

IT Security Policy

Version:	13.0
Classification:	Public
Date of approval:	06.12.2024
Implementation date:	06.12.2024

Table of contents

1. Introduction, purpose and scope.....3

2. Organisation and responsibility.....3

3. Data of natural persons.....4

4. IT risk management.....4

5. IT security management5

6. Management of cyber risks6

7. Operational capabilities7

 7.1 Management7

 7.2 Asset management.....7

 7.3 Protection of information7

 7.4 Employee safeguards7

 7.5 Physical security7

 7.6 System and network security8

 7.7 Application security.....8

 7.8 Secure configuration8

 7.9 Identity management and access management8

 7.10 Threat and vulnerability management.....8

 7.11 Continuity.....8

 7.12 Safeguarding of supplier relationships.....9

 7.13 Legal and compliance capability9

 7.14 Management of information security incidents9

 7.15 Safeguarding of information security.....9

8. Dating of JN Data’s IT Security Policy.....10

1. Introduction, purpose and scope

JN Data A/S (hereinafter “JN Data”) provides IT operations and infrastructure to customers and owners in the financial sector and is deemed systemically important for the financial sector by the Danish Financial Supervisory Authority. Accordingly, JN Data is subject to stricter requirements for data, system and operational security.

The purpose of JN Data’s IT Security Policy is to ensure the implementation and maintenance of an adequate level of security for the company’s assets, which includes stipulating principles and requirements for IT security and risk management to ensure a high level of confidentiality, integrity and accessibility. This includes complying with standards, laws and executive orders and with requirements and norms stipulated by the sector, customers and the internal organisation. In terms of scope, JN Data is subject to the Danish Financial Business Act (lov om finansiel virksomhed).

JN Data’s IT Security Policy has been operationalised in the form of IT security requirements, pursuant to ISO/IEC 27001:2022. Furthermore, relevant security measures from ISO/IEC 27002:2022 have been included to ensure a structured approach to information security. Personal data protection has been integrated pursuant to ISO/IEC 27701:2019, and the IT risk management policy is based on ISO/IEC 27005:2022 as a frame of reference to ensure effective, proactive risk management.

JN Data’s IT Security Policy and the underlying IT security requirements apply to all information, data and assets in JN Data, both within and outside the company. Anyone who uses or accesses these is subject to standards, requirements and guidelines. This applies to all permanent employees, temporary employees/replacements, consultants, business partners, etc.

When outsourcing IT operations, JN Data’s security level must be safeguarded in collaboration with the service provider. This means that the service provider, its facilities and any employees with access to JN Data’s information, data and assets must comply with JN Data’s IT security level as a minimum.

Upon entering into contracts, the service provider must undergo a risk assessment and must adhere to the requirements stipulated for reporting, ongoing control and monitoring of the service provider and of the services it provides to JN Data.

2. Organisation and responsibility

The supervision of JN Data’s management of IT and cyber risks must be placed in separate, independent control functions. Accordingly, JN Data has organised the management of IT and cyber risks on the basis of the Three Lines of Defence Model, in which JN Data’s primary operational organisation constitutes the first line of defence, the ‘Risk Management’ and ‘Regulatory Compliance’ departments constitute the second, and ‘Internal System Audit’ constitutes the third.

The first line of defence is responsible for managing JN Data’s IT and cyber risks, including the establishment, maintenance, compliance and follow-up of IT security requirements and supportive security measures. The first line is also responsible for reporting on the operational efficacy of the IT security requirements.

The second line of defence is responsible for supervising the first line of defence, which includes challenging, advising, controlling and reporting on the first line of defence’s management of JN Data’s IT and cyber risks.

The third line of defence is responsible for implementing the mandatory and independent system audit activities.

3. Data of natural persons

JN Data must ensure compliance with data protection regulations in every respect. In terms of data security, this is done by establishing relevant technical and organisational security measures that ensure the protection of personal data by taking account of the types of personal data, including special categories of personal data and the rights of the data subjects.

4. IT risk management

An IT risk management framework must be implemented and maintained to ensure that IT risks in JN Data are analysed, managed, monitored and reported.

IT risk assessments pursuant to JN Data's IT risk management process are based on a criticality assessment of the potential impact on JN Data in the event that confidentiality, integrity and/or accessibility of Systems, Services and Processes (SSP) are compromised.

