ICT Security Policy

Table of contents

1. Purpose and scope

The purpose of this ICT Security Policy (hereinafter the Security Policy) is to ensure that a high level of IT resilience is implemented and maintained at the Jyske Bank Group (hereinafter the Group), also entailing that principles and requirements of IT security management are defined to ensure that the level of IT security and the desired risk profile in the IT area can be adhered to. This translates into strong cyber defence and resilience in critical and important functions.
The Security Policy must each year be laid down on the basis of a current risk assessment and be communicated to employees and relevant parties, including upload to the Group's website.
The Security Policy applies to all employees of Jyske Bank, Jyske Realkredit, Jyske Invest and Jyske Finans as well as to all third parties who have access to the Group's ICT assets or process the Group's information.

2. IT security level

2.1 Ambition

The IT security level must be based on the Group's ambition to obtain and to maintain a level of digital operational resilience that is sufficient to handle the current cyber threat with elements that are 'best in class'. In addition, the level of security must at all times be sufficient to ensure that the organisation operates within the Group's defined risk appetite for ICT.
The security level must be determined in such a way that it matches the development of the threat level at a national level, it must be based on risk assessments, and it must comply with the legislation and requirements applicable to the sector.

The IT security level must enable the Group to maintain a defence against cyber threats in the form of efficient technological arrangements, processes and human resources. The resilience of the Group's ICT systems and its use of IT must be secured in order to ensure stable operations of the Group's critical functions and business processes and to secure cyber resilience as efficient protection against cyber attacks from threatening players who are highly organised and launch sophisticated attacks.

2.2 Cyber security and sustainability goals

Jyske Bank is conscious that cyber security is not just an internal issue to secure stable operations of the Group's critical functions and business processes, but due to its role as one of the largest financial institutions in Denmark, the Group's activities relating to cyber security must also affect the Group's sustainability goals (ESG). Compliance with the requirements of this Security Policy will contribute to meeting these goals, which will further encourage the Group's employees to comply with the Security Policy.

2.3 Security documentation

The Security Policy must be supplemented with documented initiatives through a Digital Operational Resilience Strategy (DORS) that describes how to attain or maintain the IT security

level. In addition, the Security Policy must be elaborated on through supporting guidelines and business procedures detailing how the requirements herein are to be operationalised.

The requirements that have been defined in guidelines and business procedures must be adhered to at any time. A risk assessment of deviations from the Security Policy must be carried out. In the event of material deviations that are accepted temporarily, exemptions from the Security Policy must be given.

2.4 Security Policy approval

The Security Policy must be approved by the Group Supervisory Board at least once a year or in connection with material changes that require revision. Likewise, the Group Supervisory Board shall approve targets and objectives with which the Group Executive Board must ensure compliance in connection with the ongoing follow-up on compliance with the Security Policy.

3. Organisation and responsibilities

The Group Executive Board has the overall responsibility for compliance with the Security Policy and must ensure that the organisation supports the Security Policy by establishing clear guidelines, showing visible commitment and by clearly delegating responsibility. The Group Executive Board must secure sufficient staffing of the Security Function and that this function consists of qualified employees reflecting the Group's needs.

At least one member of the Group Executive Board must possess the necessary IT professional competence and knowledge within IT security to secure implementation and to make necessary decisions about the maintenance of IT security in the Group.

The Group Executive Board has appointed an officer responsible for IT security, including an IT Security Function and empowered this function, independent of organisational level, to enforce the Security Policy.

The Jyske Bank Group uses a "Three Lines Model" to secure that the Security Policy is adhered to and that IT operational risks are handled and monitored. This takes place through several organisational functions in the Group.

- The first line is made up of the line organisation and especially the organisational functions that relate to information processing, operations and IT development. It is the responsibility of the first line to identify, assess and handle risks when detecting them. The first line also includes the IT Security Function, which monitors compliance with the IT security level and whether the Group stays within the risk tolerance for IT operational risks. The first line prepares reports about and recommendations for activities that support compliance with the Security Policy.
- The second line is made up of the Risk Management Function and the Compliance Function.

