IT Security Policy

Contents

1. Purpose and scope

The purpose of this IT Security Policy (hereinafter the security policy) is to ensure that a high level of IT security is implemented and maintained in the Jyske Bank 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 security profile for in the IT area can be adhered to.

2. IT security level

The IT security level must be based on the Jyske Bank Group's ambition to obtain and to maintain a level of security that is sufficient to handle the current cyber threat with elements that are 'best in class'. In addition, the security level must ensure that the risks that are involved in connection with and expected to be involved in connection with the IT use are adjusted to the Jyske Bank Group's risk tolerance for the area.
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 robustness of Jyske Bank Group's IT systems and its use of IT must be secured in order to ensure stable operations of the Group's business processes and to secure cyber robustness as efficient protection against cyberattacks from threatening players who are highly organised and launch sophisticated attacks.

The security policy must be supplemented with a strategy that describes how to attain the IT security level. In addition, the security policy must be elaborated on through supporting descriptions of methods, frameworks, guidelines and business procedures detailing how the requirements herein are to be operationalized.

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

The security policy must be approved by Jyske Bank's Group Supervisory Board at least once a year or in connection with material changes that require revision.

3. Organisation and responsibilities

The 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 Jyske Bank Group uses a three lines of defence 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 second line is made up primarily of the security department (IT Security and Risk Management), which monitors compliance of the IT security level and the risk level for IT operational risks. As regards monitoring of the risk level of IT operational risks, the security department also refers to the risk management function, which must ensure that risk controls can be defined and performed independently. Hence the risk management function defines for the security department the requirements of the performance of risk controls. The compliance function (Compliance) and the risk management function (Risk Management) also handle second line responsibilities in respect of control, monitoring and reporting of IT operational risks, as there is a high degree of correlation between the security policy, "Compliance policy" and "the Jyske Bank 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 Supervisory Board.

4. IT risk management

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

IT Security and Risk Management is responsible for assisting the organisation identifying IT risks, assessing control 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 Jyske Bank Group Operational risk policy.

To ensure the highest degree of efficiency and coherence in the work across the areas, the IT resort director shall on an ongoing basis coordinate the risk-management efforts with the group chief risk officer and the operational risk function.

5. Data protection

The Jyske Bank Group's activities depend on the handling of personal data, both regular data and sensitive data. The majority of the data consists of ordinary data, but a large part of these is confidential data what must not come to the knowledge of unauthorised persons or the public. Of the personal data that the Jyske Bank Group processes, the largest part relate to clients, while only a small part relate to employees and other groups.

Processing of the extent stated above will often imply a strong inherent risk that personal data are processed incorrectly, which may result in wrong decisions or that personal data may be disclosed to unauthorised persons and hence result in violation of the registered person's rights.

To reduce the inherent high risk related to the handling of registered personal data, the following principles and measures must be adhered to when processing personal data:

- **Data are on loan:** Personal data must not be shared with unauthorised persons, must be treated respectfully and must be returned in the same or a better condition than the one in which they were received. Hence personal data are not owned by the Jyske Bank Group, but something we borrow from the clients/employees, etc.
- **Risk-based approach:** On the basis of which risks the registered person is exposed to, a risk assessment must be carried out of any type of processing of personal data, and the sufficient, and necessary security measures as well as precautions must established, so the risks in question are reduced to an acceptable level. When this is not possible, the processing must stop.
- **Awareness**: All employees who gain knowledge of personal data must receive training and instruction in how to process personal data.
- **Overview**: An overview must be in existence of where in our internal environments personal data are stored and for which purposes personal data are used. Also, an overview must be in existence of which data processors and sub-processors process personal data on behalf of the Jyske Bank Group.
- **Data minimisation:** Only data that are necessary in order to fulfil the purpose of any given processing activity must be collected and processed, and also it must be made clear to the registered person why the specific data must be collected. When personal data are no longer necessary data, they must be anonymized or deleted..
- **Confidentiality**: Personal data must only be accessible to authorised persons, and sufficient and necessary security measures must be established to ensure that unauthorised persons cannot access the personal data. This applies to both internal and external threats.
- **Integrity:** Personal data must be correct, and it must not be possible for unauthorised persons modify these.
- **Accessibility:** Personal data must be accessible for the purposes for which they have been collected.
- **Privacy by design**: All systems and processes, future as well as existing ones, must be arranged/prepared in such a way that they comply with these principles and the guidelines of the Danish Data Protection Agency.
- **Control of confidence:** Efficient controls must be carried out to ensure:
  - that the employees' handling of personal data comply with the above principles;
  - that systems and processes are designed with focus on privacy by design;
  - that suppliers comply with the same principles and maintain a sufficient security level as regards protection of the personal data they process on behalf of Jyske Bank.
- **Rectifying measures:** Necessary and relevant measures must be established to rectify the personal data breaches that will unavoidably take place.

