MeteoViva

Information Security Guideline

1 Introduction

As a SaaS (Software as a Service) provider, automated information processing plays a key role in the service provision of MeteoViva GmbH. Therefore, confidentiality, integrity and availability of the processed data are 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 execution of tasks and thus for information security. It is responsible for

- the creation of organizational framework conditions for the sustainable guarantee of information security,
- defining and establishing the necessary responsibilities and powers,
- 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 and all security precautions and security measures,

MeteoViva GmbH has established, implements, 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 which are necessary 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 with regards to information security.

2 Scope

This guideline applies to all employees and German locations of MeteoViva GmbH. The guidelines and the resulting regulations and measures must be observed and complied with by all employees of MeteoViva GmbH. MeteoViva GmbH reserves the right to take legal action in the event of non-compliance.

3 Principles and objectives of information security

3.1.1 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. It is irrelevant in which form the information is presented.

This includes in particular the analysis and handling of risks which endanger the above-mentioned security objectives, and which are reduced to an acceptable level through the implementation of 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 electronically processed and stored. In this context:

- **Confidentiality**: Confidential data, information and programs must be protected against unauthorized access and unauthorized disclosure. The objects to be protected include the stored or transported message contents, detailed information about the communication process (who, when, 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. Integrity of information means its completeness and correctness. Completeness means that all parts of the information are available. Information is correct if it reflects the described facts unaltered. On the other hand, the term integrity also refers to IT systems, since the integrity of information and data can only be ensured if they are processed and transmitted properly
- **Availability**: The functions of the hardware and software in the system and network area as well as 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 is ensured for the data processed on them at all times and under all circumstances. This expressly includes all employees involved and German locations. Information security concerns are to be considered for:

- the classification, labelling, handling, transmission and protection of information
- the control of access to information,
- the development, introduction, operation and maintenance of products
- of personnel security,
- the procurement and removal / 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 concerns must be taken into account

- in the design of the organization,
- in the creation and filling of functions and roles,
- in the management, training and further education of employees,

- the design of management, core and support processes,
- cooperation with other authorities and external parties,
- the selection and use of aids,
- the development and provision of products and services.

Security measures shall be economically proportionate to the damage that may be caused by security incidents. This is defined by the value of the information to be protected and the IT systems. As a rule, the effects on the physical and mental integrity of people, the right to informational self-determination, financial damage, damage to reputation and the consequences of violations of the law must be assessed. The necessary resources (personnel, material and investment resources) must be provided for the implementation of the necessary and appropriate security measures.

- If attacks on the security of the IT infrastructure of MeteoViva GmbH are imminent or known to occur, or if other security risks arise, the availability of IT applications, data and networks may be temporarily restricted in accordance with the risk of threats and damage. In the interest of the functionality of the entire company, protection against damage is paramount. Reasonable restrictions in operation and comfort must be accepted. This applies in particular to the transitions to other networks, especially to the Internet.
- The employees are to be sensitized and qualified to the necessary extent with regard to information security.

3.2 Objectives

The objectives set out in the following sections are designed to meet the legal, regulatory and contractual requirements placed on MeteoViva. They are reviewed at least annually and updated as necessary.

3.2.1 Confidentiality

The data collected, stored, processed and passed on in IT systems must be treated confidentially according to their classification and protected against unauthorised access at all times. For this purpose, the group of persons to whom access is to be granted must be determined for all data. Access to IT systems, IT applications and data as well as information is to be restricted to the group of persons absolutely necessary. Each employee shall be granted access authorisation only to the data that he/she requires to perform his/her official duties.

3.2.2 Authenticity

The data collected, stored, processed and passed on 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 alteration and deliberate falsification. All software products should always provide up-to-date and complete information. Any restrictions in the processing of information or procedures must be documented.

3.2.4 Availability

For all IT systems used in production, the times at which they are to be available must be specified. Business interruptions during these times must be avoided as far as possible, i.e. limited in number and duration. The description of the necessary availability includes

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

Regularly scheduled downtimes, especially for maintenance purposes, also need to be specified.

4 Responsibilities

4.1 Management

The management of MeteoViva GmbH assumes overall responsibility for the ISMS. It issues binding rules on information security and makes them known to the employees. It ensures that the current rules can be read at any time.

4.2 Employees

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

4.3 Contractors

Persons and companies that do not belong to MeteoViva GmbH but provide services for them (contractors) must comply with MeteoViva's specifications for compliance with the information security objectives in accordance with this guideline. The Client shall inform the Contractor of these rules and shall oblige the Contractor to comply in an appropriate manner. This also includes that the Contractor must inform the Client in the event of recognizable defects and risks of security measures used.

5 Information Security Organisation

5.1 Information Security Officer

MeteoViva GmbH appoints a Corporate Information Security Officer (CISO), who is responsible for all matters and questions of information security. It must be ensured that this employee has an appropriate proportion of his or her working time available to carry out his or her duties as an CISO.

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

6 Implementation

This guideline forms the basis for the preparation of further subject-specific guidelines, information security concepts and detailed regulations and service instructions on information security. It is implemented within the framework of an IS process and certification according to ISO 27001.

7 Continuous improvement

The information security process is to be regularly reviewed for its topicality and effectiveness. This includes, among other things, a regular revision of the current risk assessment and handling. In particular, the implemented measures are to be regularly examined to see whether they are known to the employees concerned, can be implemented, and can be integrated into the operating process.

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

The employees are required to pass on possible improvements or weaknesses to the appropriate departments.

The desired level of security and data protection is ensured by a continuous revision of the regulations and their compliance. Deviations are analysed with the aim of improving information security and keeping it constantly up to date.

Julich, March 30th, 2020

Signatures of the management

Dr. Stefan Hardt Dr. Jan Scheffler

Document History

Classification	Public		Last Review:	09.06.2020
Distribution	Employees, Customers, interested parties		Next Review:	28.08.2020
File Name	Information Security Guideline.docx			
Version	Date	Change	Author	Clearance
0.1	08.06.2020	Translation of German document in Version 3.0	Stefan Hardt	
1.0	09.06.2020	Review and Signoff		Stefan Hardt Jan Scheffler