Security Policy

1. Objective

The objective of the Security Policy (the “Policy”) is to set control requirements for the management of Information Technology (IT) & Security risks in the NordBank (the “Group”).

The Group is exposed to risk relating to the security of assets and people. Systematic and coordinated management of these risks is essential for protecting the interests of the Group’s customers and stakeholders, and for meeting applicable regulatory requirements. The aim is to achieve specific objectives on information security, in line with business objectives. The EU and Danish regulatory requirements in-scope of this Policy are documented in Appendix A.

The failure to comply with the Security Policy is a serious violation and may lead to action being taken in accordance with the applicable employment regulation, including but not limited to warning, redundancy, suspension or dismissal.

2. Scope

The Policy covers requirements to be implemented in order to mitigate IT and Security Risks and comply with business objectives and applicable regulatory requirements. In scope of this policy is risk of loss due to breach of confidentiality, lack of authenticity, failure of integrity of systems and data, or unavailability of systems and data. In addition, this includes risks related to damage of physical assets and security of people. Risk mitigation in the context of managing initiatives (i.e. projects) related to technology is addressed in the IT Risk Management Policy.

Requirements in this Policy are supplemented by controls specific to business continuity management and data management (including privacy), as outlined in the Business Continuity & Crisis Management Policy and Data Risk Management Policy, as well as in appropriate governing information. Furthermore, principles of the Security Policy should be applied in a third party management context as outlined in the Non-Financial Risk Policy and its instructions.

2.1. Target group

This Policy is relevant for all employees across the Group, including employees who own assets who are responsible for implementing instructions and procedures, including but not limited to System Owners and Service Owners, and employees within Technology and Services organisation who are responsible for defining instructions and procedures by which the principles of this Policy should be implemented.

The Management Body of a subsidiary may approve this Policy with deviations to ensure the Policy is fit for purpose for the subsidiary. The policy administrator in the subsidiary should discuss the rationale behind the deviation and ensure that the administrator of the Group Policy is consulted on any deviation.

The administrator of this Policy must document and report any deviations from the Policy to the Executive Leadership Team of NordBank. The Executive Leadership Team shall report all material deviations from Group Policies to the Board of Directors of NordBank.

3. Policy Content

Principle 1 IT and Security risks must be addressed through a control framework

Instructions, business procedures and standard operating procedures must be documented or supported in an online repository detailing controls to be implemented to mitigate IT & security risks.

Controls must be identified based on the control requirements detailed in this Policy and applicable regulatory requirements.

Controls must be designed to address the IT and Security risks per the ERM taxonomy.

Quantity and skills of resources must be adequate to support implementation of security controls.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of policy and regulatory requirements related to IT and Security Risk, including ensuring sufficient resources*

➢ *The ELT is accountable for delegating subject matter expert responsibilities for implementation, including the mandate of the SME for assigning specific responsibilities*

➢ *The Security Function is responsible for designing and implementing a control framework for IT and Security Risk*

➢ *The Security Function is responsible for ensuring an appropriate level of control for IT and Security Risk*

➢ *The Security Function is responsible for demonstrating and reporting adherence both to the Policy and to relevant regulatory requirements related to IT and Security Risk*

➢ *Subject matter experts, as delegated by the responsible ELT member, are responsible for defining implementation and operational responsibilities, standards and processes for their respective areas through governing information*

➢ *Subject matter experts, as delegated by the responsible ELT member, are responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *Non-Financial Risk (NFR) is responsible for providing relevant risk based monitoring and control of the control framework, including instructions, procedures and control management activities against policy and regulatory requirements*

➢ *NFR and Group Compliance (GC) are responsible for identifying in-scope regulations, providing guidance on how compliance with those regulations should be met through implementation activity, and relevant risk based monitoring and control of compliance reporting*

➢ *Group Internal Audit (GIA) is responsible for evaluating the effectiveness of the processes used for risk management, controls, and governance*

Principle 2 Due care must be taken for the safety and security of employees

Subprinciple 2.1 The duty of care towards employees in general must comply with local regulations and reflect industry standards.

Employees that face elevated and foreseeable physical or psychological risks must be offered training and tools to manage those risks and provided the necessary support and help to address identified risks and concerns.

