Information security policy at SpareBank 1 SMN

Date: 1.11.2021
Approved by: The Board of Directors

Object
The information security policy for the SpareBank 1 SMN group is designed to assure a systematic and risk-based approach with a view to reducing vulnerabilities and the risk of incidents. Procedures and measures aim to safeguard information assets and to prevent data from going astray, including data related to integrity, confidentiality, accessibility and regulatory requirements.

The information security policy supports the group's strategic choices and day-to-day operations.

Definitions

Information security aims to safeguard SMN's values. In practice this means giving due weight to:

- ***Integrity,*** such that information and systems are correct, complete and updated at all times.
- ***Confidentiality,*** such that classified, confidential or sensitive corporate information does not go astray and can only be accessed by persons who need the information in order to perform their duties.
- ***Accessibility,*** such that information and systems needed to perform official duties are accessible to relevant personnel. This entails that roles and rights have been duly defined.
- ***Regulatory requirements,*** such that integrity, confidentiality and accessibility assure regulatory compliance.

Responsibilities

The **Board of Directors** is responsible for approving the Information Security Policy.

The **Executive Director – Technology and Development** is responsible for ensuring that the group has in place a governance system for compliance with this policy, with clearly defined roles, responsibilities and reporting channels within the organisation.

The ***Head of IT and Security*** is responsible for developing and implementing the operative follow up of the Information Security Policy, in addition to setting strategic goals for information security.

The **Information Security Officer** is responsible for ensuring that information security matters are attended to through risk assessments, systems-related solutions and employee training.

Information Security at SpareBank 1 Utvikling is responsible for incident reporting, operational information security with respect to shared infrastructure and solutions, risk assessments of shared systems and services and coordination of joint activities between the alliance companies.

All managers with line or project responsibilities along with owners of IT systems and IT infrastructure are responsible for ensuring that the principles set out in the Information Security Policy are complied with in their respective areas of responsibility.

All employees are required to undergo mandatory training and to be familiar with SMN’s basic information security policy guidelines. Employees can direct queries to their immediate superior or to the information security officer.

Principles

Any requirement or need for information security measures shall be based on a risk assessment and regulatory factors.

Outsourcing of IT functions

SMN shall, where advantageous, use external providers to operate, maintain and develop its IT systems and IT infrastructure. Service providers shall comply with SMN’s requirements with respect to information security.

Risk assessments shall be an integral part of the processes associated with outsourcing – ranging from the initial outsourcing idea to provider presentations, provider selection and SMN’s day-to-day follow-up of service providers – to ensure that the provider’s services are compliant with SMN’s requirements.

General security requirements

SMN has specific documented procedures for important security-related processes. The procedures mentioned below in this chapter are reviewed and updated annually.

a. Regulatory requirements

SMN shall comply with applicable regulatory requirements at all times.

b. Risk management

SMN’s requirements with respect to information security for IT systems and processes for line management and projects shall be based on risk assessments. Those in charge shall be aware of threats and vulnerabilities facing SMN and have a grasp of what the business can tolerate in terms of direct and indirect losses. Risk assessments shall be conducted upon the introduction of new systems/services or when changes are made to existing systems/services.

Risk assessments shall also consider the risk posed by the group’s own employees or persons affected by the group’s activities.

c. Classification of information

SMN shall have in place an information classification system.

d. Classification of IT systems

SMN shall have in place a method for classification of IT systems. A review of the IT system classification shall be conducted annually and shall provide a clear understanding of the respective systems’ criticality.

e. Access control

Access to SMN’s IT systems shall be based on defined roles and rights. Access shall be justified by the needs of the employee concerned and be modified in the event of changes in role or position. Each year a review of accesses to the IT systems shall be conducted with a view to withdrawing rights that are no longer needed. Users with extended rights, such as administrators, shall be subject to the requisite oversight on a continuous basis.

f. Surveillance of IT systems and infrastructure

Mechanisms for technical surveillance of activities in SMN’s IT systems and infrastructure shall be in place with a view to avoiding malevolent or untoward incidents and to investigating any undesired incident in a simpler manner. Surveillance shall be technical, not breach data privacy, and be suited to the purpose of discovering and taking steps to protect against undesired incidents.

g. Security architecture

SMN shall have in place a validly documented overview of technical security installations and processes related to security functions for IT systems and IT infrastructure.

h. Crisis management and preparedness

A procedure for recovery from a crisis in which important processes are wholly or partly disabled shall be in place and duly documented. Drills to test such procedures shall be conducted at minimum annually.

Security copies and procedures for updating IT systems shall be in place as a part of the process for avoiding a crisis situation.

i. Training – information security culture

Gaining an understanding of security matters and security culture shall be a part of the mandatory training of SMN employees. Each employee is personally responsible for undergoing mandatory training. The object is to integrate security into employees’ daily tasks in order to avert incidents that could lead to financial loss, loss of data or loss of reputation. Training shall be a continuous process.

j. Physical security

Physical security encompasses access control systems, video surveillance, alarm systems, security services and associated security-related surveillance. The basic principle of the physical protection of locations shall entail a risk-based approach.

The main object shall be to prevent undesired incidents directed at the lives and health of employees, customers and visitors, and at assets, reputation, information that is processed and business operations. Access to the SMN Group’s buildings and other indoor areas shall be granted based on the individual’s need for access in order to perform his/her duties. The extent of video surveillance and handing over of image and video material to others shall be in accordance with the law.