KLASSIFIKATION ÖFFENTLICH

Informations-sicherheitspolitik

der fobi solutions GmbH

HERAUSGEBER · **FOBI SOLUTIONS GMBH** VERSION · **1.0** STAND · **SEPTEMBER 2026**

Öffentliche Fassung der Richtlinie Informationssicherheitspolitik V1.0 vom 16.09.2026

01 Bekenntnis der Geschäftsführung zur Informationssicherheit

Die Sicherheit von Informationen ist ein wesentlicher Faktor für die Geschäftsprozessunterstützung und unsere Wettbewerbsfähigkeit. Nur eine ausreichende Informationssicherheit kann den Schutz von Geschäftsinformationen, personenbezogenen Daten und die reibungslose Verfügbarkeit elektronischer Informations- und Kommunikationssysteme gewährleisten.

Wir – die Geschäftsführung – bekennen uns zu dieser Verantwortung und erlassen hierzu die vorliegende Informationssicherheitspolitik.

Nach Maßgabe dieser Politik sind alle Mitarbeiter:innen – unabhängig von ihrer Hierarchiestufe – für die Sicherheit und einen angemessenen Schutz der Informationen zuständig. Diese Maßnahmen sind auch Teil unserer Verpflichtungen gegenüber unseren Kundinnen und Kunden.

„Informationssicherheit ist eine wesentliche Säule unseres Erfolges."

Mag. Martin Reichetseder · CEO, fobi solutions GmbH

02 Geltungsbereich

Diese Politik gilt für die gesamte fobi solutions GmbH und versteht sich als Weisung an unsere Mitarbeiter:innen. Die Verantwortung für die Informationssicherheit tragen neben der Geschäftsführung als Gesamtverantwortliche alle an den Geschäftsprozessen beteiligten Personen. Die Geschäftsführung unterstützt die Maßnahmen und Strategien der Informationssicherheit aktiv und treibt die Umsetzung der Sicherheitsmaßnahmen im Unternehmen voran.

Alle Mitarbeiter:innen sind aufgefordert, Informationssicherheit, Datenschutz und physische Sicherheit nach Kräften aktiv im jeweiligen Tätigkeitsbereich umzusetzen. Bei Nichteinhaltung oder bewusster Verletzung der Unternehmensvorgaben wird der jeweilige Fall durch die Geschäftsführung untersucht und es werden angemessene Maßnahmen gesetzt.

GESCHÄFTSPARTNER:INNEN

Lieferanten, Auftragsverarbeiter und weitere Geschäftspartner:innen sind an die Vorgaben dieser Politik gebunden, soweit sie Informationen der fobi solutions GmbH verarbeiten oder auf unsere Systeme zugreifen. Die Anforderungen werden im Rahmen des Lieferantenmanagements festgelegt und überprüft.

03 Stellenwert der Informationstechnologie und Informationssicherheit

Informationssicherheit ist ein wesentlicher Treiber unserer Unternehmenspolitik und stellt für uns ein äußerst wichtiges Qualitätsmerkmal der Datenverarbeitung dar. Wir bekennen uns zur Implementierung, zum Betrieb und zur kontinuierlichen Weiterentwicklung bzw. Verbesserung unseres Informationssicherheits-managementsystems (ISMS). Alle wesentlichen strategischen und operativen Geschäftsprozesse im Unternehmen werden durch Informationstechnologie (IT) maßgeblich unterstützt. Informationstechnologie ist die Basis unseres täglichen Unternehmertums. Informationssicherheit ist daher ein zentraler Aspekt unseres Wirkens und wesentlich für all unsere Unternehmensprozesse – egal ob Support, Projektmanagement oder Wertschöpfung.

Ausfälle von Personal oder IT-Infrastruktur sowie unberechtigte Eingriffe in Geschäftsprozesse können die Geschäftstätigkeit erheblich beeinträchtigen. Wir erkennen den Klimawandel als relevanten externen Faktor an, der potenziell Einfluss auf die Informationssicherheit, die Geschäftskontinuität und die Risikosituation hat. Es ist daher essenziell, die Maßnahmen, Prozesse und Richtlinien unseres ISMS stets aufrechtzuerhalten und deren Gültigkeit zu gewährleisten.

