Spar Nord
Information security policy

spar Nord

1. Objective and scope

The objective of this information security policy is to ensure an adequate level of security for the Bank's IT assets in relation to all internal or external and intentional or unintentional threats. The policy aims to ensure that the integrity, confidentiality and accessibility of information are complied with, and that they conform with the Bank's data ethics.

The policy also stipulates the level of security at the Bank on the basis of the Board of Directors' overall approach to the Bank's risk profile, including derivative needs and requirements for the necessary security measures and checks, through the security principles described. The Danish FSA has designated the Bank as a systemically important financial institution (SIFI) and therefore the Bank provides services that are significant for the overall financial system in Denmark. The Bank's financial services have been digitalised, and they are primarily based on the use of IT, for which reason the Bank must ensure a high level of information security.

Objective

The overall objective of this policy is to ensure continuity in critical business activities by ensuring that:

- all information that is processed, stored, managed or released by the Bank has absolute integrity
- all information is accessible and is monitored and stored in accordance with the procedures for maintaining confidentiality
- selection of appropriate security measures to protect IT assets gives confidence for the Bank's stakeholders and ensures effective IT security management
- The Bank complies with current legislation and sector requirements and its role as a SIFI in the overall Danish financial IT infrastructure.

Scope

This policy applies for the Bank's organisation, underlying entities, employees, cooperation partners and contractors.

2. Relationship between the IT risk profile and the Bank's level of security

The Executive Board is responsible for ensuring completion of an annual overall risk assessment of the Bank's threats and vulnerabilities to form the basis of the Bank's IT risk profile. The risk assessment must be approved by the Board of Directors. The risk profile determines this information security policy and, via security principles and supporting security measures and controls, the policy ensures the necessary level of security desired by the Board of Directors.

Relationship with Bankernes EDB Central (BEC)

The Board of Directors has decided to outsource important and critical parts of IT operations and development of IT solutions to BEC. There is a requirement that specific measures be implemented to ensure that the level of security and compliance with the approved risk appetite are maintained in relation to the services outsourced.
The Bank is a joint owner of BEC, which, as a shared computer bureau, is subject to the Executive Order on Management and Control of Banks etc., and the Executive Order on the Performance of System Audits at Shared Computer Bureaus.

Relationship with other important suppliers

With regard to other important suppliers that have been designated as critical or important, see the criteria for outsourcing areas of activity, similar measures must be ensured to maintain and monitor the level of security.

Level of IT security

The level of security must ensure that the risks entailed in using IT have been aligned with the Bank's risk profile approved by the Board of Directors. The level must correspond to changes in the level of threat based on risk assessments and ensure compliance with regulations within the financial sector.

The level must help ensure that the Bank and its suppliers are able to maintain a defence against cyber threats with adequate technological measures, procedures and staff resources. This requires that suppliers of IT systems and the use of these are robust such that they can secure stable operation of the Bank’s business processes and an effective defence against cyber attacks from current threats.

Furthermore, the information security policy is supplemented by policies for outsourcing, IT risk management and objectives for IT contingency plans and the ISO/IEC 27001 framework with associated security measures, regulations and procedures describing how the requirements in these are to be operationalised.

3. Organisation and responsibilities

The Board of Directors and the Executive Board of the Bank are responsible overall for information security at the Bank, see the current descriptions of responsibility for the Board of Directors and the Executive Management in Annex 5 of the Executive Order on Management and Control of Banks etc.

The Executive Board is responsible for preparation, update and compliance with the information security policy, and the Bank's 2nd line of defence, the IT security function, is responsible for the day-to-day management on behalf of the Executive Board. The policy must be approved by the Board of Directors of the Bank and it must be published and communicated to employees and relevant external parties. Updates must, as a minimum, be carried out every year, or in connection with major changes in the Bank's risk profile and/or composition of assets.

Roles, responsibilities and authorities

Board of Directors
The Board of Directors is responsible for ensuring that the Bank has an appropriate organisation and adequate internal control and checks for all the risks connected with the Bank’s use of IT.

