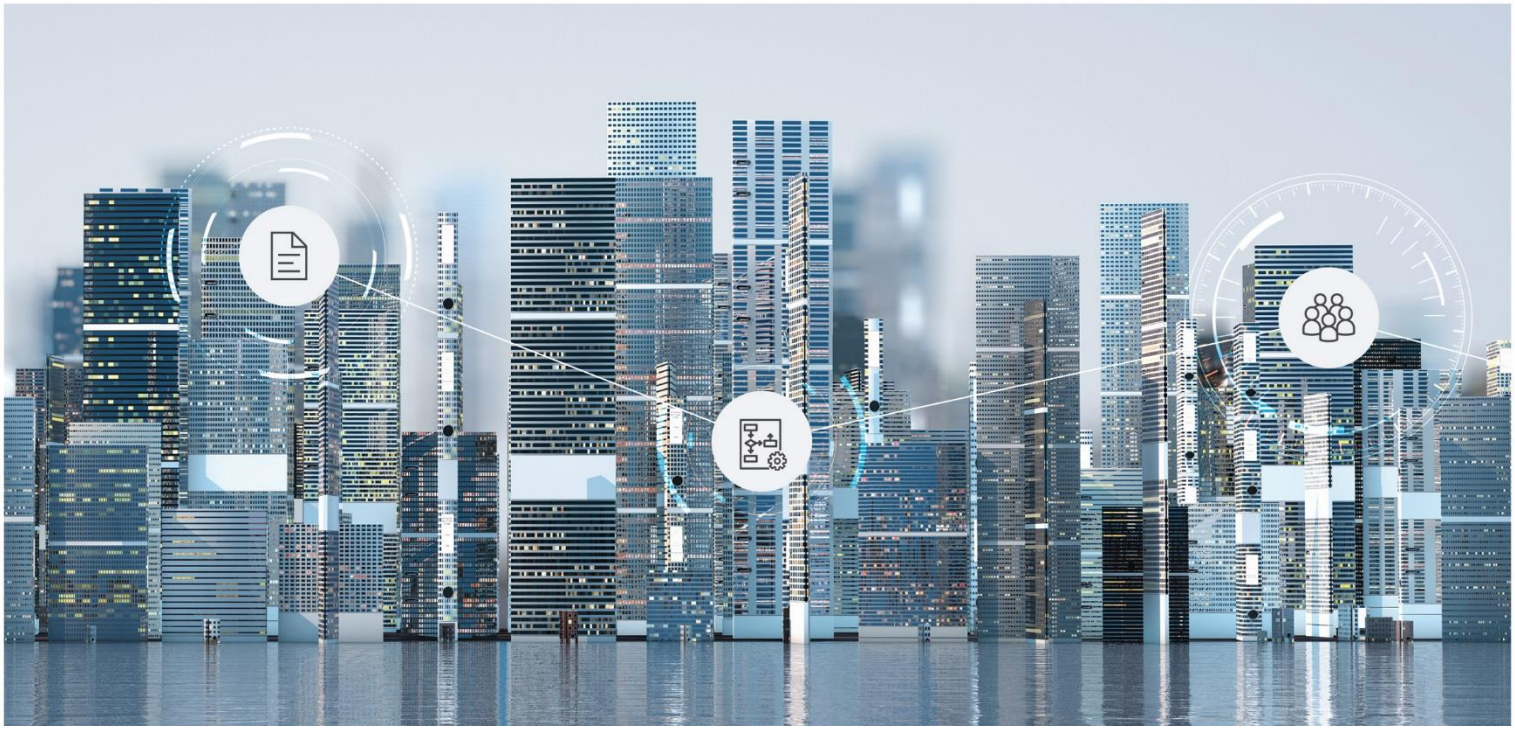

Fabasoft Konzern

Fabasoft Sicherheitsleitlinie

Gültig ab 01.05.2018

Öffentlich

Inhalt

1 Erklärung der höchsten Entscheidungsträger

Die Fabasoft als europäischer Softwareprodukthersteller und Cloud-Dienstleister sieht sich gegenüber ihren Stakeholdern in der Verantwortung für langfristiges und nachhaltiges Wirtschaften.

Fabasoft ist mehr denn je der Überzeugung, dass die ethischen Werthaltungen Europas in der Gestaltung der normativen und regulatorischen Rahmenbedingungen für den globalen digitalen Wettbewerb vor allem in der Durchsetzung eines hohen Datenschutzstandards liegt. Dieser ist der Schlüssel schlechthin für die wertvollste Währung in der digitalen Welt: Uneingeschränktes Vertrauen der Nutzerinnen und Nutzer. Aus der Arbeit an der Umsetzung dieser Überzeugungen ergibt sich das umfangreiche internationale und nationale Engagement der Fabasoft in zahlreichen Institutionen:

EU Cloud Code of Conduct
Auf europäischer Ebene engagiert sich Fabasoft insbesondere bei der Weiterentwicklung von Verhaltensnormen für europäisches Cloud Computing im Rahmen einer intensiven Mitarbeit an einem Code of Conduct (CoC). Fabasoft ist Founding Member der General Assembly.

