meteoviva

Guideline on information security

Contents

1 Introduction

As a SaaS (Software as a Service) provider, automated information processing plays a key role in the provision of services by meteoviva GmbH. The confidentiality, integrity and availability of the processed data are therefore of existential importance for the success, reputation and continued existence of the company. Against this background, an appropriate level of information security must be organised in the business processes of meteoviva GmbH.

The management of meteoviva GmbH is responsible for the proper and secure fulfilment of tasks and thus for information security. In particular, it is responsible for

- the creation of organisational framework conditions for the sustainable guarantee of information security,
- defining and establishing the necessary responsibilities and authorisations,
- the establishment of an information security management system,
- the implementation of the agreed security measures, including the provision of the necessary budgetary resources,
- sufficient and appropriate documentation of the IT infrastructure as well as all security precautions and security measures,

meteoviva GmbH has established, implemented, maintains and continuously improves an information security management system (ISMS) in accordance with the requirements of the international standard DIN ISO/IEC27001:2013.

This guideline describes the general objectives, strategies and organisational structures required for the initiation and establishment of a holistic information security process.

The terms "data" and "information" are used synonymously in this guideline. While data often refers to "raw/unprocessed data" and information to "processed/aggregated data", no distinction is made between data and information in terms of information security.

2 Scope of application

This guideline applies to all employees and German locations of meteoviva GmbH. The guideline and the resulting regulations and measures must be observed and complied with by all employees of meteoviva GmbH. In the event of non-compliance, meteoviva GmbH reserves the right to take action under labour law.

3 Principles and objectives of information security

3.1 Principles

Information security refers to the appropriate maintenance of the security objectives of confidentiality, authenticity and availability for information and associated physical, technical and personal assets in accordance with the business, legal and regulatory requirements of meteoviva GmbH. The form in which the information is presented is irrelevant.

This includes in particular the analysis and treatment of risks that jeopardise the above-mentioned security objectives and are reduced to an acceptable level by implementing appropriate measures. In addition to the security of IT systems and the data stored in them, information security also includes the security of data and information that is not processed and stored electronically. This means:

- **Confidentiality**: Confidential data, information and programs must be protected against unauthorised access and unauthorised disclosure. The objects to be protected include the stored or transported message content, the more detailed information about the communication process (who, when, for how long, with whom, etc.) and the data about the sending and receiving process.
- **Integrity**: The term integrity refers to both information and the entire IT system. The integrity of information means its completeness and correctness. Completeness means that all parts of the information are available. Information is correct if it accurately reflects the facts it refers to. On the other hand, the term integrity also refers to IT systems, as the integrity of information and data can only be ensured if they are processed and transmitted correctly.
- **Availability**: The functions of the hardware and software in the system and network area as well as the necessary information are available to the user at the right time and in the right place.

It is the declared aim of meteoviva GmbH that all facilities used for the creation, storage, backup, processing and transmission of data are selected, integrated and configured in such a way that the appropriate level of confidentiality, integrity and availability of the data processed on them is ensured at all times and under all circumstances. This expressly includes all employees involved as well as German locations. Information security concerns must be taken into account when

- the classification, labelling, handling, transmission and protection of information,
- the control of access to information,
- the development, introduction, operation and maintenance of products,
- personnel security,
- the procurement and disposal of IT products,
- the use of third-party services,
- the handling of information security incidents and emergencies
- Change management processes

Technical and organisational security measures must be designed in such a way that they are always an integral part of all business processes. Information security issues must be taken into account

- in the design of the organisation,
- in the creation and filling of functions and roles,
- in the management, training and development of employees,
- the design of management, core and support processes,
- co-operation with other authorities and external parties,
- the selection and use of aids,
- the development and provision of products and services.

The security measures must be in an economically justifiable proportion to the damage that can be caused by security incidents. This is defined by the value of the information and IT systems to be protected. As a rule, the effects on the physical and mental integrity of people, the right to informational self-determination, financial damage, reputational damage and the consequences of violations of the law must be assessed. The necessary resources (personnel, material and investment funds) must be made available to implement the necessary and appropriate security measures.