The Board of Directors must regularly, and at least once a year, review and approve the information security policy on the basis of an updated overall risk assessment that is based on the Bank's regularly maintained IT register of risks and current threats and vulnerability.

In this respect, the Board of Directors must assess whether the information security policy is adequate to ensure that risks that use of IT lead to, and are expected to lead to, are at an acceptable level for the Bank, and that the Executive Board supports the information security policy by stipulating clear information-security requirements, displaying visible commitment, and ensuring precise allocation of responsibility.

The Board of Directors is also responsible for, at least once a year, stipulating an overall objective for the Bank's IT contingency plan.

Executive Board
The Executive Board of the Bank is responsible for ensuring that the objectives of the Board of Directors for information security are implemented and complied with in the Bank, and that the information security policy, supporting requirements, and procedures for information security and IT contingency are established and maintained and take into account relevant legislation for the Bank.

The Executive Board of the Bank must ensure that roles and responsibilities for information security are documented and implemented in the Bank, that there is ongoing threat assessment, and that there is a procedure for managing exceptions and derogations, including breaches of information security.

Furthermore, the Executive Board is responsible for ensuring regular checks of compliance with the information security policy, and that there is reporting to the

Executive Board and the Board of Directors in accordance with Annex 5 of the Executive Order on Management and Control of Banks etc.

The Executive Board must ensure that there are adequate and qualified staff for continuous support of the Bank's operational IT needs and IT risk management processes. The Executive Board must ensure that the budget allocated is sufficient. The Executive Board must ensure that relevant employees and consultants who deal with the area, including people with key functions, receive relevant training on IT risks and information security. The Executive Board must ensure that a training programme is drawn up and implemented, including ongoing awareness programmes for all employees and consultants. The Executive Board must ensure that these people are trained to perform their duties and responsibilities in accordance with the relevant information security policies and requirements in order to reduce the risk of human error, theft, fraud, misuse or loss, and that they are trained in IT risk management. The training programme should provide training for Bank employees and consultants at least once a year.

The Executive Board is responsible for general information about information security. This task is to be carried out by the HR manager in connection with new employees, and in connection with changes to the information security policy and the supporting information security requirements, and at least once a year.

Members of the board of management and department directors at the Bank
All directors and department directors at the Bank are responsible for day-to-day compliance with information security requirements, as well as for communicating information security to employees, consultants and other relevant cooperation partners and contractors in their own areas of responsibility.

Directors with process responsibility
The director responsible for a specialist area is responsible for ensuring that there are written, manual Business Continuity Plans (BCP) and/or instructions covering their own business processes and for ensuring classification of these.

CIO (Director of IT)
The CIO (Director responsible for the Bank's IT) is responsible for ensuring compliance with the current information security policy and related information security requirements, including for the selected technologies, IT solutions and at critical IT suppliers.

The director is responsible for ongoing monitoring of the measures implemented by organising and implementing internal controls to ensure that these measures are designed correctly, implemented and effective.

The director must also ensure that the IT strategy sets clear IT security objectives for this policy through focus on IT systems, IT services, personnel and processes.

The director responsible for IT is also responsible for updating, maintaining and testing IT contingency plans and IT disaster recovery plans (DRP).

CISO (Chief Information Security Officer)
The CISO is responsible for operating the Bank's information security management system (ISMS), including the annual cycle with the planned security activities (awareness, threat assessments and risk assessments, reporting, etc.).

The CISO is responsible for ensuring follow-up on information security and IT risks pursuant to Annex 5 of the Executive Order on Management and Control of Banks etc., including ongoing verification of compliance with the information security policy, and supporting requirements and processes for information security.

The CISO is also responsible for updating and maintaining IT contingency objectives on behalf of the Bank's Executive Board and Board of Directors as well as for testing the IT contingency plan at least once a year.

The CISO reports to the Executive Board and the Board of Directors periodically, and at least as often as risk reporting by the chief risk officer (CRO).

Responsibilities include powers to make any type of investigation regarding information security required to perform the function. If the CISO considers that there is or could be a serious, unidentified threat to IT security, or that the management's objectives for information security are not being complied with, then the CISO has management authority to make the decisions necessary to stop the threat and impose requirements for better initiatives to manage the risk of the threat. If the CISO exercises this authority, the CISO must report this immediately to the Executive Board.

