

— TEMPLATE · TOMORIS TOOLBOX

IT Security Policy: Template for Small and Medium-Sized Businesses

Model text for the information security policy and basic rules for all employees, with references to BSI IT-Grundschutz, the NISG 2026, and the NISV 2026

UPDATED

Oct 25, 2026

LENGTH

PDF, 10 pages

ONLINE

tomoris.com/en/downloads/it-sicherheitsrichtlinie-vorlage

AT A GLANCE

2 parts

Policy and basic rules for all employees

8

Basic rules from passwords to incident reporting

1× a year

Review by management at NIS2 entities

§ 31

NISG 2026: management ensures risk management

WHO IT IS FOR

- Executives and management bodies of small and medium-sized businesses
- Information security officers and IT managers who create or revise a policy
- Companies that fall under the NISG 2026 as an essential or important entity or are preparing for it

WHAT THIS COVERS

An IT security policy, which the BSI calls an information security guideline, sets out why a company protects information, which objectives it pursues, and who is responsible for what. This template contains model text with placeholders, basic rules for all employees, and an implementation checklist. It shows which content BSI Standard 200-2 and IT-Grundschutz module ISMS.1 require. It also shows what has applied since October 2026 to essential and important entities under the NISG 2026 (Austrian Network and Information Systems Security Act 2026) and the NISV 2026 (Austrian NIS Regulation 2026).

This template must be adapted to your company and does not replace legal advice. The NISG 2026, the NISV 2026, and Implementing Regulation (EU) 2024/2690 in their current versions are authoritative. Clarify employment law questions, such as how to handle violations, with your legal advisor.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01	What an IT Security Policy Governs	2
02	What Belongs in It: BSI and EU Regulation	3
03	What the NISG 2026 Requires of Management	4
04	Model Text Part A: Information Security Policy	5
05	Model Text Part B: Basic Rules for All Employees	7
06	Implementation Checklist	8
07	Common Mistakes	9
08	Sources	10

01 —

What an IT Security Policy Governs

The top-level document of information security: terms used by the BSI and the EU, and the structure of this template.

The IT security policy is the top-level document of information security. The BSI calls it the information security guideline, in English the Information Security Policy (BSI Standard 200-1, chapter 7.1); Implementing Regulation (EU) 2024/2690 refers to the policy on the security of network and information systems (Annex point 1.1). It describes in generally understandable terms for which purposes, and with which means and structures, information security is to be achieved, and it contains security objectives and strategy (BSI Standard 200-2, chapter 3.4). It is management's visible commitment to its strategy (BSI Standard 200-1, chapter 3.1).

Structure of this template: Part A is the policy that management approves. Part B contains basic rules for all employees, as the BSI envisages for a guideline on secure IT use: objectives, roles, contact person, and measures to be observed (ORP.1.A16). TOMORIS recommends this separation so that the policy stays short and the basic rules are easier to adapt.

02

What Belongs in It: BSI and EU Regulation

Content under BSI Standard 200-2 and ISMS.1.A3 alongside the mandatory content from Annex point 1.1 of Implementing Regulation (EU) 2024/2690.

Minimum content is specified in BSI Standard 200-2 (chapter 3.4.3) and requirement ISMS.1.A3 of the IT-Grundschutz Compendium. For essential and important entities, the content under Annex point 1.1.1(a) to (k) of Implementing Regulation (EU) 2024/2690 is binding. The regulation specifies Art. 21(2)(a) of the NIS2 Directive and applies directly to providers such as cloud and managed services, and via § 2 NISV 2026 to all other essential and important entities. Where the BSI does not require an item for the policy itself, the table gives the related requirement in parentheses.