Alle Mitarbeiter:innen und Geschäftspartner:innen sind verpflichtet, die Informationssicherheit zu fördern und die Regelungen und Vorgaben einzuhalten. Die Richtlinien unseres ISMS gelten auch in Krisenzeiten und während Notfällen. Sie dienen als Grundlage und Anleitung all unserer IT-Sicherheitsmaßnahmen. Die Überprüfung der Einhaltung dieser Verpflichtung behalten wir uns ausdrücklich vor.

OFFENE SICHERHEITSKULTUR

Informationssicherheit ist Aufgabe jeder Person im Unternehmen.

Wir pflegen einen offenen Umgang mit Sicherheitsfragen: Anregungen, Fehler und Verdachtsfälle sollen angesprochen werden. Für Meldungen steht ein Meldekanal zur Verfügung (siehe Kapitel 8).

04 Informationssicherheitsziele

Durch diese Politik sollen die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Unternehmens-Assets, Services und Geschäftsprozessen geregelt und in weiterer Folge sichergestellt werden. Unterschiedliche Assets bilden die Grundlage für eine erfolgreiche Geschäftstätigkeit. Diese Assets sind vor lokalen und globalen Bedrohungen zu schützen, um negative Auswirkungen auf unser Unternehmen und dessen Geschäftsfelder zu verhindern.

4.1 Ziele

Um negative Auswirkungen zu vermeiden und um die Ziele dieser Politik zu erreichen, bedarf es der Implementierung und Erhaltung eines adäquaten Informationssicherheitsmanagements. Als Ziele gelten:

- Sicherstellung des Betriebes sowohl im Normalbetrieb als auch im Fehler- oder Katastrophenfall
- Daten, Applikationen oder Systeme sollen nicht unberechtigt verändert werden können, bzw. jegliche Veränderung bei Anwendung erkennbar sein (**Integrität**)
- Einhaltung der aus gesetzlichen Vorgaben resultierenden Anforderungen (insbesondere Haftungsrisiken und Sorgfaltspflicht gemäß GmbH-Gesetz, Datenschutzgesetz u. a.)
- Sicherung der investierten Werte (Schutz gegen Diebstahl, Schutz von geistigem Eigentum)
- Daten sollen nur dem Personenkreis zugänglich gemacht werden, der auch befugt ist, darauf zuzugreifen (**Vertraulichkeit**, Need-to-know-Prinzip)
- Daten und Applikationen stehen in vereinbartem Maß zur Verfügung (**Verfügbarkeit**)
- Schutz personenbezogener Daten und der Privatsphäre der Mitarbeiter:innen, Kundinnen und Kunden
- Sicherung der Qualität, Stabilität, Kontinuität und Wertschöpfung im Interesse aller Bereiche im Unternehmen

4.2 Prinzipien zur Zielerreichung

Zur Wahrung der Informationssicherheitsziele werden im Rahmen der Informationssicherheitsstrukturen im Unternehmen folgende Prinzipien angewandt:

01 Bekenntnis der Geschäftsführung zur Informationssicherheit

02 Ausrichtung an gesetzlichen Anforderungen

03 Schaffen einer Informationssicherheitsorganisation

04 Integration von Informationssicherheit in alle Unternehmensprozesse

05 Orientierung an international anerkannten Informationssicherheitsstandards und Best-Practice-Ansätzen (ISO/IEC 27001)

06 Implementierung von adäquaten Informationssicherheitsmaßnahmen

07 Bereitstellung von erforderlichen Ressourcen

08 Schulung und Integration aller Mitarbeiter:innen im Bereich der Informationssicherheit

4.3 Anforderungen an die Informationssicherheitsziele

Die Geschäftsführung stellt sicher, dass die Informationssicherheitsziele die folgenden Punkte berücksichtigen und mit diesen im Einklang stehen:

- **Organisationsziele und Governance**
- **Gesetzliche, regulative und normative Vorgaben**
- **Ausrichtung an Kundenanforderungen**
- **Zur Verfügung stehende Ressourcen**

Die in dieser Politik genannten Ziele sind übergeordnete Schutzziele. Sie bilden den Rahmen für die Festlegung der Informationssicherheitsziele nach Kapitel 6.2 der ISO/IEC 27001:2022; diese Ziele werden mit ihren Kennzahlen, Verantwortlichen und Terminen in der Richtlinie Zielsetzungen Informationssicherheit geführt und in der Managementbewertung bewertet.