The Risk Management Function monitors compliance with the overall risk level, including IT operational risks. As regards monitoring of the risk level of IT operational risks, the Security Function also refers to the Risk Management Function, which must ensure that risk controls can be defined and performed independently. Hence, the Risk Management Function can define requirements of the Security Function as regards the performance of risk controls. The Security Function must perform these irrespective of the organisational affiliation with the first line.
The Compliance Function also performs control activity in respect of legislation on IT security. The Compliance Function and the Risk Management Function must prepare reports on IT security according to "Policy of the Compliance Function of the Jyske Bank Group" and "Group Operational Risk Policy".

- The third line is made up by Internal Audit, which is responsible for performing an independent audit of the overall handling of risks and the internal controls in the Group - and for reporting its work to the Group Supervisory Board.

4. IT risk management

The Group's exposure to IT operational risk must be monitored and reported to management. The handling of IT operational risks must adhere to and support the Group's guidelines for the handling of operational risks across the Group. Management of IT operational risks is subject to the Group's Operational Risk Policy, including risk targets and risk appetite.

The IT Security Function is responsible for assisting the organisation, identifying IT risks, assessing security measures and controls as well as quality assurance of the individual sub-elements of the IT risk assessments so they comply with the guidelines described in the Group's operational risk policy.

To ensure the highest degree of efficiency and coherence in the work across the areas, the IT Area Manager shall on an ongoing basis coordinate the risk-management efforts with the Group's chief risk officer and the operational risk management function.

5. Data protection

The data processed by the Group consists to a great extent of confidential data, including customer and personal data. The majority of these data originates from customers, while a smaller proportion originates from employees and other groups. The processing of confidential data in a group of the size of Jyske Bank entails a risk that data may be processed incorrectly and that data may be disclosed to unauthorised persons and possibly be exploited by such persons.

To minimise the risk of confidential data being processed in any unintended manner, the Group works on the basis of fundamental principles for processing and protecting confidential customer and personal data.

- Legality, reasonableness and transparency: The processing must be based on the principles of legality, reasonableness and transparency.

- Limitation of purpose: In particular when collecting and processing personal data, the reasoned purpose of the use of the data must be clearly defined.
- Data minimisation: Wherever possible, the processing and storage of personal data in particular will be limited to what is necessary to meet the purpose of the processing in question.
- Correctness: Customer and personal data are updated continuously, and incorrect data are deleted or rectified.
- Limitation to storage: Personal data in particular are subject to storage limitation and are only stored as long as needed in relation to the purposes of our collection and processing.
- Integrity and confidentiality: Confidential data that are processed by the Group must not be disclosed to unauthorised persons, be lost or be damaged. Applicable data protection and privacy legislation is incorporated into the Group's guidelines, business procedures and processes based on a low risk tolerance for breaches of the Group's security of the processing in line with the ambition set for the Group's digital operational resilience level. Processes and security measures are continuously being optimised in order to minimise risks.

The IT Security Function, including the DPO, supports the Group's compliance with obligations under data protection and privacy legislation through reporting, providing advice and monitoring.

6. Management of third-party risks

When entering into contractual arrangements with third party providers and their subcontractors, if any, for the use of ICT services, the IT security level of the Group shall be maintained. This means that the security principles of the Security Policy must be adhered to. Moreover, in case of outsourcing it must be assessed whether the targets and objectives for compliance with the IT Security Policy can be met.
Third-party ICT service providers supporting a critical or important function must comply with the latest and highest security standards.

All contractual arrangements for the use of ICT services must be recorded, including which services support critical or important functions.
Special attention should be paid to managing potential security incidents and risks in relation to suppliers and third-party ICT services on which critical or important functions are significantly dependent. Likewise, as regards security, the supplier must be assessed in respect of responsibility and ability to maintain the level of security adopted by the Group. Risks and necessary measures must be identified through a security assessment and a risk assessment.