Policy content with references in the BSI and in Annex point 1 of Implementing Regulation (EU) 2024/2690

CONTENT	BSI	IR 2024/2690
Scope	ISMS.1.A3; 200-2, ch. 3.4.3	not mentioned in point 1.1.1
Importance of information security, approach to security management	ISMS.1.A3; 200-2, ch. 3.4.3	Point 1.1.1(a)
Security objectives related to business objectives and strategy	ISMS.1.A3	Point 1.1.1(b), (c)
Management commitment to enforcement and resources	Enforcement: 200-2, ch. 3.4.3 (resources: ISMS.1.A1)	Resources: point 1.1.1(e)
Roles, responsibilities, organizational structure	ISMS.1.A3	Points 1.1.1(g) and 1.2
List of topic-specific policies	not required (target-group-specific guidelines: ISMS.1.A16)	Point 1.1.1(i)
Improvement, performance review, metrics	Performance review: 200-2, ch. 3.4.3; improvement: ISMS.1.A11	Point 1.1.1(d), (j)
Documentation to be retained and retention period	not required (documentation: ISMS.1.A13)	Point 1.1.1(h)
Communication to employees and external parties	ISMS.1.A3	Point 1.1.1(f), with acknowledgment
Approval by management, with date	in writing, formally approved: 200-2, ch. 3.4.4	Point 1.1.1(k)

Review

200-2, ch. 3.4.5: at least every two years

Point 1.1.2: at least annually
and when required

03 —

What the NISG 2026 Requires of Management

§ 31 governance, § 32 risk management, and the NISV 2026: what has applied to essential and important entities since October 2026.

Since October 1, 2026, the NISG 2026 has applied to essential and important entities (BGBl. I No. 94/2025, § 51 para. 2). Their management bodies, meaning the persons or bodies appointed by law, articles of association, or contract to manage the business (§ 3 no. 11), must ensure and oversee compliance with the risk management measures under § 32 (§ 31 para. 1). They must attend cybersecurity training designed for them; employees must be offered corresponding training regularly (§ 31 para. 2). The minimum content of risk management includes policies on risk analysis and information system security (§ 32 para. 4 lit. a).

On October 1, 2026, the NISV 2026 was promulgated (BGBl. II No. 290/2026); it entered into force at the end of that day (§ 9). Its § 2 declares the requirements of Implementing Regulation (EU) 2024/2690, including its annex, applicable to the other types of essential and important entities in Annexes 1 and 2 of the NISG 2026 as well. For the policy, this means: content under Annex point 1.1.1, the date of formal approval by the management bodies (lit. k), review by them at least annually and after significant incidents or significant changes with a documented result (point 1.1.2), and at least one person who reports directly to the management bodies (point 1.2.3).

If an entity cannot meet individual requirements temporarily or because of its size, it implements compensating measures, documents them with reasons, and reviews their effectiveness at least annually; this does not apply to requirements that only apply to the extent appropriate, applicable, or feasible (§ 4 NISV 2026). Anyone who breaches the training obligations commits an administrative offense; the same applies to anyone who fails to implement risk management measures, unless the authority learned of this only through the self-declaration (§ 45 para. 1 no. 1 to 3). The penalty range is up to €10 million or 2% of worldwide annual turnover in the previous year for essential entities, and up to €7 million or 1.4% for important entities, whichever is higher in each case (§ 45 para. 2 and 3).

The NIS2 Directive requires management bodies to approve the measures, oversee their implementation, and be held accountable (Art. 20(1)); in Austria, the wording of § 31 NISG 2026 is authoritative. Whether your company is affected is governed by §§ 24 to 26 together with Annexes 1 and 2. For all others, the content of this template consists of recommendations based on the BSI.

04 —

Model Text Part A: Information Security Policy

Eight sections with placeholders in square brackets, plus roles and a signature field for management.

Replace every placeholder in square brackets, delete anything that does not apply, and derive the objectives from your business objectives and your risk analysis. The eight sections cover all rows of the table in Section 2; NIS2 entities should not delete anything there without review.

1 Purpose and scope

This policy defines why and how [Company] protects information. It applies to [the entire company | sites, divisions], to management, managers, and all employees, to external persons working for [Company], and to information in any form: on paper, in IT systems, in cloud services, and on mobile devices.