Subprinciple 2.2 Employees and their property shall be protected and safeguarded during work and work-related travel

Employees shall be provided appropriate tools to anticipate, prepare, and mitigate relevant risks prior to and during work-related travel.

Subprinciple 2.3 Employees who have been a target of crime, physical or psychological harm or threats in their line of work will be offered the necessary support

Employees must be offered the necessary support following an incident at work or in relation to their work or work-related travel.

Roles and Responsibilities

The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

Principle 3 Suitable resources must be in place to perform IT and Security Risk management requirements

Security background checks must be undertaken against staff members relevant to their job function. All employees must undertake security trainings relevant to their job function, promoting a culture of IT and Security Risk as everyone's responsibilities and ensuring employees understand responsibilities and procedures related to IT and Security Risk. Training must be conducted on an annual basis, or more frequently, as required to address human error, theft, fraud, misuse and related IT and security risks. Resources are sufficient and appropriate to support IT and Security Risk Management processes and Strategy implementation.

Roles and Responsibilities

➢ *The ELT should ensure that the quantity and skills of financial institutions' staff is adequate to support IT operational needs, IT and security risk management processes on an ongoing basis and to ensure the implementation of IT strategy*

➢ *The ELT should ensure that the allocated resource (including budget) is appropriate to fulfil the above*

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities (including the provision of training and awareness of IT and security risk management practices), along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

➢ *All employees are responsible for undertaking security training relevant to their job function*

Principle 4 Assets must be managed to protect from damage, disclosure, loss or fraudulent use

Subprinciple 4.1 A comprehensive, accurate and up-to-date asset inventory must be maintained

The asset inventory must be sufficiently detailed to enable the prompt identification of an asset, its location, classification and ownership. The asset inventory must store the configuration of the assets and the links and interdependencies between the different assets.

Subprinciple 4.2 Asset mapping

Assets must be mapped to business functions and supporting processes and an up to date overview is maintained at a minimum for critical business functions

Subprinciple 4.3 Assets maintained in the inventory must have an asset owner

Asset owners must be designated to ensure proper management of an asset over the entire asset lifecycle. Assets owners must be periodically reviewed for appropriateness and re-established as necessary.

Subprinciple 4.4 Asset must be monitored to ensure they are supported and within policy compliance requirements.

Acceptable use of assets must be identified, documented and defined, and compliance monitored, including continuation of support by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes . In order to prevent unauthorised disclosure, modification, removal or destruction of assets, these must be handled in accordance to their specification or classification, purpose, level of confidentiality, and legal, contractual and license requirements.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

Principle 5 Information must be classified and managed in accordance with Information classification

Subprinciple 5.1 Information and media must be appropriately classified

Classifications of information and media must be based on business, security and regulatory requirements.

Subprinciple 5.2 Information must be managed according to its Information classification

Information and media must be processed and handled in accordance to their classification. An information management process must be defined and maintained detailing appropriate ownership, control, and use based on its classification

Roles and Responsibilities

➢ *NFR is responsible for developing, reviewing and updating the Information Classification Taxonomy and detailing roles and responsibilities for the classification of information*

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *All employees are responsible for classifying and managing information in line with associated instructions*

Principle 6 Unauthorised logical access to assets must be prevented and detected

Subprinciple 6.1 Access rights must be managed based on the principles of least privilege and segregation of duties

An account should hold the minimum access rights that are strictly required to execute their duties i.e. principle of ‘least privilege’, or to prevent the allocation of access rights that may be used to circumvent controls i.e. principle of segregation of duties.

Subprinciple 6.2 The use of shared accounts must be controlled

All use of shared accounts must be restricted and ensure that users who have performed actions in the IT systems can be identified.

Subprinciple 6.3 Privileged access rights must be limited

Privileged system access must be implemented with strong controls to strictly limit and closely supervise accounts with elevated system access entitlements (e.g. administrator accounts). Privileged account access must be protected and managed using a privilege access management tool.

Subprinciple 6.4 User activity must be logged and monitored for all IT assets

All users must be logged and monitored against breach of access right principles defined in 6.1, at a minimum, all cases of privileged access must be logged and monitored. Access logs must be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and IT assets.

