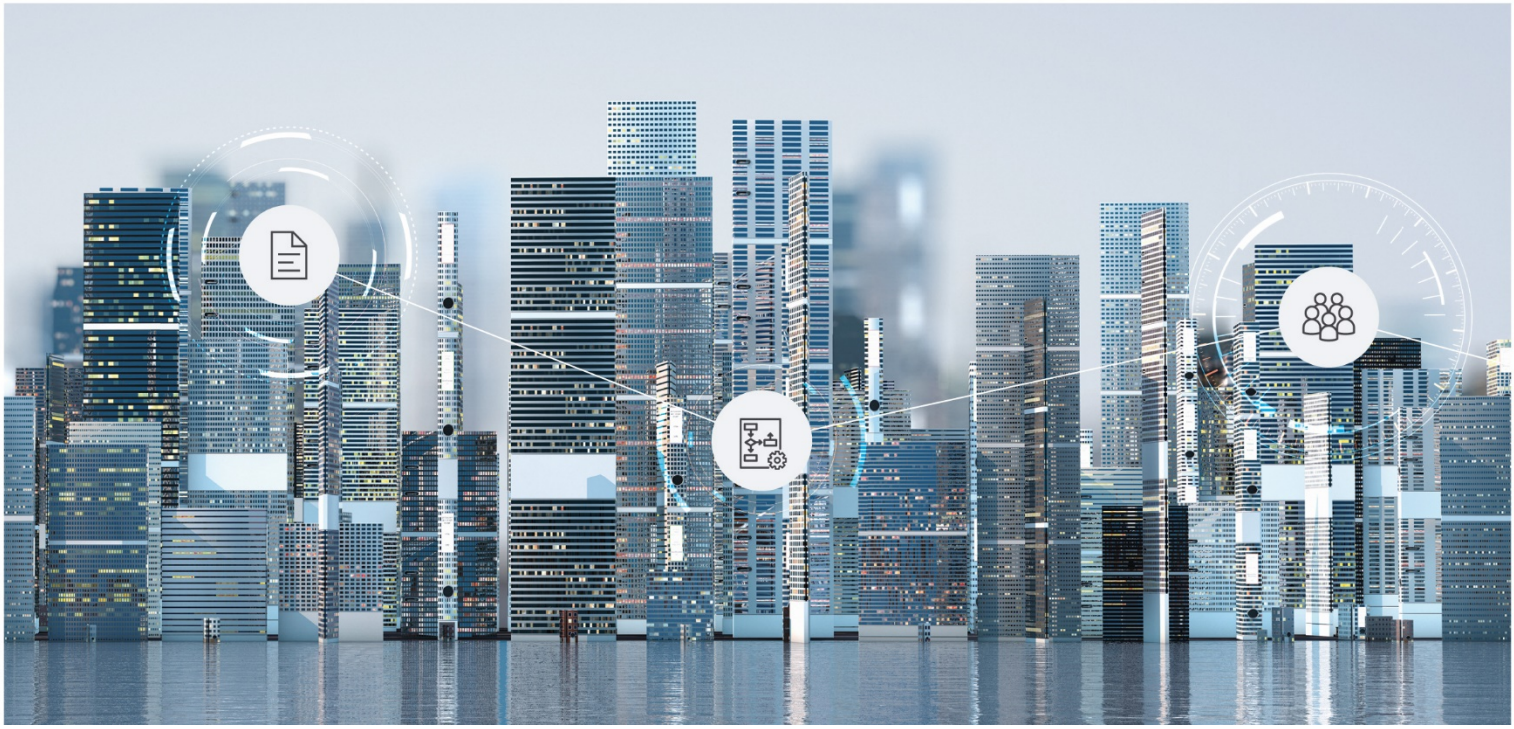

Fabasoft Konzern

Leitlinie zur Informationssicherheit

Gültig ab 09.09.2022

Öffentlich

Inhalt

1 Erklärung des Vorstands der Fabasoft AG

Fabasoft zählt zu den führenden Softwareproduktunternehmen und Cloud-Dienstleistern für digitale Dokumentenlenkung sowie elektronisches Dokumenten-, Prozess- und Aktenmanagement in Europa. Zahlreiche namhafte Privatunternehmen und Organisationen der öffentlichen Verwaltung vertrauen seit mehr als drei Jahrzehnten auf die Qualität und Erfahrung von Fabasoft.

