Information security policy

[company name]

> **Note**
> How to use this template: replace every entry in square brackets, adapt the suggested wording to your company and delete the grey fill-in guidance before approval. Top management signs the policy.

Document control

Document ID	[ISMS-LL-001]
Version	[1.0]
Date of approval	[DD.MM.YYYY]
Document owner	[information security officer]
Classification	[public / internal / confidential / strictly confidential]
Approved by	[name] (management)
Reference	ISO/IEC 27001:2022, Clause 5.2, A.5.1

What is this document for?

Top-level document of the ISMS: principles, objectives and responsibilities for information security. Addressed to all employees, signed by senior management and reviewed at least annually.

1. Importance of information security for our company

Guidance (Clause 5.2 a): Why is information security important for your business? Concrete and easy to understand.

Our design data, customer data and an available production facility are the foundation of our business success. Our customers entrust us with confidential information and expect us to deliver reliably.

2. Scope

Guidance: Who and where the policy applies to.

This policy applies to all employees, temporary agency staff and service providers who process information of [company name] at the sites [sites], when working remotely or on service assignments.

3. Security objectives and framework for objectives

Guidance (Clause 5.2 b): Overarching objectives from which annual measurable objectives are derived.

- Protection of confidential customer and design data
- High availability of production and the supporting IT
- Compliance with statutory and contractual requirements
- Rapid detection and handling of security incidents

4. Principles

Guidance: Key principles of conduct and design.

- Access only as far as necessary (need-to-know)
- Security is part of every change and every project
- Security incidents are reported immediately – reporting is not punished
- Production systems are given particular protection

5. Responsibilities

Guidance (Cl. 5.3): Roles of senior management, information security officer, managers and employees.

Senior management bears overall responsibility. The information security officer steers the ISMS and reports directly to senior management. Managers implement the rules in their areas. All employees comply with the rules and report anything unusual.

6. Commitment to requirements and improvement

Guidance (Clause 5.2 c, d): Explicit commitment by management.

Senior management undertakes to meet all applicable information security requirements and to continually improve the ISMS. It provides the necessary resources for this.

7. Handling of violations

Guidance (Clause 7.3, A.6.4): Note on the consequences of violations (agreed in line with employment law).

Violations of this policy and the subordinate policies may have consequences under employment law.

8. Subordinate policies

Guidance (A.5.1): List the policies that put this policy into practice (title, version, date) and any further rules kept outside the ISMS.

- [Access control and permissions policy, version, date]
- [Security incident management policy, version, date]
- [Further rules, e.g. works agreement on IT use]

Entry into force

This policy enters into force on approval and is made known to all employees.

Place, date	Signature of top management

Change history

Version	Date	Change	Author	Approval

About this template

Template version	1.0-3b5fe1f0
Content as of	26 September 2026
Published by	Made with Complass, https://complass.eu

Source: document template "Information security policy" of the ISO 27001 project in Complass. In Complass you keep the policy with review, four-eyes approval, versions and employee acknowledgement.

This template is not legal advice. It does not replace checking which requirements apply to your company and does not guarantee any audit or certification result.

License: Creative Commons Attribution 4.0 International (CC BY 4.0). You may use, change and pass on the template, also commercially, as long as you name the source. Attribution: "Template: Complass (complass.eu), CC BY 4.0". https://creativecommons.org/licenses/by/4.0/deed.en