier's premises which may affect the operation or IT security of JN Data are reported to JN Data without undue delay.

When new supplier agreements are concluded, the parties must assess, according to a risk-based approach, whether the supplier must assist JN Data in emergency situations. If the supplier is deemed critical, this must be supported in the contractual agreement.

When new supplier agreements are concluded, the parties must agree how any exchange of information and software is to take place for the supplier agreements if this is considered relevant. This will be based on JN Data's classification model for IT assets, cf. 5.12.

When new supplier agreements are concluded in which the deliverable is software, the parties must ensure that the deliverable can be integrated into the central access management system.

When new supplier agreements are concluded in which all or part of the IT delivery is to be provided by an external supplier, the agreement must include requirements for auditing. The scope of the audit must be assessed taking proper account of risk, highlighting key factors that may have an impact on the IT security of JN Data.

When agreements are concluded with consultants, the parties must ensure that JN Data has the opportunity to carry out sufficient background verification and screening of the individual consultants, cf. 6.1.

When supplier agreements are concluded, the parties must ensure that the supplier undertakes that its employees and any consultants comply with agreed IT security requirements at JN Data. The supplier must also sign a non-disclosure agreement on behalf of its consultants.



When supplier agreements are concluded that deal with outsourced development, there must be a document that ensures that the supplier contractually commits to comply with JN Data's requirements and guidance concerning secure development, cf. 8.25 to 8.29.

When agreements are concluded in which suppliers gain access to or otherwise process personal data, the parties must consider whether to enter into a data processor agreement.

5.21 Managing information security in the ICT supply chain

There must be a formalised document that describes requirements and guidelines for managing and maintaining IT security in the supply chain. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

A definition must be in place that clarifies which suppliers are key suppliers for JN Data's operations and IT security.

There must be a list of key suppliers in the supply chain.

Agreements between JN Data and suppliers must also apply to the supplier's partners and subcontractors that are deemed relevant to the delivery, and the supplier must ensure that they are monitored and documented.

Follow-up of key suppliers in the supply chain must take place in accordance with the established procedures, cf. 5.22.

5.22 Monitoring, review and change management of supplier services

There must be a formalised document that describes requirements and guidelines for managing, monitoring and changing supplier agreements. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to ensure that supplier agreements are formally monitored and reviewed in accordance with the established IT security requirements.

There must be an annual cycle that ensures that relevant IT security requirements for the individual supplier contract are checked annually in order to ensure compliance with the contractual requirements. Any deviations must be documented, and mitigating actions must be initiated.



If it is considered to be relevant, a cooperation organisation must be established between JN Data and the supplier/consultant, with an agreed frequency of meetings, to ensure ongoing follow-up of delivery and IT security requirements.

Security events identified on the supplier's premises must be reviewed and binding safeguards must be assessed to determine whether they can continue to counter relevant threats.

There must be a formalised document that describes how changes can be made to supplier agreements and services that affect IT security, and how any changes are communicated to the business.

If supplier agreements or services are changed, steps must be taken to ensure that agreed IT security requirements remain sufficient. The assessment of IT security requirements must be defined and documented taking proper account of risk.

Audits must be carried out and any comments made must be followed up to the extent described in the supplier agreement. Any comments must be documented and mitigating safeguards must be implemented where deemed necessary.

Upon termination of contractual obligations between the supplier/consultant and JN Data, documents must be established to ensure that all accesses are withdrawn.

5.23 Information security for use of cloud services

There must be a formalised document that describes requirements and guidelines for the procurement, use, management and termination of cloud services, including cloud service and delivery models. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a formalised document that ensures that cloud services are assessed before they are deployed with a view to implementing necessary safeguards.

Cloud security principles must be established and documented for managing, configuring and setting up cloud services. The principles must apply to all architecture layers.

There must be an annual cycle that ensures that relevant document in JN Data are assessed and updated in accordance with defined cloud security principles.

Procurement

New cloud services must be procured in accordance with the security requirements for entering into new supplier agreements, cf. 5.20, as well as for monitoring and reviewing supplier agreements, cf. 5.22.

Access management

Access to cloud services must comply with the security requirements for access control, cf. 5.15, and identity management, cf. 5.16. An assessment must take place as to whether the same identity can be used in the cloud as in the remaining infrastructure.

Authentication for cloud services must comply with the security requirements for authentication information, cf. 5.17. Safeguards must be implemented to prevent unauthorised access to cloud services.

Privileged access to cloud services must comply with the security requirements for privileged access rights, cf. 8.2, and the principles in Access Rights cf. 5.18.

Change management

Changes to cloud services must take place in accordance with the security requirements for change management, cf. 8.32.

Significant changes to cloud services that may affect IT security must be communicated to relevant customers.

Monitoring and logging

Logging in cloud services must take place in accordance with the security requirements for logging, cf. 8.15.

Abnormal behaviour in cloud services must be monitored and handled in accordance with the security requirements for security monitoring, cf. 8.16.

An assessment must take place as to whether to implement safeguards that monitor relevant bandwidth with the aim of detecting misuse of resources (such as DDoS).

An assessment must take place as to whether to implement safeguards that ensure ongoing monitoring and alerting of agreed factors.

An assessment must take place as to whether to implement safeguards that monitor and report on changes to agreed baselines for cloud services.

There must be formalised documents that describe the communication plan and escalation ladder in the event of an IT security incident in cloud services.

IT assets

JN Data must have a list of cloud services which is maintained on an ongoing basis with the level of detail agreed for the type of cloud service in question. The list must contain information, in accordance with the guidelines for the inventory of information and other associated IT assets, cf. 5.9.



Protection of data

Data in cloud services must be encrypted in accordance with the security requirements for cryptography, cf. 8.24.

The labelling of data in cloud services must be in accordance with the security requirements for the labelling of information, cf. 5.13.

The classification of cloud services must be in accordance with the security requirements for the classification of IT assets, cf. 5.12.

Data in cloud services must be processed in accordance with the guidelines for the acceptable use of information and other associated IT assets, cf. 5.10.

Data in cloud services must be deleted in accordance with contractual requirements, cf. 5.31.2.

Storage

Cloud services and surrounding infrastructure must be backed up in accordance with the security requirements for information backup, cf. 8.13.

Patch Management

Cloud services and cloud components must be patched in accordance with the security requirements for the management of technical vulnerabilities, cf. 8.8. If patch management activities take place on the supplier's premises, they must be in accordance with agreed security requirements in supplier agreements, cf. 5.20.

Exit strategy

There must be a formalised document that ensures that an exit strategy has been agreed for all cloud services.

Storage and redundancy

In geographical terms, data must be stored in accordance with applicable statutory, regulatory and contractual requirements, cf. 5.31.

An assessment must take place as to whether to implement safeguards ensuring redundancy of information and IT assets, cf. 8.14.

