maincubes one GmbH
Bockenheimer Anlage 15
D-60322 Frankfurt a. M.
www.maincubes.com

Managing Directors: Oliver Menzel,
Albrecht Kraas,
Dr. Markus Wiedenmann
Commercial Register No.: 95527,
Frankfurt/Main VAT ID:
DE286899718

maincubes
SECURE DATACENTERS

# Information Security Management System Guidelines

## maincubes one GmbH

**Confidentiality level: Public**

### Document information

**Processing note**

| | Name and position | Version | Date | Signature |
|---|---|---|---|---|
| Created by: | ISMS Working Group | 1.0 | 3/16/2018 | |
| Reviewed by: | Consultant | 1.4 | Via Workflow | Via Workflow |
| Approved by: | CTO | 1.4 | Via Workflow | Via Workflow |

**Change history**

| Date | Processor | Version | Reason for change / changes |
|---|---|---|---|
| 4/18/2018 | ISMS Working Group | 1.1 | Maintenance and continuous improvement of the ISMS as an obligation for every employee |
| 5/23/2018 | ISMS Working Group | 1.2 | Responsibilities limited to roles |
| 8/2/2018 | ISMS Working Group | 1.3 | Preparation for the extension of the scope of application |
| 3/6/2019 | ISMS Working Group | 1.4 | Adaptation of the document control: elimination of personal data. |

Contents

## 1. Preamble

These guidelines are part of the ISMS ISO27001 of maincubes. The framework will be successively introduced in other companies of the maincubes Group that are located in non-German-speaking countries. In order to be able to use this uniform framework there as well, translations in English or in the respective national language are attached in addition to the binding German text.

## 2. Gender equality notice

In the following document, the masculine grammatical gender is used to describe tasks, functions or roles for reasons of simplification. The chosen grammatical gender in this document addresses persons of all genders to whom tasks, functions or roles are assigned without any evaluation of their gender, physical or mental abilities, or any other evaluation.

## 3. Purpose, scope of application and users

These ISMS Guidelines define the purpose, orientation, principles and basic rules for the Information Security Management System (ISMS) based on ISO/IEC 27001:2013.

The management of maincubes one GmbH hereby adopts the following ISMS Guidelines.

The objective of these Guidelines is to define the purpose, orientation, principles and basic rules for information security management at maincubes one GmbH.

maincubes one GmbH focuses its corporate policy on being specialised in the core competencies colocation and secure exchange. Thus, maincubes one GmbH supports its customers in the optimal design of their work processes.

maincubes one GmbH offers its customers and partners secure services in rack, cage or suite and electricity in top quality and energy efficiency from Germany.

In order to warrant these services, maincubes one GmbH is highly committed to fulfilling its business processes, and in order to be able to cooperate with national and international customers and partners, it relies on the availability of modern information and communication technology.

In addition, there are obligations to warrant information security based on legal regulations and contractual obligations towards project partners, employees and customers.

Protecting the company's information and communications infrastructure against misuse, manipulation, interference, spying out confidential information, etc. - in short: information security - is therefore becoming increasingly important.

For this reason, management has adopted the following Guidelines for the use of the company's information technology.

These Guidelines are an invitation and obligation to act in compliance with the law and to treat the IT infrastructure of the company and its customers responsibly.

These Guidelines apply to employees, trainees, apprentices, interns, undergraduates, working students and part-time employees (hereinafter, "employees") and all external persons with a function within the scope of the Information Security Management System. They are to be made known to all employees and the relevant external parties in an appropriate manner.

## 4. Terms and abbreviations

- **Confidentiality:**
  - The feature that information is not made available or disclosed to unauthorized persons, units or processes.
- **Integrity:**
  - Feature for ensuring the accuracy and completeness of assets.
- **Availability:**
  - Feature of being accessible and usable to an authorised unit on request.
- **Information security:**
  - Maintaining the confidentiality, integrity and availability of information
- **Information Security Management System**
  - Part of the overall management system covering the development, implementation, execution, monitoring, review, maintenance and improvement of information security on the basis of a business risk approach.

## 5. Information security objectives and safeguards

maincubes one GmbH places compliance with regulatory and legal requirements as well as unconditional orientation on the operational needs for compliance with contracts with employees, customers, cooperation partners at the forefront of information security.

maincubes one GmbH safeguards its interests, especially its working capacity, trustworthiness and reliability for cooperation partners and customers as well as public reputation, especially with regard to IT-based tools and means of communication.

Risk analysis is the basis for the Information Security Management System (ISMS). It is based on the company values, potential risks to them and the probability of the occurrence and effects of such risks. The risk analysis takes into account legal requirements as well as customer-specific and internal requirements. The criteria for risk analysis are described in detail in the methodology for risk analysis and risk treatment.

maincubes one GmbH has implemented, announced and lives a process for handling information security incidents.