System owner
The director responsible for a specialist area is the system owner for own, purchased IT systems used by the Bank both internally and externally, including cloud solutions. As a minimum, the system owner is responsible for ensuring:

- that the system is commercially in accordance with the necessary business needs
- that the system is compliant with the current information security policy and supporting requirements
- that risk assessments are prepared on systems
- that systems and their data are classified, see the model for data classification
- management of audit reports relating to the system in question
- governance agreements relating to the system
- strategic and economic development of the system
- user profiles in the system
- performance of the business functionality for the supplier, in collaboration with the ISA and the BSA.
- preparation of the system road-map
- approval of implementation of new systems or major changes to systems
- contributions to the establishment of SLAs with suppliers, as well as BSAs and ISAs
- that systems comply with requirements on confidentiality, accessibility and integrity
- ongoing monitoring of the measures implemented, by organising and implementing internal controls to ensure that these measures are designed correctly, implemented and effective.

IT security committee

The IT security committee is authorised by the Board of Directors to make IT-related decisions with significance for the Bank's IT risk. The committee is also advisory and supports business in issues regarding information security and risk management.

The committee is responsible for evaluation and control of the risk profile of significant IT risks. Moreover, the committee supports the Bank's work on information security policy and supporting information security requirements. The committee is also authorised to approve new and changed information security requirements on behalf of the Executive Board.

The committee evaluates and ensures approvals of exemptions for non-compliance with information security policy and supporting information security requirements, including management of a full register for exemptions. The committee must also report on the status of approved exemptions to the Executive Board and the Board of Directors. The committee must report to the Executive Board concerning new approvals after these have been granted.

Business continuity manager (BCM)
Business Continuity Manager (BCM) must ensure compliance with the bank's objectives for preparedness through testing and development of BCPs (Business Continuity Plans) as well as cooperation with business, IT and critical suppliers. The BCM must also ensures compliance with Disaster Recovery Plans (DRPs) implemented by business, IT and critical suppliers. The BCM also reports to the Bank management on tests and trials of BCPs.

Bank employees
Individual employees are responsible for complying with the information security policy and supporting information security requirements for their work and, at least once a year, for acquainting themselves with any changes.

Principles for implementation of the policy in detailed information security requirements and procedures

Spar Nord IT and the relevant business areas are responsible for implementing the processes necessary to operationalise the information security policy.
As the 2nd line of defence, IT Security advises about information security requirements and IT security measures. The function must be familiar with the IT security measures applied to counter risks.

Compliance

The Bank applies the principle of segregation of functions on three lines to ensure compliance with the information security policy, and that IT operational risks are managed and monitored. This is through the following functions at the Bank:

Line	1st line	2nd line	3rd line
Function	Risk ownership	Objective and control	Compliance
Responsibility and tasks	1: Responsible for implementation of risk management activities. 2: Support business by designing processes and facilitating the risk process.	1: Define requirements and overall methodology. Follow-up and report on compliance with the information security policy. Follow-up on reports prepared. Ensure that risk management processes are operating satisfactorily. 2: Supervise that the Bank organises its IT processes with a view to compliance with applicable legislation.	1: Complete audit procedures to ensure compliance with legislation.
Location	1: "The Business", Process owners and system owners 2: Spar Nord IT	1: IT risk management function 2: Compliance	1: Internal audit function

1st line comprises the line organisation and in particular the organisational functions that work with processing information and technology. This line is responsible for identifying, assessing and managing risks, when they are identified.

2nd line primarily consists of the risk management function to monitor compliance with the level of IT security and the risk levels for operational IT risks in accordance with the function description of the risk management function. The compliance department monitors and checks for compliance with relevant legislation for the financial sector.

3rd line comprises Internal Audit, which is responsible for performing independent audit of overall management of risks and internal controls in the Bank as well as reporting on its activities to the Board of Directors.

4. Managing IT risks

The Bank's exposure to operational IT risks must be in accordance with the IT risk management policy and the operational risk policy.
IT security is responsible for assisting the organisation with identification of IT risks, assessment of control measures, and checks.

