Leitlinie zur Informationssicherheit

Ziele und Strategie des Informationssicherheitsmanagementsystems (ISMS)

— Vorwort

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

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 etablieren wir am FZI ein eigenes Informationssicherheitsmanagementsystem (ISMS) und werden uns freiwillig nach der DIN EN ISO/IEC 27001 zertifizieren lassen. 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 (FZI) interdisziplinär Unternehmen und öffentliche Institutionen durch die Entwicklung wissenschaftlicher Konzepte, Schulungen, Software-, Hardware- sowie Systemlösungen und setzt diese prototypisch um.

Das FZI verarbeitet laufend Informationen und 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.

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.

Das FZI hat sich zum Ziel gesetzt, das führende unabhängige Institut für IKT-Forschungstransfer in Europa zu werden. Um diesem Anspruch gerecht zu werden und gleichzeitig der beschriebenen Bedrohungslage adäquat begegnen zu können, muss ein wirksames und angemessenes Sicherheitsniveau mit Blick auf die verarbeiteten Informationen gewährleistet werden. Zu diesem Zweck betreibt das FZI ein Informationssicherheitsmanagementsystem (ISMS).

— Geltungsbereich

Das Einhalten der Vorgaben, die das ISMS definiert, ist für alle mit dem FZI verbundenen Personen bindend. Hierzu zählen insbesondere die Vorstände, die Direktor*innen, die Beschäftigten, die Studierenden, die Gäste sowie weitere Personen, die die Infrastrukturen des FZI nutzen. Weiterhin umfasst der Geltungsbereich alle digitalen und analogen Systeme, auf denen relevante Informationen verarbeitet werden. Die Führungskräfte des FZI, insbesondere die Bereichs- und Abteilungsleitungen, sind dazu aufgerufen, Informationssicherheit vorzuleben und die Mitarbeitenden ihrer Organisationseinheit zu ebendiesem Verhalten zu motivieren.

— 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 Mitarbeitenden, Kunden und Projektpartnern
- Sicherstellung der Konformität zur ISO27001 Norm 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 Kunden und Partnern
- 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 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 Mitarbeitenden 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 DIN EN ISO/IEC 27001 beabsichtigt.

— Vorgehensweise

Um ein adäquates Informationssicherheitsniveau zu gewährleisten, hat das FZI Prozesse und Aufgaben entwickelt, die durch den Chief Information Security Officer (CISO) betreut und gesteuert werden. Unterstützt wird er durch die in den einzelnen Organisationseinheiten bestimmten Information Security Officer (ISO).

Ein essentieller Teil des Informationssicherheitsrisikomanagements findet in den Forschungsprojekten des FZI statt. Die Leitung einer Organisationseinheit ist dafür verantwortlich, gemeinsam mit der jeweiligen Projektleitung den Schutzbedarf von Informationen in Projekten einzuschätzen und festzulegen. Anschließend wird über eine Zuordnung von verwendeten Diensten zum Projekt festgestellt, ob der Schutzbedarf des Projekts dem Sicherheitsniveau der verwendeten Dienste entspricht. Sollte dies nicht der Fall sein, ist es notwendig, eine Risikobewertung und -behandlung vorzunehmen. Die adäquate Behandlung eines Risikos ist stets eine individuelle Maßnahme, die im Rahmen des Projekts definiert, dokumentiert, umgesetzt und überwacht wird. Die Rollen CISO und ISO können die Verantwortlichen dabei unterstützen.

Die Leitungen und ISOs von Organisationseinheiten werden mit Blick auf das Informationssicherheitsmanagementsystem 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 für Mitarbeitende des FZI und andere Personen, die diese Richtlinien organisieren. Damit wird sichergestellt, dass alle Personen über die Bedrohungslage informiert sind und gleichzeitig die Maßnahmen kennen und umsetzen.

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

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

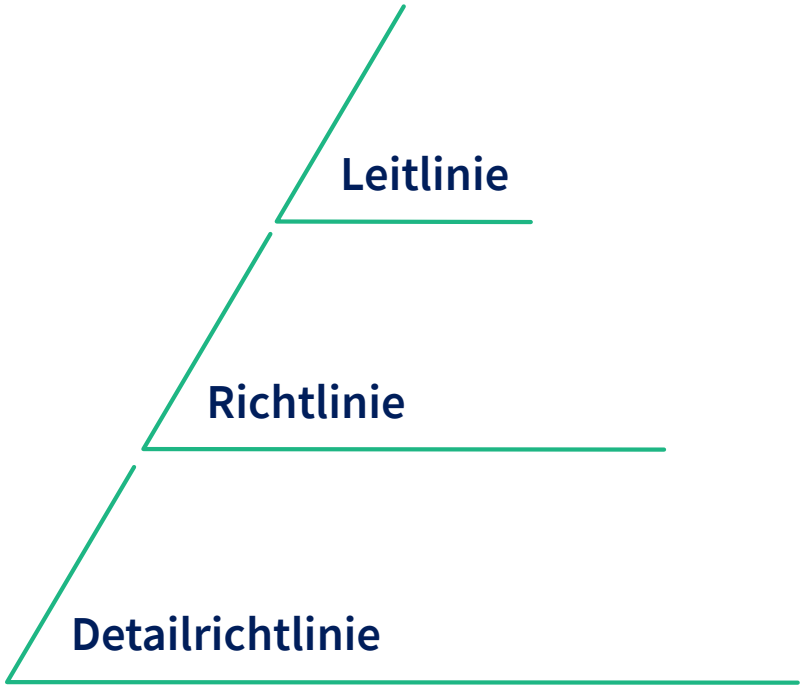
Weiterführende Informationen werden im unternehmensinternen Informationsportal veröffentlicht und regelmäßig aktualisiert.

— Richtlinien

Die Leitlinie für Informationssicherheit beschreibt die grundlegenden Ziele und Prinzipien der Informationssicherheitspolitik des FZI. Dementsprechend wird eine Richtlinie für Informationssicherheit abgeleitet, welche die Vorgaben zu speziellen Themenbereichen umfasst, die Informationssicherheit betreffen. Die Details zur Umsetzung von Informationssicherheit in den einzelnen Themenbereichen lassen sich wiederum den Detailrichtlinien entnehmen. Sie enthalten u.a. den Geltungsbereich, technische Spezifikationen und Umsetzungen zur Erreichung der Ziele.

Die Leitlinie, Richtlinien und Detailrichtlinien sind im FZI-Portal abrufbar.

Das Einhalten der Vorgaben, die das ISMS definiert, ist für alle Beschäftigte, Vorstände, Direktor*Innen und Gäste des FZI bindend (vgl. Geltungsbereich S.6). Die Führungskräfte des FZI, insbesondere die Bereichs- und Abteilungsleitungen, sind dazu aufgerufen, Informationssicherheit vorzuleben und die Mitarbeitenden ihrer Organisationseinheit zu ebendiesem Verhalten zu motivieren und die Einhaltung der Leit-, Richt- und Detailrichtlinien sicherzustellen.



— 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: Juli 2022

— FZI FORSCHUNGSZENTRUM INFORMATIK

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

www.fzi.de