European Security Certification Framework
Das European Security Certification Framework (EU-SEC) ist ein Forschungsprojekt mit dem Ziel, den Geschäftswert, die Effektivität und die Effizienz von bestehenden Zertifizierungssystemen für Cloud-Security zu verbessern. Fabasoft ist Mitglied im Konsortium.

European Telecommunications Standards Institute
Das European Telecommunications Standards Institute (ETSI) ist ein anerkanntes Normungsgremium der Europäischen Normungsorganisation (ESO) und arbeitet an der Standardisierung von Telekommunikations-, Rundfunk und anderen elektronischen Kommunikationsnetzen und -diensten. Fabasoft ist ETSI-Mitglied.

Der Vorstand der Fabasoft AG verabschiedet hiermit folgende Sicherheitsleitlinie als Bestandteil der Fabasoft Gesamtstrategie.

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

Der Vorstand der Fabasoft AG

2 Stellenwert der Informationssicherheit

Informationsverarbeitung spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Die Fabasoft Kernkompetenz liegt in der Entwicklung innovativer Produkte zur Digitalisierung von Geschäftsprozessen, der Bereitstellung von Cloud-Services und im kontextsensitiven Finden. Die Verfügbarkeit sowie der Schutz von Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung sind daher von existenzieller Bedeutung.

Als zukunftsorientiertes Software-Unternehmen setzt Fabasoft auf eine frühzeitige Umsetzung der Anforderungen der EU-Richtlinie 2016/1148 (*Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union*).

In Anbetracht der aktuellen globalen Cyberangriffe auf Unternehmen in allen Bereichen der Wirtschaft legt Fabasoft höchste Priorität auf den kontinuierlichen Ausbau ihrer Cyber Resilience[1].

Die Häufigkeit und Auswirkungen von Sicherheitsvorfällen nehmen permanent zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Jedes System kann auch zu einem Angriffsziel vorsätzlich schädigender Handlungen werden, die auf die Störung oder den Ausfall des Betriebs der Systeme gerichtet sind. Solche Sicherheitsvorfälle können die Ausübung wirtschaftlicher Tätigkeiten beeinträchtigen, beträchtliche finanzielle Verluste verursachen, das Vertrauen der Nutzerinnen und Nutzer untergraben und IT-Serviceprovidern großen Schaden zufügen.

Fabasoft kann einen Ausfall von IT-Systemen insgesamt kurzfristig kompensieren, und stellt damit die höchste Verfügbarkeit von Services auch in Teilbereichen sicher.

3 Informationssicherheitsziele

Vertraulichkeit. Kundendaten, Geschäftsdaten und Daten der Entwicklungsbereiche unterliegen höchsten Vertraulichkeitsanforderungen. Sie dürfen nicht unrechtmäßig zur Kenntnis gelangen (limitierte Zugriffsberechtigungen, Vertraulichkeitsstufen, Verschlüsselung). Alle Fabasoft Mitarbeiter sind zur Wahrung des anwendbaren Datengeheimnisses verpflichtet.

Integrität. Daten und Informationen müssen richtig und vollständig sein. IT-Systeme müssen durchgängig funktionieren. Daten und Informationen dürfen ohne Genehmigung nicht verändert werden.

Authentizität. Informationen dürfen nur von autorisierten Personen bearbeitet werden. Es muss gewährleistest werden, dass Informationen echt und glaubwürdig sind und es sich um manipulationsfreie IT-Systeme und IT-Anwendungen handelt.

Nachvollziehbarkeit. Veränderungen von Informationen müssen eindeutig erkennbar und nachvollziehbar sein (Versionierung).

Verfügbarkeit. Informationen müssen entsprechend der vertraglich zugesicherten Service Levels verfügbar sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf Fabasoft und ihre Stakeholder haben. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

Verantwortung. Alle Mitarbeiterinnen und Mitarbeiter sind sich ihrer Verantwortung beim Umgang mit Daten und IT-Systemen bewusst. Compliance und Awareness für Informationssicherheit wird in allen Unternehmensbereichen gelebt und gefördert.

Zertifizierungen. Zertifizierungen nach international anerkannten Normen und Standards werden im Rahmen unabhängiger, externer Audits regelmäßig erneuert und verleihen dem Fabasoft Sicherheitsniveau Transparenz. Effektive Kontrollen zur Erfüllung der Anforderungen sind fester Bestandteil der Fabasoft Prozesse.

[1] Als Cyber Resilience versteht man die Widerstandskraft eines Unternehmens gegen Angriffe auf die Informationssicherheit. Dabei beinhaltet der Begriff auch die Cyber-Security, geht aber noch weit über diese hinaus.