Relationship between the information security policy and the IT risk management policy

The Board of Directors has decided that IT security management at the Bank is to be risk-based, and therefore the information security policy is to keep IT risks at a level acceptable to the Board of Directors. This is by the Bank completing an overall risk assessment for use in updating the information security policy and to ensure that the information security policy fully considers the current risk profile.

5. Outsourcing

The level of IT security for the Bank is maintained by outsourcing and onward outsourcing to external suppliers. This means that the security principles in the information security policy must be complied with. Any outsourcing of significant or non-significant areas of activity must follow the rules of the outsourcing policy and must be registered centrally to facilitate regular checks of IT security at suppliers.

Relationship between critical and strategic IT suppliers

In accordance with the requirements of the Executive Order on Outsourcing for Credit Institutions, etc., in its decision to outsource parts of IT operations, the Board of Directors has ensured that suppliers have the expertise and capacity required to perform the outsourced tasks satisfactorily, including that suppliers have the authorisations required by relevant legislation for the IT area.
The Bank must ensure monitoring that suppliers comply with relevant legislation on the area. In this respect, the Bank uses annual reports from the data centre’s external and internal system auditors.

The Bank must prepare internal rules to ensure that tasks are performed by suppliers satisfactorily. The rules contain procedures for how the Bank ensures that suppliers meet the obligations in the contract and submit reports to the Board of Directors so that the Board of Directors has insight into whether activities are being carried out satisfactorily.

Relationship between the information security policy, and the policy for outsourcing areas of activity

IT risks related to the use of outsourcing must be included in IT risk management, and must be reported on an equal footing with other risks. Furthermore, it must be ensured that appropriate measures to address the risks identified in relation to the outsourced activities are incorporated in agreements with outsourcing suppliers, and that the effectiveness of these is regularly monitored and controlled, see the policy for outsourcing areas of activity.

6. Security principles

The information security policy is supported by a series of security principles described in more detail in supplementary requirements and procedures. The most important principles for compliance with this policy are described in the section below.

6.1 Contingency plans and business continuity

The Executive Board must ensure that an IT contingency plan is in place. The plan must be prepared on the basis of business impact analyses, and it must contain goals for recovery of normal operations in the event of errors, break-down, loss of data or systems, as well as full or part destruction of buildings, hardware and channels of communication, in compliance with the objectives of the Board of Directors for IT contingency plans.

The Executive Board must ensure that necessary redundancy and multi-centre operations are considered regularly in order to ensure maintenance of the Bank's most important functions.

The objective of the Bank's contingency planning is that it must be possible to recover critical business IT solutions, for use by a limited number of employees from temporary premises, within the objectives mentioned in the objective for IT contingency, after the decision on the implementation of the contingency plan has been made. This is referred to as emergency operation.

The IT contingency plan must support the Bank's needs and objectives for time limits for resumption to normal operations. Preparation of the IT contingency plan must include other relevant contingency plans, including the Bank’s business continuity plans and disaster recovery plans from critical system suppliers.

The period for emergency operation must be planned in accordance with the objective for IT contingency, after which full capacity must be available. During this period there may be reduced opening hours for selected systems until there is certainty that all the day-to-day routines have been re-established.

The Executive Board must ensure that contingency plans are tested regularly. The scope of the tests must be set on the basis of relevant scenarios and the Bank's threat scenario. The Executive Board must report significant results from tests of contingency plans to the Board of Directors.

The Executive Board must ensure that contingency plans, activity plans and recovery procedures are updated regularly, and at least once a year, on the basis of the test results, threat assessments and risk assessments.

These contingency plans must be supported by relevant business continuity plans (BCP) and disaster recovery plans (DRP).

6.2 Employees, cooperation partners and contractors

It must be ensured that Bank employees, cooperation partners and contractors are appropriate for their roles, by being conscious of compliance with their responsibilities for information security.

The Bank must secure its IT assets and system access on changes or termination of employment relationships and cooperation agreements.