5.24 Information security incident management planning and preparation

5.24.1 Planning and preparation of security incidents

There must be a formalised document that describes requirements and guidelines for managing and handling IT security events and IT security incidents. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

All IT security events must be monitored so that potential IT security incidents can be identified. All identified IT security incidents must be detected, classified, analysed and reported. They must be prioritised according to the established criticality.

Safeguards must be implemented to ensure continuous monitoring and alerting.

Escalation of IT security events must be considered according to the type and criticality of the event.

Safeguards must be implemented to ensure logging of activities in the context of IT security event management.

For the assessment of, response to and learning from IT security incidents, see the following guidelines, cf. 5.25, 5.26 and 5.27.

5.24.2 Planning and preparation of incidents and major incidents

There must be a formalised document that describes requirements and guidelines for governing and managing incidents and major incidents. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Appropriate technical and organisational measures must be implemented to enable monitoring and timely identification of potential incidents. All incidents must be recorded in a register.

It must be clearly defined what constitutes an incident and when it qualifies as an IT-security incident, in order to ensure proper handling and escalation.

A responsibility and escalation matrix must be developed and maintained, indicating who is involved, when and at what level, in the event of an incident.

All activities and decisions related to incident management must be documented and continuously evaluated. Special attention must be given to ensuring full traceability of incidents.

Where deemed relevant, a root cause analysis must be conducted to identify causes and prevent recurrence. Lessons learned from incidents must be systematically recorded and used to improve processes and security measures.

In cases of breaches of the confidentiality, integrity, or availability of personal data, a specific assessment must be made to determine whether the incident must be reported to the Danish Data Protection Agency (Datatilsynet) in accordance with the GDPR – and whether affected individuals must be informed.

Procedures must also be in place to ensure that relevant incidents are reported to the Danish Financial Supervisory Authority (Finanstilsynet) in accordance with applicable regulatory requirements.

5.25 Assessment and decision on information security events

There must be a formalised document that describes requirements and guidelines for assessing and deciding on IT security events. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a clear description of how IT security events are categorised and prioritised.

All IT security events must be analysed and assessed in order to determine whether the IT security event can be categorised as an IT security incident or an IT security breach. If the security event is categorised as a security incident, the guidelines and requirements governing the response must be followed, cf. 5.26, and if not, the incident process must be followed.

5.26 Response to information security incidents

There must be a formalised document that describes requirements and guidelines governing the response to IT security incidents. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

An Incident Response Plan must be in place that describes how JN Data responds to IT security incidents.

Safeguards must be implemented to ensure that IT security incidents are only accessible by employees with a work-related need.

Safeguards must be implemented to ensure that involved activities are logged correctly and in accordance with the logging guidelines, cf. 8.15.

A communication plan must be in place to ensure that relevant information about the IT security incident is communicated to relevant internal and external stakeholders.

The reporting and coordination of IT security events must comply with external reporting requirements to relevant authorities, cf. 5.5.

Escalation of IT security incidents and breaches must be considered according to the type and criticality of the event. When a crisis response is activated and business continuity plans are applied, the relevant guidelines must be followed, cf. 5.29 and 5.30.

If IT security incidents occur, the guidelines for collection, storage and handling of evidence, cf. 5.28, and for learning from the incident, cf. 5.27, must be complied with.

5.27 Learning from information security incidents

There must be a formalised document that describes requirements and guidelines for lessons learned from IT security incidents. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Lessons learned from IT security incidents must be collected and evaluated, and used in event and incident management preparation, cf. 5.24.

Based on the IT security incident and breach, an assessment must take place as to whether to implement additional safeguards in JN Data to potentially avoid or limit future IT security incidents and breaches.

Based on analysis and evaluation, an assessment must take place as to whether to include lessons learned and trends in cross-departmental improvements and/or activities.

5.28 Collection of evidence

There must be a formalised document that describes requirements and guidelines for collecting, storing and processing evidence in relation to IT security incidents. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to protect the evidence from alteration, tampering and unauthorised access.

The collection, storage and processing of evidence must comply with all applicable statutory requirements and regulations, including the General Data Protection Regulation.

Adequate logging and registration must be implemented in connection with the collection and processing of evidence to ensure integrity and the chain of custody.

Safeguards must be implemented to ensure that the processing of confidential data and information is only available to employees with a special work-related need.

5.29 Information security during disruption

There must be a formalised document that describes requirements and guidelines for IT security during outages and disruptions. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

An emergency response plan must be in place that includes a defined emergency response organisation to take responsibility during outages and disruptions. Periodically (at least annually), the emergency response plan must be updated, approved by the VP Group and tested.

A crisis management plan must be developed, documented, and implemented, including both a master contingency plan and an emergency response plan. These plans must be based on the results of Business Impact Analyses (BIA).

The crisis communication plans must be tested at least once a year, as well as when significant changes are made to IT systems that support critical or important functions.

There must be an annual cycle for emergency response drills performed by JN Data. The annual cycle must be updated periodically (at least annually).

Recovery plans for critical IT assets in JN Data must be in place, based on the classification of the IT asset, cf. 5.12. The recovery plans must be updated and tested periodically (at least annually) according to the criticality and classification of the IT asset.

For critical suppliers and services, business contingency plans must be in place in case disruptions occur.

5.30 ICT readiness for business continuity

There must be a formalised document describing requirements and guidelines for information and communication technology (ICT) intended to support business continuity. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Business impact analyses (BIAs) must be performed to identify critical business processes and related resources that are necessary to maintain JN Data's operational continuity.

Business impact analyses (BIAs) must be carried out at least annually or when significant changes are made to JN Data's structure, activities and technologies.



An overview of ICT activities supporting critical business processes must be in place. The overview must be reviewed and updated periodically (at least annually).

A continuity plan (BCP) must be in place describing how JN Data ensures that critical ICT activities are maintained during and after unforeseen events.

All ICT continuity plans, including communication plans and recovery plans, must be periodically updated and tested at least once a year.

An ICT continuity plan which supports continuity and recovery plans must be in place, describing how JN Data handles an ICT disruption. Continuity and recovery plans must be reviewed, updated and tested periodically (at least annually).

5.31 Legal, statutory, regulatory and contractual requirements

5.31.1 Legal, statutory and regulatory requirements

There must be a formalised document that describes requirements and guidelines for managing and monitoring relevant and applicable legal and regulatory requirements and their prompt implementation. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

An overview of all relevant and applicable legal and regulatory requirements must be identified and prepared. The overview must document the responsibility for complying with the relevant and applicable legal and regulatory requirements.

There must be a formalised document that ensures that changes to the identified relevant and applicable legal and regulatory requirements are monitored, documented and communicated to the person responsible.

The person responsible must ensure that implementation takes place in accordance with legal and regulatory requirements.

5.31.2 Contractual requirements

There must be a formalised document that describes requirements and guidelines for managing and monitoring customer-facing contractual requirements. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to monitor and follow up compliance with contractual requirements.

