Nykredit

Totalkredit

Fotograf: Brian Buchardt

IT security policy

September 2020

Document owner:	STHY, IT Security	
Approver and approval date:	Board of Directors of:	
	Nykredit A/S	3 November 2020
	Nykredit Realkredit A/S	3 November 2020
	Totalkredit A/S	30 October 2020
	Nykredit Bank A/S	29 October 2020
	Nykredit Portefølje Administration A/S	29 October 2020
	Nykredit Leasing A/S	28 October 2020
	Nykredit Mægler A/S	12 November 2020

Date	Author	Version	Description
07.11.2019	RE	2.0	Approved by the above Boards of Directors
21.02.2020	RE	2.0	Updated and approved by Leasing and Mægler
30.08.2020	NAST	2.1	Details on risk management, security requirements and exemptions.

CONTENTS

1. THE PURPOSE OF THIS POLICY 4

2. SCOPE 4

3. OVERALL IT SECURITY OBJECTIVE 4

4. GOVERNANCE AND MANAGEMENT MODEL 5

4.1. ORGANISATION AND RESPONSIBILITIES 5

5. IT RISK AND RISK MANAGEMENT 6

6. CLASSIFICATION OF INFORMATION 7

7. SECURITY REQUIREMENTS 7

7.1. EXEMPTIONS 9

8. INCIDENT AND CONTINGENCY MANAGEMENT 10

8.1. CONTINGENCY OBJECTIVE 10

1. THE PURPOSE OF THIS POLICY

The purpose of the IT security policy is to determine the Nykredit Group's overall IT security requirements based on the desired risk profile. This is to support the delivery of Nykredit's strategic objectives for the use of electronic data processing, including compliance with statutory and regulatory requirements. Moreover, the IT security policy sets out a cybersecurity framework to protect Nykredit against cyberattacks.

Division of responsibilities, guidelines, procedures, risk assessments and IT security contingency plans are some of the elements of this overall policy.

2. SCOPE

The IT security policy covers all technical, process and human factors that may affect the services and systems applied by Nykredit for the purpose of electronic data processing, including services and systems delivered by subsuppliers.

The policy applies to all Nykredit's staff and external consultants and also defines the standard of IT security expected by Nykredit from IT service providers.

For the purpose of this policy and related handbooks, guidelines, business procedures and similar documents, IT security means:

Safeguarding all IT information assets involved in, or contributing to, the processing of digital information by means of technology, humans and processes, all of which are key to achieving adequate and optimum security.

3. OVERALL IT SECURITY OBJECTIVE

The provision of IT services must be efficient, reliable and secure, as IT usage is an essential element of Nykredit's business operations. Nykredit wants to follow industry best practice, combined with an approach where the costs of security measures are balanced against their security value for Nykredit.

Nykredit's IT environment must be secure enough to resist commonly known cyberattacks and resilient enough to allow the restoration of systems according to the contingency objective. Also, the potential compromising of one IT system or computer should not be able to jeopardise Nykredit's entire IT environment.

The IT security level must always be aligned with the Executive Board's expectations and the Board of Directors' defined risk appetite. This is ensured through security assessments providing Confidentiality, Integrity and Availability requirements. In addition, the implemented security measures should be continuously reviewed and tested, in light of sector standards and current threats.

IT security traditionally breaks down into the following areas:

Confidentiality
Confidentiality means that data are protected from unauthorised access, use and disclosure. No unauthorised person can access data that could be misused to the detriment of Nykredit, Nykredit's customers, business relations or staff.

Integrity
Integrity means that the consistency, accuracy and reliability of data are maintained throughout the data life cycle, and data are protected from unauthorised modification.

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

4. GOVERNANCE AND MANAGEMENT MODEL

To ensure that Management is sufficiently involved in IT security, Nykredit has established a governance and management model adopted by the Board of Directors and the Executive Board and embedded in the organisation in general.

The model consists of the IT security policy, an IT security handbook, business procedures, organisational decision-making procedures and organisational activities supporting the IT security level and ambitions set out by the Board of Directors in this policy.