The IT risk management process underpins and supports JN Data's business areas in terms of preparing IT risk assessments of SSPs. Each SSP undergoes a risk assessment to understand the potential threat. The IT risk assessment identifies the inherent IT risk, which, in combination with security measures and controls, documents whether the residual IT risk is within JN Data's risk appetite. If an IT risk assessment identifies a need to take mitigating action, specific Risk Treatment plans are drawn up for the purpose of reducing the residual IT risk to an acceptable level of risk.

5. IT security management

The first line of defence is responsible for IT security management and for the establishment and maintenance of the Information Security Management System (ISMS), as this protects JN Data’s IT assets in line with owner, customer and regulatory requirements and with best practice and threat assessments.

Based on this policy, the IT security requirements that are to be operationally managed pursuant to each ISO 27001 control are drawn up in collaboration with the business areas.

An area manager is designated for each ISO 27001 control to help ensure the establishment of the requisite IT security requirements and business procedures in order to safeguard the requisite level of security and respond to the operational risks in the area.

Compliance with the agreed level of IT security is continuously monitored through reviews and implemented verification checks, which are designed on the basis of current IT security requirements and specified business procedures. The verification checks are reviewed by the first line of defence and the results of these are communicated to JN Data’s VP group and to its customers’ IT security departments.

The chosen security level must ensure that JN Data is capable of maintaining a robust, up-to-date defence against insider and cyber risks and must comprise effective technological measures and adequate human resources and expertise.

JN Data’s IT Security Policy must be approved by JN Data’s Board of Directors at least once a year, or in the event that significant changes require it to be revised.

6. Management of cyber risks

JN Data must continuously ensure that proper security measures are implemented to respond to the current threat landscape and protect the IT systems and IT services provided by JN Data.

JN Data must establish the gathering and analysis of strategic, tactical and operational threat information and intelligence related to existing and emerging threats. This must be based on JN Data’s risk profile, which must be reviewed on a regular basis.

JN Data participates in information-sharing communities to manage cyber risks. These communities can share information on, for example, threat information and intelligence, including compromise indicators, tactics, techniques, procedures and configuration tools.

In order to be capable of continuously adapting these security measures, JN Data must conduct security tests at appropriate intervals on the basis of the associated risk and ensure that the results are assessed and that the requisite mitigating measures are implemented. Security tests must be carried out pursuant to applicable legislation and recognised standards.

As part of the security tests, JN Data will test the efficacy of security measures that address IT and cyber incidents, which will include the conducting of threat-based penetration tests. This testing must comply with applicable legislation and have a scope that corresponds to the current threat landscape at any given time.

7. Operational capabilities

JN Data’s IT Security Policy must be supported by fifteen (15) ISO operational capabilities, which in turn must be defined in IT security requirements and underlying formalised business procedures. All the capabilities are described below:

7.1 Management

JN Data’s IT Security Policy must be maintained, approved, and communicated on a regular basis to ensure its efficacy and compliance with stipulated requirements. The line management must be actively involved and must support the security initiatives, as well as ensure that employees comply with policies and IT security requirements.

JN Data must continuously follow up on whether JN Data’s IT Security Policy and requirements (which include underlying processes, frameworks, method descriptions and business procedures) maintain the predetermined level of security to a sufficient extent.

7.2 Asset management

JN Data must identify and classify all information assets, including hardware, software, data and documents. The criticality of IT assets must be assessed against a common classification model that defines the classification of systems, services, processes (SSPs) and data, and appropriate safeguards must be implemented. JN Data must maintain a Configuration Management Database (CMDB) containing information and supportive IT assets.

7.3 Protection of information

Business procedures must be established for the processing and use of information and IT assets to ensure proper protection and use. Information must be classified and labelled to protect data and meet the need for confidentiality, integrity and availability. JN Data must maintain business procedures that stipulate requirements for the transfer of information in order to maintain a predetermined level of IT security for internal and external transfers.

In addition, technical measures must be implemented to ensure that user devices are protected against internal and external threats when employees perform daily operational tasks and other activities, to ensure compliance with agreed and regulatory requirements.

7.4 Employee safeguards

The background of job applicants must be verified before employment to ensure that prospective employees have the requisite skill sets and comply with company restrictions concerning personal, financial and criminal-liability issues. Upon employment, newly hired employees must be made aware of their IT security obligations.

JN Data must have guidelines for sanctions that apply to any permanent employee, temporary employee/replacement and/or consultant who violates JN Data’s IT security requirements in effect at any time.

An annual cycle of work must be maintained to ensure that all employees and selected consultants receive both general and targeted training in IT security.