There must be a formalised document to ensure that changes to applicable contractual requirements are communicated and implemented.

There must be a formalised document that ensures that customer-related enquiries are centralised. Sharing of information and documentation must follow the guidelines for classification, cf. 5.12, and labelling of documentation, cf. 5.13.

5.32 Intellectual property rights

There must be a formalised document that describes requirements and guidelines for the protection, maintenance and use of intellectual property rights, including software licences and open-source licences. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a list of approved and purchased software- and open-source licences containing relevant information allowing the monitoring of software- and open-source licences. The list must be updated and maintained on an ongoing basis.

Only purchased and approved software and open-source licences may be installed. For JN Data, safeguards must be implemented that prevent the use of unauthorised software and licensed products.

Safeguards must be implemented to prevent the maximum number of users or resources allowed in the licence from being exceeded.

The expiration of software and licensed products must be documented in accordance with the guidelines for the life cycle of IT assets, cf. 5.9, and for the decommissioning of software.

5.33 Protection of records

There must be a formalised document that describes requirements and guidelines for the protection of documentation. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Appropriate safeguards must be implemented to protect documentation and prevent it from being compromised. Safeguards must be designed to protect against loss, destruction, falsification, unauthorised access and unauthorised disclosure.

Documentation must be handled and protected in accordance with the applicable classification and the relevant guidelines, cf. 5.12.

5.34 Privacy and protection of PII

There must be a formalised document that describes requirements and guidelines for privacy and personal data protection. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Organisational and technical safeguards to protect personal data must be implemented based on a risk assessment that takes into account the consequences of processing for the data subjects.

5.35 Independent review of information security

There must be a formalised document that describes requirements and guidelines for analysing, assessing, and reporting on IT security. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a formalised document that describes activities for collecting, analysing, effectiveness, assessing and reporting JN Data's IT security compliance.

5.36 Compliance with policies, rules and standards for information security

There must be a formalised document that describes requirements and guidelines for monitoring IT security compliance. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be an annual cycle that ensures that activities aimed at monitoring and assessing IT security compliance in JN Data are analysed and reviewed at least once a year.

Aspects that do not meet the IT security requirements must be planned and corrected within a defined timeframe.

There must be a formalised document that ensures adequate reporting of the measured IT security level.

5.37 Documented operation procedures

There must be a formalised document that describes requirements and guidelines for managing and archiving activities and key documents. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a description of the documentation structure for all key areas. The documentation structure must illustrate the relationship between policies, subject-specific policies, processes, procedures and other key documents.

Policies, subject-specific policies, processes, procedures and other key documents must be documented in the relevant business-approved templates, and must follow the specified rules and guidelines relating to governance and structuring.

There must be a formalised document that describes how policies, subject-specific policies, processes, procedures and other key documents are to be archived to ensure control, monitoring and protection of the documentation.

There must be a formalised document that ensures that policies, subject-specific policies, processes, procedures and other key documents are reviewed and maintained periodically (at least annually).

When documents are shared and transferred, the relevant guidelines must be followed, cf. 5.14.

6 People controls

6.1 Screening

There must be a formalised document that describes requirements and guidelines for screening and background verification of all employees and consultants. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Screening and background verification of all employees and consultants in JN Data must be carried out in accordance with the relevant guidelines.

Periodic (at least annual) background verification reviews must be implemented for employees and consultants with access to Swift environments.

The screening and verification of employees and consultants must be in accordance with relevant legislation.

6.2 Terms and conditions of employment

There must be a formalised document that describes requirements and guidelines for terms and conditions of employment, including a description of possible disciplinary processes if the obligations



regarding IT security are not complied with. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

At the time of their appointment, all employees and consultants must be made aware of their responsibilities and obligations regarding IT security, including in particular the preservation of confidentiality. This responsibility must apply during employment and also after termination, cf. 6.5.

All employees and consultants must sign a non-disclosure agreement in accordance with the relevant guidelines, cf. 6.6.

6.3 Information security awareness, education and training

There must be a formalised document that describes requirements and guidelines for awareness and training of employees and consultants. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be an annual cycle for awareness campaigns and training in IT security and data protection.

Safeguards must be implemented to ensure that all employees and consultants complete the planned awareness programme.

The IT security policy and the IT security requirements must be available to all employees and consultants on JN Data's intranet. The IT security and data protection policy must be presented to new employees and consultants at the time of onboarding.

Safeguards must be implemented to assess the security level in JN Data based on selected results from awareness activities. If considered necessary, the results of awareness activities must be followed up.

Every year, all employees and relevant consultants with access to JN Data's IT assets must sign a declaration that they have read and understood the IT security policy and IT security requirements.

For employees and consultants with access to PCI environments, awareness campaigns must contain information about data classification and the protection of data and the vulnerabilities that may affect IT security.

6.4 Disciplinary process

There must be a formalised document that describes requirements and guidelines for possible disciplinary processes in the event of a breach of IT security. Responsibilities must be defined and tasks delegated for all identified activities.



All relevant safeguards must be described in the formalised document.

Conduct that results in misuse or a breach of IT security must be investigated, and possible disciplinary processes must be considered.

Safeguards must be implemented to protect the identity of employees and consultants with ongoing disciplinary cases.

Cases must be handled in accordance with relevant legal, statutory, regulatory, contractual and business requirements.

6.5 Responsibilities after termination or change of employment

There must be a formalised document that describes requirements and guidelines concerning responsibilities and obligations after termination or change of employment or contracts. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised routine.

Responsibilities and obligations must apply after the employment or contract is terminated and must follow the guidelines for terms and conditions of employment, cf. 6.2, and non-disclosure agreements, cf. 6.6.

There must be a formalised document for communicating changes to the employment relationship in order to ensure, for example, that access to and permissions for systems and data are withdrawn promptly in the event of termination or changes to the employment relationship.

6.6 Confidentiality or non-disclosure agreements

There must be a formalised document that describes requirements and guidelines for confidentiality declarations and non-disclosure agreements, obliging JN Data's employees, suppliers, customers and other business partners to keep confidential and otherwise prevent unauthorised use and disclosure of JN Data's confidential information. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised routine.

6.7 Remote working

There must be a formalised routine that describes IT security requirements and guidelines applicable to remote working. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.



Technical and organisational IT security safeguards must be implemented if remote access is provided to information and IT assets.

6.8 Information security event reporting

There must be a formalised document that describes requirements and guidelines for reporting security events. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to enable reporting of security events for all employees and relevant consultants.

7 Physical controls

7.1 Physical security perimeters

There must be a formalised document that describes requirements and guidelines for managing and using physical perimeter security for areas containing IT assets. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Perimeter security must be defined on the basis of the requirements for the applicable IT assets located in the area and must comply with the classification guidelines, cf. 5.12.