05 Verpflichtungen der Geschäftsführung

Die Geschäftsführung verpflichtet sich mit dieser Politik ausdrücklich:

- → die für die Informationssicherheit zutreffenden gesetzlichen, regulativen, normativen und vertraglichen Anforderungen zu erfüllen
- → das Informationssicherheits-managementsystem (ISMS) fortlaufend zu verbessern
- → die für Betrieb und Weiterentwicklung des ISMS erforderlichen Ressourcen bereitzustellen

06 Verantwortung und Organisation

GESCHÄFTSFÜHRUNG	Die Geschäftsführung trägt die Gesamtverantwortung für die Informationssicherheit. Sie erlässt diese Politik, stellt die erforderlichen Ressourcen bereit und entscheidet über die Behandlung und die Akzeptanz wesentlicher Risiken.
CISO	Der Chief Information Security Officer (CISO) verantwortet die fachliche Steuerung, Koordination und Weiterentwicklung des Informationssicherheitsmanagementsystems (ISMS) und berichtet direkt an die Geschäftsführung.
MITARBEITER:INNEN	Alle Mitarbeiter:innen sind – unabhängig von ihrer Hierarchiestufe – für die Sicherheit und einen angemessenen Schutz der Informationen in ihrem Tätigkeitsbereich zuständig; sie melden erkannte Sicherheitsvorfälle und Schwachstellen.

Die einzelnen Rollen, ihre Aufgaben und ihre Vertretung sind in der Richtlinie Rollenbeschreibungen festgelegt.

07 Umsetzung des Managementsystems

Zur Erreichung der genannten Ziele setzen wir auf folgende Elemente. Sie sind in eigenen Richtlinien geregelt, die diese Politik konkretisieren:

01 Risiken und Chancen für die Informationssicherheit werden systematisch erfasst, bewertet, behandelt und laufend überwacht; über die Behandlung und die Akzeptanz wesentlicher Risiken entscheidet die Geschäftsführung. → **Richtlinie Risikomanagement**

02 Informationen werden nach ihrem Schutzbedarf klassifiziert und entsprechend gehandhabt und geschützt. → **Richtlinie zur Informationssicherheit**

03 Geschäftspartner:innen werden nach ihrem Schutzbedarf eingestuft und bewertet; Sicherheitsanforderungen werden vereinbart und überprüft. → **Richtlinie Lieferantenmanagement**

04 Alle Mitarbeiter:innen werden regelmäßig geschult und für Informationssicherheit sensibilisiert. → **Richtlinie Bewusstsein**

05 Sicherheitsvorfälle werden erkannt, bewertet, behandelt und ausgewertet; aus ihnen werden Verbesserungsmaßnahmen abgeleitet. → **Richtlinie Data Breach & IT Security Incident Management · Richtlinie Kontinuierliche Verbesserung**

06 Interne Audits, Kennzahlen und die Managementbewertung bewerten regelmäßig die Wirksamkeit und die Angemessenheit des Managementsystems. → **Richtlinie interner Auditplan · Richtlinie Zielsetzungen Informationssicherheit · Richtlinie Managementreport**

08 Sicherheitsvorfälle und Hinweise melden

Kundinnen, Kunden, Geschäftspartner:innen und andere externe Hinweisgeber:innen können Hinweise auf Sicherheitsvorfälle oder Schwachstellen ohne Anmeldung über den Meldekanal „.LOUPE Information Security Incidents“ melden:

MELDEKANAL · OHNE ANMELDUNG

.LOUPE Information Security Incidents

Hinweis melden →

Innerhalb des Unternehmens ist ein Sicherheitsvorfall unverzüglich über .LOUPE zu melden; Ansprechpartner ist der CISO.

