innoscripta

2026

GUIDELINE

INFORMATION SECURITY

Contents

Foreword ---------- 02

I. Guiding principle and importance of information security ---------- 03

II. Our expertise, our head start ---------- 04

III. Implementation ---------- 05

IV. Responsibility of the management ---------- 06

V. Final provisions and scope of application ---------- 07

Contact person and contact ---------- 08

Foreword

Information security is a decisive factor for the success and protection of any company. To ensure that information security is effectively and sustainably guaranteed, a clear and structured approach is required. For this reason, an information security management system (ISMS) introduced and continuously developed to strengthen the security of information and keep it up to date.

Clear responsibilities are defined and the necessary resources, such as training, personnel and budget, are provided to support the implementation of information security. The Information Security Officer (ISB) is a central point of contact for all questions relating to this topic. This person coordinates and monitors all activities relating to information security and supports the specialist departments in adapting their processes to the security standards. An information security guideline forms the basis of security management. It defines the objectives, importance and responsibilities in the area of information security. In addition, there are supporting guidelines that are developed in cooperation with the specialist departments.

The close cooperation between the Management Board, specialist departments and the ISB creates a practice-oriented and active information security culture that is practiced throughout the company.

Information security is a key element in ensuring the long-term success of a company and is therefore a top priority. All employees are required to the established guidelines and specifications.

For better readability, no gender-specific formulations are used and all terms apply equally to all genders.

innoscripta SE, January 2026

Michael Hohenester

Verified by signNow
03/02/2026 16:38:02 UTC
fb07a503870c4e07951a

Michael Hohenester
Management Board

Alexander Meyer

Verified by signNow
03/02/2026 17:20:05 UTC
13b200c2e073430088b3b

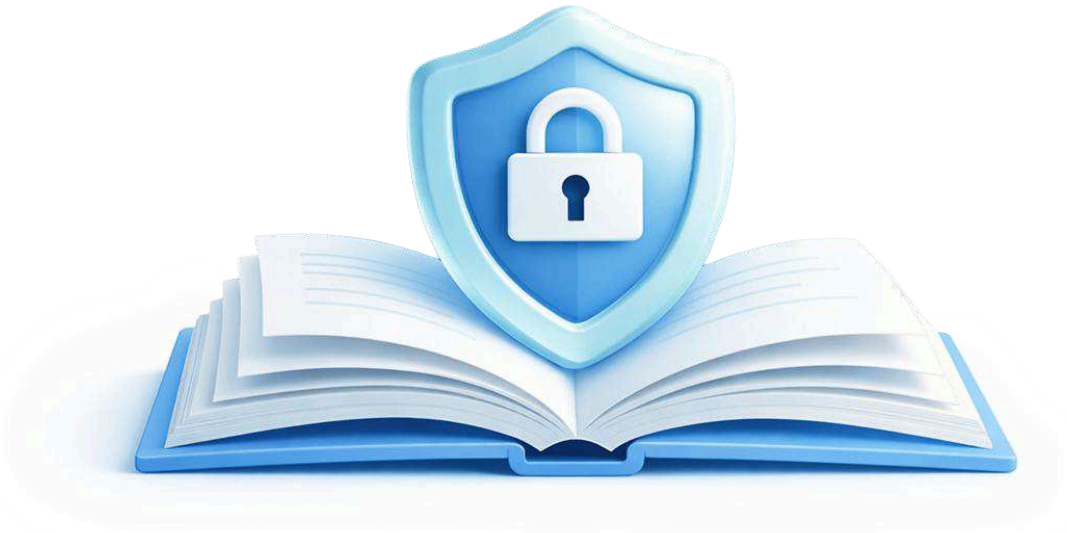
Alexander Meyer
Management Board

I. Guiding principle and importance of information security

Information security is a central guiding principle and an indispensable part of innoscripta SE's corporate philosophy. It forms the basis for ensuring the reliability of our systems, processes and services and strengthening our reputation as a reliable partner for customers and business partners. A high level of protection for the confidentiality, integrity and availability of our information is crucial to ensure the long-term success and stability of our company.

To underline this high priority, the Management Board has established a comprehensive information security management system (ISMS) in accordance with the ISO/IEC 27001 standard. This system ensures that information security is deeply integrated into our operational processes and is an integral part of every employee's daily work. All employees are obliged to the defined security guidelines and demonstrate a strong awareness of information security in their daily tasks.

Information security is not just a formal requirement but an essential part of our corporate objectives that is actively supported by management and practiced by each individual. Identifying and immediately reporting vulnerabilities is an integral part of every employee's responsibility to ensure the continued security and integrity of our systems.



II. Our Expertise, Our Head Start

Technical Safety

The level of security is significantly strengthened by targeted technical measures and a secure IT design. This includes investments in the protection of sensitive areas and critical facilities. It is the responsibility of every employee to comply with these measures and to contribute to their secure use in order to ensure the integrity of the systems and the protection of sensitive data.

Least-Privilege Principle

Access authorizations and information are granted exclusively and specifically to those who need them to perform their tasks. The recipients must be aware of how sensitive the information is and who belongs to their group of recipients. This applies to authorizations in IT systems as well as physical access rights.

Personal Responsibility

Each individual is required to actively assume responsibility. Employees are obliged to be alert to weak points, suspicious events, and security-relevant incidents, and to report them immediately. Understanding consistent compliance with internal security guidelines is a prerequisite and expected of everyone. This commitment strengthens information security and protects the values and integrity of the company in the long term.

Correct Handling of Documents and Data Carriers

The handling of documents and data carriers with confidential content is essential for the protection of information. Employees are obliged to minimize the printing of sensitive information, store documents and storage media securely, and dispose of them properly. Compliance with these measures is the responsibility of each individual to ensure confidentiality and security.

