maincubes one GmbH
Tilsiter Str.1
D-60487 Frankfurt a. M.
www.maincubes.com

GF: Oliver Menzel, Albrecht Kraas,
Dr. Markus Wiedenmann
HRB: 95527, Frankfurt/Main
USt-ID: DE286899718

Informationssicherheits-Managementsystem Leitlinie

Information Security Management System Guidelines

Vertraulichkeitsstufe: öffentlich / Confidentiality level: Public

Dokumenteninformation / Document information

Bearbeitungsvermerk / Processing note

	Name und Funktion/ Name and position	Version/ Version	Datum/ Date	Unterschrift/ Signature
Erstellt von/ Created by	Arbeitskreis ISMS/ ISMS Working Group	1.0	16.03.2018	
Geprüft von/ Reviewed by	ProcessHouse via Workflow	1.7	Via Workflow	Via Workflow
Genehmigt von/ Approved by	CTO via Workflow	1.7	Via Workflow	Via Workflow

Änderungshistorie / Change history

Datum/ Date	Bearbeiter/ Editor	Version/ Version	Änderungsgrund – Änderungen/ Reason for changes(s)
18.04.2018	Arbeitskreis ISMS/ ISMS Working Group	1.1	Erhaltung und fortlaufende Verbesserung des ISMS als Verpflichtung für jeden Mitarbeiter ergänzt. / Maintenance and continuous improvement of the ISMS as an obligation for every employee
23.05.2018	Arbeitskreis ISMS/ ISMS Working Group	1.2	Verantwortlichkeiten auf Rollen beschränkt. / Responsibilities limited to roles.
02.08.2018	Arbeitskreis ISMS/ ISMS Working Group	1.3	Vorbereitung der Erweiterung des Anwendungsbereiches / Preparation for the extension of the scope of application
06.03.2019	Arbeitskreis ISMS/ ISMS Working Group	1.4	Anpassung Dokumentenlenkung: Entfernung personenbezogener Daten / Adaptation document control: removal of personal data
15.01.2020	Arbeitskreis ISMS/ ISMS Working Group	1.5	Dokumentenreview und englische Fassung erstellt / Einfügen Bedeutung DC Manager

			Document review and English version created / insert meaning DC Manager
30.06.2020	ProcessHouse	1.6	Formale Anpassung an die Dokumentenlenkung / Formal adaptation to document control
11.05.2021	ProcessHouse	1.7	Formale Anpassung an die Dokumentenlenkung / Formal adaptation to document control

Inhaltsverzeichnis

1. Präambel

Note: English-speaking readers of this document will start at **„Ende des deutschen Teils – Begin of the English part“** (see table of contents).

Die vorstehende Leitlinie ist Bestandteil des ISMS ISO27001 der maincubes. Das Rahmenwerk wird sukzessive in weiteren Unternehmen der maincubes Gruppe eingeführt, die sich auch im nicht-deutschsprachigen Ausland befinden. Um auch dort dieses einheitliche Rahmenwerk verwenden zu können, sind neben dem bindenden deutschen Text Übersetzungen in Englisch oder in der jeweiligen Landessprache als Anhang beigefügt.

2. Gleichstellungshinweis

Im folgenden Dokument wird für die Beschreibung von Aufgaben, Funktionen oder Rollen aus Vereinfachungsgründen die männliche Schreibweise gewählt. Mit der gewählten Schreibweise werden in diesem Dokument alle Geschlechter angesprochen, denen Aufgaben, Funktionen oder Rollen zugeordnet werden, ohne eine Wertung ihres Geschlechts, ihrer physischen oder psychischen Fähigkeiten, oder eine sonstige Wertung vorzunehmen.

3. Zweck, Anwendungsbereich und Benutzer

Diese ISMS Leitlinie ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für das Informationssicherheits-Managementsystem (ISMS) auf Basis der ISO/IEC 27001:2013.

Die Geschäftsführung der maincubes one GmbH verabschiedet hiermit folgende ISMS-Leitlinie.

Zielsetzung dieser Leitlinie ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für das Informationssicherheits-Management im Hause der maincubes one GmbH.

Die maincubes one GmbH richtet ihre Unternehmenspolitik darauf aus, spezialisiert in den Kernkompetenzen Colocation und Secureexchange zu sein. So unterstützt die maincubes one GmbH ihre Kunden bei der optimalen Gestaltung ihrer Arbeitsprozesse.