Wir zählen zu den Vorreitern im Bereich Informationssicherheit und Datenschutz. Diese Rolle muss aktiv gelebt werden. Nur wer höchste Ansprüche an sich selbst stellt und diese auch erfüllt, kann Kunden von seiner Glaubwürdigkeit überzeugen. Aus diesem Grund hat der Schutz von Kunden- und Unternehmensdaten absolute Priorität. Dies wird durch Zertifizierungen und Prüfungen gemäß international anerkannter Standards untermauert. Wir adressieren dieses Transparenz- und Informationssicherheitsbedürfnis durch folgende Aspekte: Die Softwareprodukte werden in Europa entwickelt und in sicheren Rechenzentren, die strengen Anforderungskriterien entsprechen müssen, betrieben. Dies baut insbesondere auf dem Fundament eines europäischen Wertesystems für Datensicherheit, Zugriffssicherheit, Rechtssicherheit und für zertifizierte Qualitätsstandards auf.

Die Informationssicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sowie die laufende Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen sind somit zentrale Werte von Fabasoft in all unseren Geschäftstätigkeiten.

Der Vorstand der Fabasoft AG verabschiedet hiermit folgende Leitlinie zur Informationssicherheit als Bestandteil der Fabasoft Gesamtstrategie.

Prof. Dipl.-Ing. Helmut Fallmann

Vorsitzender des Vorstands - CEO

Matthias Wodniok

Mitglied des Vorstands

Ing. Oliver Albl

Mitglied des Vorstands - CTO

2 Einleitung

Fabasoft hat ein Managementsystem für Informationssicherheit etabliert, das insbesondere die Normen ISO/IEC 27001im Zusammenhang mit ISO/IEC 27018 sowie den Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) des Bundesamts für Sicherheit in der Informationstechnik (BSI), die Trust Services Criteria TSC/SOC 2 sowie den EU Cloud Code of Conduct adressiert. Das vorliegende Dokument ist die Leitlinie zur Informationssicherheit der Fabasoft AG und der mit ihr verbundenen Unternehmen. Die Richtlinie gilt für alle Mitarbeiter:innen im Fabasoft Konzern.

3 Stellenwert der Informationssicherheit und des Datenschutzes

Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sind zentrale Werte von Fabasoft in all ihren Geschäftstätigkeiten. In Anbetracht der hinsichtlich Anzahl, Intensität und Raffinesse global zunehmenden Cyberangriffe auf Unternehmen in allen Bereichen der Wirtschaft unternimmt Fabasoft intensive Anstrengungen für den kontinuierlichen Ausbau ihrer Cyber Resilience. Das im Unternehmen installierte Informationssicherheitsmanagementsystem (ISMS) und Datenschutzmanagementsystem (DSMS) inklusive der technischen und organisatorischen Maßnahmen werden laufend überprüft, bewertet und evaluiert sowie durch interne und externe Audits auf seine Aktualität, Effektivität, Wirksamkeit und Compliance mit international anerkannten Normen, Standards und Kriterienkatalogen geprüft. Die daraus folgenden Zertifikate und Prüfberichte verleihen dem Fabasoft Informationssicherheits– und Datenschutzniveau Transparenz.

Fabasoft begleitet alle Mitarbeiter:innen in Form eines kontinuierlichen Prozesses auf ihrem Entwicklungsweg zu einem ausgeprägten Informationssicherheits- und Datenschutzbewusstsein. Um dieses Bewusstsein für die daraus entstehenden Risiken zu schärfen, werden regelmäßig professionelle Awareness-Trainings durchgeführt und mögliche Bedrohungsszenarien simuliert. Alle Mitarbeiter:innen sind sich ihrer Verantwortung beim Umgang mit Daten und IT-Systemen bewusst. Compliance und Awareness für Informationssicherheit und Datenschutz wird in allen Unternehmensbereichen gelebt und gefördert.

4 Informationssicherheitsziele

Die nachstehenden Informationssicherheitsziele werden durch technische und organisatorische Maßnahmen im Rahmen des bestehenden ISMS sichergestellt. Diese Maßnahmen adressieren die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Authentizität der zu schützenden Informationen und werden regelmäßig überprüft, bewertet und evaluiert.

Vertraulichkeit

Kundendaten, Geschäftsdaten und Daten der Entwicklungsbereiche unterliegen höchsten Vertraulichkeitsanforderungen. Sie dürfen nicht unrechtmäßig zur Kenntnis gelangen (limitierte Zugriffsberechtigungen, Vertraulichkeitsstufen, Verschlüsselung, ...). Informationen dürfen nur von autorisierten Personen eingesehen werden. Alle Fabasoft Mitarbeiter:innen sind zur Wahrung des anwendbaren Datengeheimnisses und zur Wahrung der Vertraulichkeit verpflichtet.

Integrität

Daten und Informationen müssen richtig und vollständig sein. IT-Systeme müssen durchgängig funktionieren. Daten und Informationen dürfen ohne Genehmigung nicht verändert werden. Veränderungen von Informationen müssen eindeutig erkennbar und nachvollziehbar sein (Versionierung).