- If attacks on the security of the IT infrastructure of meteoviva GmbH threaten or become known or other security risks arise, the availability of IT applications, data and networks may be temporarily restricted in accordance with the risk of threat and damage. In the interests of the functionality of the company as a whole, protection against damage takes priority. Reasonable restrictions in operation and convenience must be accepted. This applies in particular to transitions to other networks, especially the Internet.
- Employees must be sensitised and trained to the necessary extent with regard to information security.

3.2 Goals

The objectives set out in the following sections serve to fulfil the legal, regulatory and contractual requirements placed on meteoviva. They are reviewed at least once a year and updated if necessary.

3.2.1 Confidentiality

The data collected, stored, processed and forwarded in IT systems must be treated confidentially in accordance with their classification and protected against unauthorised access at all times. To this end, the group of persons to whom access is to be authorised must be determined for all data. Access to IT systems, IT applications, data and information must be restricted to the absolutely necessary group of persons. Each employee is only authorised to access the data they need to fulfil their official duties.

3.2.2 Authenticity

The data collected, stored, processed and forwarded in IT systems should be able to be assigned to their origin at any time so that the characteristics of authenticity, verifiability and trustworthiness can be ensured.

3.2.3 Integrity

Information and software products must be protected against unintentional modification and intentional falsification. All software products should always provide up-to-date and complete information. Any process or information processing-related restrictions must be documented.

3.2.4 Availability

For all IT systems used in production, the times during which they should be available must be defined. Business interruptions should be largely avoided during these times, i.e. their number and duration should be limited. The description of the necessary availability includes

- the regular operating hours,
- the maximum tolerable duration of individual failures.

Regularly scheduled downtimes, particularly for maintenance purposes, must also be defined.

4 Responsibilities

4.1 Management

The management of meteoviva GmbH assumes overall responsibility for the ISMS. It issues binding rules on information security and communicates them to employees. It ensures that the current rules are available at all times.

4.2 Employees

All employees ensure information security through responsible behaviour and comply with the laws, regulations, guidelines, instructions and contractual obligations relevant to information security. They handle the IT systems, data and information they use correctly and responsibly.

4.3 External service providers

Persons and companies that do not belong to meteoviva GmbH but provide services for it (contractors) must comply with the client's requirements for compliance with the information security objectives in accordance with this guideline. The client shall inform the contractor of these rules and obligate it to comply with them in an appropriate manner. This also means that the Contractor must inform the Client of any recognisable deficiencies and risks in the security measures used.

5 Information security organisation

5.1 Information security officer

meteoviva GmbH appoints an Information Security Officer (ISO) who is responsible for all matters and questions relating to information security. It must be ensured that this employee has an appropriate proportion of their working time available to fulfil their duties as ISO.

In addition to the ISO, a security management team is appointed with one employee from each department who takes a leading role in the implementation of and compliance with information security in their respective areas.

6 Realisation

This guideline forms the basis for the creation of further, subject-spefific guidelines, information security concepts and detailed regulations and instructions on information security. They are implemented as part of an IS process and certification in accordance with ISO 27001.

7 Continuous improvement

The information security process must be regularly reviewed to ensure that it is up to date and effective. This includes, among other things, a regular review of the current risk assessment and treatment. In particular, the measures implemented must be regularly analysed to determine whether they are known to the employees concerned, can be implemented and can be integrated into the operational process.

The management levels support the continuous improvement of the safety level.

Employees are encouraged to pass on possible improvements or weaknesses to the relevant departments.

The desired level of security and data protection is ensured by continuously reviewing the regulations and ensuring compliance with them. Deviations are analysed with the aim of improving information security and keeping it constantly up to date.

8 Signatures of management

Jülich, 05.04.2024

Digital
unterschrieben
von Stefan Hardt
Ort: Jülich

Digital
unterschrieben
von WOLFGANG
UWE GROßMANN

Dr Stefan Hardt

Uwe Großmann