Information Security Guidelines

Goals and Strategy of the Information Security Management System (ISMS)

— Foreword

The Board of Excecutive Directors of the FZI
(from left to right): Jan Wiesenberger,
Prof. Dr.-Ing. J. Marius Zöllner, Prof. Dr. Stefan Nickel

Dear Readers,

At the FZI, attaining and sharing research knowledge are our most valuable currency. They are key towards successfully transferring technology from the laboratory to production in order to apply innovative ideas in business and for the common good. However, this also makes them interesting goals.

The loss of data due to data leaks, industrial espionage or cyberattacks represents a major risk for us and our partners. As one of the leading independent institutes for applied cutting-edge research and research transfer in the field of information and communication technology, we accept this responsibility and want to continuously improve in the field of secure communication and knowledge transfer.

For this purpose, we have established our own information security management system (ISMS) at the FZI, which is certified according to ISO 27001. In addition to a secure and trustworthy exchange of knowledge, this enables our research partners to gain transparent insights into our working methods.

The ISMS helps us to deal with data and information more consciously and purposefully in our everyday work. It also serves as orientation for transfer and communication decisions.

Convenient and practical platforms can be problematic for sharing information due to security reasons. Nevertheless, their use can make sense for workflow when the data is not critical. With the ISMS, we can offer flexibility instead of excluding certain platforms altogether. Decisions thus become more conscious and understandable for all parties involved.

With the introduction of the ISMS, we have laid a further building block for the continuous development of the FZI. We would like to thank all employees who have been involved in designing and implementing our ISMS.

INFORMATION SECURITY GUIDELINES

Security cannot be achieved
via technical measures alone.

— Introduction

As a non-profit foundation, the FZI Research Center for Information Technology supports companies and public institutions in an interdisciplinary manner by developing scientific concepts, training, software, hardware and system solutions and implementing them as prototypes.

At the FZI, information is processed constantly. Both the performance and reputation of the FZI depend to a large extent on how this information is handled. The protection of this information is therefore in the interest of all persons associated with the FZI and its partners. The need for protection extends to technical and business processes associated with the processing of information.

Current situation

The situation of information security in Germany shows that research institutions are increasingly becoming the focus of actors who are especially interested in the results of applied technology research.

Certified information security management system

The FZI has set itself the goal of becoming the leading independent institution for ICT research transfer in Europe. To live up to this claim and at the same time to be able to adequately counter the threat situation described above, an effective and appropriate level of security must be ensured regarding the information processed in order to maintain performance. For this purpose, the FZI operates an information security management system (ISMS) that considers legal, regulatory, contractual and ethical provisions in accordance with the guiding principles of the FZI.

With its ISMS, the FZI has implemented the requirements of ISO 27001 in order to meet international standards for information security management systems. The FZI was officially certified in June 2023 according to ISO 27001.

— Scope

Compliance with the requirements defined by the ISMS is binding for all persons associated with the FZI. This includes particularly board members, directors, employees, students, guests and other persons who use the infrastructures of the FZI. Furthermore, the scope includes all digital and analog systems on which relevant information is processed.

— Goals

With its ISMS, the FZI pursues the following fundamental objectives, which serve as the basis for all relevant decisions:

- Prevent damage to the FZI, its employees, project and contract partners
- Assurance of conformity to the ISO 27001 standard by independent external auditors
- Effective and adequate protection of information and information processes against misuse, negligent actions and random events with the potential to cause damage
- Compliance with laws, legal provisions and contractual regulations with contract and research partners
- The broadest possible freedom in research and teaching under consideration of information security

Security is defined in the context of protection goals that relate to the information, processes and services to be safeguarded. Business information that is received, created, processed and stored as part of the work activities at the FZI must be protected in accordance with these objectives, whereby the specific need for security always depends on the individual case. The ISMS at the FZI is based on the following protection goals for information:

- **Confidentiality**
  Protecting against unauthorized access and disclosure
- **Availability**
  Ensuring access by authorized persons
- **Integrity**
  Safeguarding against unauthorized, unknown and unnoticed changes

— Principles

To ensure an adequate level of security, the FZI's information security policy is based on the following fundamental principles:

- **Holistic** – Security is not separate from business processes but must be considered as an aspect of technical and business decisions.
- **Project-based** – Based on projects, protection goals, risks and measures can meet the different requirements of the individual projects.
- **Sense of responsibility** – Security cannot be achieved by technical measures alone but requires responsible action in dealing with information and information processing systems and procedures. Raising employee awareness is intended to motivate and enable them to act on their own responsibility.
- **Risk Awareness** – Potential risks to information security are identified, assessed, and addressed appropriately.
- **Measurability** – The effectiveness and appropriateness of measures to achieve protection goals can be verified. Based on measurability, the aim is to continuously improve safety-relevant processes and measures.