Subprinciple 6.5 Access rights must be granted, withdrawn and modified in a timely manner

Access rights must be granted, withdrawn and modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed. In the case of termination or role change, access rights should be withdrawn in a timely manner. Temporary elevated access required for the performance of emergency changes must be appropriately authorised, documented and revoked in a timely manner.

Subprinciple 6.6 Access rights must be periodically reviewed

Access rights must be periodically reviewed by business personnel to ensure that user access is maintained in accordance with the principles outlined in Subprinciple7.1. Access rights identified as part of the review as conflicting with these principles must be withdrawn in a timely manner. The business personnel performing the review must be independent and must not review their own access as part of the review.

Subprinciple 6.7 Authentication methods must be commensurate with the criticality of systems

Robust authentication methods must be established to ensure that access control policies and procedures are complied with. Authentication methods used should be commensurate with the criticality of systems, information or the process being accessed. This must, at a minimum, include complex passwords or stronger authentication methods (such as two-factor authentication), based on the identified risk.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

Principle 7 Unauthorised physical access to assets and premises must be prevented and detected

Subprinciple 7.1 Appropriate physical countermeasures, preventive and detective procedures must be implemented and maintained

Physical security measures must be defined, documented and implemented to protect premises, data centres and sensitive areas from unauthorised access and from climate and environmental hazards.

What measures and procedures are appropriate must be determined based on the risk of unauthorised access and the level of sensitivity, criticality, and value of the premises, information residing in it and safety of individuals.

Subprinciple 7.2 Physical access to assets must be permitted to only authorised individuals.

Authorisation must be assigned in accordance with the individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access rights are promptly revoked w hen not required.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

Principle 8 Measures must be implemented to prevent the occurrence of security incidents

Subprinciple 8.1 Identification of Vulnerabilities.

Potential vulnerabilities must be assessed and remedied considering the IT and security risk and other risks associated with the change, including by ensuring that software and firmware are up to date. This applies to software used by both the undertaking's internal and external users.

Subprinciple 8.2 Security controls must meet the requirements set in the secure configuration baseline

Requirements for a minimum-security baseline configuration must be established and reviewed to ensure all IT System and Network assets have implemented a consistent and secure set of security controls.

Subprinciple 8.3 Network controls must be applied to protect IT assets and Information

Networks must be segmented to ensure critical IT assets within those segments are secure and accessed on principle of least privilege. Data loss prevention systems must be in place and the encryption of network traffic in accordance with the Information Classification.

Subprinciple 8.4 Endpoints must be secured to protect IT assets

Requirements and procedures must be established and reviewed to evaluate all endpoints including servers, workstations and mobile devices in the corporate network are secure and have uniform security controls implemented to protect end users, corporate network, IT assets and data.

Subprinciple 8.5 Mechanisms must be in place to verify the integrity of software, firmware and data.

Requirements and procedures must be in place to verify the integrity of software, firmware and data.

Subprinciple 8.6 Data at rest and data in transit must be encrypted

Requirements and procedures must be implemented and reviewed periodically to ensure appropriate encryption techniques are implemented to protect the authenticity, confidentiality, integrity and unauthorised access to data at rest and in-transit, in accordance with Information Classification requirements

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

Principle 9 Measures must be implemented to detect and mitigate against threats and vulnerabilities

Subprinciple 9.1 Measures for detecting unauthorised access and breaches of confidentiality, integrity and availability of assets must be implemented

Processes must be defined to identify, protect and detect security anomalies, report security incidents in timely manner in order to ensure security threats are mitigated and minimised. Logs must be captured and maintained to support activities such as anomaly detection.

Subprinciple 9.2 Processes must be implemented to provide appropriate and effective capabilities for continuously detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity, availability and authenticity of the information assets.

Subprinciple 9.3 Processes must be implemented and organisation structures established to identify and continuously monitor security threats that could materially affect their abilities to provide services.

Subprinciple 9.4 Security reviews, assessment and testing must be undertaken to identify threats and vulnerabilities

A security review, assessment and testing framework must be established to validate the effectiveness of security measures. For instance, gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews must be performed periodically. Security tests should be carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures, and include vulnerability scans and penetration tests commensurate to the level of risk identified. This includes consideration of Threat-Led Penetration Testing(TLPT).