Die maincubes one GmbH bietet ihren Kunden und Partnern sichere Services in Rack – Cage – Suite und Strom in bester Qualität und Energieeffizienz, geführt aus Deutschland.

Um diese Leistungen zu gewährleisten, ist die maincubes one GmbH in einem höchsten Maße zur Erfüllung der Geschäftsprozesse verpflichtet, und um mit nationalen und internationalen Kunden und Partnern zusammenarbeiten zu können, auf die Verfügbarkeit moderner Informations- und Kommunikationstechnik angewiesen.

Darüber hinaus bestehen Verpflichtungen zur Gewährleistung der Informationssicherheit aufgrund gesetzlicher Bestimmungen und vertraglicher Verpflichtungen gegenüber Projektpartnern, Mitarbeitern und Kunden.

Dem Schutz der Informations- und Kommunikationsinfrastruktur des Unternehmens vor Missbrauch, Manipulation, Störungen, dem Ausspähen vertraulicher Informationen usw. – kurz: der Informationssicherheit – kommt daher eine immer größere Bedeutung zu.

Aus diesen Grund hat die Geschäftsführung die nachstehenden Leitlinien für den Umgang mit der Informationstechnik des Unternehmens beschlossen. Diese Leitlinien sind Aufforderung und Verpflichtung zu gesetzeskonformen Verhalten und zu einem verantwortungsbewussten Umgang mit der IT-Infrastruktur des Unternehmens und der Kunden.

Diese Leitlinien gelten für Mitarbeiterinnen und Mitarbeiter sowie Auszubildende, Trainees, Praktikanten, Diplomanden, Werkstudenten und geringfügig Beschäftigte (im Folgenden auch Mitarbeiter genannt) und alle Externen mit einer Funktion im Anwendungsbereich des Informationssicherheits-Managementsystems. Sie werden allen Mitarbeitern und den entsprechenden Externen in geeigneter Weise zur Kenntnis gegeben.

4. Begriffe und Abkürzungen

- **Vertraulichkeit:**
  - Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.
- **Integrität:**
  - Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten.
- **Verfügbarkeit:**
  - Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich und nutzbar zu sein.
- **Informationssicherheit:**
  - Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
- **Informationssicherheits-Managementsystem (ISMS):**
  - Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.

5. Informationssicherheitsziele und Schutzmaßnahmen

Die maincubes one GmbH stellt sowohl die Einhaltung regulatorischer und gesetzlicher Anforderungen, als auch die unbedingte Ausrichtung an den betrieblichen Erfordernissen zur Einhaltung von Anforderungen aus Verträgen mit Mitarbeitern, Kunden und Kooperationspartnern in den Mittelpunkt der Informationssicherheit.

Die maincubes one GmbH schützt Ihre Interessen, insbesondere die Arbeitsfähigkeit, die Vertrauenswürdigkeit und Zuverlässigkeit für Kooperationspartner und Kunden sowie das Ansehen in der Öffentlichkeit, auch und gerade in Bezug auf die IT-basierten Arbeits- und Kommunikationsmittel.

Basis des Informationssicherheits-Managementsystems stellt die Risikoanalyse dar. Sie basiert auf den Unternehmenswerten, deren möglichen Gefährdungen und der Wahrscheinlichkeit des Auftretens sowie den Auswirkungen dieser Gefährdungen. Die Risikoanalyse berücksichtigt sowohl gesetzliche Anforderungen wie auch kundenspezifische und interne Anforderungen. Kriterien und Funktionsweise der Risikoanalyse werden detailliert in der Methodik zur Risikoanalyse und Risikobehandlung beschrieben.

Die maincubes one GmbH hat einen Prozess für die Handhabung von Informationssicherheitsvorfällen implementiert, bekanntgegeben und lebt diesen.

