Fabasoft Group

Guideline for Information Security

Valid as of 9th September 2022

Public

Distribution, publication or duplication is prohibited.

Contents

1 Statement of the Managing Board of Fabasoft AG

Fabasoft is one of the leading European software manufacturers and cloud service providers for digital document control as well as electronic document, process and record management. Numerous prominent private companies and public sector organisations have placed their trust in the quality and experience of Fabasoft for more than three decades.

We rank as a pioneer in the field of information security and data protection. This role must be actively practised. Only if you place high demands on yourself and fulfil these, you can convince customers of your trustworthiness. For this reason the protection of customer and corporate data takes absolute priority. This is underpinned by certifications and audits in compliance with internationally recognised standards. We addresses this desire for transparency and information security with the following aspects: The software products are developed in Europe and operated in secure data centres, which must comply with strict requirement criteria. This builds in particular upon the foundations of a European values system for data security, access security, legal compliance and certified quality standards.

The aims of information security, namely confidentiality, integrity, availability and authenticity, as well as continuous reviewing, assessment and evaluation of the effectiveness of the technical and organisational measures are therefore key values for Fabasoft in all our business activities.

The Managing Board of Fabasoft AG hereby adopts the following Guideline for Information Security as part of the overall Fabasoft strategy.

Prof. Dipl.-Ing. Helmut Fallmann

Chairman of the Managing Board – CEO

Matthias Wodniok	Ing. Oliver Albl
Member of the Managing Board	**Member of the Managing Board - CTO**

2 Introduction

Fabasoft has developed a management system for information security, which addresses in particular the standard ISO/IEC 27001 in conjunction with ISO/IEC 27018, the catalogue of criteria C5 (Cloud Computing Compliance Criteria Catalogue) of the Federal Office for Information Security (BSI), the Trust Services Criteria TSC/SOC 2 and the EU Cloud Code of Conduct. This document constitutes the Guideline for Information Security of the Fabasoft AG and its affiliated companies. The guideline applies to all employees of the Fabasoft Group.

3 Significance of information security and data protection

Confidentiality, integrity, availability and authenticity are key values for Fabasoft in all its business activities. In view of the fact that global cyber-attacks against companies in all sectors are increasing in number, intensity and refinement, Fabasoft is making every effort to continue with the expansion of its cyber resilience. The information security management system (ISMS) and data protection management system (DPMS) established within the company, including the technical and organisational measures, are reviewed, assessed and evaluated regularly by means of internal and external audits with regard to their topicality, effectiveness, efficiency and compliance with internationally recognised standards and criteria catalogues. The resulting certificates and test reports lend transparency to the level of information security and data protection at Fabasoft.

Fabasoft supports all employees in the form of a continuous process on their path to developing a pronounced awareness for information security and data protection. Regular professional awareness training courses are held and possible threat scenarios simulated in order to raise the awareness for the ensuing risks. All employees are aware of their responsibility with regard to the handling of data and IT systems. Compliance and awareness for information security and data protection is embodied and promoted in all corporate divisions.

4 Aims of information security

The following aims of information security are ensured by technical and organisational measures within the framework of the existing ISMS. These measures address the confidentiality, integrity, availability and authenticity of the information to be protected and are regularly reviewed, assessed and evaluated.

Confidentiality

Customer data, business data and data from development areas are subject to the highest demands of confidentiality. No unauthorised persons may gain knowledge of them (restricted access authorisations, levels of confidentiality, encryption, …). Information may only be accessed by authorised persons. All Fabasoft employees are obligated to maintain the applicable data secrecy and confidentiality.

Integrity

Data and information must be correct and complete. IT systems must function end-to-end. Data and information must not be altered without approval. Alterations to information must be clearly identifiable and transparent (versioning).

Availability

Information must be available in compliance with the contractually assured service level. Downtimes must not have any significant impact on Fabasoft and its stakeholders. Information must be processed on systems and services that guarantee the necessary availability. In the event of a breakdown, systems and services must be restored within the agreed period.

Authenticity

It must be guaranteed that information is true, verifiable and credible and that manipulation-free IT systems and IT applications are used.

5 Responsibilities

5.1 The Managing Board of Fabasoft AG

As part of its overall responsibility, the Managing Board determines the aims of information security and by defining the persons responsible for controls and processes, by providing the necessary time and financial resources and by defining the framework conditions ensures that said aims can be achieved.

5.2 Persons responsible for controls and processes

The persons responsible for controls and processes ensure that the controls and processes assigned to them are adequate, effective and efficient. They guarantee that relevant internal and external sources of information are taken into consideration for the functioning of the controls and processes and that the controls are carried out at the defined time or within the defined interval. They communicate the necessary information for the control aims and for their implementation (control performance) to those carrying out the control.

Any new applications, procedures, processes or infrastructure components introduced within the remit of the persons responsible for controls and processes must be integrated. Whereby they ensure here that the risks with regard to information security (confidentiality, integrity, availability and authenticity) are not increased by these new components and procedures or take appropriate countermeasures.

5.3 Head of Security Operations

The Head of Security Operations is responsible for the implementation of the controls and processes as part of information security, supports and controls the activities of the Security Operations Team and consults with the Managing Board.

5.4 Security Operations Team

The Security Operations Team plans the activities necessary for maintaining and enhancing information security, in particular within the framework of the Patch Management, Vulnerability Management and Security Incident Management processes. External penetration tests are coordinated regularly in the Security Operations Team and the general situation with regard to information security and information security incidents discussed. The Security Operations Team is involved in information security-relevant issues and supports the persons responsible for controls and processes as well as departments with ensuring information security.

5.5 Privacy Team

The Privacy Team plans the activities necessary for maintaining and enhancing data protection and data security, in particular within the framework of data protection documentation and responding to the enquiries of data subjects. The Privacy Team cooperates with the commissioned external Data Protection Officers and plans the coordination and implementation of data protection requirements. The Privacy Team is involved in data protection-relevant issues and supports the persons responsible for controls and processes as well as departments with ensuring data protection and data security.

5.6 Employees

Employees are regularly sensitised to information security and data protection, in order to raise security awareness and expertise and so continuously improve security behaviour.

Employees are fully aware of the importance of information security and data protection and take an active role in this respect. They handle the IT systems and the data stored and processed on these in a responsible manner and take care to protect corporate, business and data secrets. Employees implement information security in line with the guidelines and procedures adopted by Fabasoft.