Requirements must be communicated for acceptable use of IT, including descriptions of responsibilities. As a minimum, the requirements should include the following:

Employees:

- Procedures for reporting information security incidents
- Conditions for use and confidentiality of personal passwords
- Use of email, including attention to mailphishing, CEO fraud and ransomware
- Processing of confidential customer data (inside and outside the Bank)
- Use of mobile devices (working from home and during transport)
- Penalties in the event of breach of user responsibility.

Cooperation partners and contractors:

- Declaration of confidentiality
- Procedure for reporting information security incidents
- Use of email, including attention to mailphishing, CEO fraud and ransomware
- Conditions for use and confidentiality of personal passwords
- Penalties in the event of breach of user responsibility.

6.3 Operations

Operational supplies are managed by the Bank's own IT department and external operational suppliers. These suppliers must have adequate IT resources at all times to maintain secure and stable operations according to the current operating agreement. Suppliers must also have qualified staff, hardware, facilities and the necessary capabilities, to prevent and combat cyber attacks.

Suppliers must have procedures to manage incidents, changes and problems, they must identify, assess and manage IT risks, and they must be included as data sources in the Bank's own risk-management process. Operations must be conducted in accordance with the requirements in this information security policy and supporting descriptions of methods, policies, rules and procedures.

It must be possible to classify incidents in terms of materiality, so that the Bank can ensure the right management and observe its obligations to report significant events.

The Bank's links to networks must be protected against unauthorised access from external users, and the system supplier must have implemented adequate protection against intrusion to the Bank's internal network.

The use of favourable access rights, users' use of system solutions, as well as other actions on the system solutions must be logged to the required and adequate level, and according to the risk identified.

There must be ongoing checks of suppliers' compliance with the principles of operations, see the provisions in the outsourcing policy on routine management and control.

6.4 Protection and management of IT assets

There is a requirement that the significance of IT assets can be identified on the basis of the support they provide for the Bank's business processes. Therefore, an owner of IT assets must be appointed and it must be possible to identify an asset by use and classification, and the asset must be correspondingly protected against physical and business logic threats. This applies in particular for cyber threats and threats that can lead to errors on the IT assets with significant consequences for the Bank's customers, employees and cooperation partners.

IT assets must be secured against unauthorised access, modification, removal and destruction of the data stored on the media. Risk assessments must be used to identify whether IT assets are protected adequately in relation to the Bank's risk tolerance.

6.5 Back-up and security copying

It must be ensured that important data (defined in accordance with the relevant data and system classification model) is security copied in accordance with established rules that contain requirements for periodical testing and storage of a copy under appropriate conditions to protect the Bank against loss of data.

It must be ensured that the frequency of security copying of systems and data is based on the Bank's risk assessments, business impact analyses (BIA), and the relationship with plans for business continuity, including data criticality and consideration of the principles for Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Security copies must be stored securely and be inaccessible for unauthorised persons and users. Logical and physical segregation of functions must be ensured with regard to the back-up environment so that no one can access all copies of data.

It is required that system suppliers can document the above requirements regarding backup and security copying through regular reporting of control activities and annual auditor's reports.

6.6 Access to information and systems

Access to information and systems must be managed in accordance with documented procedures that take into account the principles for segregation of functions in section 6.10 so that customer access to customer-oriented applications is not included.

It must be ensured that access rights are only granted to the extent necessary and relevant to enable individual employees to complete their specific work tasks.

All allocations and changes of access to systems and data must be performed centrally and by specifically entrusted employees. Request and approval functions must be segregated, and all requests must be documented and stored such that they can subsequently be used for audit and follow-up.

All user access must be traceable to a person and use unique user identification.

There must be procedures for logging user activity. It must be ensured that the logging process is risk-based, aiming to enable identification and investigation of irregular activity. Logdata must be secured against manipulation under both transport and storage.

Allocation of favourable access rights must be limited to an absolute and time-limited minimum, and the exercise of such rights must be specifically logged and monitored for any abuse. Only the immediate manager/director with insight into the work needs may approve favourable access rights. Quarterly follow-up of system access and rights must be ensured.

6.7 System development and maintenance of business applications

In all development of business applications, it must be ensured that development activities are of the required standard of quality and security by participating in the required test activities, steering committees and other fora.