7. Security Principles

The Security Policy is supported by a series of security principles, which must be elaborated on in supplementary guidelines and business procedures. The most important principles for adhering to this policy are described below:

7.1. Awareness

Ongoing information and training of the Group's employees in the area of ICT security and digital operational resilience as well as protection of personal data will ensure a sustainable security culture. An assessment must be made of targeted IT security training of employees who work with activities associated with risks, including third-party providers. To limit security risks, awareness information and awareness activities must also enable users of the Group's digital solutions to use these in a secure way.

7.2. Segregation of duties

Segregation of duties must be implemented and monitored to a sufficient degree to ensure segregation of IT operations, systems development and conduct of business. Segregations of duties must ensure minimisation of risks associated with individual functions or persons who perform material acts that may compromise security.

Segregation of duties is implemented primarily through organisational structures and segregated organisational functions. Moreover, implementation takes place by segregation of access to systems that may result in large losses due to wrong usage.

7.3. Risk assessment and security level

Risk assessments must have been carried out to form the basis of central assessments and decisions, and also, risk assessments of ICT systems that are material to the critical functions must have been carried out. As part of the risk assessment activities, business processes must have implemented assessments of consequences to support the preparation of the Group's risk profile, and ICT systems must be sufficiently assessed as regards vulnerability. This applies in particular to ICT systems that are necessary to support critical functions. There must be sufficient total registration of the correlation between critical functions, business processes and supportive material ICT systems.
Among other things, the security of as well as the risk associated with new ICT systems that support the Group's critical functions must be assessed before they are put into operation.

The risk assessments must offer a sufficient overview of IT operational risks as well as of preventive controls and security measures.

Data sources offering insight into IT risks must be identified and included as part of the risk assessments so that the IT risk management process can continuously be updated on the basis of actual errors, problems and vulnerabilities.

7.4. Protection of ICT assets

ICT assets must to a satisfactory extent be identified and protected against physical and logical threats. This applies in particular to cyber threats and threats that may result in defective ICT assets, which will have significant consequences for customers, employees, business partners and

other persons registered at the Group.

Security assessments and risk assessments must be performed to identify whether ICT assets are protected to a sufficient degree considering the Group's risk appetite and according to legislation on protection of data, where risks relating to the data subject (the individual) must be assessed.

The operation and efficiency of the material measures for the protection of ICT assets must be maintained and to a material degree be verified.

ICT assets must be secured by sufficient logical and physical arrangements.

7.5. Access to data and ICT systems

Access rights must be justified by work-related requirements, must as far as possible be role-based and must be able to be monitored and logged in such a way that tracking and investigation in connection with security breaches can be carried out to a satisfactory extent.

Privileged users must be subject to special restrictions compared to general users.

Classification models must exist for systems and data to give a sufficient overview of the most material ICT assets and access to these.

7.6. System development and maintenance of ICT systems

Procedures must be in existence to secure that risks associated with development, protection of personal data, configuration and maintenance of new and changed ICT systems are identified, assessed and handled.

Procedures for managing changes must be available in such a form that material changes and material risks relating to changes and implementation are identified, assessed and handled pro-actively as an integral part of the development phase and are tested before being realised in production.

The need for a two-step approval process is assessed in connection with the application of processes that are subject to the principles of segregation of duties.

It is a requirement that as a minimum, documentation is prepared and maintained for all ICT systems supporting critical functions and configurations, and that changes to these are assessed in relation to risk and documented in a way that will ensure traceability.

7.7. Operational management.

At any time, sufficient IT resources must be procured to maintain secure operations; such

resources include personnel, hardware and facilities.

Operations must take place according to the requirements stated in this Security Policy as well as supporting method descriptions, policies, guidelines and business procedures.

