IT Security and Business Continuity Policy

October 2025

Nykredit Totalkredit

Nykredit Realkredit A/S
CVR 12 71 92 80

Sundkrogsgade 25
2150 Nordhavn

Tlf. 70 10 90 00
kundeservice@nykredit.dk

Document Approval, Responsibility and Publication

Approved by the Board of Directors in

Nykredit Realkredit A/S (November 5 2025)

Totalkredit A/S (November 3 2025)

Nykredit Bank A/S (November 3 2025)

Nykredit Portefølje Administration A/S (October 31 2025)

Nykredit Leasing A/S (November 11 2025)

Nykredit Mægler A/S (October 30 2025)

Sparinvest S.A. (April 23 2025)

Following preceding processing by the Group Risk Committee
The Group Risk Committee has processed the Policy on behalf of the Executive Boards October 21 2025.

The Policy has been processed by the Audit and Board Risk Committees October 28 2025.

Document Responsibility:

Simon Thyregod, STHY

Unit:

DCI

Publication:

The Document Responsible makes sure that the document, immediately following approval, is published at:

	In Danish	In English
PolicyPortal	✓	✓
Intranet - Onboardingportalen	✓	✓

Contents

1. Background and Purpose

The purpose of Nykredit's IT Security and Business Continuity Policy is to set out the Nykredit Group's ("Nykredit") overall IT security and business continuity requirements based on the Nykredit's risk profile and the current threat level by managing IT risk in accordance with Nykredit's *Politik for ikke-finansielle risici og Bestyrelsens retningslinjer for Nykredit Realkredit-koncernen* (Policy for non-financial risk and the Board of Directors' guidelines for the Nykredit Realkredit Group). Further, the Policy aims to realise *Nykredits strategi for digital operationel robusthed og cybersikkerhed* (Nykredit's Digital Operational Resilience and Cybersecurity Strategy).

The Policy is designed to meet the requirements set out in Regulation no 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector ("DORA"), including regulatory and implementing technical standards specifying tools, methodologies, processes and policies. The Policy should be read in conjunction with *Direktionens retningslinjer for kontroller i Nykredit-koncernen* (The Executive Board's Guidelines for Controls in the Nykredit Group).

The *IT Security and Business Continuity Policy* will be updated and approved by the Group's Boards of Directors at least once a year and in the event of significant changes.

1.1 Commitment to maintain Financial Stability

The Policy sets out the overall principles for Nykredit's IT security practices. These principles are further specified as IT security requirements in Nykredit's *IT Security Requirements*, which constitute an important element of Nykredit's internal control environment. In addition, the Policy provides the framework for Nykredit's business continuity efforts and the recovery of Nykredit's critical business areas in the event of severe service disruptions. This is implemented through Nykredit's Crisis Management Plan, business continuity plans and disaster recovery plans.

1.2 Objectives

To acknowledge Nykredit's societal responsibility as a Systemically Important Financial Institution, the objective is to maintain an adequate level of IT security. Furthermore, it is to ensure the confidentiality, authenticity, integrity and availability of Nykredit's IT assets in accordance with Nykredit's risk appetite.

The continuity of critical business functions during and after severe service disruptions should be ensured, and business losses shall be limited to a minimum for Nykredit and Nykredit's business partners.

1.2.2 Business Continuity Objectives

Nykredit has set a number of specific business continuity objectives:

- Nykredit must be able to able to manage incidents that are not major, without noticeable operational impact
- In the event of critical incidents, Nykredit must be able to set up emergency operations to avoid significant impact on Nykredit's business conduct. Objectives specifying how to establish emergency operations should be defined in the individual IT solutions' disaster recovery plans
- Nykredit must be able to maintain emergency operation of critical business processes until Nykredit's IT solutions have been fully restored
- Nykredit must be able to establish emergency operations without dependencies on individual systems.

2. Scope and Definitions

2.1 Scope

The *IT Security and Business Continuity Policy* applies to the Nykredit Group.