4 Informationssicherheitsmanagement

Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation eingerichtet. Es ist ein IT Security Administrator benannt worden. Der IT Security Administrator berichtet in dieser Funktion direkt an das Management.

Dem IT Security Administrator werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die vom Vorstand festgelegten Informationssicherheitsziele zu erreichen.

Der IT Security Administrator wird durch die Fabasoft Mitarbeiterinnen und Mitarbeiter ausreichend in seiner Arbeit unterstützt.

Der IT Security Administrator wird bei Bedarf frühzeitig in alle Projekte eingebunden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

Die IT-User halten sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des IT Security Administrators.

Für die Fabasoft Standorte in Österreich und Deutschland wurden ausgewiesene Experten als externe Datenschutzbeauftragte bestellt. Innerhalb von Fabasoft ist ein Privacy Team für Datenschutzbelange zuständig und steht als Ansprechpartner sowohl für die externen Datenschutzbeauftragten als auch für alle Fabasoft Mitarbeiterinnen und Mitarbeiter zur Verfügung (E-Mail: privacy@fabasoft.com bzw. privacy@mindbreeze.com). Die externen Datenschutzbeauftragten und das interne Privacy Team haben ein ausreichend bemessenes Zeitbudget für die Erfüllung ihrer Pflichten zur Verfügung. Sie sind angehalten, sich regelmäßig weiterzubilden.

5 Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen eingerichtet. Es ist durch Unterweisungen und ausreichende Dokumentationen sichergestellt, dass Vertreter ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen in den Fabasoft Gebäuden wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Zum Schutz der IT-Systeme kommen Computer-Viren-Schutzprogramme sowie Intrusion Detection Systeme zum Einsatz. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-User durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Durch eine umfassende Datensicherung wird gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

Um größere Schäden infolge von Notfällen zu begrenzen bzw. diesen vorzubeugen, wird auf Sicherheitsvorfälle zügig und konsequent reagiert. Maßnahmen für den Notfall sind in einem separaten Notfallvorsorgekonzept zusammengestellt. Damit verfolgen wir konsequent unser Ziel, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Sofern IT-Dienstleistungen an externe Stellen ausgelagert werden, werden von uns konkrete Sicherheitsanforderungen in den Service Level Agreements vorgegeben. Das Recht auf Kontrolle wird festgelegt.

Meldungen zu sicherheitsrelevanten Vorfällen werden geprüft und entsprechend der Vorgaben im Security Incident Management behandelt, gegebenenfalls auch in Zusammenarbeit mit Behörden. Ursachen und Maßnahmen zur Vermeidung oder Verringerung von Auswirkungen von Security Incidents werden festgelegt und deren Abarbeitung kontrolliert.

IT-User nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil.

Im Rahmen der Aus- und Weiterbildung legt Fabasoft besonderes Augenmerk auf Datenschutz- und Informationssicherheitsthemen. Bereits zu Beginn ihrer Tätigkeit erhalten alle neuen Fabasoft Mitarbeiterinnen und Mitarbeiter im Rahmen der *About Fabasoft* eine grundlegende Schulung über Datenschutz und Informationssicherheit – insbesondere in Hinblick auf sicherheitsrelevante Fabasoft Richtlinien.

Anhand der in der Fabasoft Cloud zentral verfügbaren Richtlinien, die auch über das Intranet erreichbar sind, können sich alle Mitarbeiterinnen und Mitarbeiter zum Thema Informationssicherheit informieren. Es wird auch darauf hingewiesen, dass Verstöße gegen Gesetze und interne Vorgaben Sanktionen oder Disziplinarmaßnahmen nach sich ziehen können. Fabasoft unterstreicht damit die Wichtigkeit der Sicherheitsthematik auch innerhalb des Unternehmens, nimmt eine Vorbildfunktion ein und liefert Denkanstöße.

Um das persönliche Bewusstsein für Informationssicherheit und Datenschutz zu stärken sind alle Mitarbeiterinnen und Mitarbeiter zur Absolvierung von regelmäßigen eLearing Tutorials verpflichtet. Für Fabasoft Mitarbeiterinnen und Mitarbeiter, deren Tätigkeit eine besonders hohe Sicherheitsrelevanz aufweist, werden regelmäßig relevante Weiterbildungsmaßnahmen organisiert.

6 Verbesserung der Informationssicherheit

Das Informationssicherheitsmanagementsystem wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft (interne und externe Audits).

Der Vorstand sowie alle Führungskräfte unterstützen die ständige Verbesserung des Sicherheitsniveaus. Die Fabasoft Mitarbeiterinnen und Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Der Vorstand, die Führungskräfte sowie alle Mitarbeiterinnen und Mitarbeiter bekennen sich dazu, die erforderlichen Maßnahmen zur Weiterentwicklung im Bereich Sicherheit gemeinsam umzusetzen.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.