III. Implementation

To implement the information security requirements, innoscripta SE has established an information security management system (ISMS) in accordance with the international standard **ISO/IEC 27001:2022** and taking into account relevant legal and industry-specific requirements. The ISMS is based on the continuous improvement process of the PDCA model (**P**lan, **D**o, **C**heck, **A**ct). The aim is to regularly verify and ensure the appropriateness, completeness, sustainability, effectiveness, and efficiency of the implemented security processes and protective measures.

Plan
Set

Strategies, objectives, and processes of the ISMS are defined, as well as procedures, methods, tools, and responsibilities.

Do
Implement and Execute

The defined processes and procedures are implemented in accordance with the ISMS objectives, and the necessary measures are put in place.

Check
Monitor and Check

The effectiveness of the implemented measures as well as compliance with the defined processes are monitored, measured, and regularly reviewed.

Act
Maintain and Improve

Based on the review results, corrective and improvement measures are derived to continuously optimize the ISMS.

IV. Responsibility and Management

The company management is responsible for information security and the necessary resources to ensure and further develop an appropriate level of security.

Managers actively promote safety awareness among employees and ensure that information and IT security standards are complied with.

V. Final Provisions and Scope of Application

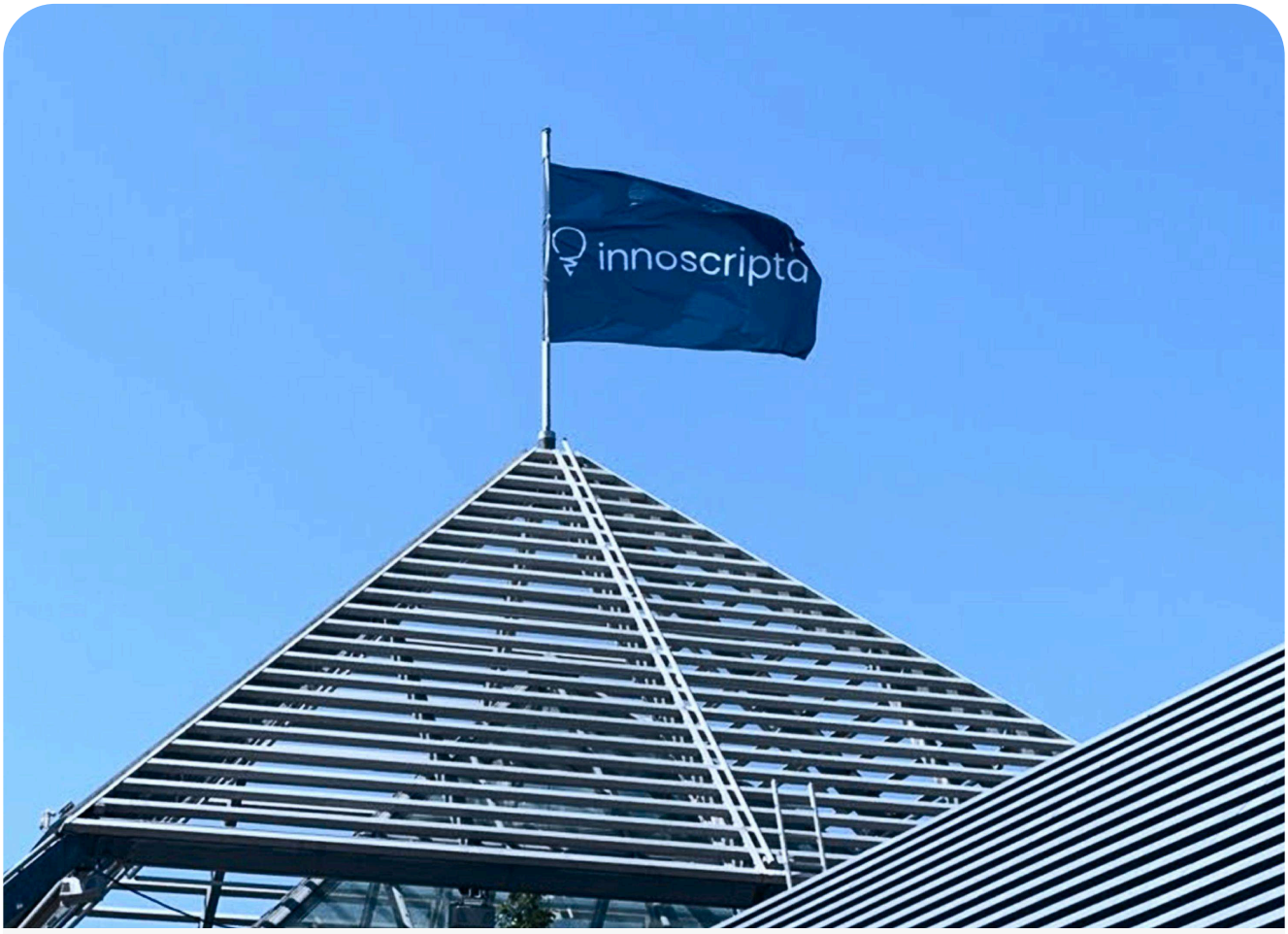
The information security policy is based on company-wide guidelines and process descriptions that contain detailed organizational and security rules and are used exclusively internally. The scope of the underlying information security management system is defined centrally and described in detail in an accompanying scope document.

These regulations apply to all employees, departments, and external partners of innoscripta SE and form binding standards for the secure handling of information.

Contact Person and Contact

Julia Erber
Information Security Officer

datenschutz@innoscripta.com



innoscripta SE

Arnulfstraße 60
80335 München

www.innoscripta.com