The Policy covers all organisational, people, physical and technical factors involved in Nykredit's business conduct. The Policy applies to all employees and external consultants at Nykredit.

Nykredit works with a number of suppliers that may impact the level of IT security through the provided services. This particularly applies to the services provided by JN Data and BEC Financial Technologies ("BEC"). JN Data must comply with Nykredit's IT Security Requirements, as specified in the master IT agreement with JN Data. BEC must implement and maintain a level of IT security corresponding to that set out in IT Security Requirements. Taking a risk-based approach, other suppliers must also comply with Nykredit's level of IT security.

Appendix 1 provides an overview of the applicability of this Policy, the IT Security Requirements and exemptions in Nykredit and for JN Data and BEC.

Appendix 2 provides examples of Nykredit companies' responsibilities in relation to IT security.

2.1.1 Exemptions

The IT Security Requirements applies to the Nykredit Group, with the exception of Nykredit Mægler. Nykredit Mægler's IT risk landscape differs significantly from that of Nykredit. To that end, Nykredit Mægler has developed their own set of IT security requirements based on IT Security Requirements.

Nykredit Leasing and IT Security & Privacy have agreed that Nykredit Leasing's compliance with IT Security Requirements corresponds to their IT risk landscape and IT setup. To that end, Nykredit Leasing reports incidents to IT Security & Privayc, and exemptions must be approved and monitored by IT Security & Privacy. Furthermore, Nykredit Leasing's IT solutions must be registered in Nykredit's central solution register.

2.2 Definitions

IT security entails the protection of IT assets, with a particular focus on protecting their confidentiality, integrity, authenticity and availability.

IT assets means all kinds of IT-related resources that support the business. It includes software, hardware and data.

Confidentiality means that data is protected from unauthorised access, use and disclosure. Unauthorised persons cannot access data that could be used to harm Nykredit, Nykredit's customers, business relations or employees.

Integrity means that the consistency, accuracy and reliability of data are maintained throughout the data life cycle, and that data is protected from unauthorised modification. For Nykredit, this particularly applies to protection against manipulation in financial systems.

Authenticity means that data derives from its original source. At Nykredit, the concept of authenticity is included in the concept of integrity.

Availability means that IT systems and data must be available for authorised use. This is ensured by timely maintenance, backup and protection of IT solutions and data as well as the planning and testing of recovery procedures.

Contingency planning entails the business' response to a sudden crisis, by activating predefined plans on how to operate in a focused, timely and effective manner during the crisis.

Business Impact Assessment ("BIA") is the assessment of the potential impact of, for instance, severe service disruptions or data leaks. A BIA can be done at different levels, such as business processes, business functions or IT solutions. BIAs contribute in determining business criticality and provide the basis for establishing the requirements of IT security and operations as well as business continuity activities.

Contingency plans are plans and procedures set out to respond to crisis situations and severe service disruptions. Business continuity plans can include several types of plans, such as the Crisis Management Plan, business continuity plans and disaster recovery plans. The different types of business continuity plans are described in detail in section 5.2.

3. Organisation and responsibilities

Boards of Directors and Executive Boards

The Board of Directors of Nykredit Realkredit A/S is ultimately responsible for ensuring an adequate level of IT security to manage identified IT risks, so that these stay within Nykredit's risk appetite, cf. *Nykredit's Politik for ikke-finansielle risici og Bestyrelsens retningslinjer for Nykredit Realkredit-koncernen*. Further, the Board of Directors is ultimately responsible for ensuring adequate contingency planning.

The Board of Directors of Nykredit Realkredit A/S and the Boards of Directors of the individual Nykredit companies authorise their Executive Boards to ensure that IT security and contingency measures are implemented in accordance with the principles and framework set out in the Policy.

Group Risk Committe

The Group Risk Committee monitors the IT risk level on behalf of the Group Executive Board. The Group Risk Committee receives reports from the IT Risk Committee, which consists of Nykredit's CIO, CISO, Head of Infrastructure & Operations and a business representative, as well as an observer from Risk & Conduct.