The system supplier, whether internal or external, must meet recognised standards and use the least three environments (operating, test and development environments) by developing new business systems and a documented change and implementation system.

For critical system components that are connected to the internet, satisfactory vulnerability scanning must be completed prior to start-up. The Bank's internet-oriented and internally developed applications must always be resilient to the current threat scenario.

All start-ups and changes in systems must be carried out in accordance with a controlled and documented process that the system supplier owns and is obligated to use.

This requires that there is a procedure for test activities to ensure confidentiality and integrity of data according to the data classification.

6.8 Project management

Information security must be integrated into project models and as a permanent element in completion of projects. In the performance of projects, all information risks must be identified, analysed and managed, including that the information managed in projects is classified and that measures are implemented to protect the confidentiality, integrity and accessibility of the information and of the systems and applications used for processing.

Information security must be maintained throughout the lifetime of projects, and risks and mitigating measures must be verified and evaluated.

6.9 Risk assessment

The planned method for risk assessment from the IT risk-management policy must be used.
Risk assessments of critical IT assets must be performed in a continuous process to identify significant risks, and to determine necessary security measures.

6.10 Segregation of functions

Segregation of functions must be implemented and monitored sufficiently to minimise the risk that individual functions or persons who perform essential tasks can compromise security.
Overall segregation of functions and persons must be ensured across the following areas:

- Systems development
- Testing
- Systems operation
- Business activities

ERP systems must be designed with full segregation between business users and administration users and operator users.

6.11 Awareness

Regular information and training for Bank employees about information security and protection of personal data must be implemented to ensure an effective security culture. Targeted information security training for employees in contact with risky activities must be assessed.

6.12 Breach of information security policy and information security requirements

All employees must easily be able to report incidents with consequences for information security, and they must be informed about their responsibilities in this respect. Incidents must be reported to Spar Nord IT, who will decide whether the incident is to be reported immediately to the Executive Board.

The Board of Directors must be informed about significant breaches of information security policy, and relevant stakeholders must also be informed.

6.13 Penalties in the event of breach of the policy

All correspondence to and from Bank IT workplaces may be extracted and submitted in connection with legal proceedings involving Spar Nord Bank.

Unlawful use of systems, data, mail services, internet services, etc. will be reported to the police. The consequences of unlawful use as well as other forms of abuse will be decided by the Executive Board of the Bank.

7. Reporting, control and follow-up

The Board of Directors must be informed about significant information security incidents. This information must be submitted regularly, and at least once a year when the policy is updated. Significant incidents must be reported clearly and promptly to the Board of Directors and the Executive Board as well as to other cooperation partners, including in particular the Danish FSA, and the Centre for Cyber Security.

The Executive Board must ensure that arrangements be established for monitoring and control of compliance with the information security policy, and report non-compliance to the Board of Directors. The effectiveness of the measures initiated must be verified by independent reviews and validated by implementation of technical testing. The results of the reviews and tests must be included in reporting on compliance with the information security policy and in assessment and reporting of the IT risk exposure.

8. Exemptions from the policy

The Executive Board may, when circumstances require, grant exemption from the instructions and requirements in the information security policy. Exemptions must be monitored and risk assessed regularly.

Exemptions from the information security policy must be reported to the Board of Directors periodically. Any exemptions granted must be documented and stored in a central register of exemptions and must be managed by the Bank's IT security committee.

9. Approval of the policy

This information security policy enters into force following approval from the Board of Directors on 1 July 2023 and replaces the information security policy hitherto in force.

References to other documents

Internal, current:

a) Risk assessment for revision of the information security policy
b) IT strategy
c) IT security requirements
d) Policy for outsourcing areas of activity
e) Policy for operational risk management
f) Policy for IT risk management
g) Policy for data governance and data protection policy
h) Objectives for IT contingency
i) Statutory report on data ethics 1

External:

j) Current information security standard, ISO/IEC 27001 - Appendix A and ISO/IEC 27002:2022
k) Executive Order on Management and Control of Banks etc., Executive Order no. 1254 of 11/06/2021, Annex 5, IT strategy, IT risk management policy and IT security policy

1.