7.8. Backup

Backup must be made of ICT systems and data.

The backup frequency for ICT systems and data must be based on RTO and RPO requirements as well as the classification of the data.

Backups of systems and data must be stored securely and be unavailable to unauthorised persons and users. Logic and physical segregation of duties must be ensured in relation to the backup environment.

The backup environment must be robust to cyber attacks and must be monitored and tested for security with a view to detecting errors and deviations.

7.9. Disaster recovery

The objective of the disaster recovery must, as a minimum, be stated in the Policy for ICT Operational Stability.

The objective of the disaster recovery shall include the objectives for the re-establishment of normal operations in the event of errors, crashes, loss of data or ICT systems as well as destruction in part or in full of premises, equipment and routes of communication.
The objective of the disaster recovery must also relate to extreme, yet plausible scenarios.

The IT disaster recovery plan must describe how the disaster recovery/emergency organisation is made up and in which cases it must be convened.

The IT disaster recovery plan is to be supported by BCPs securing that operations of critical functions can be maintained to an acceptable degree in the event of system crashes, errors and disruption of the use of IT.

To a predominant degree, ICT systems and data supporting critical functions must be supported by multi-centre operations so that accessibility is secured in the event of a crash at a data centre.

On the basis of a risk assessment, it must be determined that the logical distance and geographic distance between the operations centres are sufficient to ensure that an ICT-related incident that puts one operations centre out of operation will not affect other operations centres at the same time. The current evaluation of the data centres used by the Jyske Bank Group is considered

acceptable to encounter ICT-related incidents that may arise on the basis of current circumstances relating to infrastructure, weather conditions, politics and technology.

Regular disaster recovery tests and exercises of the IT disaster recovery plan must be held, both internally and in cooperation with material suppliers.
Experience from disaster recovery tests and exercises shall be included as data sources providing input to the IT risk management, including the determination and evaluation of control and security measures.

Rules for reporting on disaster recovery incidents, tests and exercises must be established. Disaster recovery incidents, tests and exercises must be reported to the Group's Supervisory Boards and the Executive Boards.

The Group's Supervisory Board must approve the Policy for ICT Operational Stability in the event of material changes and at least once a year to ensure that it is in line with the Group's risk appetite.

7.10. Security tests

Based on the biggest risks for the Group, security tests must be performed for the relevant most critical arrangements. The extent of the tests and the arrangements that are to be tested must be prioritised based on the way in which the Group has chosen to manage risks. By this is meant that if a risk scenario depends materially on preventive measures, testing of these may be more important than rectifying measures.

As a minimum, security tests of all ICT systems and applications that support critical or important functions must be performed at least once a year, and threat-based penetration tests (TLPT) every 3 years. The extent of the testing activity may vary based on threat scenario and risk level. Other systems must be tested within a 3-year period.

Since the Group uses important IT components, supporting critical and important functions that have been outsourced, security tests hereof must also be considered, and it must be ensured that it is possible to execute them where deemed necessary.

7.11. ICT incident and problem management

Efficient procedures for ICT-related incident and problem management must be defined to ensure that IT risks and consequences for at least critical functions are identified, assessed and handled and incorporated as data sources in the risk management process.
All ICT-related incidents must be recorded.
Efficient communication and reporting about IT security incidents must ensure fast and efficient handling, so that any impact on the business conduct is minimised as much as possible.

Reasons for IT security incidents must be identified and eliminated so that repetitions are avoided. Major ICT-related incidents must be reported to the Centre for Cybersecurity (Center for Cybersikkerhed) and the Danish FSA (Finanstilsynet).

7.12. Logging and monitoring

Procedures must be prepared for risk-based logging of user activities, exemptions, errors, ICT related incidents and critical IT operations. Risk-based monitoring as well as examination of logs must be established.
Logging and monitoring of critical IT operations as well as activities performed by privileged users must be prioritised.