Subprinciple 9.5 Threats and vulnerabilities must be identified, evaluated and remediated

Threats and vulnerabilities identified through security reviews must be evaluated and remediated through implementing critical security patches or other mitigating controls.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

Principle 10 IT and Security Incidents must be identified, prioritised and remediated in a consistent manner to enable resumption of business activity

Subprinciple 10.1 Incident and problem management

An incident and problem management process must be implemented to identify, monitor and log IT and Security incidents.

Subprinciple 10.2 Security Incidents must be identified, assessed, categorised and remediated

Security Incidents must be identified, assessed, categorised and remediated according to a priority based on criticality.

Subprinciple 10.3 Roles and responsibilities for different incident scenarios must be documented and communicated

Security Incident response plans must be drafted and communicated to required stakeholders detailing roles and responsibilities based on different scenarios. Response plans must be updated on a periodic basis to take into account new scenarios based on the threat landscape.

Subprinciple 10.4 Internal and external communication plans must be developed and executed

Internal communication plans, including incident notification and escalation procedures, must be documented and executed following an incident to alert senior management to incidents and ensure resource is dedicated to remediation. Timely information must be provided to external parties as appropriate and in line with applicable regulation.

Subprinciple 10.5 Root causes must be identified and remediated to minimise reoccurrence of security incidents

Root causes analysis and remediation, including Problem Management, must enable the identification, analysis and solving of the root cause behind one or more Security Incidents. Lessons learned from these analyses must be updated in security measures accordingly.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

Principle 11 IT system performance and capacity must be monitored to prevent, detect and respond to issues

Performance of IT systems must be managed to align to business requirements. Performance and capacity planning and monitoring processes must be implemented to prevent, detect and respond to important performance issues of systems and capacity shortages in a timely manner.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

Principle 12 IT Changes must be recorded, assessed, approved and verified in a controlled manner

Subprinciple 12.1 IT Changes must be requested, categorised and prioritised

IT Changes must be requested and include change criticality, type, rating and business rational and prioritised accordingly.

Subprinciple 12.2 IT Changes must be reviewed and approved

IT Changes are approved by appropriate levels of management based on risk and impact levels and business need.

Subprinciple 12.3 IT Changes must be implemented in a controlled manner

IT Changes must be implemented in a manner which meets the Security Policy and regulatory requirements. Changes must be tested prior to release.

Subprinciple 12.4 Adequate safeguards must be established for emergency changes

All emergency and critical changes must follow a defined process for raising, testing, documenting, assessing and approving the change that allows for prioritisation whilst maintaining security standards.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation* *and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas

➢ NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information

Principle 13 IT Service Continuity process must be implemented to provide acceptable level of service continuation following an event

The Group has a Business Continuity & Crisis Management (BCCM) Policy, that is enabled by the IT Service Continuity process, stating the requirements as well as roles and responsibilities associated with the continuity of business operations in the event of severe disruption impacting the Group. The BCCM Policy can be found on the Policy portal.

Subprinciple 13.1 IT systems and services must be impact assessed

Service impact analysis must be conducted to understand exposure to severe service disruptions and assess potential impacts considering the criticality of the supporting business processes. Redundant infrastructure must be established for systems supporting critical business processes.

Subprinciple 13.2 Response and recovery plans must be developed

Service continuity plans must be designed incorporating recovery time objective and a recovery point objective. The response and recovery plans specify conditions for timely activation of service continuity plans and corresponding actions. Recovery plans must detail the requirement to establish multi-centre operations for all critical IT systems, and demonstrate sufficient distance between them in the event of an incident occurring.

Subprinciple 13.3 Response and recovery plans must be tested and updated on a periodic basis

Service continuity plans for critical business functions, supporting processes, Information and their interdependencies (including those provided by third parties, where applicable) must be tested and updated, at least annually.

Subprinciple 13.4 Data backup and recovery processes must be defined

The scope and frequency of backups must be set out in line with business recovery requirements and the criticality of the data and systems, and evaluated according to the performed risk assessment Backups must be tested periodically, stored securely and sufficiently remote from primary site.