Safeguards must be implemented to prevent unauthorised access to JN Data's locations and buildings.

Alerting, monitoring and testing of burglary and fire systems must be implemented at JN Data's premises.

7.2 Physical entry

There must be a formalised document that describes requirements and guidelines for managing and monitoring physical access controls to secure areas containing IT assets. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Only authorised employees and consultants must have access to JN Data's locations and buildings. Access is granted on the basis of a work-related need and in accordance with the access management guidelines, cf. 5.15 and 5.18.



There must be a staffed reception area during daylight hours. The reception area must be monitored in order to control physical access.

Safeguards must be implemented to control access to areas containing data and where other associated IT assets are kept. Authentication information and access logs must be stored in accordance with the logging guidelines, cf. 8.15, and relevant legislation.

7.3 Securing offices, rooms and facilities

There must be a formalised document that describes requirements and guidelines for managing and maintaining the physical security of offices, rooms and facilities. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Physical safeguards must be implemented to prevent confidential information and activities from being visible and readable by unauthorised persons.

Details of premises in secure areas and related documentation must be kept confidential and inaccessible by unauthorised persons.

7.4 Physical security monitoring

There must be a formalised document that describes requirements and guidelines for managing, protecting and maintaining physical security monitoring of premises. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to ensure that critical areas inside and outside the JN Data's locations are monitored. Safeguards must be in accordance with the classification of the IT asset concerned, cf. 5.12.

There must be a periodic review of the implemented security monitoring to check for and detect unauthorised access and suspicious behaviour.

Monitoring systems must be tested periodically (at least annually) for functionality.

Every monitoring system must be used in accordance with data protection and personal data protection legislation.

Descriptions of the installation and details of physical security monitoring must be kept confidential and accessible only to authorised personnel.

7.5 Protection against physical and environmental threats

There must be a formalised document that describes requirements and guidelines for managing and protecting against physical and environmental threats. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented according to a risk-based approach, identifying and assessing potential consequences of physical and environmental threats and limitations.

All buildings and IT assets must be equipped with adequate protection against environmental threats based on a risk assessment.

For JN Data, when new IT assets are commissioned, an assessment must take place as to whether the IT asset is to be duplicated at separate locations. The assessment must be made on the basis of the environmental threat and according to a risk-based approach.

7.6 Working in secure areas

There must be a formalised document that describes requirements and guidelines for working in secure areas. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Only authorised employees and consultants may have access to JN Data's secure areas. Access is granted on the basis of a work-related need and in accordance with the access rights guidelines, cf. 5.18.

Safeguards must be implemented to ensure that access to specially secured areas is approved by the CISO.

Work in secure areas must be done by employees and consultants with security clearance. If there are deviations from the above, the work must be supervised by an authorised employee with security clearance.

7.7 Clear desk and clear screen

There must be a formalised document that describes requirements and guidelines for storing physical paper, tidy desks, clear screens, portable storage media and screen locks. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

PCs and other user endpoint devices (personal IT equipment) must be secured with a screen lock and password when they are not supervised by the user.

Documents containing confidential information or which are highly classified must be supervised or kept securely under lock and key.

7.8 Equipment siting and protection

There must be a formalised document that describes requirements and guidelines for the management, maintenance and protection of IT equipment. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Equipment and IT assets must be sited in areas according to a risk-based approach and must comply with the classification of the IT asset concerned, cf. 5.12, and the guidelines on protection against physical and environmental threats, cf. 7.5.

7.9 Security of assets off-premises

There must be a formalised document that describes requirements and guidelines for the siting and protection of IT assets that store and process information outside JN Data's locations. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Equipment and IT assets used outside JN Data's locations must be protected according to the same guidelines and principles as internal IT assets, taking into account special risks associated with external use.

Safeguards must be implemented to ensure adequate protection of IT assets outside JN Data's locations, including encryption, location tracking and remote deletion of content on devices.

When IT assets are transported outside JN Data's area, this must be in accordance with the transfer guidelines for IT assets, cf. 5.14.

7.10 Storage media

There must be a formalised document that describes requirements and guidelines for managing and registering removable storage media throughout the life cycle. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to ensure adequate protection and safekeeping of removable storage media. Safeguards must be in accordance with the classification of the storage media concerned, cf. 5.12.



If there are removable storage media containing confidential information or personal information, data must be encrypted and the transfer guidelines for IT assets, cf. 5.14, must be complied with.

Storage media must be disposed of and recycled in accordance with the secure disposal guidelines, cf. 7.14.

7.11 Supporting utilities

There must be a formalised document that describes requirements and guidelines for managing and monitoring IT assets in the event of power failures and other disruptions. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Adequate supporting utilities must be provided at JN Data's location. The assessment must use a risk-based approach and must apply the principle of avoiding a single point of failure.

Safeguards must be implemented to ensure monitoring and alerting of infrastructure.

Periodic reviews of the provided utilities must be implemented to verify capacity, maintenance and interaction with other supporting utilities.

The infrastructure must be tested for functionality periodically (at least annually).

7.12 Cabling security

There must be a formalised document that describes requirements and guidelines for managing and securing power and data communication cables. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Cable security safeguards must be implemented. This security must use a risk-based approach relating to the location and operational impact of the connection.

Safeguards must be implemented to prevent unauthorised access to the cables. Access is granted on the basis of a work-related need and in accordance with the access rights guidelines, cf. 5.18.

Cables must be labelled, registered and documented in accordance with the classification of IT assets, cf. 5.12.

Safeguards must be implemented to ensure the protection of distribution frames against unauthorised access.



The primary electricity supply must undergo a thermographic survey periodically (at least annually) to identify potential risks.

7.13 Equipment maintenance

There must be a formalised document that describes requirements and guidelines for equipment testing and maintenance. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Periodic review and maintenance of equipment must be implemented. Equipment maintenance must be in accordance with the supplier's recommended inspection frequency (at least annually).

Equipment maintenance at JN Data's location must take place in accordance with the guidelines for working in secure areas, cf. 7.6.

Repairs and preventive maintenance must be registered and documented.

7.14 Secure disposal or re-use of equipment

There must be a formalised document that describes requirements and guidelines for managing the secure disposal and re-use of equipment used as storage media. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to ensure that equipment does not contain storage media prior to disposal or recycling. Disposal and deletion of storage media must comply with the guidelines, cf. 7.10 and 8.10.

Safeguards must be implemented to ensure that signs and labels that can identify JN Data or IT assets are removed before disposal.

The disposal and destruction of equipment must be documented and logged in accordance with IT asset life cycle guidelines, cf. 5.9.

8 Technical controls

8.1 User endpoint devices

There must be a formalised document that describes requirements and guidelines for the protection of user endpoint devices (personal IT equipment) in which information is stored and processed.

Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

All PCs and user endpoint devices must be configured and used in accordance with the relevant guidelines.