Contingency Committee

Nykredit's Contingency Committee is the organisational unit responsible for implementing contingency measures and the Group's contingency plans, cf. *Kommissorium for Nykredit Beredskabskomite* (Mandate of Nykredit's Contingency Committee). This includes both IT and business contingency measures.

The Contingency Committee is responsible for preparing and maintaining the Crisis Management Plan, cf. *Kommissorium for Nykredit Beredskabskomite*.

IT Security & Privacy
IT Security & Privacy is responsible for Nykredit's IT security practices, and for ensuring that IT risks are managed within Nykredit's risk appetite. IT Security & Privacy and the individual business units constitute the first line of defence.

Based on the IT Security and Business Continuity Policy, IT Security & Privacy defines Nykredit's level of IT security for the use of IT. This is set out in the IT Security Requirements, and is specified in business procedures etc. IT Security & Privacy monitors and reports on Nykredit's and significant IT suppliers' compliance with Nykredit's defined level of IT security.

IT Security & Privacy assists Nykredit with interpretation and consultancy regarding Nykredit's IT Security Requirements.

Business Units
The business units are locally responsible for compliance with the *IT Security and Business Continuity Policy*, *IT Security Requirements* and related business procedures, rules etc., and that this compliance is documented. To that end, the business units and IT Security & Privacy constitute the first line of defence. Furthermore, the business units are responsible for preparing, maintaining and testing business continuity plans for their respective business areas in accordance with the *IT Security Requirements*. The heads of the business areas (level 2) carry the overall risk responsibility and approve the business continuity plans. At least once a year, the heads of the business areas ensure that the business continuity plans are tested and reviewed and subsequently updated and approved.

In crisis situations, the heads of the business areas will have management authority as usual.

Independent Control Functions and Internal Audit
Risk & Conduct monitors and controls that IT risks and other non-financial risks are sufficiently managed. Moreover, Compliance monitors and controls compliance risks in relation to IT. Risk & Conduct and Compliance constitute the second line of defence.

Internal Audit audits the internal control system, and determines if the internal control system reflects the risk level as set out by the Board of Directors. Internal Audit constitutes the third line of defence and reports directly to the Board of Directors.

4. Principles of IT Security

The objectives and principles of IT security set out in this Policy must be defined as IT security requirements. IT security requirements are security controls and other risk mitigation measures which serve to protect Nykredit's IT assets from loss of confidentiality, authenticity, integrity or availability. These requirements must be described in the IT Security Requirements. For each IT security requirement, roles and responsibilities must be defined using the RACI model[1].

The IT security approach must be based on the ISO 27000 series, including the management of IT security set out in 27001, security controls in 27002:2022 and privacy protection in 27701:2019. A Statement of Applicability (SoA) must be prepared to document the applicability of security controls.

The principles of IT security are divided into four main areas. Significant elements of the areas are described below.

4.1 Organisational Controls

4.1.1 Asset Management
IT assets and their life cycle must be centrally monitored and managed. IT assets must have an appropriate level of IT security corresponding to their risks. IT assets must not enter production without prior approval by IT Security & Privacy.

IT assets, including legacy IT assets, must be registered in a central solution register with relevant information such as interdependencies and disaster recovery requirements.

4.1.2 Data Classification
Data must be classified according to their need for protection. Nykredit classifies data into three categories, as described below:

- Publicly available data: This category contains information that is publicly available, except for public personal data.
- Internal data: This category contains business information that is freely accessible within the Nykredit Group.

[1] RACI (**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed) is a matrix used to define responsibilities.

- Confidential data: This category contains confidential business information about the Nykredit Group and its business conduct as well as all types of personal data, as defined in the General Data Protection Act.

The categories are specified further in the *IT Security Requirements*. If data is not classified, it should be considered classified as *Internal data*.

4.1.3 Access Control
IT assets must be subject to appropriate access control. Access rights must always be granted according to the principles of need-to-know, need-to-use and least-privileged, and are subject to approval based on the segregation of duties principle. Access rights must be reviewed with appropriate frequency.