The IT security policy defines the overall IT security framework. The IT security handbook lays down specific IT security requirements ensuring that IT security remains within the framework defined in the IT security policy. These are supplemented by business procedures, organisational decision-making procedures and organisational activities, including risk and other relevant reporting.

4.1. ORGANISATION AND RESPONSIBILITIES

The overall responsibility for IT security in the individual companies of the Nykredit Group lies with the Board of Directors and the Executive Board of each company.

The Risk Committee is in charge of the ongoing monitoring of IT security management and the IT risk level on behalf of the Group Executive Board.

The IT Security Committee, consisting of the CIO, the CISO, the Head of IT Delivery and the Head of IT Infrastructure & Operations, handles technical IT security challenges and regularly reports to the Risk Committee.

IT Security is responsible for preparing and maintaining the IT security policy and related security requirements based on a risk assessment of the Group's IT usage. It plays an active, supervisory and reporting role with respect to IT security policy compliance across Nykredit, reporting to the Group's Executive Boards.
The IT security policy is updated and approved by the Boards of Directors annually or in case of material changes.

IT security policy compliance is ensured by the individual Executive Boards specifying requirements in the IT security handbook, which is updated and approved by the respective Executive Boards annually or in case of material changes.

The individual organisational entities of the Group are responsible, on a local, day-to-day basis, for compliance with the IT security policy and the IT security handbook and related business procedures, rules, etc and for documentation of such compliance. To ensure the anchoring of this responsibility, all IT solutions must have an unambiguous owner, and this must be registered centrally.

Responsibilities are outlined in Chart 1, and the responsibilities in each line of defence are described in detail below.

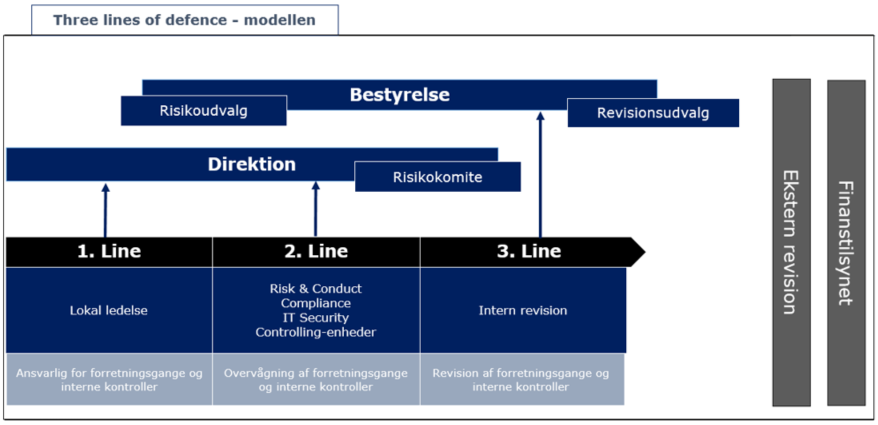
Three lines of defence - modellen
Bestyrelse
Risikoudvalg
Revisionsudvalg
Direktion
Risikokomite
1. Line
2. Line
3. Line
Lokal ledelse
Risk & Conduct Compliance
IT Security
Controlling-enheder
Intern revision
Ansvarlig for forretningsgange og interne kontroller
Overvågning af forretningsgange og interne kontroller
Revision af forretningsgange og interne kontroller
Ekstern revision
Finanstilsynet

Chart 1– 3 Lines of defence

First line – local management
Nykredit applies a principle of decentralised responsibility. That means that the line management is responsible for sustaining IT security locally through day-to-day business procedures. The line management is therefore responsible for identifying the IT security requirements that are within its remit, for complying with them and for subsequently monitoring compliance by implementing relevant controls.

Second line – Compliance, Risk Management, IT Security
The Executive Board specifies security requirements, supported by IT Security. IT Security supports the organisation, offering interpretation and advice concerning Nykredit's IT security requirements. In addition, IT Security regularly checks compliance with the stipulated security requirements. Likewise, relevant process owners monitor compliance with their processes and thus act as a second line of defence with respect to process users.