Safeguards must be implemented to prevent unauthorised software being installed and changes being made to the configuration of PCs and user endpoint devices.

There must be a list showing the registration of user endpoint devices that have been issued.

Data-carrying user endpoint devices must be disposed of in accordance with the relevant guidelines, cf. 7.14.

8.2 Privileged access rights

There must be a formalised document that describes requirements and guidelines for managing privileged access rights. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

The granting of privileged access rights must be restricted and must be managed in accordance with the guidelines for access control and access rights, cf. 5.15 and 5.18.

All privileged access rights must be managed centrally. If there are deviations from centralised management, all local administrator and privileged access rights must be approved, documented and reassessed every six months in accordance with JN Data's exemption document, cf. 5.1.

Privileged access rights must be subject to an approval process. Safeguards must be implemented to ensure that privileged access is periodically (at least every three months) reassessed and approved.

Safeguards must be implemented to ensure monitoring and logging of activities for privileged users in accordance with the logging guidelines, cf. 8.15.

8.3 Information access restriction

There must be a formalised document that describes requirements and guidelines for access management, including restricting access to information and other associated IT assets. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to prevent unauthorised access to information and other associated IT assets.

Access to information and other associated IT assets must be restricted and removed when there is no longer a work-related need. Accesses must be closed down in accordance with the relevant guidelines, cf. 5.18 and 6.5.

8.4 Access to source code

There must be a formalised document that describes requirements and guidelines for managing access to source code. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Source code must be stored in source code management systems.

Access for reviewing and approving changes to source code, and the granting of accesses, must follow the guidelines for access management, cf. 5.15, and the segregation of duties, cf. 5.3.

Access to source code must be reassessed periodically (at least every six months) in accordance with the relevant guidelines, cf. 5.15.

Safeguards must be implemented to ensure an audit log of all accesses and changes to source code in accordance with the logging guidelines, cf. 8.15.

8.5 Secure authentication

There must be a formalised document that describes requirements and guidelines for managing and protecting authentication when systems and applications are accessed. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Appropriate authentication methods must be implemented which verify user identity based on the classification of the information being accessed and in accordance with the relevant guidelines, cf. 5.12.

Where technically feasible, passwordless authentication, such as Single sign-on (SSO), FIDO key, or biometrics, must be used as the preferred authentication method for user identification when systems and applications are accessed.

When critical IT assets are accessed, multi-factor authentication (MFA) must be implemented in addition to the authentication method used.

When systems, applications and data are accessed from mobile devices, multi-factor authentication must be used.

Adequate logging of failed and completed unauthorised authentication attempts must be implemented in accordance with the logging guidelines, cf. 8.15.

8.6 Capacity management

There must be a formalised document that describes requirements and guidelines for managing, monitoring and planning capacity. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a formalised document ensuring that capacity requirements are defined in accordance with the specified requirements and guidelines.

Capacity monitoring must be implemented for all IT infrastructure platforms.

Capacity measurements must be carried out periodically to ensure that IT capacity shortages are prevented.

Safeguards must be implemented to ensure that capacity is upgraded and adjusted according to the load.

Continuous follow-up and coordination of capacity management must be implemented across JN Data and JN Data's customers.

8.7 Protection against malware

There must be a formalised document that describes requirements and guidelines for malware protection in these areas: detection, protection and response. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to monitor and detect suspicious behaviour and activity at an early stage.



Endpoint detection and response (EDR) and antivirus software must be installed in all endpoints for which JN Data is responsible.

Safeguards must be implemented to ensure that EDR and antivirus software is checked for updates daily.

Safeguards must be implemented to ensure that all endpoints are periodically scanned for malware.

Safeguards must be implemented to ensure that all incoming and outgoing communication is scanned for malware in accordance with the network security guidelines, cf. 8.20.

Malware events must be registered, investigated and reported, following the relevant guidelines, cf. 5.26.

8.8 Management of technical vulnerabilities

There must be a formalised document that describes requirements and guidelines for managing and handling technical vulnerabilities and installing security patches. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to ensure that threats, known vulnerabilities, and security updates are detected.

Technical vulnerabilities must be assessed according to a risk-based approach relating to criticality, and handled accordingly. If there are exceptions, safeguards must be implemented to reduce the identified risk.

IT assets must be monitored for relevant security patches on an ongoing basis and in accordance with contractual requirements.

For IT assets in scope of SWIFT and PCI DSS, 'critical' security patches must be installed within 30 days from the release date.

Vulnerability scans must be performed periodically (at least monthly) on all JN Data's and JN Data's customer's systems. On platforms where automated vulnerability scans cannot be performed, a process-initiated vulnerability review must be conducted every three months.

Exceptions to the vulnerability scans must be documented, reported and approved.

External approved scanning vendor (ASV) vulnerability scans must be performed periodically (at least every three months) in PCI environments. On platforms where ASV scans cannot be performed, a process-initiated review must take place every three months with reporting of which systems cannot perform ASV scans.



Security patches must be tested before being installed in production environments in accordance with the change management guidelines, cf. 8.32.

Monthly reporting must be implemented between JN Data and JN Data's customers to ensure ongoing follow-up of security updates.

8.9 Configuration management

There must be a formalised document that describes requirements and guidelines for managing, documenting, implementing and monitoring security configurations for relevant IT assets in JN Data. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Configurations that may affect the security level of JN Data must be identified and handled in accordance with the security configuration documents.

Changes to security configurations must be in accordance with the change management guidelines, cf. 8.32.

Security baselines for operating systems, database management systems and web servers in JN Data must be implemented based on recognised standards: CIS Benchmark or STIG. Exceptions to defined baselines must be centrally documented and approved.

Baseline scans of operating systems, database management systems and web servers must be performed periodically (at least every six months).

For PCI DSS areas, baseline scans of operating systems, database management systems and web servers must be performed every three months.

For the PCI DSS area, all components are subject to requirements for managing, documenting, and monitoring security configurations.

Security baselines and configurations must be evaluated periodically (at least every six months) in order to assess whether it is still possible to mitigate newly identified threats.

There must be a formalised document that ensures reporting and follow-up of completed baseline scans.

For relevant IT Assets, which are not defined as an operating system, database management system or a web server, security configurations must be based on best practice, vendor recommendations and guidelines from the IT Security Requirements.

Security configurations must be evaluated periodically (at least every six months) in order to ensure, that they remain in compliance with best practices, vendor recommendations and guidelines from the IT Security Requirements.

Security configurations must be evaluated periodically (at least every six months) in order to ensure that the IT Assets is configured in accordance with the documented security configurations.

8.10 Information deletion

There must be a formalised document that describes requirements and guidelines for deleting information. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Personal data must be deleted when it is no longer needed for the purpose for which it was originally collected. Personal data can be deleted by ordinary deletion or anonymisation.

Data must also be deleted in accordance with the guidelines for classification of IT assets, cf. 5.12, and contractual requirements, cf. 5.31.2.