Die nachfolgenden übergeordneten allgemeingültigen Ziele wurden durch die Geschäftsführung der maincubes one GmbH festgelegt:

Die maincubes one GmbH…

- …stellt die Verfügbarkeit von Systemen und Diensten bei der Produktentwicklung sicher.
- …schützt Integrität und Vertraulichkeit der erzeugten bzw. verwendeten Daten und Programme.
- …stellt den Schutz von Authentizität, Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit von erhaltenen, erzeugten, verarbeiteten und gespeicherten Informationen, z. B. Dokumentation, Designspezifikation zu den eigenen Produkten, Quellcode eigener Produkte, Testdaten, Entwicklungs- und Testumgebungen und von Kunden bereitgestellte Anforderungen, Spezifikationen oder Testdaten sicher
- …prüft Korrektheit und Qualität eingesetzter Fremdsoftware.
- …schützt Gebäude, Räume, IT-Systeme vor unberechtigtem Zutritt oder Zugang.
- …vermeidet Verstöße gegen gesetzliche oder vertragliche Vereinbarungen.
- …erwartet eine hohe Verlässlichkeit des Handelns, auch in Bezug auf den Umgang mit Informationen (Verfügbarkeit, Vertraulichkeit, Integrität).
- …wahrt einen guten Ruf des Unternehmens in der Öffentlichkeit.
- …strebt einen möglichst störungsfreien Betrieb der IT-Systeme an, um eine hohe Verfügbarkeit der Informationsverarbeitung und der Daten zu gewährleisten. Bei einem Ausfall der Informations- und Kommunikationstechnik im Geschäftsablauf durch Sicherheitsmängel darf der Regelbetrieb nicht stark beeinträchtigt werden.
- …schützt die Integrität der IT-Systeme und Daten, um regulatorische und gesetzliche Anforderungen und Anforderungen aus Verträgen mit Mitarbeitern, Kunden und Kooperationspartnern zu erfüllen und die Zuverlässigkeit der Informationsverarbeitung zu gewährleisten.
- …schützt ihre IT-Systeme und Daten vor Missbrauch, zweckwidriger Nutzung und vor der Nutzung durch Unbefugte, um sich selbst, die Beschäftigten, Kunden, Partner und sonstige Dritte zu schützen.
- …schützt ihre IT-Systeme und Daten vor unberechtigtem Zugriff, um das Ausspähen von Daten zu verhindern.
- …wahrt die Persönlichkeitsrechte ihrer Mitarbeiter.

- …führt regelmäßige Audits zur Sicherstellung der Einhaltung der Anforderungen durch.

- …hat das Ziel, einen vollständigen Überblick über die Lage der Informationssicherheit im Unternehmen zu erlangen und damit eine risikoorientierte und betriebswirtschaftliche Steuerung der risikominimierenden Maßnahmen zu ermöglichen.

- …hat das Ziel, das Unternehmen in die Lage zu versetzen, Unternehmenswerte gleich welcher Art angemessen zu bewahren und zu schützen, unabhängig von dem IT-Sicherheits-Knowhow von Einzelpersonen.

- …hat das Ziel, jeden Mitarbeiter des Unternehmens durch Aus- und Weiterbildung in die Lage zu versetzen, gemäß seiner Rolle und Aufgabe an dem Schutz der Informationswerte aktiv mitzuwirken.

Die Maßnahmen zur Erreichung der Ziele umfassen sowohl technische und organisatorische Vorkehrungen, als auch für alle Mitarbeiter verbindliche Regeln und Vorgaben. Sie werden in Form von Leitlinien, Policies und Verfahrensanweisungen etc. verfasst und an einer zentralen Stelle im Intranet hinterlegt. Sie sind zu befolgen.

Die Strategie wurde mit der Überlegung ausgearbeitet, alle zur Verfügung stehenden Ressourcen effizient zu nutzen. Es sollen alle Bereiche der maincubes one GmbH in die Lage versetzt werden, ihre Informationen mit den Möglichkeiten der modernen Technik und den Methoden der Informationssicherheit zu schützen.

6. Verantwortlichkeiten

Das Erreichen und das Erhalten eines angemessenen Sicherheitsniveaus erfordert ein kontinuierliches Engagement von allen an der Informationsverarbeitung und an deren Planung und Administration beteiligten Personen.

- **Die Geschäftsleitung** trägt die Gesamtverantwortung für die Informationssicherheit und insbesondere für die Risikoakzeptanz. Sie initiiert und koordiniert die entsprechenden Aktivitäten und sorgt für die nötige Priorität und Aufmerksamkeit für Fragen der Informationssicherheit. Die Geschäftsleitung ist insbesondere verantwortlich für die organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung der Informationssicherheit (Informationssicherheitsprozess) sowie für die technische und personelle Ressourcen-Ausstattung für die Informationssicherheit und deren angemessene Einbettung in die Strukturen und die Hierarchie des Unternehmens.