The following general objectives have been defined by the management of maincubes one GmbH:

**maincubes one GmbH...**

- ...ensures the availability of systems and services in product development.
- ...protects integrity and confidentiality of the data and programs generated or used.
- ...ensures the protection of authenticity, confidentiality, integrity, commitment and availability of received, generated, processed and stored information, e.g. documentation, design specification of own products, source code of own products, test data, development and test environments and requirements, specifications or test data provided by customers.
- ...checks the correctness and quality of the third-party software used.
- ...protects buildings, rooms, IT systems from unauthorized access.
- ...avoids violations of legal or contractual agreements.
- ...expects a high degree of reliability of action, also with regard to the handling of information (availability, confidentiality, integrity).
- ...maintains a good reputation of the company with the public.
- ...strives for trouble-free operation of the IT systems in order to guarantee a high degree of availability for information processing and data. In the event of a loss of the information and communication technology in the course of business due to security deficiencies, regular operations must not be severely impaired.
- ...protects the integrity of IT systems and data to meet regulatory and legal requirements and requirements from contracts with employees, customers and cooperation partners and to ensure the reliability of information processing.
- ...protects its IT systems and data from misuse, improper use and unauthorized use to protect itself, its employees, customers, partners and other third parties.
- ...protects its IT systems and data from unauthorized access to prevent the data spying.
- ...protects the personal rights of its employees.
- ...carries out regular audits to ensure compliance with the requirements.
- ...aims to obtain a complete overview of the information security situation in the company and thus to enable risk-oriented and business administrative control of the risk-mitigating measures.
- ...aims to enable the company to adequately preserve and protect corporate assets of any kind, regardless of the IT security know-how of individuals.
- ...has the goal of enabling every employee of the company to actively participate in the protection of information assets according to their role and task through training and further education.

The measures to achieve these goals include technical and organisational preparedness as well as binding rules and standards for all employees. They are written in the form of guidelines, policies and procedural instructions and stored in a central location on the intranet. They are to be followed.

The strategy was developed with the aim of making efficient use of all available resources. All areas of maincubes one GmbH should be enabled to protect their information with the possibilities of modern technology and information security methods.

## 6. Responsibilities

Achieving and maintaining an adequate level of security requires continuous commitment from all those involved in information processing, planning and administration.

- **Management** bears overall responsibility for information security and in particular for risk acceptance. It initiates and coordinates the relevant activities and ensures the necessary priority and attention for information security issues. Management is particularly responsible for the organisational anchoring of activities for the establishment, maintenance and further development of information security (information security process) as well as for the technical and personnel resources for information security and their appropriate embedding in the structures and hierarchy of the company.

- **The Information Security Working Group** supports management in the company-wide coordination and control of information security measures. It develops concrete proposals of a technical and organisational nature to improve information security. It is also responsible for assessing existing information security, identifying new threats and coordinating the individual security measures in such a way that an appropriate level of security is achieved with as little effort as possible.

- **The IT managers or the information security officer** in cooperation with the data centre manager, the chief technology officer, and external consultants define measures that they believe must be taken to improve and maintain security in their respective areas of responsibility. They also react on their own responsibility in the event of breaches of and non-compliance with safety regulations.

- **The administrators** implement the necessary technical and organisational measures to secure the IT infrastructure in close coordination with the respective IT managers. They develop concrete instructions for the users of the IT infrastructure, also with regard to information security. They are invited to submit suggestions for improving information security to the working group or to those responsible for IT.

- **Supervisors with personnel responsibility** ensure that the technical and organisational measures for information security are implemented with regard to the employees reporting to them or the users working in their area of responsibility.

- Through his or her behaviour, **every user** contributes to the guarantee and continuous improvement of information security and thus bears responsibility for information security. Each user is individually informed about the available security measures and mechanisms and takes care to apply them consistently. To this end, all employees receive information, training and support in handling the IT systems and with regard to the security mechanisms that affect them.

## 7. Sanctions

Every employee of maincubes one GmbH is obliged to handle the information, applications, IT systems and communication networks of the company with care. Intentional or grossly negligent breaches of information security, such as, for example:

- the misuse of data, which can lead to financial or reputation losses
- unauthorised access to or alteration of information and unauthorised transmission
- the use of hardware and/or software that has not been approved or tested before use
- the illegal use of company information
- endangering the information security of customers, other companies or institutions

may result in disciplinary consequences, including termination of employment, but may also result in criminal and civil law consequences. Claims can be asserted in the event of financial loss, liability and/or recourse.