Ongoing monitoring of critical business functions, IT administration, potential internal and external threats, as well as monitoring to reveal internal or third parties' abuse of access must be established.

7.13. ICT security of project management

The Group's method for managing IT projects must enable identification and assessment of risks before they materialise.
In connection with IT projects that may result in changes to the risk profile for the Group, the IT Security Function must be involved and be consulted to ensure that the requirements of the Security Policy are complied with. If, as a result of the IT project, high risks materialise, the Risk Management Function must be involved with a view to assessing whether the Group's risk tolerance is exceeded.

7.14. Quality assurance

Procedures must be prepared to ensure sufficient quality assurance of risk assessments, changes and the general application of IT.

The quality assurance must be documented and logged to an extent that facilitates detection and troubleshooting relating to access control, change management, risk assessments and security breaches.

7.15. Violation of ICT Security Policy and security rules

In the event of serious breaches of the Security Policy, the Group's Executive Boards and the Supervisory Boards must be informed and a response matching the extent of the breach must be undertaken.

Measures and sanctions in the event of a breach of the Security Policy as well as supporting guidelines and business procedures must be recorded in writing.

7.16. Reporting, control and follow-up

Operational and verification controls in the 1st and 2nd lines must be implemented and maintained in order to ensure that the IT security level is acceptable and matches the current threat and risk landscape.

On an on-going basis, follow-up must be undertaken to ascertain whether, to a sufficient degree,

the Security Policy and its supporting frameworks, method descriptions, guidelines and business procedures ensure that the desired IT security level is maintained.

Reports on the IT security level must on an on-going basis be submitted to the Group's Executive Boards and the Supervisory Boards.

7.17. Exemptions from the ICT Security Policy

A centralised and documented exemption management process must be established to ensure structured and organised logging of exemptions from the Security Policy, its principles or the underlying guidelines and business procedures.

Exemptions must be granted on a risk-based approach and must always be limited in time.

Exemptions in relation to the Security Policy, its principles or underlying guidelines can be granted by the Group's Supervisory Board and Executive Board and by the head of the Security Function. Exemptions from the underlying business procedures can be granted by executive employees in the Security Function.

Exemptions must always be approved by the person(s) assuming the responsibility for the risk associated with the exemption.

The Security Function is responsible for the processing of applications for exemptions, which also entails responsibility for ascertaining that applications include a sufficient risk assessment so decisions can be made on an informed basis.

Reporting on exemptions is handled by the Security Function.

7.18. Use of artificial intelligence (AI)

The Group must use artificial intelligence (AI) in a safe and responsible manner.

AI systems must support the Group's strategy without compromising information security, data protection, data ethics, and customer trust.

A restrictive approach to AI development has been adopted in the Group, with a focus on the responsible implementation of new technology in accordance with the AI Regulation and a heightened security focus on the use of AI solutions in connection with the Group's critical or important functions.

AI systems are risk assessed and classified in accordance with applicable external and internal requirements, and appropriate technical and organisational measures are established to ensure transparency, resilience, and human control. The use of external AI services is monitored and may only take place where it is commercially justified and security-wise sound, and in accordance with the Group's guidelines for handling third-party risks.

8. Approval of ICT Security Policy

This policy was received by

The Group Executive Board of Jyske Bank A/S Silkeborg, on 25.11.2025

Lars Mørch

Erik Gadeberg

Ingjerd Blekeli Spiten

Peter Schleidt

Jacob Gyntelberg

This policy has been approved by

The Group Supervisory Board of Jyske Bank A/S Silkeborg, on 25.11.2025

Kurt Bligaard Pedersen

Anker Laden-Andersen

Rina Asmussen

Lisbeth Holm

Birgitte Haurum

Bente Overgaard

Per Schnack

Glenn Söderholm

Henriette Hoffmann

Marianne Lillevang

Michael C. Mariegaard