OPR-Finance

Information & Data security policy

1. The Purpose of the Information & Data Security Policy

This security policy defines the objectives, responsibilities and means of the information security work of the whole organization (OPR-Finance) in operation. The policy is complemented by separate guidance and process descriptions.

2. Security Policy Objectives

Security ensures that all information and data that is required to be protected is identified, classified, and protected appropriately. The aim is that information is not used unauthorized, data is not changed or destroyed uncontrollably, and the data should be made available.

3. Responsibility for Security

OPR management has an overall responsibility for the security and more specifically the responsibilities are defined as follows:

- Security Officer: The Data Protection Officer is responsible for the organization and maintenance of the data protection throughout the organization. It is the responsibility of the security officer to prepare presentations to improve data security, collect and transmit information on security issues, and periodically review the security situation. The security officer reports to the organizational management about security exceptions and security status.
- Process Owner: The process owner is responsible for the systems used in the process and their data and data security.
- System-Responsible: The system administrator is responsible for the operational implementation and maintenance, in cooperation with the process owner.
- Supervisors are responsible for ensuring that their own subordinates are aware of and complying with the security guidelines.
- The entire staff is responsible for the measures taken under their user ID. In addition, they are responsible for complying with security policy, security principles and security guidelines in their own work, and are required to notify on exceptions detected to their supervisor and/or to the officer responsible for the data security.

4. Means of the Security Management

Risk management
Security risks are identified as part of the organizational operational risk management. A management plan is tried to be drawn up for identified risks, the necessary measures are scheduled and held accountable.

Data classification and protection
All data and systems are strived to be classified according to their security requirements. The classification of data and information, and information systems is the responsibility of the owner of the information. If the system contains data of several security classes, this system will be processed according to the highest security class of the data.

Monitoring and follow-up

Responsibility for monitoring and follow-up of the whole is at the Information Security Officer. These activities also include monitoring the compliance with the guidelines given and monitoring the situation of the technical control procedures.

Managing security incidents

The security incident management process defines how to perform when a security or a suspected security breach happens. More significant security incidents are dealt with in the management review.

Business continuity and disaster recovery

Key systems have been identified and adequate measures have been taken to protect them and ensure continuity. For outsourcing partners, the aim is to ensure a sufficient level of information security and continuity planning through contractual and audit right.

Training and induction

New employees are told why information security is important to be considered and the information security guidelines to be followed are introduced. Security awareness is provided to the organization's employees as a training and/or via fact sheets. The superiors are responsible for maintaining and monitoring the security awareness of their subordinates.

5. Validity and Review of the Policy

This security policy is valid from the date of acceptance. Policies are regularly reviewed by the management, making the necessary updates.