72 h

MELDEFRIST BEHÖRDE

Bei einer Verletzung des Schutzes personenbezogener Daten melden wir diese – sofern ein Risiko für Betroffene besteht – unverzüglich und möglichst binnen 72 Stunden der Datenschutzbehörde (Art. 33 DSGVO); bei voraussichtlich hohem Risiko benachrichtigen wir die Betroffenen unverzüglich (Art. 34 DSGVO). Als Auftragsverarbeiter informieren wir unsere Kundinnen und Kunden unverzüglich (Art. 33 Abs. 2 DSGVO).

09 Verbindlichkeit, Bekanntmachung und Verfügbarkeit

Diese Politik ist für alle Mitarbeiter:innen verbindlich. Das Unterzeichnen der relevanten organisatorischen Regelungen bzw. eine entsprechende Bestätigung der Kenntniserlangung und des Verständnisses durch unsere Mitarbeiter:innen – bereits bei Arbeitsantritt – ist Grundlage für die Einhaltung unserer Vorgaben. Alle Änderungen werden in einem unternehmensweiten Prozess bekanntgegeben und müssen unterzeichnet werden. Alle Mitarbeiter:innen haben damit Kenntnis über die Aussagen dieser Politik, Zugang zu ihrer schriftlichen Fassung und Wissen um ihre Pflichten zur Informationssicherheit.

KLASSIFIKATION ÖFFENTLICH

Diese Politik ist als „öffentlich“ klassifiziert. Sie ist auf **www.loupe.at** veröffentlicht und wird interessierten Parteien – insbesondere unseren Kundinnen und Kunden sowie unseren Partnern – zur Verfügung gestellt; darüber hinaus Lieferanten und Behörden, soweit dies angemessen ist. Ansprechpartner für alle Fragen zu dieser Politik ist der Chief Information Security Officer (CISO) der fobi solutions GmbH.

10 Mitgeltende Dokumente

Richtlinie zur Informationssicherheit	Richtlinie Bewusstsein
Richtlinie Zielsetzungen Informationssicherheit	Richtlinie Data Breach & IT Security Incident Management
Richtlinie Rollenbeschreibungen	Richtlinie Kontinuierliche Verbesserung
Richtlinie Risikomanagement	Richtlinie interner Auditplan
Richtlinie Lieferantenmanagement	Richtlinie Managementreport
Richtlinie Dokumentenlenkung	Code of Conduct

11 Gültigkeit und Inkraftsetzung

Dieses Dokument ist ab Verlautbarung verbindlich gültig. In Kraft seit 16.09.2026. Das vorliegende Dokument wird mindestens einmal im Jahr auf seine Aktualität und Wirksamkeit hin überprüft und gegebenenfalls überarbeitet, wobei Änderungen von Rahmenbedingungen, Aufgaben und die Unternehmensstrategie berücksichtigt werden.

FÜR DIE GESCHÄFTSFÜHRUNG

Mag. Martin Reichetseder
CEO

Wer hinter dieser Politik steht

.LOUPE ist eine Compliance-Plattform und Beratungsmarke der fobi solutions GmbH. Seit 2018 verbinden wir Governance-Software mit Beratung aus der Praxis.

MEDIENINHABER & HERAUSGEBER

fobi solutions GmbH
Steinsiedlung 11
4222 St. Georgen an der Gusen
Österreich
UID: ATU73020839

KONTAKT

E **office@loupe.at**
W **www.loupe.at**
hub.loupe.at/kontakt

FRAGEN ZU DIESER POLITIK

Ansprechpartner für alle Fragen zu dieser Politik ist der Chief Information Security Officer (CISO) der fobi solutions GmbH. Schreiben Sie an **office@loupe.at** oder nutzen Sie **hub.loupe.at/kontakt**.

Built for people. Powered by expertise. Enhanced by AI.