Roles and Responsibilities

➢ The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents

➢ Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas

➢ NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information

Principle 14 IT assets must be protected during acquisition and development

Subprinciple 14.1 Security requirements must be defined and approved All applications must have documented functional and non-functional requirements considering the key business, security, performance and scalability needs. Functional and non-functional requirement must be translated into a high-level design specification for system acquisition, implementation and maintenance.

Subprinciple 14.2 Systems must be tested and approved prior to first use

A methodology must be developed for testing and approving systems based on the criticality of IT assets to ensure security control requirements are met. The testing must identify potential security weaknesses, policy violations and incidents.

Subprinciple 14.3 Environments must be segregated

The development, testing and other non-production environments must be segregated from the production environment. Controls must be in place to ensure adequate segregation of duties, governance of environments, and protection of authenticity, integrity and confidentiality of environments and mitigate the impact of unauthorised changes.

Interaction between environments requires at a minimum:

- Documented business justification and risk decision

Verification that controls are in place in non-production environments similar to controls in place in the production environment

- Governance to ensure that access to production data in non-production environments is granted under the same rules and requirements as set for the production environment, including consultation with the data owner
- Regulatory requirements which are specific to the use of production data in non-production environments must be adhered to during implementation, operation, and maintenance.

Subprinciple 14.4 Integrity of source code and configurations must be protected

Measures should be implemented to protect the integrity of the source code and configurations from malicious and un-intentional alteration.

Subprinciple 14.5 Processes for procurement and development of IT systems

Processes for the procurement and development of IT systems should also apply to IT systems developed or managed by the business function's end users outside the Technology & Services organisation (e.g. end user computing applications).

Any IT system that is procured by a business function including non-Technology & Services functions must be delivered into the NordBank environment by Technology & Services.

Subprinciple 14.6 Development standards must be applied to critical End User Computing applications

Development standards must also be applied to critical applications developed outside of Technology &

Services. A register of these applications that support critical business functions or processes must be maintained and security requirements applied.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *NFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

Principle 15 An IT Project Management and project governance process must be implemented that defines roles, responsibilities and accountabilities to effectively support the implementation of the IT strategy

Subprinciple 15.1 IT Project management procedure

The IT project management procedure must, as a minimum, include:

a) Project objectives.
b) Roles and responsibilities.
c) A project risk assessment.
d) A project plan, a time frame and the different steps.
e) Most important milestones.
f) Change management requirements.

Subprinciple 15.2 IT Security Requirements

The IT project management procedure must ensure that IT security requirements are analysed and approved by a function that is sufficiently independent and has the right competences.

Subprinciple 15.3 Status and reporting

The establishment and progress of IT projects and the derived risks must be reported depending on the importance and scope of the IT projects. The reporting must be done on a regular basis and when relevant. Project risks must be included in the risk management framework. The reports must be submitted to the board of directors to the relevant extent.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *MLNFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

➢ *Technology & Services deliver all procured technology into the Group's eco system except for EUCs which may be developed per this Policy by all organisation units*

➢ *Business and group functions must register all end user computing applications supporting critical business functions*

Principle 16 IT Operations Management – IT operates, monitors and controls IT systems and services

Subprinciple 16.1 Procedures

Procedures must define how the undertaking operates, monitors and controls IT systems and services, and must comprise documentation of critical IT operations and maintenance of the updated overview of IT assets.

Subprinciple 16.2 Performance

Ensure that performance of IT operations is aligned to business requirements. Maintain and improve, when possible, efficiency of IT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks.

Subprinciple 16.3 Logging and monitoring

Implement logging and monitoring procedures for critical IT operations to allow the detection, analysis and correction of errors.

Subprinciple 16.4 IT Asset Lifecycle

Monitor and manage the life cycles of IT assets, to ensure that they continue to meet and support business and risk management requirements. Monitor IT assets to ensure they are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported IT assets should be assessed and mitigated.

Roles and Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of security requirements and assigning a subject matter expert responsible for defining implementation and operational activities, along with responsibilities, including designing controls, standards and processes for their respective areas through governing documents*

➢ *Delegated subject matter expert is responsible for driving implementation and documenting compliance of security requirements for their respective areas*

➢ *MLNFR is responsible for providing relevant risk based monitoring and control over risk management including governing information*

5. Escalation

The owner of the Policy must report to Executive Management on significant breaches to the Policy.