7.5 Physical security

Measures must be put in place to ensure that the physical facilities are protected against unauthorised access. Surveillance must be set up to detect and prevent unauthorised access and protect against physical and environmental threats. All data centres must be equipped with adequate safeguards to protect or detect power failures, water ingress, fire or high temperatures to prevent the destruction of IT assets and other equipment.

JN DATA

JN Data must have guidelines that stipulate employees' obligations to maintain tidy desks and to lock their screens in order to reduce the risk of unauthorised access to confidential data.

7.6 System and network security

Network devices must be monitored to prevent them being compromised over the network. The network must be subdivided into security boundaries, and access to external websites must be restricted to reduce the risk of malware.

Security measures must be updated on a regular basis to protect systems and networks. Network traffic must be monitored on a continuous basis to detect and respond to suspicious activity, thus ensuring a high level of protection against cyberattacks.

The use of programs that can circumvent security measures must be limited and monitored. Development, testing and production environments must be segregated and secured, and all changes must follow a formalised change-management process.

7.7 Application security

JN Data will develop and maintain secure applications by using secure coding and conducting security tests on a regular basis. Software installation procedures must be maintained to protect the integrity of systems and prevent vulnerabilities. Furthermore, there must be guidelines for security, development and programming activities throughout the development phase.

7.8 Secure configuration

JN Data must possess documentation of the configuration of hardware and software, which must be monitored and assessed on an ongoing basis to ensure the proper functioning of hardware and software and prevent unauthorised changes. Guidelines for cryptography and encryption-key management must be maintained and implemented to protect data confidentiality, authenticity, and integrity.

7.9 Identity management and access management

JN Data must have procedures in place for the assigning, revoking, correcting and managing of identities and accesses to prevent unauthorised access. These procedures must include both general and privileged user access. Guidelines must be in place for the separation of functions for roles, supported systemically by the central user-admin system.

Access to source codes and software libraries must be based on secure authentication.

7.10 Threat and vulnerability management

JN Data must identify, assess, and address threats and vulnerabilities by conducting scans and updates on a regular basis. A vulnerability management process must be implemented to prioritise and rectify vulnerabilities quickly, which ensures a proactive approach to threat management. JN Data's exposure must be continuously evaluated, and appropriate measures must be taken to prevent the exploitation of vulnerabilities.

7.11 Continuity

A policy for operational IT stability must be drawn up to cover continuity management within JN Data. This policy must describe the overarching requirements for a contingency plan, communication plans, Disaster Recovery Plans (DRP) and other plans to ensure that IT assets are re-established within the agreed time.

Exercises must be carried out on a regular basis, and the plans must be updated on the basis of the lessons learnt from these exercises to ensure that the company is well prepared to manage unforeseen incidents.

7.12 Safeguarding of supplier relationships

JN Data must maintain formalised business procedures that stipulate the requirements for managing any IT risks arising from suppliers' products and services to maintain a predetermined level of IT security.

IT security requirements must be agreed with suppliers and monitored regularly to ensure that JN Data's IT security requirements are complied with throughout the supply chain. Non-conformity with the contract must be registered, and the supplier must prepare a remediation plan that mitigates the risks described.

7.13 Legal and compliance capability

JN Data will maintain business procedures to ensure that agreed and regulated requirements for IT security management and compliance are embedded in the business areas. In addition, procedures must be in place to ensure that compliance with requirements is monitored and assessed and that results are reported on an ongoing basis to the agreed internal and external parties.

7.14 Management of information security incidents

JN Data must establish efficient processes for detecting, reporting and managing security incidents. The procedures must include an escalation process to ensure that relevant parties are informed in a timely manner and pursuant to agreed and regulatory requirements.

A number of safeguards aimed at monitoring and analysing activities in the infrastructure must be maintained to identify suspicious activity or deviations from normal behaviour that could indicate an IT security incident. JN Data must have a dedicated IT security function that assesses threats on the basis of current threat information and takes action to minimise the damage.

7.15 Safeguarding of information security

JN Data's IT security must be assessed on a regular basis to ensure the efficacy of security measures. Risk assessments, including technical safety assessments, must form the basis for key decisions and cover both new and existing systems.

Business procedures that continuously improve the security measures on the basis of identified vulnerabilities, threat level and risk assessments must be implemented.



8. Dating of JN Data’s IT Security Policy

This IT Security Policy, version 13.0, was approved on 06.12.2024 by the Board of Directors of JN Data A/S.