Third line – the systems audit function
The systems audit function makes up the final layer of the model. The systems audit function comprises an internal systems audit unit and an external systems auditor. The systems audit unit performs an audit of the internal control system and checks that it is in accordance with the level set by the Board of Directors. The systems audit function reports directly to the Board of Directors.

5. IT RISK AND RISK MANAGEMENT

Management of IT risk and IT security risk is part of Nykredit's overall risk management framework, which is the responsibility of Risk & Conduct and based on Nykredit's operational risk management policy, including principles of classification and recording. The objectives of IT risk management are aligned with the objectives of other operational risk management.

Nykredit applies four risk levels, Low, Medium, High and Critical (previously Very High) taking into consideration financial losses, working days lost, regulatory compliance and Nykredit's reputation. The Board of Directors defines the risk appetite within these levels and areas in the operational risk management policy. The policy sets requirements for the reduction or maintenance of the level of operational risks, including IT risks and IT risk management. The following IT risk areas and risks have been identified:

RISK AREA	RISKS
Systems and data	Unintended data loss
	Business impact due to an internal error caused by Nykredit IT
	Non-compliance relative to regulatory rules and requirements
Integration and suitability of IT systems	Technological debt
	IT application without a licence
	Robots (error processing, loss of integrity, hacking)
	Business impact due to early release of solutions (beta versions)
Dependence on external factors, including subsuppliers	Critical incidents at suppliers
	Business impact due to lack of supply chain management
	Cyber espionage/activism/terrorism
	Cybercrime committed against Nykredit or customers
	Cloudbursts, fires, natural disasters etc
	IT crime against ATMs
	Theft of and intentional damage to IT
Nykredit's organisation including non-segregation of duties	Insufficient skills/knowledge about maintaining important day-to-day operations
	Fraud etc (internal/insider in IT)
	IT outside the scope of IT
	Staff use of private devices

IT Security is responsible for preparing an IT risk assessment twice a year as well as in connection with important changes. This is sent to Operational Risk Management, which is responsible for ensuring that it is reviewed by the Executive Board and the Board of Directors. Risk assessments identify and assess relevant IT risks related to Nykredit's systems and data, the integration and suitability of Nykredit's IT systems, dependence on external factors, including subsuppliers, Nykredit's organisation and any lack of segregation of functions. IT Security is responsible for identifying and assessing IT risks as well as describing compensating measures. Operational management is responsible for following up in this connection and reporting operational risks.

They also assess external threats, material changes and the potential consequences of identified IT risks for Nykredit. This way, risk assessments are used to determine whether IT risks remain within the risk appetite defined by the Board of Directors, to improve IT security on an ongoing basis and as a basis for changes and/or verification of the IT security policy.

IT incidents must always be registered with IT Security. IT incidents affecting Nykredit's IT risk profile are reported by IT Security to Risk & Conduct, which will address and categorise them like other risks and report them to the Board of Directors. Furthermore, the IT Security Committee will be presented with an overview of incidents and statistics.

6. CLASSIFICATION OF INFORMATION

Nykredit classifies information into three overall categories: *Public information*, *internal information* and *confidential information*.

CLASSIFICATION	DESCRIPTION
Public information	Information that is publicly available, except public personal data.
Internal information	Business information that is freely accessible within the Nykredit Group.
Confidential information	Confidential business information about the Nykredit Group and its business conduct as well as all types of personal data, as defined in applicable personal data legislation.

Each category is subject to differentiated confidentiality requirements, and all security requirements in the IT security policy, the IT security handbook and the blue leaflet are based on these categories.

If information is not classified, it should be considered "Internal information".

7. SECURITY REQUIREMENTS

The security requirements are the security measures and controls needed to protect Nykredit's IT information assets.

Nykredit operates under the security requirements defined in ISO 27001, Annex A. Nykredit ensures that the inclusion/exclusion of ISO 27001 controls is justified. This is the responsibility of IT Security.