Within the framework of these principles, conformity with ISO 27001 standard is ensured.

— Procedure

The roles and responsibilities in information security

Information security management is a joint task. For this reason, all employees contribute to ensuring an adequate level of information security. The executives are responsible for information security at the FZI. The FZI has developed processes and tasks for this purpose, which in turn are supervised and controlled by the Chief Information Security Officer (CISO). They are supported by the Information Security Officers (ISO) appointed in the individual organizational units.

Risk management

An essential part of information security risk management takes place in the research projects: Here, managers work together with the project leaders to determine the need for protection of information in projects. A joint review is then conducted to determine whether the services used in the project provide the level of security that the project requires. If this is not the case, a risk assessment and response is carried out. The CISO and ISO roles can support the responsible managers and project leaders in this process.

Regular training and awareness

Management and the ISO of the organizational units are regularly trained regarding the ISMS and handling risks so that they can use information security management effectively and efficiently as a tool for increasing information security in their respective organizational unit.

The CISO also organizes awareness-raising measures at regular intervals, including training courses and awareness campaigns geared towards FZI employees.

Dealing with security incidents and requests

To ensure that information security incidents and questions about information security management can be brought directly to the attention of the CISO, the FZI has established an internal ISM service desk. This guarantees follow-up on inquiries and incidents.

Regular review of the ISMS

ISMS performance is evaluated on a regular basis and adjusted via measures as needed.

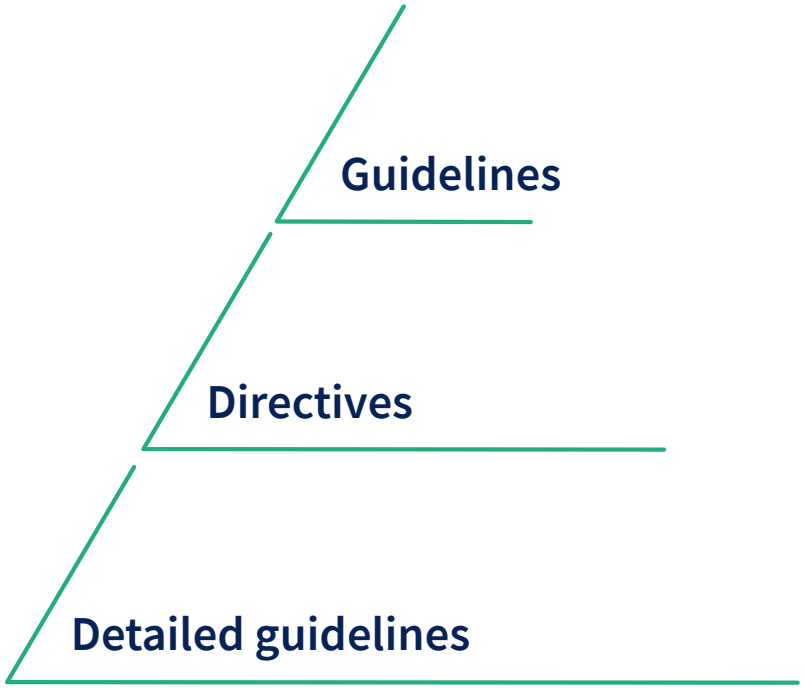
Regular information about the ISMS

Information regarding the ISMS is published and regularly updated in the FZI-internal information portal.

— Guidelines

These guidelines for information security describe the fundamental goals and principles of the FZI‘s information security policy. Accordingly, guidelines for information security are derived that set out how the defined information security goals should be implemented. The specifics for implementing information security in the individual subject areas can in turn be found in the detailed guidelines, which contain, among other things, the scope of application, technical specifications and implementations.

Compliance with the requirements defined by the ISMS is binding for all persons associated with the FZI (cf. Scope p.6). The managers of the FZI – especially division and department heads – act as role models by setting an example on information security and motivating the employees of their organizational units to behave in this way, and ensuring compliance with the guidelines, directives and detailed guidelines.



— Legal notice

Questions?
Please feel free to contact us!
You can reach us by email at **fzi@fzi.de**.

Publisher
FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10-14
76131 Karlsruhe
www.fzi.de/en

Photo credits
Cover photo: ipopba – Adobe Stock
Page 2: Henning Stauch – FZI
Page 4: NicoElNino – Adobe Stock
Page 6: Markus Breig – FZI
Page 7: sdecoret – Adobe Stock
Page 11: FZI

Status: November 2023

— FZI Research Center for Information Technology

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

www.fzi.de/en