When JN Data acts as data controller, technical and organisational safeguards must be implemented so that the deletion of personal data takes place in accordance with the established deletion deadlines.

When JN Data acts as data processor on behalf of the customer, technical and organisational safeguards must be implemented so that deletion of personal data takes place in accordance with the customer's instructions.

Periodic checks of compliance with the deletion deadlines must be implemented.

8.11 Data masking

There must be a formalised document that describes requirements and guidelines for masking data. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a formalised document that ensures that an assessment takes place as to whether data and information should be masked, pseudonymised or anonymised when used.

Safeguards must be implemented to ensure that data and information are masked in accordance with the relevant guidelines.

8.12 Data leakage prevention

There must be a formalised document that describes requirements and guidelines for preventing leakage of critical data and information. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to prevent and detect leakage of critical data and information from IT assets that process, store or disclose critical information.

8.13 Information backup

There must be a formalised document that describes requirements and guidelines for managing and maintaining backups. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a formalised document that describes requirements and guidelines for agreed baselines, including frequency, retention period, RTO, RPO and the method for handling backups. The retention period of backup data must be based on data criticality and classification, cf. 5.12.

Backups must be configured in accordance with agreed backup baselines and contractual requirements. Deviations from baselines must be documented, approved and retained.

Safeguards must be implemented to ensure monitoring and adequate handling of failed backup jobs.

Safeguards must be implemented to ensure the logical and physical segregation of backup data in accordance with the guidelines for the segregation of duties, cf. 5.3.

Safeguards must be implemented to ensure that backups are taken into account when new IT assets are implemented or existing ones changed.

Safeguards must be implemented to ensure that there are at least two copies of backup data and that these are sited at different physical locations.

Periodic testing of backup data recovery must be carried out. All critical IT assets must be tested at least once every three years.

Backup data must be adequately protected and stored in accordance with the physical security guidelines, cf. 7.1, and deleted when the retention period of the information expires in accordance with the relevant guidelines, cf. 8.10.

8.14 Redundancy of information processing facilities

There must be a formalised document that describes requirements and guidelines for redundancy of information processing and IT assets. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Redundancy must be implemented for business-critical IT assets, in accordance with the business impact analysis (BIA), cf. 5.30, and the classification of the IT asset in question, cf. 5.12.

Safeguards must be implemented to ensure that business-critical IT assets can be decommissioned separately from one of the locations in the event of an emergency response situation.

Safeguards must be implemented to ensure failover of business-critical IT assets in the event of outages and disruptions. Failover must be tested periodically (at least annually).

The physical and technical infrastructure must be designed in such a way as to ensure that no single failure can affect the overall infrastructure.

8.15 Logging

There must be a formalised document that describes requirements and guidelines for logging, including management, collection, storage and integrity protection. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a formalised document that describes log retention requirements and guidelines.

Safeguards must be implemented to prevent unauthorised access to modify log data, to ensure that it is not possible to modify or delete log data related to one's own actions.

All system errors and warnings must be logged to ensure that the necessary documentation is available for troubleshooting.

Log data collected in decentralised IT assets must be sent in real time to central logging facilities to protect data integrity.

All log data must be stored and deleted in accordance with the contractual requirements, cf. 5.31.2, and the relevant guidelines, cf. 8.10 and 8.13.

Access to log data must be limited and in accordance with the guidelines for the segregation of duties, cf. 5.3, and access management, cf. 5.15.

Safeguards must be implemented to ensure alerts are issued if suspicious behaviour is detected.

For PCI DSS, log data must be retained for at least 12 months. The most recent 3 months of log data must be available for processing and analysis.

For PCI DSS environments, security measures must be implemented to ensure that log data from systems that store, process and transmit PCI DSS data are reviewed daily.

8.16 Monitoring activities

There must be a formalised document that describes requirements and guidelines for monitoring and handling abnormal behaviour and activities. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

A 24/7 arrangement must be in place for monitoring IT security, including endpoints and networks, across JN Data and JN Data's customers.

There must be a formalised document that describes abnormal behaviour and unwanted activities in IT assets.

Safeguards must be implemented to ensure adequate monitoring of relevant it-assets to detect abnormal behaviour and activity. The level of monitoring must be based on the particular threat profile.

For PCI DSS environments, safeguards must be implemented to ensure alerts for changes in files at least once a week.

8.17 Clock synchronisation

There must be a formalised document that describes requirements and guidelines for time synchronisation. The standard time zone used in JN Data must be specified in the document. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

IT assets used for processing information must be configured to synchronise with an approved time server according to the selected standard time zone.

Any deviation from the selected time zone must be approved and documented in accordance with the change management guidelines, cf. 8.32.

Safeguards must be implemented to ensure that all IT assets in JN Data are synchronised with the same time zone.

Adequate authentication and access control for the time synchronisation service must be implemented to prevent unauthorised access. Access and authentication must comply with the relevant guidelines, cf. 5.15 and 5.17.

8.18 Use of privileged utility programs

There must be a formalised document that describes requirements and guidelines for the management and use of utility programs. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

All utility programs that can circumvent system and application procedures must be marked in the inventory of IT assets, cf. 5.9.

Safeguards must be implemented to ensure that only employees with a work-related need are able to access utility programs and obtain authentication. Accesses must be managed in accordance with the relevant guidelines, cf. 5.15 and 5.17.

Safeguards must be implemented to ensure that utility programs are updated in accordance with the relevant guidelines, cf. 8.8.

Safeguards must be implemented to ensure that the use of utility programs is logged in accordance with the logging guidelines, cf. 8.15.

8.19 Installation of software on operational systems

There must be a formalised document that describes requirements and guidelines for managing and maintaining changes and installing software in systems in operation. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a list of approved software in JN Data. All approvals must be based on a security assessment. Only software with security clearance may be installed in JN Data's operating environments.

There must be an annual cycle to ensure that security- and risk assessment are carried out on the relevant IT assets.

Operating software must be updated and installed by authorised personnel in accordance with the software installation guidelines.

Safeguards must be implemented to ensure that software in production environments is installed or updated on the basis of a test. On the basis of the test, an assessment takes place as to whether the installation and update are compatible with the existing infrastructure.



For customers of JN Data, upon request, software without security clearance can be installed in the customers' own production environments, if an assessment determines that there are no security consequences for the other customers in the community, or for the general JN Data infrastructure.

Software installation in operating environments must follow the IT asset cycle and classification guidelines, cf. 5.9 and 5.12.

8.20 Network security

There must be a formalised document that describes requirements and guidelines for network security. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Network diagrams and configuration files must be in place for network devices. The documentation must be reviewed and updated on an ongoing basis (at least annually).

Network equipment and components must be registered in the inventory of IT assets, cf. 5.9, and classified in accordance with the relevant guidelines, cf. 5.12.