The security requirements are designed to maximise the protection of IT information assets, increase staff efficiency where possible, ensure compliance with regulatory requirements relating to IT usage and avoid unnecessary costs. Operating under the best practice requirements of ISO 27001:2017 ensures the professionalism, quality and strength of Nykredit's IT security deliverables and solutions.

Each security requirement is described in Nykredit's IT security handbook with appendices. To this end, the individual divisions and units in Nykredit prepare and document the relevant business procedures, methods, guidelines, check lists etc.

The security requirements of the IT security handbook cover the following main areas (based on Annex A of ISO 27001):

- ***Information security policies*** *(Chapter 5)*
  All documents containing rules, limits or guidelines related to IT security must meet Nykredit's general requirements for such documents. There must also be a document owner who is required to ensure that such are updated at least once a year or in connection with major changes.

- ***Organisation of information security*** *(Chapter 6)*
  IT activities are organised under Digital, Change & IT in the COO area. As a main rule, IT development and IT operations are organised in separate units. However, Nykredit also applies agile development methodologies, including DevOps, which combine development and operations in one organisational unit. Digital, Change & IT provides IT support for the activities of all Nykredit's organisational units where required.

  Appropriate segregation of duties must be in place within user administration, review and authorisation, log information, backup data as well as IT development and operations.
  The Head of the department is responsible for ensuring compliance and verification of the above at least once a year or in connection with important changes.

  IT Security must always be consulted when new IT solutions are designed, procured and/or implemented.

- ***Human resources security*** *(Chapter 7)*
  All staff members and consultants must read and understand relevant IT security information and follow this.

- ***Asset management*** *(Chapter 8)*
  All Nykredit solutions must be registered centrally with an unambiguous owner. In addition, all solutions must have an appropriate level of IT security based on a risk-based approach.

  All solutions must be used as intended and where appropriate be returned to Nykredit when no longer in use.

- ***Access control*** *(Chapter 9)*
  Solutions should have an appropriate degree of access control and follow relevant business procedures for the area. All accesses must be reviewed at least once a year by the immediate supervisor and where possible, also by the solution owner.

- ***Cryptography*** *(Chapter 10)*
  Nykredit's solutions should all use an appropriate degree of encryption. The solution owner is responsible for ensuring this and for obtaining authorisation from IT Security.

- ***Physical and environmental security*** *(Chapter 11)*
  Procurement, Facility Management and IT has the overall responsibility for ensuring an appropriate level of physical and environmental security. However, all users of solutions have a responsibility for ensuring usage in the manner described.

- ***Operations security – including operating procedures, logging, monitoring and safety backups*** *(Chapter 12)*
  All solutions must include relevant operating documentation describing the applied logging, backup, monitoring and safety backups to comply with the IT security handbook and relevant business procedures. The responsibility for this lies with the solution owner.

- ***Communications security*** *(Chapter 13)*
  Solution owners must ensure that communication routes are adequately protected

and meet the internal guidelines laid down by IT Security.

- ***System acquisition, development and maintenance, including quality assurance*** *(Chapter 14)*
  Nykredit's development methods must support the design of systems of the agreed quality and IT security. Systems must be developed, acquired and implemented according to an approved and well described method, specifying eg change management, testing and quality assurance requirements. Quality assurance must be an integral part of Nykredit's development methods.

- ***Supplier relationships*** *(Chapter 15)*
  Written agreements must be concluded with external business partners, and the requirements to be met by suppliers must be based on Nykredit's business needs. To make the security requirements as effective as possible, critical risks in relation to suppliers and deliverables must be identified. The requirements will then be designed so as to address the identified critical risks. To that end, Nykredit must ensure compliance with current legislation and sector requirements.

  Upon conclusion of an agreement, services provided by a supplier of business-critical or sensitive deliverables must be regularly monitored and assessed for the purpose of evaluating the security level of the deliverables. This is the responsibility of the contract owner, assisted by IT Security.

