Leitlinie zur Informationssicherheit

Ziele und Strategie des Informationssicherheitsmanagementsystems (ISMS)

— Vorwort

Der Vorstand des FZI (v. l. n. r.):
Jan Wiesenberger, Prof. Dr.-Ing. J. Marius Zöllner
Prof. Dr. Stefan Nickel

Liebe Leserinnen und Leser,

das Erlangen von Wissen in der Forschung und dessen Austausch sind unsere wertvollste Währung am FZI. Es sind Schlüssel für einen erfolgreichen Technologietransfer vom Labor in die Produktion, um innovative Ideen für die Wirtschaft und zum Wohle der Gesellschaft umzusetzen. Dies macht sie allerdings auch zu interessanten Zielen.

Der Verlust von Daten durch Datenlecks, Industriespionage oder Cyberattacken stellt für uns und unsere Partner entsprechend ein großes Risiko dar. Als eines der führenden unabhängigen Institute für angewandte Spitzenforschung und Forschungstransfer im Bereich der Informations- und Kommunikationstechnologie stellen wir uns dieser Verantwortung und wollen uns stetig im Bereich der sicheren Kommunikation und des Wissenstransfers verbessern.

Hierzu haben wir am FZI ein eigenes Informationssicherheitsmanagementsystem (ISMS) etabliert, welches nach der ISO 27001 zertifiziert ist. Unseren Forschungspartnern ermöglichen wir so neben einem sicheren und vertrauensvollen Wissensaustausch transparente Einblicke in unsere Arbeitsweise.

Das ISMS unterstützt uns im Alltag bei der Arbeit bewusster und zielgerichteter mit Daten und Informationen umzugehen. Ebenso dient es als Orientierung bei Transfer- und Kommunikationsentscheidungen.

Bequeme und praktische Plattformen können aus Sicherheitsgründen problematisch beim Austausch von Informationen sein. Dennoch kann deren Verwendung bei unkritischen Daten für den Workflow Sinn ergeben. Mit dem ISMS können wir eine Flexibilität anbieten, statt bestimmte Plattformen gänzlich auszuschließen. Entscheidungen werden somit bewusster und nachvollziehbarer für alle Beteiligten.

Mit der Einführung des ISMS haben wir einen weiteren Baustein für die kontinuierliche Weiterentwicklung des FZI gelegt. Wir danken allen Mitarbeitenden, die an der Ausgestaltung und Umsetzung unseres ISMS mitgewirkt haben.

LEITLINIE INFORMATIONS-SICHERHEIT

Sicherheit lässt sich nicht allein durch technische Maßnahmen erreichen.

— Einleitung

Als gemeinnützige Stiftung unterstützt das FZI Forschungszentrum Informatik interdisziplinär Unternehmen und öffentliche Institutionen durch die Entwicklung wissenschaftlicher Konzepte, Schulungen, Software-, Hardware- sowie Systemlösungen und setzt diese prototypisch um.

Am FZI werden laufend Informationen verarbeitet. Sowohl die Leistungsfähigkeit als auch die Reputation des FZI hängen maßgeblich vom Umgang mit diesen Informationen ab. Der Schutz dieser Informationen liegt deshalb im Interesse aller mit dem FZI verbundenen Personen und seiner Partner. Der Schutzbedarf erstreckt sich dabei auf technische und geschäftliche Prozesse, die mit der Verarbeitung von Informationen verbunden sind.

Informationssicherheitssituation

Das Lagebild der Informationssicherheit in Deutschland zeigt, dass Forschungseinrichtungen verstärkt in den Fokus von Akteuren geraten, die insbesondere an den Ergebnissen angewandter Technikforschung interessiert sind.

Zertifiziertes Informationssicherheits-managementsystem

Das FZI hat sich zum Ziel gesetzt, die führende unabhängige Einrichtung für IKT-Forschungstransfer in Europa zu werden. Um diesem Anspruch gerecht zu werden und gleichzeitig der beschriebenen Bedrohungslage adäquat begegnen zu können, muss zur Aufrechterhaltung der Leistungsfähigkeit ein wirksames und angemessenes Sicherheitsniveau mit Blick auf die verarbeiteten Informationen gewährleistet werden. Zu diesem Zweck betreibt das FZI ein Informationssicherheitsmanagementsystem (ISMS), welches entsprechend den Leitprinzipien des FZI rechtliche, regulatorische, vertragliche und ethische Bestimmungen berücksichtigt.

Um international gültigen Standards hinsichtlich eines Informationssicherheitsmanagementsystems gerecht zu werden, hat das FZI mit seinem ISMS die Anforderungen der ISO 27001 umgesetzt. Das FZI ist offiziell seit Juni 2023 nach der ISO 27001 zertifiziert.

