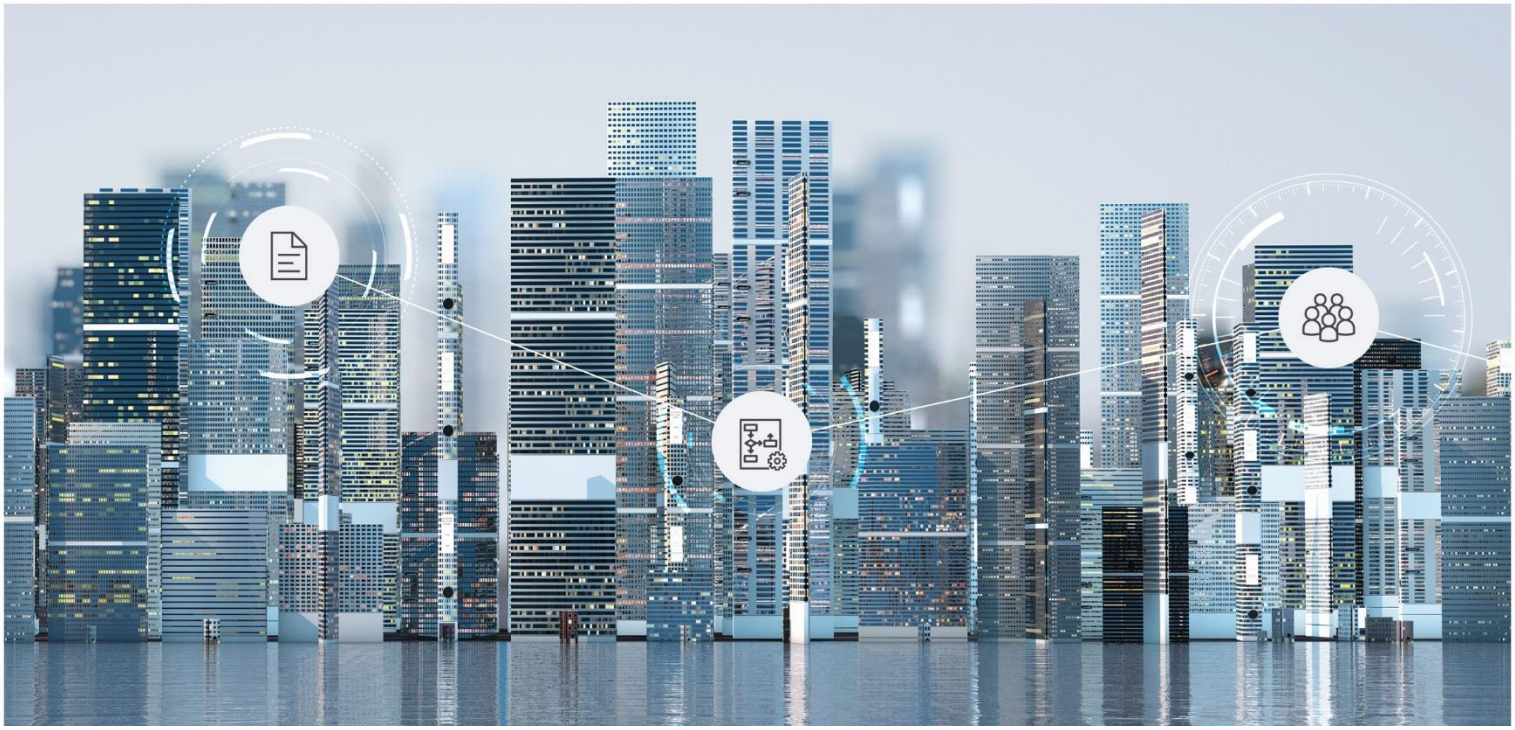

Fabasoft Group

Fabasoft Security Guideline

Valid as of 1st May 2018

Public

Contents

1 Statement of the most senior decision makers

As a European manufacturer of software products and a cloud service provider, Fabasoft is aware of its responsibility vis-à-vis its stakeholders with regard to long-term and sustainable management.

Fabasoft is more than ever convinced that the ethical values in Europe in respect to the design of normative and regulative framework conditions for global digital competition lie most especially in the enforcement of a high standard of data protection. This is the key per se for the most valuable currency in the digital world: namely the unlimited trust of users. Its work on the implementation of this conviction has led to the extensive international and national involvement of Fabasoft in numerous institutions:

EU Cloud Code of Conduct
On a European level Fabasoft is active in particular in supporting the further development of behavioural standards for European cloud computing as part of its intensive participation in the development of a Code of Conduct (CoC). Fabasoft is a founding member of the General Assembly.

European Security Certification Framework
The European Security Certification Framework (EU-SEC) is a research project whose work is aimed at improving the goodwill, effectiveness and efficiency of existing certification systems for cloud security. Fabasoft is a member of the Consortium.

European Telecommunications Standards Institute
The European Telecommunications Standards Institute (ETSI) is an officially recognised standardisation body of the European Standards Organisation (ESO) that is active in the fields of the standardisation of telecommunication, radio and other electronic communication networks and services. Fabasoft is a member of the ETSI.

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

Prof. Dipl.-Ing. Helmut Fallmann **Leopold Bauernfeind**

The Managing Board of Fabasoft AG

2 Significance of information security

The processing of information plays a key role in the fulfilment of our tasks. All important strategic and operative functions and tasks are supported to a great extent by information technology (IT). The core competence of Fabasoft lies in the development of innovative products for the digitisation of business processes, the provision of cloud services and context-sensitive searches. The availability of information and its protection against unauthorized access and alteration is therefore of vital importance.