- **Der Arbeitskreis Informationssicherheit** („AK ISMS“, eingebettet in das ProcessHouse) unterstützt die Geschäftsleitung bei der firmenweiten Koordinierung und Lenkung der Informationssicherheitsmaßnahmen. Er erarbeitet konkrete Vorschläge technischer und organisatorischer Art zur Verbesserung der Informationssicherheit. Er hat darüber hinaus die Aufgabe, die bestehende Informationssicherheit zu bewerten, neue Gefahren zu erkennen und die einzelnen Sicherheitsmaßnahmen so zu koordinieren, dass ein angemessenes Sicherheitsniveau mit möglichst geringem Aufwand erreicht wird.

- **Die IT-Verantwortlichen bzw. der Informationssicherheitsbeauftragte** in Zusammenarbeit mit dem Datacenter Manager, dem Chief Technology Officer und externen Beratern legen Maßnahmen fest, die aus ihrer Sicht zur Verbesserung und Erhaltung der Sicherheit in ihrem jeweiligen

Wirkungsbereich ergriffen werden müssen. Sie reagieren außerdem eigenverantwortlich bei Verstößen gegen die und bei Nichtbeachtung von Sicherheitsvorgaben.

- **Die Administratoren** setzen in enger Abstimmung mit dem jeweiligen IT-Verantwortlichen die notwendigen technischen und organisatorischen Maßnahmen zur Absicherung der IT-Infrastruktur um. Sie erarbeiten konkrete Handlungsanweisungen für die Benutzer der IT-Infrastruktur auch in Bezug auf die Informationssicherheit. Sie sind aufgefordert, Vorschläge für die Verbesserung der Informationssicherheit dem Arbeitskreis bzw. den IT-Verantwortlichen zu unterbreiten.

- **Die Datacenter Manager** sind verantwortlich für den technischen und organisatorischen Betrieb des Rechenzentrums. Sie sorgen dafür, dass die Anforderungen der ISO 27001 bei der Planung und Umsetzung betrieblicher RZ-Prozesse erfüllt werden. Sie sind maßgeblich an der Implementierung, Überwachung und Weiterentwicklung des ISMS bei maincubes beteiligt.

- **Die Vorgesetzten mit Personalverantwortung** stellen sicher, dass die technischen und organisatorischen Maßnahmen zur Informationssicherheit in Bezug auf die ihnen unterstellten Mitarbeiter bzw. die in ihrem Verantwortungsbereich tätigen Nutzern umgesetzt werden.

- **Jeder Nutzer** trägt durch sein Verhalten zur Gewährleistung und fortlaufenden Verbesserung der Informationssicherheit bei und trägt damit Verantwortung für die Informationssicherheit. Jeder Nutzer wird individuell über die zur Verfügung stehenden Sicherheitsmaßnahmen und -mechanismen informiert und achtet darauf, sie konsequent anzuwenden. Zu diesem Zweck erhalten alle Mitarbeiter Informationen, Schulung und Betreuung im Umgang mit den IT-Systemen und in Hinblick auf die sie betreffenden Sicherheitsmechanismen.

7. Sanktionen

Jede/r Mitarbeiter/in der maincubes one GmbH ist zu einem sorgfältigen Umgang mit den Informationen, den Anwendungen, informationstechnischen Anlagen und Systemen und den Kommunikationsnetzen des Unternehmens verpflichtet. Vorsätzliche oder grob fahrlässige Verletzungen der Informationssicherheit, wie zum Beispiel:

- der Missbrauch von Daten, der zu finanziellen oder Reputationsverlusten führen kann
- der unberechtigte Zugriff auf Informationen oder ihre Änderung und unbefugte Übermittlung
- die Verwendung nicht zugelassener oder nicht vor der Anwendung geprüfter Hard- und/oder Software
- die illegale Nutzung von Unternehmensinformationen
- die Gefährdung der Informationssicherheit von Kunden, anderer Unternehmen oder Institutionen

können disziplinarische Folgen bis hin zur Kündigung des Arbeitsverhältnisses, aber gegebenenfalls auch straf- und zivilrechtliche Konsequenzen nach sich ziehen. Bei finanziellem Schaden können Haftungs- und/oder Regressforderungen geltend gemacht werden.

„Ende des deutschen Teils – Begin of the English part“

Attachment: Information Security Management System Guidelines

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.