4.1.4 IT Project Management
IT projects must be managed through a formalised approach. IT security must be an integral part of Nykredit's project management methodology.

4.1.5 Acquisition, Development and Maintenance of IT Solutions
The acquisition, development and maintenance of IT solutions must be managed through a formalised methodology to ensure that the IT solution's quality is as agreed. IT security and quality assurance must be an integral part of Nykredit's development methodology, which must also include change management and testing requirements.

4.1.6 Management of IT Related Incidents
Nykredit must establish and communicate a process for detecting, managing, reporting and responding to IT related incidents, including the definition of relevant roles and responsibilities in the context hereof.
The process must ensure detection and monitoring of cyber threats and anomalous activities at Nykredit and at suppliers, as well as continuous learning from and evaluation of resolved incidents.

4.1.7 Information Sharing Arrangements
Nykredit must participate in relevant forums to improve the digital operational resilience and ensure the exchange of intelligence, knowledge and information about IT risk, IT security, threats and incidents. Nykredit informs the Danish FSA upon entering and exiting memberships with relevant forums.

4.2 Human Controls
4.2.1 Human Resources
Nykredit must specify the IT security activities and responsibilities and assign employees and business units responsible for these.

Employees must understand and acknowledge the IT security responsibilities of their daily job function. This includes complying with relevant guidelines and undergoing relevant training to the necessary extent and at the necessary frequency.

Employees not complying with *the IT Security and Business Continuity Policy* or the *IT Security Requirements* may be subjected to disciplinary actions in accordance with relevant Nykredit procedures.

4.3 Physical Controls
4.3.1 Clear Screen and Desk Policy
To maintain the confidentiality, integrity, authenticity and availability of Nykredit's data, the use of workstations must be in compliance with the "clear screen" and "clear desk" principles. This applies at Nykredit locations as well as outside Nykredit.

4.4 Technical Controls
4.4.1 IT Operations
IT security must be an integral part of the use, monitoring, control and recovery of Nykredit's systems and data.

4.4.2 Network Security Management
Security measures must be implemented to ensure the confidentiality, integrity, authenticity and availability of networks and network devices at Nykredit.

Appropriate segmentation of networks and filtering of traffic between them must be provided where possible. Segmentation should be used to segregate internal and external zones, different business areas as well as development and test environments.

Access to external web resources must be appropriately managed to avoid exposure to harmful or malicious content.

4.4.3 Protection of Data in Transit

To maintain the confidentiality, integrity, authenticity and availability of Nykredit's data, adequate security measures must be implemented to protect data in transit. The mechanisms must reflect the need to protect data based on the criticality of the data.

To the extent possible, attempts to move or leak confidential data must be detected and investigated.

4.4.4 Encryption and Cryptographic Controls

IT assets should be encrypted appropriately, reflecting the risks of the assets. Where encryption is not possible, other security measures must be implemented to ensure an appropriate level of IT security.

Encryption keys must be managed throughout their life cycle.

4.4.5 Backup

To ensure efficient recovery of Nykredit's IT solutions and applications and business continuity in the event of severe service disruptions, IT assets must undergo backup at planned intervals and to a sufficient extent. Also, in the event of major IT-related incidents, Nykredit shall ensure that sufficient redundancy resources and capacity are allocated.

To meet the anticipated need for recovery, backup of systems and data must be tested at planned intervals, at least on an annual basis, and to a sufficient extent.

5. Contingency Planning

5.1 Business Impact Assessment (BIA)

Nykredit's contingency planning must be based on a comprehensive Business Impact Assessment (BIA). The BIA shall assess the criticality of Nykredit's business processes, functions, IT solutions, third-party dependencies and IT assets with related dependencies to prioritise them following a risk-based approach. The protection of Nykredit's IT assets and services must be based on the BIA to ensure redundancy.

The BIA must be updated annually as well as in connection with significant legal or organisational changes, changes in the threat landscape or changes in Nykredit's risk profile.

