MEKO AB
Box 19542
SE- 111 64Stockholm
Visiting address:
Klarabergsviadukten 70, Stockholm
Tel: +46 (0)8 464 00 20

IT Security Policy

Table of Contents

MEKO AB
Box 19542
SE- 111 64Stockholm
Visiting address:
Klarabergsviadukten 70, Stockholm
Tel: +46 (0)8 464 00 20

1. Introduction

1.1 Background and purpose

This policy is intended to describe and establish the internal framework regarding the governance and management of Cyber security within MEKO.

The policy defines MEKOs Cyber security management system. This policy document describes the overall intentions and direction of the organisation regarding Information security, which are formally approved by the CEO of the MEKO. The information security management system includes the MEKO Information security policy, its associated instructions, organization and the processes and procedures that cover information security work. The structure of the Information security management system is based on international standards and technical security frameworks.

Information is a strategic asset as it is indispensable for the business. Consequently, both assets and information must have adequate security protection. The information to be protected can occur in many different forms, printed in text or written, oral or electronic, both stored and during communication. Much of the everyday information handled within MEKOs operations is confidential and sensitive and thus information security is critical for MEKO.

The Information security policy shall reflect relevant applicable laws and regulations at any time in markets where MEKO is present.

The purpose of MEKOs information security work is to protect the customers, employees, and assets, including information assets against information security-based risks and threats.

The purpose of the information security policy is to define internal rules for Information security. This is done by defining Information security requirements through the management system and monitoring and verifying compliance with those requirements.

This Information security policy covers MEKO, with all employees, consultants and service providers within all Business Areas. This policy is developed in collaboration and coordinated with the Business Areas' overall principles for Information security. In addition to the requirements imposed on Information security by MEKO, this policy constitutes the Business Areas' minimum common level of information security. This policy also covers activities that MEKO has outsourced to internal and/or external parties.

This policy shall be annually reviewed and submitted to the Board of Directors for approval.

1.2 Definitions

In this policy, the following terms have specified meaning:

Incident: An undesirable event that has or is likely to have a negative impact on MEKOs operations, assets or trust.

Asset: Information or systems (hardware or software), material or non-material within the

MEKO AB
Box 19542
SE- 111 64Stockholm
Visiting address:
Klarabergsviadukten 70, Stockholm
Tel: +46 (0)8 464 00 20

assets that are worthy of protection.

Asset register: List of all IT assets kept up to date by the owners of the assets.

Continuity plan: A plan that describes how business operations should be maintained in the event of an incident or major business disruption.

Cyber Security: Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Information security: The purpose of information security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable.

Information Security Management System (ISMS): Tools that help establish, implement, operate, monitor, audit, maintain and improve the desired level of Information security. ISMS includes all policies, procedures, documents, records, plans, guidelines, agreements, contracts, processes, practices, methods, activities, roles, responsibilities, relationships, tools, techniques, technologies, resources, and structures that MEKO use to protect and preserve information, to manage and control information security risks, and to achieve business objectives.
An *ISMS* is part of a management system.

Integrity: Within the narrow context of information security, the term integrity means to protect the accuracy and completeness of information.

IT security: The technical working methods, processes and tools needed to ensure the security management of information.

Operational risk: Risk for losses due to inaccurate or incorrect internal processes, human error, personnel-related incidents, IT and information security incidents, external and/or internal fraud, improperly implemented models or execution of models, legal incidents, compliance-related incidents, and external events.

1.3 Definition of information security

MEKO defines Information security as all forms of security work and security protection. This definition covers the work and protection of information, IT security, cybersecurity, physical security, and personal security. This means that classic security work (in the form of physical and personal protection) is based on the information perspective and therefore these areas are included in MEKOs Information security policy.

Information security within MEKO is therefore specifically about protecting people, information, and physical property. For information, it is further important that it:

- is protected (confidentiality)
- is accurate (integrity), correct, and complete
- is available as required (availability)
- is possible to identify who has access to the information (traceability)

MEKO AB
Box 19542
SE- 111 64Stockholm
Visiting address:
Klarabergsviadukten 70, Stockholm
Tel: +46 (0)8 464 00 20

2. Objectives and strategy with information security

The CISO function is the function that develops requirements and monitors MEKOs work within information security (see definition above). The governance of information security shall be coordinated with the MEKOs overall corporate governance.

The CISO function is the function within MEKO that is responsible for the development and ongoing maintenance of MEKOs Information security strategy. MEKOs information security strategy shall be approved by the CEO.

MEKOs objective with the information security work is that information security at any given time should be dynamic and with reasonable consideration to manage both historical, current, and future risks and threats. By dynamic, information security work should be performed with a risk-based approach and adapted to the MEKO needs at all times. The cost of information security protection shall be weighed against the risk exposure to determine a reasonable cost for information security protection. The information security protection work must therefore be proactive and at any time comply with the requirements and rules imposed on MEKOs business. Furthermore, information security must at least comply with the requirements and expectations that the MEKOs customers and partners have on the business. Compliance with applicable regulations and obligations is an objective of information security work. Information security should also protect the trademarks and reputation in the market.