— Anwendungsbereich

Das Informationssicherheitsmanagementsystem (ISMS) gilt für die gesamte Struktur, alle Räumlichkeiten, Organisationseinheiten und arbeitsbezogene Tätigkeiten des FZI. Es umfasst wissenschaftliche Tätigkeiten im Rahmen von Projekten sowie sämtliche unterstützende Prozesse. Die Einhaltung der Vorgaben des ISMS ist für alle am FZI tätigen Personen bindend. Hierzu zählen insbesondere die Vorstände, die Direktor*innen, die Beschäftigten, die Studierenden und die Gäste aus allen Forschungs- und Zentralbereichen.

Die gesamte Norm findet Anwendung am FZI, es werden keine Ausschlüsse von den Forderungen der ISO 27001 gemacht.

— Ziele

Das FZI verfolgt mit seinem ISMS die folgenden grundlegenden Ziele, die als Basis für alle relevanten Entscheidungen gelten:

- Abwendung von Schäden vom FZI, seinen Beschäftigten, Projekt- und Vertragspartnern
- Sicherstellung der Konformität zur ISO 27001 durch unabhängige externe Auditor*innen
- Wirksamer und angemessener Schutz von Informationen und Informationsprozessen vor Missbrauch, fahrlässigem Handeln und zufälligen Ereignissen mit Schadenspotenzial
- Einhaltung von Gesetzen, rechtlichen Bestimmungen und vertraglichen Regelungen mit Vertrags- und Forschungspartnern
- Weitestmögliche Freiheit von Forschung und Lehre unter Berücksichtigung der Informationssicherheit

Sicherheit wird im Rahmen von Schutzzielen definiert, die sich auf zu schützende Informationen, Prozesse und Dienste beziehen. Geschäftliche Informationen, die im Rahmen der Arbeitstätigkeit am FZI empfangen, erstellt, verarbeitet und gespeichert werden, sind nach diesen Zielen zu schützen, wobei der konkrete Schutzbedarf stets vom Einzelfall abhängt. Dem ISMS am FZI liegen folgende Schutzziele für Informationen zu Grunde:

- **Vertraulichkeit**
  Schutz vor Zugriff Unberechtigter und Offenlegung
- **Verfügbarkeit**
  Gewährleistung des Zugriffs durch Berechtigte
- **Integrität**
  Schutz vor unberechtigter, unbekannter und unbemerkter Veränderung

— Prinzipien

Um ein adäquates Sicherheitsniveau zu gewährleisten, beruht die Informationssicherheitspolitik des FZI auf folgenden grundlegenden Prinzipien:

- **Ganzheitlichkeit** – Sicherheit ist nicht losgelöst von Geschäftsprozessen, sondern muss als Teilaspekt in technischen und geschäftlichen Entscheidungen betrachtet werden.
- **Projektbezogenheit** – Auf Basis von Projekten werden Schutzziele, Risiken und Maßnahmen betrachtet, um den unterschiedlichen Anforderungen der einzelnen Projekte entsprechen zu können.
- **Verantwortungsbewusstsein** – Sicherheit lässt sich nicht allein durch technische Maßnahmen erreichen, sondern erfordert verantwortungsvolles Handeln im Umgang mit Informationen und informationsverarbeitenden Systemen und Prozessen. Durch Sensibilisierung der Beschäftigten soll zu eigenverantwortlichem Handeln motiviert und befähigt werden.
- **Risikobewusstsein** – Mögliche Risiken für die Informationssicherheit werden identifiziert, bewertet und angemessen behandelt.
- **Messbarkeit** – Die Wirksamkeit und Angemessenheit von Maßnahmen zur Erreichung von Schutzzielen ist nachprüfbar. Auf Basis der Messbarkeit wird eine ständige Verbesserung der sicherheitsrelevanten Prozesse und Maßnahmen angestrebt.

Im Rahmen dieser Prinzipien wird die Konformität mit der Norm ISO 27001 sichergestellt.

— Vorgehensweise

Die Rollen und Verantwortlichkeiten in der Informationssicherheit

Informationssicherheitsmanagement ist eine Gemeinschaftsaufgabe. Aus diesem Grund tragen alle Beschäftigten dazu bei, ein adäquates Informationssicherheitsniveau zu gewährleisten. Die Führungskräfte tragen die Verantwortung für die Informationssicherheit am FZI. Das FZI hat dazu Prozesse und Aufgaben entwickelt, die wiederum durch den Chief Information Security Officer (CISO) betreut und gesteuert werden. Unterstützt wird dieser durch die in den einzelnen Organisationseinheiten bestimmten Information Security Officer (ISO).

Risikomanagement

Ein essentieller Teil des Informationssicherheitsrisikomanagements findet in den Forschungsprojekten statt: hier legen die Führungskräfte gemeinsam mit den Projektleitungen den Schutzbedarf von Informationen in Projekten fest. Anschließend wird gemeinsam geprüft, ob die im Projekt genutzten Dienste das Sicherheitsniveau bieten, welches das Projekt benötigt. Sollte dies nicht der Fall sein, wird eine Risikobewertung und -behandlung vorgenommen. Die Rollen CISO und ISO können die verantwortlichen Führungskräfte und Projektleitungen dabei unterstützen.