5.2 Contingency Plans

The *IT Security and Business Continuity Policy* is implemented through a Crisis Management Plan, business continuity plans, disaster recovery plans, IT contingency plans and crisis communication plans. They are specified as below:

The **Crisis Management Plan** is the Contingency Committee's overall plan for a contingency situation. The Crisis Management Plan covers organisation, stakeholders, activities and communication in a contingency situation for Nykredit. The Crisis Management Plan must be regularly updated and updated following tests and activation.

Business continuity plans cover all manual procedures and business processes in the business areas, including agreements with external business partners. Business continuity plans ensure that Nykredit will remain operational at an acceptable level in case of disruptions, by describing how the business areas will continue their activities during the recovery of the IT environment. Business continuity plans shall be based on BIAs on the respective business area, and must be prepared for all critical business processes. The Group's heads of the individual business areas are responsible for the business continuity plans.

Disaster recovery plans for IT solutions and applications describe the technical measures and conditions for restoring the individual IT components of solutions. The disaster recovery plans take into account their significance to critical business functions and processes and their exposure to cyberthreats. All business-critical IT solutions must have a disaster recovery plan in place, and these plans must include recovery objectives corresponding the solution's criticality.

IT contingency plans cover Nykredit's IT setup, whether outsourced or not, including the recovery of IT operations in case of disruptions. Based on the BIA, Nykredit's IT contingency plans must be prioritised following a risk-based approach.

Crisis communication plans ensure proper communication of major incidents, breakdowns or threats to customers, clients, business partners and the general public. The crisis communication plans must be prepared with reference to Nykredit's general communication policy, which defines communicative roles and responsibilities in the event of severe service disruptions.

5.3 Testing of Contingency Measures

Nykredit's contingency planning must be tested on an annual basis or in the event of significant changes to business-critical IT solutions. This is to ensure that contingency measures and supporting contingency plans are up-to-date and that Nykredit is adequately resilient to ensure the continued operation of critical business functions in the event of severe service disruptions. Tests must be based on the BIA.

To ensure continuous learning, the test results must be documented, and any shortcomings in the contingency planning must be addressed and reported to Nykredit's Boards of Directors.

6. Monitoring and development

6.1 Monitoring

As described above, monitoring is carried out at various levels in the Nykredit Group.

IT Security & Privacy monitors the level of IT security across the Group to identify exemptions from the implementation of the *IT Security and Business Continuity Policy* and *IT Security Requirements* and to maintain the appropriate level of IT security despite these exemptions. Furthermore, IT and compliance risks in the second line of defence are monitored by Risk & Conduct and Compliance respectively, while Internal Audit audits the internal controls through inspections. The Contingency Committee is responsible for overseeing contingency planning efforts to ensure its effectiveness and compliance with relevant regulatory requirements.

Monitoring includes, but is not limited to, tracking and reporting on defined objectives, documentation and analysis of incidents with the purpose of learning and identifying areas of improvement, as well as periodical inspections to ensure compliance with internal policies and regulatory requirements.

The level of IT security must be assessed through various methods of verification, including auditing and technical testing. Methods must vary such that Nykredit monitors the IT security level in breadth and depth.

6.2 Updates

The *IT Security and Business Continuity Policy* and related business procedures and contingency plans must be reviewed and updated annually or in the event of major incidents. An update may be done on the basis of legal, technological, organisational or business changes, or input from employees, business partners or supervisory authorities.

6.3 Continuous Development

The protection of Nykredit's IT assets must undergo development and improvements continuously, taking into account learnings from service disruptions or other security incidents, best practice in the financial sector, learnings from global events and knowledge acquired through participation in relevant communities.

7. Policy Deviation or Violation

If the provisions set out in this Policy or the IT Security Requirements cannot be met, or the risk is disproportionate to its financial or business consequences, IT Security & Privacy may, on behalf of the Boards of Directors and Executive Boards, grant exemptions from the Policy or the *IT Security Requirements*, provided that compliance with the IT security objective is upheld. Exemption cannot be granted from requirements if such exemption will result in noncompliance with applicable legislation or risks outside the risk appetite.