3. Organization

3.1 Information Security function

The information security function is an operational function dedicated to the introduction, control and testing of information security protection, based on the requirements of this management system. The information security function is managed by the local Information Security Officer, ISO, that shall continuously report the status to the CISO.

The information security function's mandate includes stopping ongoing developments and changes if high risk exists. The information security function may exercise a mandate after reconciliation with the CISO but needs to inform both the Risk Coordinator in the Business Area and CIO.

The ISO ensures that the Business Areas has processes, controls, and system support to meet the requirements of Information and IT security policy and guidelines.

The information security function reports organizationally to the local CIO and is responsible for:

- drive and develop security within the Business Area,
- develop instructions in information and IT security,
- implement these guidelines in the business,

MEKO AB
Box 19542
SE- 111 64Stockholm
Visiting address:
Klarabergsviadukten 70, Stockholm
Tel: +46 (0)8 464 00 20

- point of contact against CISO, audits, insurance company,
- monitor security on any form of outsourcing of activities,
- investigating suspected fraud and irregularities,
- ensure that technical solutions and architecture are in line with security requirements,
- carry out audits of suppliers in the IT field,
- train employees within IT security in the company with a focus on the IT department,
- contact person for Security Operations Centre in case of information security incidents,
- manage incidents in the IT security area,
- participate in forums for assessing new products and IT systems,
- security advisor to the Business Area,
- responsible for CSMS in the Business Area,
- reports risk to CISO and Risk Manager (BA), and
- reports on security to Business Area stakeholders.

3.2 Security Forum

Convened by the CISO, the Forum's function aims at training, coordination, and follow-up of the effective running of information security work over-time in the different teams. The Forum shall also monitor the need for support in the activities and propose improvements in the field of information security. Risk reporting on all levels is performed in the forum between CISO and ISO teams. The Forum is responsible for collaboration, setting the strategy and operating accordingly with communication to the Business Areas stakeholders.

4. Governance principles for information security

MEKO and its outsourced activities shall comply with the MEKOs information security management system. MEKOs management system is based on security standards and industry practice. The management system shall consist of this information security policy and of supportive separate guidelines and local instructions.

All digital or physical information assets (e.g. but not limited to, computers, phones, licenses, mailboxes, documents, code, IP) provided to, or produced by, MEKO employees and contractors as part of their engagement for the company is the exclusive property of MEKO. MEKO reserves the right to manage, read, modify or transfer this data as they see fit.

MEKO AB
Box 19542
SE- 111 64Stockholm
Visiting address:
Klarabergsviadukten 70, Stockholm
Tel: +46 (0)8 464 00 20

5. Steering documentation

In the field of Information security, the following steering documents are available:

- ***Group Security Processes*** describe high-level processes areas mandatory across the group, specifically within Asset Management, Log Management, Incident Response & Escalation, Identity & Access Management, Change Management, Third-Party Risk Management & Employee Cybersecurity Responsibilities. Processes shall be further interpreted and tailored to Business Area environments in local Procedures & Guidelines.
- **Information Security Guideline** describe what security controls shall be defined at MEKO, what processes and tools that is required on a Group level,
- **Information Security Instructions** describe how security controls shall be defined at MEKOs Business Areas, how processes and tools are implemented and managed in the local Business Area level,
- **Disaster Recovery management and Business continuity plans** describes the management of scenarios such as interruptions in IT delivery, no access to premises or staff not being available. Outage plans are drawn up within the IT business to restore systems and services according to the business's accessibility requirements.

Local instructions describe how users of the information assets should manage systems and devices. Procedures and instructions are established locally for each function or department to ensure compliance with these governing documents.

6. Consistency in case of abuse

Security responsibilities in an information-sensitive business such as the MEKO are everyone's responsibility. IT systems are monitored through automated checks and follow-up of suspected abuse is carried out regularly. Intrusion into IT systems, misuse of information or breach of obligations under this policy may be subject to disciplinary action. Employees may also be liable for the damages that have occurred. Serious violations of the policy can lead to a written disciplinary warning or in severe cases, ground for termination of employment. In addition, criminal proceedings may apply, in accordance with the legislation in force.

MEKO AB
Box 19542
SE- 111 64Stockholm
Visiting address:
Klarabergsviadukten 70, Stockholm
Tel: +46 (0)8 464 00 20

7. Follow-up and determination

7.1 Compliance and follow-up

The CISO is responsible for monitoring and monitoring compliance with the Risk management framework and security risks. The CISO shall ensure that Cyber risks are identified, measured, assessed, monitored, and reported regularly to the CIO, COO, RCC and Head of Risk Management at MEKO.

The ISOs shall monitor MEKO and its relevant suppliers' compliance with the Information Security Management System and report to CISO.

7.2 Update and determination

This Information Security Policy shall be reviewed and determined by the CFO of MEKO at least annually. The Chief Information Security Officer (CISO) shall ensure that the policy is correct and complies with internal and external regulations. CISO shall also ensure that the policy is prepared for the approval of the CEO. The CEO of MEKO shall approve any major changes in the updated Information Security Policy.

This policy was adopted by the Board of Directors at the Board meeting in MEKO AB (publ) on May 15, 2025