Significant breaches include, but are not limited to:

- Failure to adhere to set tolerances
- Inappropriate or insufficient approvals
- Inappropriate or insufficient reporting
- Unmanaged changes in risk exposures

The owner of the Policy must escalate any breaches of the standards and requirements set in the Policy to the appropriate governing body, including if the maintenance of the Policy is not able to be completed in accordance with the governing document framework.

6. Review

This Policy must be revised when needed and at least annually.

Appendix A

The principles in the Security Policy are strongly aligned to applicable areas of the EBA guidelines for ICT and Security risk management and the Executive Order on Management and Controls of Banks, Annex. In addition, the principles in the Security Policy S

EU regulation:

- DORA EU – Digital Operational Resilience Act

GDPR EU 2016-679

- CRD IV EU 2013-36
- CRR IV EU 575-2013
- NIS EU Directive
- NIS EU Annex to the Communication
- PSD2 EU Regulation
- EU Cyber Security Act
- MIFID II EU Directive

Danish regulation:

- The Financial Business Act (LBK nr 1447 af 11/09/2020)
- Executive Order on Management and Controls of Banks, Annex 5 (BEK nr 1103 af 30/06/2022)
- The Payments Act (LBK nr 1719 af 27/11/2020)

Guidelines:

- Cyber EU EBA GL-2019-04
- ICT EBA-GL-2019-04
- TIBER

Appendix B

The following terms used in this Policy:

Activity Work that a company or organisation performs in a Business Process. Types of Activities include sub-processes, tasks, and references to other processes.

Application A representation of a system that is exposed to users. Applications can be, for example, mobile apps, web portals, collaboration tools, advisory tools, development tools.

Assets Assets include, but are not limited to:

- Hardware
- Software
- Applications, including End User Computing
- Technology Infrastructure
- Technology Processes
- Facilities
- Premises
- Information, whether tangible or intangible
- Services hosted internally or externally, including cloud services
- Networks and Information systems

Which are found in and relevant to the business environment and worth protecting.

Availability Services and information is available and useable when required

Authenticity Risk The risk of compromised trustworthiness of the system or data source

Board of Directors Is the highest Management Body of the separate legal entity in the Group. In the event that a subsidiary does not have a Board of Director, the responsibilities placed upon the Board of Directors by this Policy, falls upon the Board of Management of that subsidiary.

Business Process A defined set of Activities that represents the steps required to achieve a business objective being a specific outcome to a stakeholder. It includes the flow and use of information and resources.

A Business Process provides an end-to-end view including front to back, back to front relationships.

Confidentiality Information only available, or disclosed to, authorised individuals, entities or processes.

Criticality An assessment which considers, at a minimum, the confidentiality, integrity,availability and authenticity requirements aligned to the non-financial risk matrix.

Criticality of an application or service should consider the criticality of the business process that it supports.

Configuration Baseline An agreed description of the attributes of an asset at a point in time which serves as a basis for defining change.

Data at rest Inactive data stored in a digital form.

Data in transit Data that flows over a network.

Endpoint An internet capable hardware device on a network e.g. servers, desktops, laptops, phones.

Emergency Change A change that must be introduced as soon as possible – for example, to respond to a disruptive event.

IT and Security Event Event unplanned by the financial institution that has or will probably have an adverse impact on the integrity, availability, confidentiality and/or authenticity of services.

End User Computing (EUC)

Defined as user-developed applications including the use of spreadsheets and databases that are not maintained and operated by IT.

Executive Leadership Team (ELT)
Executive Leadership Team of NordBank or the subsidiary equivalent.

Functional requirements Describe the intention of a service and can be expressed as tasks or functions that the component is required to perform.

Firmware Permanent software programmed into a read-only memory (ROM).

Group Means NordBank and its Group Entities.

Integrity Information and information processing is accurate, complete and consistent.

IT Asset Hardware or software, irrespective of where it resides, that provides value to business activity. This includes for example computer programs, applications, cloud services, software modules, software tools, networks, websites, electronic databases and devices.