Exemptions from requirements are subject to a risk assessment, must be presented to the Executive Board and the Board of Directors by way of an annual report and must be reviewed at planned intervals. Exemptions must also be included in the current IT risk landscape. Thus, exemptions of critical risk must be reflected directly in the risk reporting by IT Security & Privacy to the Group Risk Committee.

Before an exemption is granted, a written application must be made to document the decisions made. Exemptions must be temporary. At planned intervals, IT Security & Privacy must make sure that deadlines have been met.

8. Rapportering

IT Security & Privacy is to report regularly to the IT Risk Committee, the Group Risk Committee, the Board Risk Committee as well as Executive Boards and Boards of Directors, cf. the table below.

IT Security & Privacy submits quarterly reports to the IT Risk Committee. Cf. *Kommissorium for Nykredit Beredskabskomite*, the IT Risk Committee has been delegated the responsibility of monitoring and management of Nykredit's IT risks, including the Group's IT security. The IT Risk Committee semi-annually provide reports on its main areas to the Group Risk Committee. Should IT Security & Privacy deem it relevant, separate reporting on IT risks may be provided to Executive Boards, and in special cases to Boards of Directors.

In addition, IT Security & Privacy is to report to the Board Risk Committee semi-annually, and to the individual Boards of Directors annually. Such reporting must include an overall assessment of the IT risk landscape, the Group's IT security and the contingency measures.

Finally, four times a year IT Security & Privacy is to report on IT risk scenarios to Risk & Conduct, who is responsible for the reporting of risks to Executive Boards and Boards of Directors. Reporting provided to Risk & Conduct must describe, categorise and assess the identified IT risks. They should also present any controls and other risk mitigation measures implemented to ensure risks are within Nykredit's risk appetite. Reporting must be done at company level.

IT Security & Privacy is also obliged to report major incidents to the Executive Boards and Nykredit's Board of Directors, if relevant. Furthermore, Nykredit must report to relevant supervisory authorities in the event of major incidents or disruptions.

Reporting	Frequency	Recipient
Security Report (Update in IT risks, IT security and contingency planning)	Quarterly	IT Risk Committee
IT risk scenarios in Risk Management Report	Quarterly	Group Risk Committee
IT risk landscape	Semi-annualy	Risikokomiteen
Semi-annual Report (Relevant areas and updates on IT risks, IT security, IT operations and contingency planning)	Semi-annually	Group Risk Committee (Executive Boards) Board Risk Committee Boards of Directors

9. Commencement

The *IT Security and Business Continuity Policy* enters into force at the time of approval by the Boards of Directors.

Appendices

Appendix 1: *Scopes of the Policy*

	Nykredit Realkredit A/S	Nykredit Bank A/S	Totalkredit A/S	Nykredit Portefølje Administration A/S	Nykredit Leasing A/S	Nykredit Mægler A/S	Sparinvest S.A.	JN Data A/S	BEC Financial Technologies a.m.b.a.
IT Security and Business Continuity Policy	X	X	X	X	X	X	X		
IT Security Requirements	X	X	X	X	X		X	X	(X)
Exemptions	X	X	X	X	X	X	X	X	

Appendix 2: IT Security Tasks at Nykredit Group Companies

	Nykredit Realkredit A/S	Nykredit Bank A/S	Totalkredit A/S	Nykredit Portefølje Administration A/S	Nykredit Leasing A/S	Nykredit Mægler A/S	Sparinvest S.A.	JN Data A/S	BEC Financial Technologies a.m.b.a.
Conducting IT security assessments	X	X	X	X	X		X		
Registering solutions in SEACOR	X	X	X	X	X	X	X		
Reporting incidents	X	X	X	X	X	X	X	X	X
Subject to IT security testing (controlling activities etc).	X	X	X	X	X	X	X	X	X