  If the supplier processes personal identifiable information, a data processing agreement must be concluded which meet the internal guidelines in this respect.

- ***Information security incident management*** *(Chapter 16)*
  See paragraph on incident and contingency management.

- ***Information security aspects of business continuity management*** *(Chapter 17)*
  See paragraph on incident and contingency management.

- ***Compliance, including compliance with relevant legislation*** *(Chapter 18)*
  The solution owner is responsible for ensuring that the solution complies with current legislation and policies as well as any business procedures, guidelines etc.

  Local controls are performed to check that the security requirements are implemented and effective. IT Security and Compliance perform second line controls according to a risk-based approach. If control measurements show that security requirements are not as effective as expected, relevant measures will be taken to improve their effectiveness.

  IT Security performs ongoing and at least once a year controls of IT security policy compliance for all Nykredit Group companies that the policy applies to, including significant subsuppliers. The results are reported to the Boards of Directors of the respective companies.

7.1. EXEMPTIONS

If the rules laid down in the IT security policy or the IT security handbook cannot be met, or the risk is disproportionate to its financial or business impact, IT Security may, on behalf of the Board of Directors and Executive Board, grant exemptions from requirements laid down in the IT security policy or the IT security handbook.
Exemptions from requirements must be based on risk assessments, presented to the Executive Board and the Board of Directors by way of an annual report and be reviewed at least annually. Exemptions must also be included in the current IT risk landscape. Exemptions for critical risk categories must thus be reflected directly in the risk reporting from IT Security to the Risk Committee.

Before an exemption is granted, a written application must be made to IT Security documenting all decisions. All exemptions are valid for a maximum of 12 months and IT Security must at least once a quarter check whether time limits are met.

Exemption may never be granted for breach of relevant legislation such as the GDPR, nor will exemption be granted where the associated risk is considered Critical (previously Very High).

8. INCIDENT AND CONTINGENCY MANAGEMENT

If breaches of the IT security policy, the IT security handbook or any other factors that could jeopardise Nykredit's IT security are identified, they will be addressed by IT Security based on the established IT security incident procedure.

Staff breaching the IT security policy or the IT security handbook may be subjected to disciplinary measures in accordance with Nykredit's staff administration rules.

Nykredit's Contingency Committee is the organisational entity responsible for implementing compliance with IT security policy rules on contingency planning and the Group's overall contingency plans, covering IT as well as business aspects.

The member of the Group Executive Board responsible for the Group IT area chairs the Committee.

The Contingency Committee is responsible for implementing the Group's contingency plans, covering IT as well as business aspects, and the Committee also constitutes the emergency staff in case of disasters, major accidents etc.

8.1. CONTINGENCY OBJECTIVE

The overall contingency objective is that a contingency situation relating to Nykredit's IT support must not lead to significant business losses nor jeopardise Nykredit's future business conduct. Consequently, all business-critical systems should be operated across multiple data centres.

Group contingency plans have been implemented as:

- The master contingency plan, ie the Contingency Committee's overall plan for a contingency situation. The plan covers organisation, stakeholders, activities and communication in a contingency situation.
- IT contingency plans covering Nykredit's entire IT setup, whether outsourced or not, including restoration of IT operations in case of disasters; the responsibility for these plans rests with Infrastructure & Operations.
- Business contingency plans covering all manual procedures and business procedures, including agreements with external business partners aimed at ensuring that Nykredit will remain operational at an acceptable level in case of disasters. The responsibility for these plans rests with the heads of the Group's individual business areas.
- The heads of the individual business areas are responsible for preparing business contingency plans covering their own areas in accordance with the guidelines set out, for approving these and for arranging, at least once a year, that these are reviewed (tested etc) and subsequently updated and approved.
- In emergency situations, the heads of the individual business areas will have their usual executive powers and staff responsibility for the purpose of performing the business activities supported by the business contingency plans and will also have the executive responsibility for the business activities aimed to bring operations back to normal.

Business and IT contingency plans as described above need to be prepared for foreign entities as well. These activities fall within the remit of the Contingency Committee.