IT Change The addition, modification or removal of anything that could have an effect on IT services or applications.

IT Incident Unplanned interruption to an IT service or reduction in the quality of an IT service of failure of a Configuration Item that has not yet impacted an IT service. This includes ICT-related Incident i.e. a single Event or a series of linked Events unplanned by the Group that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data.

IT & Security Risks L2 Risk types further specifying the L1 Risk type Information Technology (IT) and Security Risk, which is comprised of the following:

- Availability risks
- Integrity risks
- Confidentiality risks
- Authenticity risks

IT Service Continuity Process for identifying and effectively responding to potential threats and their impact to the availability of services and applications ensuring the continued delivery of products and services during and after an incident.

Information Information is data which is perceived and interpreted in a particular manner to provide meaning. There are three different Information formats: digital, physical and verbal.

Information Classification Classification of information to ensure information and data is managed in accordance to business and regulatory requirements.

Logical Access Control The identification, authentication and authorisation protocols to interact with assets. Logical access controls restrict access to IT assets on the principles of least privilege.

Least Privilege The principle of only providing access to the information and assets required to perform a role.

Level of Control The design of the control aligned to control requirements which mitigates risk to an acceptable level

Non-functional requirements
Describe the system or service quality attributes such as security, reliability, performance, maintainability, scalability, and usability. They serve as constraints or restrictions on the design of the system.

Physical Access Physical Security Interactions with assets in the physical environment. The Security Measures that are designed to deny unauthorised access to facilities, equipment and resources and to protect personnel and property from damage and harm (such as espionage, theft, or terrorist attacks).

Patch Set of changes to software designed to update, fix, improve it or address security vulnerabilities.

Performance and Capacity Management
Ensures that the performance and capacity of IT services or applications and the IT infrastructure are able to deliver the agreed targets and services.

Process Owner The person accountable for the management of a Business Process and its execution during its lifecycle. By default, this also includes the underlying Activities of the Business Process as well as the related Operational Guidelines and SOPs.

Problem Management The process by which analysis is undertaken to identify the cause of one or more IT incidents in order to remediate root causes and prevent or minimise the likelihood of IT incidents occurring.

Privileged Access Administrator Access Right to any technical infrastructure (server, database, network, storage, workstations, etc.). Administrator Access Right to an application, which manages infrastructure, is also privileged Access Right. Administrator accesses inside other applications are not defined as privileged Access Rights.

Recovery Time Objectives (RTO)
Recovery Time Objective (RTO) means the defined time that the Business Process and supporting services can and should be recovered in after a disruption.

Recovery Point Objectives (RPO)
Recovery Point Objectives (RPO) means the maximum time period during which it is acceptable for data to be lost in case of a disruption

Security Incident An occurrence that actually or potentially jeopardises the confidentiality, integrity,availability or authenticity of an asset, the safety of employees or damage to physical assets or that constitutes a violation or imminent threat of violation of the Security Policy. IT Incidents are a subset of Security incidents.

Segregation of Duties Service Internal control designed to prevent error or fraud by ensuring that no individual has excessive control over systems, transactions or data.
A coherent, ready-to-use deliverable that combines assets, components, processes, and resources needed to deliver a specific outcome which brings value to a service recipient while hiding implementation and technical complexity. Different service classes include business service, application service, and technical service. Services can be internal, offshored, intra-Group outsourced, or third party outsourced. This includes ICT Services i.e. means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.

Service Owner The person accountable for the management of a Service and its execution during its lifecycle.

System A set of IT assets used to process, store, maintain and operate data and information, which supports and controls business processes.

System Owner The person accountable for the management of an Application and its execution during its lifecycle

Threat Third Party Any cause of an incident that could negatively impact an asset.
A separate legal entity or company. The Third Party may also be a Subsidiary. This also includes ICT Third Party Service Provider i.e. a Third Party providing Information Communication and Technology-services. Can also be Outsourcing. An ICT Third Party Service Provider can be deemed as critical by the ESAs (European Supervisory Authorities)

Threat-Led Testing Penetration
means a framework that mimics the tactics, techniques and procedures of real- life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the Group’s critical live production systems;

Vulnerability Organisation flaw or control weakness that might be exploited by a threat.