Regelmäßige Schulungen und Sensibilierung

Die Leitung und ISO der Organisationseinheiten werden mit Blick auf das ISMS und das Management von Risiken regelmäßig geschult, damit sie für ihre jeweilige Organisationseinheit das Informationssicherheitsmanagement als Werkzeug effektiv und effizient zur Steigerung der Informationssicherheit nutzen können.

Der CISO organisiert zudem in regelmäßigen Abständen Sensibilisierungsmaßnahmen, u.a. in Form von Schulungen und Awarenesskampagnen, welche sich an die am FZI Beschäftigten richten.

Umgang mit Sicherheitsvorfällen und Anfragen

Um zu gewährleisten, dass Informationssicherheitsvorfälle sowie Fragen zum Informationssicherheitsmanagement direkt an den CISO herangetragen werden können, hat das FZI einen internen ISM-Servicedesk etabliert. Somit ist die Nachverfolgung von Anfragen und Vorfällen sichergestellt.

Regelmäßige Überprüfung des ISMS

Die Performanz des ISMS wird regelmäßig evaluiert und bei Bedarf mit Maßnahmen angepasst.

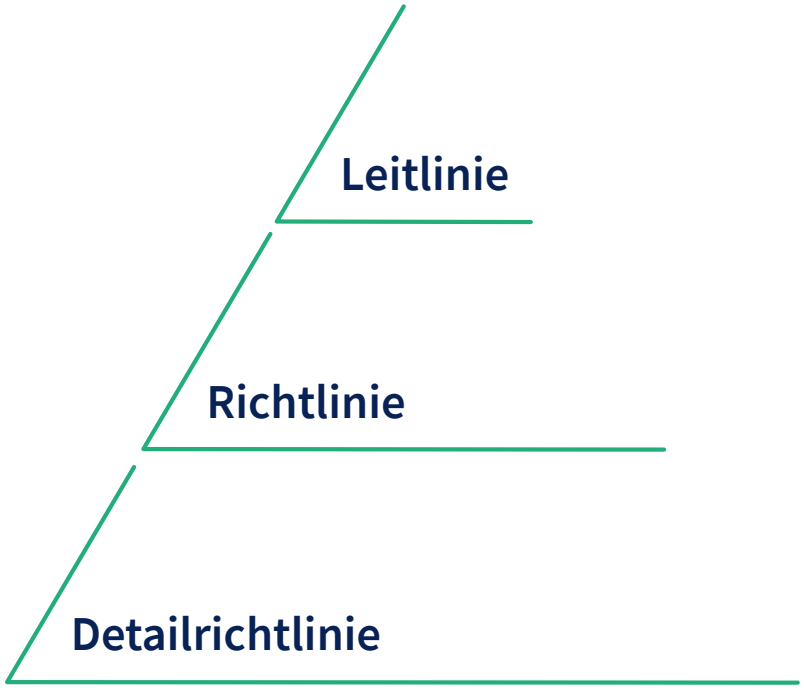
Regelmäßige Informationen über das ISMS

Informationen hinsichtlich des ISMS werden im FZI-internen Informationsportal veröffentlicht und regelmäßig aktualisiert.

— Richtlinien

Die Leitlinie für Informationssicherheit beschreibt die grundlegenden Ziele und Prinzipien der Informationssicherheitspolitik des FZI. Dementsprechend wurde eine Richtlinie für Informationssicherheit abgeleitet, welche darlegt, wie die definierten Ziele der Informationssicherheit realisiert werden sollen. Die Details zur Umsetzung von Informationssicherheit in den einzelnen Themenbereichen lassen sich wiederum den Detailrichtlinien entnehmen, welche u.a. den Anwendungsbereich, technische Spezifikationen und Umsetzungen enthalten.

Das Einhalten der Vorgaben, die das ISMS definiert, ist für alle mit dem FZI verbundenen Personen bindend (vgl. Anwendungsbereich S.6). Die Führungskräfte des FZI, insbesondere die Bereichs- und Abteilungsleitungen, nehmen hier eine Vorbildfunktion ein, indem sie Informationssicherheit vorleben und die Beschäftigten ihrer Organisationseinheit zu ebendiesem Verhalten motivieren und die Einhaltung der Leit-, Richt- und Detailrichtlinien sicherstellen.



— Impressum

Fragen?
Kommen Sie gerne auf uns zu!
Sie erreichen uns per E-Mail unter **fzi@fzi.de**.

Herausgeber
FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10–14
76131 Karlsruhe
www.fzi.de

Bildnachweis
Titelbild: ipopba – Adobe Stock
Seite 2: Henning Stauch – FZI
Seite 4: NicoElNino – Adobe Stock
Seite 6: Markus Breig – FZI
Seite 7: sdecoret – Adobe Stock
Seite 11: FZI

Stand: März 2026

— FZI FORSCHUNGSZENTRUM INFORMATIK

HAID-UND-NEU-STR. 10 – 14
76131 KARLSRUHE

www.fzi.de