As a future-thinking software company Fabasoft is focusing on early implementation of the requirements of EU Directive 2016/1148 (*measures for a high common level of security of network and information systems across the Union*).

In view of the global cyber-attacks currently taking place against companies in all sectors of the economy, Fabasoft is making every effort to continue with the expansion of its cyber resilience[1].

The frequency and impact of security incidents are increasing permanently and constitute a great threat to the interference-free operation of network and information systems. Every system can become the attack target of wilfully damaging actions aimed at the destruction of the systems or disruption of their operation. Such security incidents can compromise the pursuit of economic activities, cause significant financial losses, undermine the trust of users and greatly damage IT service providers.

Fabasoft is able to compensate the overall failure of IT systems in the short term, thus ensuring maximum availability of services, even in sub-areas.

3 Aims of information security

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). All Fabasoft staff are obligated to maintain the applicable data 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.

Authenticity. Information may only be processed by authorised persons. It must be guaranteed that information is true and credible and that manipulation-free IT systems and IT applications are used.

Traceability. 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. Damage with a high financial impact must be prevented.

Responsibility. All employees are aware of their responsibility with regard to the handling of data and IT systems. Compliance and awareness in respect of information security is embodied and promoted throughout the company.

Certifications. Certifications in accordance with internationally recognised regulations and standards are regularly renewed by means of independent, external audits and lend transparency to the Fabasoft level of security. Effective controls to assure compliance with the requirements are an integral part of Fabasoft processes.

[1] Cyber resilience is understood as the ability of a company to withstand attacks against information security. Although the term includes cyber security, it in fact goes far beyond this.

4 Information security management

A security organisation has been established for the achievement of the aims of information security. An IT Security Administrator has been appointed. In this capacity the IT Security Administrator reports directly to the management.

The management has provided the IT Security Administrator with sufficient financial and time resources to enable regular further training, the obtaining of all pertinent information and to accomplish the aims of information security as defined by the Managing Board.

The IT Security Administrator receives adequate support from all Fabasoft employees.

The IT Security Administrator is involved in all projects from the outset as needed, to ensure all security-relevant issues are taken into consideration early on in the planning phase. The same applies for the Data Protection Officer where personal data are concerned.

In security-relevant questions IT users comply with the instructions of the IT Security Administrator.

For the Fabasoft locations in Austria and Germany, designated experts have been appointed as external Data Protection Officers. At Fabasoft, an internal privacy team is responsible for data protection concerns and is available for data protection matters for both the external Data Protection Officers and all Fabasoft employees (email: privacy@fabasoft.com or privacy@mindbreeze.com). The external Data Protection Officers and the internal coordinators have a time budget that is sufficient for the fulfilment of all relevant duties. They are obliged to undertake regular further training.

5 Security measures

A person has been appointed who is responsible for all processes, information, IT applications and IT systems and who also defines the respective protection needs and assigns access rights.

Deputies have been appointed for all positions of responsibility. The provision of relevant instructions and adequate documentation ensure deputies are well equipped to fulfil their duties.

There are adequate access controls in place to protect the premises and offices. Access to the IT systems on the Fabasoft premises is protected by adequate access controls and access to all data by a restrictive rights concept.

Computer anti-virus programmes and intrusion detection systems are used to protect the IT systems. All Internet connections are protected by a suitable firewall. All protective programmes are configured and managed in such a way that they constitute effective protection and prevent any manipulations. In addition, IT users support these security measures by working in a security-minded manner and reporting any irregularities to the appropriate bodies.

A comprehensive data backup system guarantees that IT operations are quickly up and running again if part of the operative databases are lost or are obviously faulty. Information is uniformly labelled and stored in such a way that it can be found again quickly.

Speedy and resolute response to security incidents in the case of emergencies ensures any extensive damage is limited or prevented. Emergency measures are compiled in a separate emergency action plan. We thus consistently pursue our aim of maintaining critical business processes even in the event of a system breakdown and restoring the availability of failed systems within an acceptable period of time.

Where IT services are outsourced, we specify precise security requirements in the service level agreements. We also reserve the right to undertake controls here.

Notifications of security-relevant incidents are investigated and processed in accordance with the instructions of Security Incident Management, if necessary also in collaboration with public authorities. Causes and actions for preventing or minimising the impacts of security incidents are defined and their implementation controlled.

IT users regularly take part in training sessions for the correct use of IT services and the security measures this involves.

Fabasoft pays special attention to data protection and information security topics in training and further training measures. All new Fabasoft employees are given a basic training in data protection and information security – especially with regard to security-relevant Fabasoft guidelines – as part of the *About* Fabasoft introduction to the company prior to starting work.

All employees can inform themselves about information security by means of the guidelines available centrally in the Fabasoft cloud, which can also be found via the Intranet. It also points out that violations of laws and internal procedures will incur sanctions or disciplinary action. In this way, Fabasoft also emphasises the importance of security issues within the company, takes on the function of a role model and provides thought-provoking impulses.

In order to boost personal awareness for information security and data protection, all employees are obliged to take part regularly in eLearning tutorials. Relevant advanced training programmes are held regularly for Fabasoft employees who perform particularly security-critical activities.

6 Improvement of information security

Our information security management system is regularly tested for topicality and effectiveness (internal and external audits).

The Managing Board and all managers support the continuous improvement of the level of security. Fabasoft employees are encouraged to pass on any suggestions for improvement or detected weak points to the competent bodies.

The Managing Board, all managers and all employees commit themselves to jointly implementing the necessary measures for further development in the area of security.

Continuous reviewing of the regulations and their compliance ensures the level of security and data protection the company strives to achieve. Any deviations are analysed with the aim of improving the security situation and keeping it permanently up-to-date in terms of state-of-the-art IT security technology.