The above principles must be implemented in the Jyske Bank Group's guidelines to comply with the security policy.

6. Outsourcing

In connection with outsourcing, including further outsourcing, to external suppliers, the IT security level for Jyske Bank must be maintained. This means , that the security principles of the security policy must be adhered to.
Any outsourcing, of material as well as non-material activity areas, must be registered centrally so continuous control can be performed of the suppliers' IT security level.

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 IT security and 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.

7.2. Segregation of duties

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

7.3. Risk assessment

Risk assessments must have been carried out to form the basis of central assessments and decisions, and also, risk assessments of systems that are material to the bank's operations must have been carried out. New systems must be subjected to a risk assessment before being 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 weaknesses.

7.4. Protection of IT assets

IT 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 IT assets, which will have significant consequences for clients, employees, business partners and other persons registered at the Jyske Bank Group.

Security assessments and risk assessments must be performed to identify whether IT assets are protected to a sufficient degree considering the Group's risk appetite and according to legislation on protection of personal 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 IT assets must be maintained and to a material degree be verified.

IT assets must be secured by sufficient logical and physical access controls.

7.5. Access to data and 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 IT assets and access to these.

7.6. System development and maintenance of systems

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

Procedures for managing changes must be available in such a form that material changes and risks relating to changes and implementation are identified, assessed and handled proactively 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 documentation is prepared and maintained for all material systems 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.

Procedures for incident management and problem solving must ensure that IT risks are identified, assessed and handled and incorporated as data sources in the risk management process.

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 systems and data.

The backup frequency for systems and data must be based on risk assessments relating to their classification.

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

7.9. Disaster recovery

The objective of the disaster recovery must, at the minimum, be stated in the disaster recovery plan.

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 systems as well as destruction in part or in full of premises, equipment and routes of communication.

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 business-critical processes 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, business-critical systems and data 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 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 events and 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 Supervisory Board and the Executive Board of Jyske Bank.

The Supervisory Board of Jyske Bank must approve the disaster recovery objective 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. 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.

7.11. Breach of security policy and security rules

In the event of serious breaches of the security policy, the Executive Board and the Supervisory Board 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 method descriptions, frameworks, guidelines and business procedures must be recorded in writing.

7.12. Reporting, control and follow-up

Operational and verification controls in the first and second 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 Executive Board and the Supervisory Board.

7.13. Exemptions from the 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 Supervisory Board, by members of the Executive Board and by the head of IT Security and Risk Management. Exemptions from the underlying business procedures can be granted by the head of IT Security and Risk Management.

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

IT Security and Risk Management 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 IT Security and Risk Management.

8. Approval of the IT security policy

This policy has been received by

The Group Executive Board of Jyske Bank A/S
Silkeborg , 26.01.2021

Anders Dam

Niels Erik Jakobsen

Peter Schleidt

Per Skovhus

This policy has been approved by

The Group Supervisory Board of Jyske Bank A/S
Silkeborg, 26.01.2021

Kurt Bligaard Pedersen	Philip Baruch	Rina Asmussen
Jens A. Borup	Anker Laden-Andersen	Keld Norup
Bente Overgaard	Per Schnack	
Johnny Christensen	Marianne Lillevang Jensen	Christina Lykke Munk