memodio GmbH

INFORMATION SECURITY POLICY

Created by:	Paul Zimmermann
Approved by:	Doron B. Stein

Change history

Date	Version	Created by	Description of change
February 6, 2024	V0.1	Paul Zimmermann	New status: in progress. Comment: /
February 9, 2024	V0.1	Paul Zimmermann	New status: in progress. Comment: /
February 9, 2024	V0.1	Paul Zimmermann	New status: in review. Comment: /
February 9, 2024	V0.2	Doron B. Stein	New status: in progress. Comment: /
February 9, 2024	V0.2	Paul Zimmermann	New status: in review. Comment: /
February 12, 2024	V0.3	Doron B. Stein	New status: in progress. Comment: /
February 12, 2024	V0.3	Paul Zimmermann	New status: in approval. Comment: /
February 12, 2024	V1	Doron B. Stein	New status: approved. Comment: /
February 15, 2024	V1.1	Paul Zimmermann	New status: in progress. Comment: /
April 22, 2024	V1.1	Paul Zimmermann	New status: in approval. Comment: No changes, has been accidentally re-opened
April 22, 2024	V2	Doron B. Stein	New status: approved. Comment: /
July 18, 2024	V2.1	Paul Zimmermann	New status: in progress. Comment: /

July 18, 2024	V2.1	Paul Zimmermann	New status: in approval. Comment: Changed classification to public, in order to publish on our webpage
July 18, 2024	V2.1	Paul Zimmermann	New status: in progress. Comment: /
July 18, 2024	V2.1	Paul Zimmermann	New status: in approval. Comment: Add paragraph that it should be made public, changed classification to public
July 18, 2024	V3	Doron B. Stein	New status: approved. Comment: /
July 22, 2024	V3.1	Paul Zimmermann	New status: in progress. Comment: /
July 22, 2024	V3.1	Paul Zimmermann	New status: in approval. Comment: Update information security commitment & Climate change information
July 22, 2024	V4	Doron B. Stein	New status: approved. Comment: /

1. Purpose, scope and users

The aim of this top-level Policy is to define the purpose, direction, principles, and basic rules for information security management.

This Policy is applied to the entire Information Security Management System(ISMS), as defined in the ISMS Scope Document.

Users of this document are all employees of memodio GmbH, as well as relevant external parties.

2. Reference documents

- ISO/IEC 27001 standard, clauses 5.2, 5.3, 6.2, 7.4 and A.6.3
- ISMS Scope Document
- Risk Assessment and Risk Treatment Methodology
- Statement of Applicability
- Register of legal, contractual and other requirements

3. Basic information security terminology

Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.

Integrity – characteristic of the information by which it may be changed only by authorized persons or systems in an allowed way.

Availability – characteristic of the information by which it can be accessed by authorized persons when it is needed.

Information security – preservation of confidentiality, integrity, and availability of information.

Information Security Management System – part of the overall management processes that take care of planning, implementing, maintaining, reviewing, and improving the information security.

4. Managing the information security

4.1. Objectives and measurement

General objectives for the whole Information Security Management System, as well as operational objectives for particular security documents are proposed by the CTOor anyone else in the organization; such objectives and their measurement frequency are approved by theCEO through the Conformio platform and are documented in the List of Security Objectives. These security objectives must be in line with the organization's business objectives, strategy, and business plans.

The CEO is responsible for regular review of security objectives and for proposing updates. All the objectives must be reviewed according to the same frequency as they are measured.

The method for measuring if the security objectives are achieved, as well as responsibilities for measurement, will be defined through the Conformio platform – this will be done when proposing and approving the security objectives. The measurement will be performed at least once a year, and the results will be presented through the Conformio platform during the management review process.

4.2. Information security requirements

This policy and the entire ISMS must be compliant with legal and regulatory requirements relevant to the organization in the field of information security, as well as with contractual obligations.

A detailed list of all contractual and legal requirements is provided in the Register of legal, contractual and other requirements.

4.3. Information security controls

The process of selecting the controls (safeguards) is defined in the Risk Assessment and Risk Treatment Methodology.

The selected controls and their implementation statuses are listed in the Statement of Applicability.

4.4. Responsibilities

Responsibilities for the ISMS are the following:

- The CTO is responsible for ensuring that the ISMS is implemented and maintained according to this Policy, and for ensuring that all necessary resources are available.
- The CTO is responsible for the operational coordination of the ISMS, as well as for reporting about the performance of the ISMS.
- The CTO must review the ISMS at least semi-annually, or each time a significant change occurs. The

purpose of the management review is to establish the suitability, adequacy, and effectiveness of the ISMS.
- The CEO will implement information security training and awareness programs for employees.
- The protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset.
- All security incidents or weaknesses must be reported to CTO.
- The CEO will define which information related to information security will be communicated to which interested parties (both internal and external), by whom, and when.

Information security is an essential value proposition that we are committed to delivering to our customers. A great deal depends on the information security (confidentiality, integrity and availability) of the information that is processed by our solutions. We express this through the following commitment:

1. We are committed to complying with all legal and contractual information security requirements of our customers and partners, and to using information provided by authorities and other organisations to continuously improve information security.
2. We train all employees with information security responsibilities to be confident and aware of information security.
3. We create the necessary technical and organisational conditions to put information security into practice.
4. We want to ensure that information security is not seen by all of us as extra work, but as important and essential for our customers. In spite of all the rules in this area, we must always keep our heads above water and not assume that compliance with the rules will be sufficient in every situation. If we have to choose between making something really safe or following a rule, we're going to choose to make it really safe - and then adjust the rule if necessary.
5 We have a commitment to continuous improvement in our information security.

We will dedicate resources to the above.

We are considering the issue of climate change and are considering its impact on information security.

4.5. Policy communication

The CTO has to ensure that all employees of memodio GmbH, as well as appropriate external parties are familiar with this policy.

5. Support for ISMS implementation

The CTO hereby declares that ISMS implementation and continual improvement will be supported with adequate resources in order to achieve all objectives set in this policy, as well to as satisfy all identified requirements.

6. Validity and document management

This document is valid as of July 22, 2024.

The owner of this document is the CTO, who must check and, if necessary, update the document every 6 months.

This policy should be made public at the memodio webpage, in order to be available to interested

parties.