ANNEX - Mapping between the information security policy and supporting information security requirements

Information security policy	Information security requirements
1. Objective and scope	5.1 - Policies and data security 5.14 Transmission of information 5.31 Legal. Legislative, regulatory and contractual requirements
2. Relationship between the IT risk profile and the Bank's level of security	5.31 Legal. Legislative, regulatory and contractual requirements 5.33 Protection of records 5.36 Compliance with policies, rules and standards for information security
3. Organisation and responsibilities	5.2 Roles and responsibilities for information security 5.4 Management responsibility 6.1 Screening (Background check of employees) 6.2 Employment terms and conditions 6.5 Responsibilities in connection with cessation or change of employment
4. Managing IT risks	5.21 Management of information security in the ICT supply chain 5.31 Legal. Legislative, regulatory and contractual requirements 5.33 Protection of records 8.8 Management of technical vulnerabilities
5. Outsourcing	5.19 Information security in supplier relationships 5.20 Management of information security in supplier agreements 5.21 Management of information security in the ICT supply chain 5.22 Monitoring, assessment and change management of supplier services 5.31 Legal. Legislative, regulatory and contractual requirements 5.32 Intellectual property rights 5.33 Protection of records

	6.3 Awareness, education and training regarding information security 6.5 Responsibilities in connection with cessation or change of employment 6.6 Non-disclosure agreements and confidentiality agreements 8.30 Outsourced development 8.31 Segregation of development, testing and production environments
6. Security principles	5.3 Segregation of functions 5.36 Compliance with policies, rules and standards for information security
6.1 Contingency plans and business continuity	5.30 ICT readiness to support of business continuity 8.14 Redundancy of data processing facilities
6.2 Employees and cooperation partners	5.10 acceptable the use of information and supporting assets 5.14 Transmission of information 5.15 Administration of access 5.19 Information security in supplier relationships 5.20 Management of information security in supplier agreements 5.24 Planning and preparation of incident management in the event of security incidents 5.31 Legal. Legislative, regulatory and contractual requirements 5.32 Intellectual property rights 5.33 Protection of records 6.1 Screening (Background check of employees) 6.2 Employment terms and conditions 6.3 Awareness, education and training regarding information security 6.5 Responsibilities in connection with cessation or change of employment 6.6 Non-disclosure agreements and confidentiality agreements 6.7 Distance work 8.15 Logging 8.18 Use of favourable supporting programs
6.3 Operations	5.14 Transmission of information 5.15 Administration of access 5.23 Information security for use of cloud services 5.29 Information security during outages 5.31 Legal. Legislative, regulatory and

	contractual requirements 5.33 Protection of records 5.35 Independent assessment of information security 5.37 Documented operating procedures 8.6 Capacity management 8.9 Configuration management 8.17 Synchronising clocks 8.18 Use of favourable supporting programs 8.19 Software installation in test and production systems 8.20 Network security 8.21 Security of network services 8.22 Segmentation of networks 8.23 Web filtering 8.24 Use of cryptography 8.26 Requirements for applications security 8.29 Security tests during development and approval 8.31 Segregation of development, testing and production environments 8.32 Change management 8.33 Information for use in tests 8.34 Protection of information during the audit
6.4 Protection and management of IT assets	5.9 Description information and the supporting assets 5.11 Return of assets 5.12 Classification of information 5.19 Information security in supplier relationships 5.31 Legal. Legislative, regulatory and contractual requirements 5.32 Intellectual property rights 5.33 Protection of records 6.6 Non-disclosure agreements and confidentiality agreements 7.1 Physical area security 7.2 Physical access control 7.3 Security of offices, premises and facilities 7.4 Physical security surveillance 7.5 Protection against natural and environmental threats 7.6 Work in secure areas 7.7. Cleared desks and locked screens 7.8 Location and protection of equipment and devices 7.9 Security of assets outside the organisation's areas 7.10 Storage media 7.11 Security of supply