Safeguards must be implemented to prevent and monitor unauthorised access and activities in the infrastructure.

Safeguards must be implemented to protect network equipment and documentation from unauthorised access.

Safeguards must be implemented to limit and filter the connection of IT assets to the network based on user requirements and approvals.

Safeguards must be implemented that prevent IT equipment that has not been provided or approved by JN Data from being connected to JN Data's internal network.

Firewall rules must be reviewed and updated periodically (at least every six months) to ensure that the rules reflect business requirements and the particular risk scenarios. Updating of the rules must be documented and be in accordance with the change management guidelines, cf. 8.32.

8.21 Security of network services

There must be a formalised document that describes requirements and guidelines for securing network equipment. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Safeguards must be implemented to control and monitor access in the network.



Authentication and access to network equipment must be subject to approval procedures and follow the general guidelines for the segregation of duties, cf. 5.3, access management, cf. 5.15, and authentication, cf. 5.17.

If the wireless network is used for communication, secure and approved network communication protocols must be used and the communication must be encrypted.

Safeguards must be implemented to ensure that only approved network communication protocols are used. If there are deviations, the protocols must be approved and follow the exemption document, cf. 5.1.

Access and use of network equipment must be monitored, controlled and logged in accordance with the relevant guidelines, cf. 8.15 and 5.19.

For PCI DSS, there must be a periodic, and at least quarterly, review of the network to identify available Access Points (Wi-Fi). If the monitoring is automatic, relevant staff must be notified through alerts.

8.22 Segregation of networks

There must be a formalised document that describes requirements and guidelines for segregating JN Data's and JN Data's customers' networks. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Adequate network segregation must be implemented. Communication between the segregated parts of the network must take place with approved network connectivity.

Safeguards must be implemented to prevent unauthorised access to JN Data's and JN Data's customers' network equipment and network documentation.

The perimeter and the segregation must be defined and documented and must undergo periodic (at least annual) review and update.

8.23 Web filtering

There must be a formalised document that describes requirements and guidelines for web filtering and access to external websites. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a list of blocked domains. The list must be maintained on an ongoing basis and must undergo periodic (at least annual) review and update.

Safeguards must be implemented to ensure that access to external websites is in accordance with the requirements for network security, cf. 8.20.

Safeguards must be implemented that block access to unauthorised websites and web-based applications.

8.24 Use of cryptography

There must be a formalised document that describes requirements and guidelines for the use and maintenance of cryptography and certificates. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a list of approved encryption protocols and algorithms, which must be maintained periodically (at least annually).

There must be a formalised document to assess whether safeguards can be implemented to limit the use of non-approved encryption protocols and algorithms.

There must be a list of encryption keys and certificates used.

Safeguards must be implemented for the central management and protection of encryption keys and certificates throughout the life cycle.

Confidential data must be encrypted at rest and in transit.

There must be a formalised document to ensure that cryptographic vulnerabilities are identified, assessed and mitigated.

8.25 Secure development life cycle

There must be a formalised document that describes requirements and guidelines for secure development throughout the development life cycle. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

The document must indicate how and when functional and non-functional requirements are handled, including requirements for IT security.

The secure development guidelines must apply to the development of new solutions, modifications to existing code or the re-use of code.

Source code must be maintained in the platform repository, which must be configured in accordance with the access control requirement cf. 5.15 and the segregation of duties requirements cf. 5.3.

8.26 Application security requirements

There must be a formalised document that describes requirements and guidelines for self-developed software and acquired applications. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Applications must be procured in accordance with IT security requirements for supplier agreements, cf. 5.20.

Self-developed software must take place in accordance with JN Data's general requirements and guidelines for development, cf. 8.25 and 8.27.

The acquisition of applications must be carried out in accordance with JN Data's general requirements and guidelines for IT asset lifecycle cf. 8.25.

IT security requirements for applications must be identified and specified based on the classification level of the application concerned and must be in accordance with the relevant guidelines, cf. 5.12.

IT security testing of self-developed software and acquired applications must be carried out in accordance with requirements and guidelines for both code and infrastructure, cf. 8.29.

When cloud services are implemented, steps must be taken to ensure that their implementation and operation meet JN Data's IT security requirements, cf. 5.23.

Applications must be registered in the inventory of IT assets, cf. 5.9.

Acquired applications must undergo a security assessment before they are put into production.

8.27 Secure system architecture and engineering principles

There must be a formalised document that describes requirements and guidelines for managing secure system architecture and development principles. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Development principles must be established, documented, maintained and applied in the context of software development in JN Data. The principles must apply to all architecture layers.

If the development is intended to process personal data, the development principles must comply with the guidelines and principles for privacy by design and privacy by default.

8.28 Secure coding

There must be a formalised document that describes requirements and guidelines for secure development. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Secure coding principles must be established for situations where new code is developed and existing code is re-used. The principles must be based on the particular threat landscape, cf. 5.7, and must be updated on an ongoing basis.

Tests must be carried out during and after development in accordance with the guidelines for security testing in development, cf. 8.29.

8.29 Security testing in development and acceptance

There must be a formalised document that describes requirements and guidelines for implementing IT security testing in the development cycle. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

During development, test of relevant safeguards must be carried out to ensure that all IT security requirements are met and implemented.

IT security testing must be defined using a risk-based approach and on the basis of criticality. Security testing can include testing of whether security functions and security configurations comply with IT security requirements.

Safeguards must be implemented to prevent the implementation of changes and updates to IT assets to production environments from compromising existing safeguards.

Testing of development activities must be carried out in separate test environments. The test must be documented and approved before implementation in JN Data's production environments.

8.30 Outsourced development

There must be a formalised document that describes requirements and guidelines for handling outsourced development. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Agreements on outsourced development must be concluded in accordance with the IT security requirements for supplier agreements, cf. 5.20.

There must be a centralised list of outsourced development activities documenting contractual development agreements, cf. 8.25 to 8.29.

There must be a formalised document that ensures central follow-up of the agreed development activities, cf. 8.25 to 8.29.

8.31 Separation of development, test and production environments

There must be a formalised document that describes requirements and guidelines for separating development, test and production environments. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Adequate logical and physical separation between development, test and production environments must be implemented to avoid unauthorised access and changes to the production environments.

Development of new and existing software must take place in the development environments, which ensure that tests can be performed under realistic conditions and give accurate results.

Safeguards must be implemented to prevent unauthorised access to development, test and production environments. Accesses and rights must be managed in accordance with the guidelines for access management, cf. 5.15, access rights, cf. 5.18, and the segregation of duties, cf. 5.3.

8.32 Change Management

There must be a formalised document that describes requirements and guidelines for change management, including the scope of documentation. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

There must be a formalised document that describes the types of changes and how they are handled. Any changes must be managed in accordance with the relevant guidelines and on the basis of a risk-based approach.

There must be a formalised document for managing emergency changes.