Verfügbarkeit

Informationen müssen entsprechend der vertraglich zugesicherten Service Levels verfügbar sein. Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf Fabasoft und ihre Stakeholder haben. Informationen müssen auf Systemen und Diensten verarbeitet werden, die notwendige Verfügbarkeit gewährleisten. Systeme und Dienste müssen im Störungsfall in der vereinbarten Zeit wiederhergestellt werden können.

Authentizität

Es muss gewährleistest werden, dass Informationen echt, überprüfbar und glaubwürdig sind und es sich um manipulationsfreie IT-Systeme und IT-Anwendungen handelt.

5 Verantwortlichkeiten

5.1 Vorstand der Fabasoft AG

Der Vorstand legt im Rahmen seiner Gesamtverantwortung die Informationssicherheitsziele fest und stellt durch Definition von Verantwortlichen für Kontrollen und Prozesse, durch Bereitstellung der dafür notwendigen zeitlichen und finanziellen Ressourcen sowie durch Festlegung der Rahmenbedingungen sicher, dass die genannten Ziele erreicht werden.

5.2 Verantwortliche für Kontrollen und Prozesse

Die Kontroll- und Prozessverantwortlichen stellen sicher, dass die ihnen zugewiesenen Kontrollen und Prozesse angemessen, effektiv und wirksam sind. Sie gewährleisten, dass für das Funktionieren der Kontrollen und Prozesse relevante interne und externe Informationsquellen berücksichtigt werden und dass die Kontrolldurchführung zum definierten Zeitpunkt oder im definierten Intervall erfolgt. Sie kommunizieren die notwendigen Informationen zu den Kontrollzielen und zur Umsetzung (Kontrolldurchführung) an die Durchführenden der Kontrolle.

Bei der Einführung neuer Anwendungen, Verfahren, Prozesse und Infrastrukturkomponenten im Bereich der Kontroll- und Prozessverantwortlichen sind diese einzubinden. Dabei stellen diese sicher, dass die Risiken hinsichtlich Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität) durch diese neuen Komponenten und Verfahren nicht erhöht werden bzw. ergreifen geeignete Gegenmaßnahmen.

5.3 Head of Security Operations

Der Head of Security Operations verantwortet die Umsetzung der Kontrollen und Prozesse im Rahmen der Informationssicherheit, unterstützt und kontrolliert die Tätigkeiten des Security Operations Team und nimmt Abstimmungen mit dem Vorstand vor.

5.4 Security Operations Team

Das Security Operations Team plant die notwendigen Tätigkeiten zur Aufrechterhaltung und Verbesserung der Informationssicherheit, insbesondere im Rahmen der Patch Management, Vulnerability Management und Security Incident Management Prozesse. Im Security Operations Team werden regelmäßige externe Penetration Tests koordiniert und die allgemeine Lage zur Informationssicherheit und Informationssicherheitsvorfälle besprochen. Das Security Operations Team wird in informationssicherheitsrelevanten Themen eingebunden und unterstützt Kontroll- und Prozessverantwortliche sowie Fachbereiche bei der Sicherstellung der Informationssicherheit.

5.5 Privacy Team

Das Privacy Team plant die notwendigen Tätigkeiten zur Aufrechterhaltung und Verbesserung des Datenschutzes und der Datensicherheit, insbesondere im Rahmen der Datenschutzdokumentation und Erfüllung der Betroffenenanfragen. Das Privacy Team stimmt sich mit den bestellten externen Datenschutzbeauftragten ab und plant die Koordination und Umsetzung der Datenschutzanforderungen. Das Privacy Team wird in datenschutzrelevante Themen eingebunden und unterstützt Kontroll- und Prozessverantwortliche sowie Fachbereiche bei der Sicherstellung des Datenschutzes sowie der Datensicherheit.

5.6 Mitarbeiter:innen

Mitarbeiter:innen werden regelmäßig zur Informationssicherheit und zum Datenschutz sensibilisiert, um das Sicherheitswissen und -bewusstsein zu schärfen und damit das Sicherheitsverhalten kontinuierlich zu verbessern.

Mitarbeiter:innen sind sich der Wichtigkeit der Informationssicherheit und des Datenschutzes bewusst und wirken aktiv mit. Sie gehen verantwortungsbewusst mit den IT-Systemen und den darauf gespeicherten und dort verarbeiteten Daten um und achten auf die Wahrung von Betriebs-, Geschäfts- und Datengeheimnissen. Mitarbeiter:innen setzen die Informationssicherheit in Einklang mit den eingeführten Richtlinien und Verfahren von Fabasoft um.