	7.12 Security of cables 7.13 Maintenance of equipment and devices 7.14 Secure disposal or reuse of equipment and devices 8.1 User units 8.6 Capacity management 8.7 Protection against malware 8.8 Management of technical vulnerabilities 8.10 Deletion/erasure of information 8.11 Data masking 8.12 Prevention of data leaks 8.14 Redundancy of data processing facilities 8.15 Logging 8.16 Monitoring of activities 8.18 Use of favourable supporting programs 8.19 Software installation in test and production systems 8.20 Network security 8.21 Security of network services 8.22 Segmentation of networks 8.23 Web filtering 8.24 Use of cryptography 8.26 Requirements for applications security 8.33 Information for use in tests 8.34 Protection of information during the audit
6.5 Back-up and security copying	5.12 Classification of information 5.23 Information security for use of cloud services 5.31 Legal. Legislative, regulatory and contractual requirements 5.33 Protection of records 8.7 Protection against malware 8.10 Deletion/erasure of information 8.12 Prevention of data leaks 8.13 Backup of information 8.14 Redundancy of data processing facilities 8.20 Network security 8.21 Security of network services 8.22 Segmentation of networks 8.23 Web filtering 8.24 Use of cryptography
6.6 Access to information and systems	5.13 Labelling of information 5.14 Transmission of information 5.15 Administration of access 5.16 Management of identification 5.17 Authentication information 5.18 Access rights 5.23 Information security for use of cloud services

	5.31 Legal. Legislative, regulatory and contractual requirements 5.33 Protection of records 5.34 Protection of privacy and protection of personal data 6.1 Screening (Background check of employees) 6.2 Employment terms and conditions 6.5 Responsibilities in connection with cessation or change of employment 6.6 Non-disclosure agreements and confidentiality agreements 6.7 Distance work 8.2 Favourable access rights 8.3 Limited access to information 8.4 Access to source code 8.5 Security authentication 8.7 Protection against malware 8.11 Data masking 8.12 Prevention of data leaks 8.14 Redundancy of data processing facilities 8.15 Logging 8.16 Monitoring of activities 8.18 Use of favourable supporting programs 8.19 Software installation in test and production systems 8.20 Network security 8.21 Security of network services 8.22 Segmentation of networks 8.23 Web filtering 8.24 Use of cryptography 8.33 Information for use in tests 8.34 Protection of information during the audit
6.7 System development and maintenance of business applications	5.23 Information security for use of cloud services 5.32 Intellectual property rights 5.35 Independent assessment of information security 5.36 Compliance with policies, rules and standards for information security 6.6 Non-disclosure agreements and confidentiality agreements 8.11 Data masking 8.14 Redundancy of data processing facilities 8.15 Logging 8.16 Monitoring of activities 8.18 Use of favourable supporting programs 8.19 Software installation in test and production systems

	8.20 Network security 8.21 Security of network services 8.22 Segmentation of networks 8.23 Web filtering 8.24 Use of cryptography 8.25 Secure development lifecycle 8.26 Requirements for applications security 8.27 Secure system architecture and development principles 8.28 Secure programming 8.29 Security tests during development and approval 8.30 Outsourced development 8.31 Segregation of development, testing and production environments 8.32 Change management 8.33 Information for use in tests 8.34 Protection of information during the audit
6.8 Project management	5.8 Information security in projects
6.9 Risk assessment	- IT risk management policy - Policy for operational security
6.10 Segregation of functions	5.3 Segregation of functions 8.31 Segregation of development, testing and production environments
6.11 Awareness	5.34 Protection of privacy and protection of personal data 6.3 Awareness, education and training regarding information security
6.12 Breaches of the IT security policy and IT security requirements	5.7 Notification about threats 5.24 Planning and preparation of incident management in the event of security incidents 5.25 Assessment and decisions regarding information security incidents 5.26 Management of information security incidents 5.27 Storage of information security incidents 5.28 Collection of evidence 5.29 Information security during outages 6.4 Penalties 6.8 Reporting information security incidents 8.15 Logging
7. Reporting, control and follow-up	5.5 Contact with the authorities 6.8 Reporting information security incidents

8. Exemptions from the policy	Process for exemptions for non-compliance with the information security policy and supporting information security requirements in HOPEX
9. Approval of the policy	N/A