Changes implemented in the production environment must be subject to test. For high-risk changes that may affect customers, JN Data must ask the customers whether they wish to perform application verification.

Safeguards must be implemented to prevent the same person from approving as well as implementing a change.

Changes to the change record must be logged and monitored in accordance with the logging guidelines, cf. 8.15.

8.33 Test information

There must be a formalised document that describes requirements and guidelines for managing test data. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Unmasked production data must not be included in test and development environments. If there are deviations, the same technical and organisational safeguards must be in place as in the production environment. Where it is not possible to implement the same safeguards, a risk assessment must be carried out and the use of production data in test and development environments must be approved in accordance with the exemption document, cf. 5.1.

When using production data in test or development environments, documents must be implemented that ensure correct and prompt deletion of unmasked data after completion of testing.

Masking of production data must be in accordance with the data masking guidelines, cf. 8.11.

8.34 Protection of information systems during audit testing

There must be a formalised document that describes requirements and guidelines for managing the IT security of IT assets during auditing and testing. Responsibilities must be defined and tasks delegated for all identified activities.

All relevant safeguards must be described in the formalised document.

Audit and test documentation may only be collected and provided to the extent that it is relevant to the audit or test in question.

All audit and test requests as well as related documentation must be registered in a central task system.

Access management must comply with the relevant guidelines, cf. 5.15 and 5.18, and access rights must be limited to read access to all IT assets. In situations where additional rights are needed, the test must be performed by an employee with the necessary rights, on behalf of the auditor.

The development of scripts and commands must comply with the relevant guidelines, cf. 8.25 and 8.27. Scripts and other commands used for audits and testing must be registered in a centralised list.

Scripts and commands must only be used in accordance with the guidelines for the use of approved software, cf. 8.19.



Monitoring and logging of audit and test activities must be carried out in accordance with the relevant guidelines, cf. 8.15 and 8.16.

Safeguards must be implemented to ensure that the transfer of audit and test documentation in an external network is encrypted, cf. 8.24.

Documentation for audit and test purposes may not be placed on shared drives or other shared logical locations. If documents or material are downloaded from JN Data's systems in the context of the exchange of material with the auditor or tester, the material must be deleted immediately after it is exchanged.

Appendix A

Area	Requirement Owner	ISO Control
Risk Management	Thejs Willem Jansen	4. IT Risk Management
Identity Access Management	Bethina Pernille Luckow	5.3 Segregation of duties
		5.15 Access Control
		5.16 Identity Management
		5.17 Authentication information
		5.18 Access rights
		8.2 Privileged access rights
		8.3 Information access restriction
		8.5 Secure authentication
Security Governance / Compliance Governance	Ziggie Svane	5.1 Policies for information security
		5.2 Information security roles and responsibilities
		5.6 Contact with special interest groups
		5.35 Independent review of information security
		5.36 Compliance with policies, rules and standards for information security
		7.7 Clear desk and clear screen
		8.34 Protection of information systems during audit testing
Awareness	Ziggie Svane	6.3 Information security awareness, education and training
Management responsibilities	Jesper Bach Schriver	5.4 Management responsibilities
Legal	Hanne Lilleøre	5.5 Contact with authorities
		6.6 Confidentiality or non-disclosure agreements

Cyber Defence Center	Simon Juul	5.7 Threat intelligence
		5.24.1 Planning and preparation of security incidents
		5.25 Assessment and decision on information security events
		5.26 Response to information security incidents
		5.27 Learning from information security incidents
		5.28 Collection of evidence
		6.8 Information security event reporting
		8.16 Monitoring activities
Project Management	Henrik Vad	5.8 Information security in project management
Asset Management	Rikke Lüth	5.9 Inventory of information and other associated assets
		5.10 Acceptable use of information and other associated assets
		5.12. Classification of information
		5.13 Labelling of information
		5.14 Information transfer
		5.33 Protection of records
		8.11 Data masking
		8.12 Data leakage prevention
Human Ressources	Susanne Holtet Wølck	6.1 Screening
		6.2 Terms and conditions of employment
		6.4 Disciplinary process
		6.5 Responsibilities after termination or change of employment

Procurement and outsourcing	Henrik Laursen	5.19 Information security in supplier relationships
		5.20 Addressing information security within supplier agreements
		5.21 Managing information security in the ICT supply chain
		5.22 Monitoring, review and change management planning and preparation
		8.30 Outsourced development
Cloud Security	Mads Vestergaard	5.23 Information security for use of cloud services
Continuity Management	Kristian Bønnelycke Al-Bedri	5.29 Information security during disruption
		5.30 ICT readiness for business continuity
		8.14 Redundancy of information processing facilities
Regulatory Compliance	Thomas Søgaard	5.31.1 Legal, statutory and regulatory requirements
Customers	Tine Goul Dam	5.31.2 Contractual requirements
Software Management	Jakob Nørgaard	5.32 Intellectual property rights
		8.18 Use of privileged utility programs
		8.19 Installation of software on operational systems
GDPR	Martin Hjort Christensen	5.34 Privacy and protection of PII
		8.10 Information deletion
Process and document Management	Rikke Lüth	5.37 Documented operation procedures
Internal IT	Frederik Bonde Lykke Nielsen	5.11 Return of assets
		6.7 Remote working

Datacenter Operations	Klaus Hemme	7.9 Security of assets off-premises
		8.1 User endpoint devices
		7.1 Physical security perimeters
		7.2 Physical entry
		7.3 Securing offices, rooms and facilities
		7.4 Physical security monitoring
		7.5 Protection against physical and environmental threats
		7.6 Working in secure areas
		7.8 Equipment siting and protection
		7.10 Storage media
		7.11 Supporting utilities
		7.12 Cabling Security
		7.13 Equipment maintenance
		7.14 Secure disposal or re-use of equipment
Software Development	Jakob Johnsen	8.4 Access to source code
		8.25 Secure development life cycle
		8.26 Application security requirements
		8.27 Secure system architecture and engineering principles
		8.28 Secure coding
Endpoint Security	Camilla Beck	8.7 Protection against malware
Capacity Management	Lærke Marie Sørensen	8.6 Capacity Management
Vulnerability Management	Søren Kjær	8.8 Management of technical vulnerabilities
		8.9 Configuration management
Backup	Keewen Keith	8.13 Information backup

Log Management	Malene Toft Volt	8.15 Logging
Network	Lisa Borup	8.17 Clock synchronisation
		8.20 Network security
		8.21 Securing of network services
		8.22 Segregation of networks
		8.23 Web filtering
Cryptography	Gitte Friis	8.24 Use of cryptography
Test Management	Søren Eriksen	8.29 Security testing in development and acceptance
		8.31 Separation of development, test and production environments
		8.33 Test information
Change Management	Frank Marschall	8.32 Change Management
Incident Management	Claus Dueholm	5.24.2 Planning and preparation of incidents and major incidents