2 Importance and security objectives

Our most important business processes are [e.g., order processing, production]; they depend on [e.g., ERP system, email]. An outage or leak of this information endangers [e.g., ability to deliver, customer trust]. We therefore protect confidentiality, integrity, and availability as appropriate to the risk. Our objectives: [e.g., customer data is accessible only to authorized persons; order processing is running again within [hours] after an outage; legal and contractual obligations are met].

3 Responsibility of management

Management bears overall responsibility for information security. It approves this policy, enforces it, leads by example in following the rules, and provides staff, budget, procedures, and technology. It receives reports on status, risks, and incidents at least [every six months] and decides how to handle residual risks.

4 Roles and organization

The information security officer is [name, function], deputy [name, function]. The information security officer coordinates information security, advises management, reports directly to it, and is involved early in major projects and new IT systems. Further roles are listed in the table below; management reviews them [annually] and after significant incidents or changes.

5 Policies and training

The security concept defines the measures based on a risk analysis. Individual topics are governed by separate policies consistent with this policy: [e.g., basic rules (Part B), access control, backup, security incidents, suppliers], approved by [function]. All employees are briefed before their first IT use and trained at least [annually]; management receives training designed specifically for it.

6 Violations and exceptions

Violations can harm [Company], customers, and partners; employees are informed of possible consequences. [Function] decides case by case how a violation is handled, in accordance with the employment contract, [works agreement], and applicable law. Exceptions to rules are permitted only with justification, for a limited time, and after approval by [function]; [information security officer] keeps an overview of them.

7

Review, metrics, and documentation

We continuously improve information security. Management reviews this policy at least [annually] and after significant incidents or significant changes, and documents the result. We measure progress by [metrics, e.g., training rate, time to install critical updates]. [information security officer] retains [documents, e.g., risk analysis, reports, training records, incident logs] for [period].

8

Entry into force

Management approved this policy on [MM/DD/YYYY]. It enters into force on [MM/DD/YYYY], replaces [previous version | none], and is communicated to all employees and the affected external partners, who confirm that they have read it. Next review no later than [MM/DD/YYYY].

Roles in information security (for Section 4)

ROLE	TASKS	WHO
Management	Overall responsibility, resources, regular reports (ISMS.1.A1, ISMS.1.A12)	_____
Information security officer	coordinates, advises management, reports directly, investigates incidents, coordinates training (ISMS.1.A4; 200-2, ch. 4.4)	_____
Deputy information security officer	takes over during absences, equally qualified (ISMS.1.A6; 200-2, ch. 4.4)	_____
IT operations	implements technical measures, such as updates and permissions (OPS.1.1.3.A15, ORP.4.A2); ideally not also the information security officer (200-2, ch. 4.4)	_____
Managers	lead by example and point out the rules (ORP.3.A1)	all
Employees and external parties	Security at their own workplace (200-1, ch. 7.2); third parties apply the rules (IR 2024/2690, Annex point 1.2.2)	all

Approval (for Section 8)

FUNCTION	NAME	DATE	SIGNATURE
Management	_____	_____	_____
Information security officer, for information	_____	_____	_____

References for the model text: Section 3 based on ISMS.1.A1 and ISMS.1.A12. Section 4 based on ISMS.1.A4, ISMS.1.A6, and Annex point 1.2 IR 2024/2690. Section 5 based on ISMS.1.A7 and ORP.3.A3. Section 6 based on ISMS.1.A8 and ORP.5.A5. Section 7 based on ISMS.1.A11, ISMS.1.A13, and Annex points 1.1.1(d), (h), (j), and 1.1.2. Section 8 based on BSI Standard 200-2, chapter 3.4.4, and Annex point 1.1.1(f), (k).

05 —

Model Text Part B: Basic Rules for All Employees

Eight rules for everyday work with placeholders, plus written acknowledgment.

Basic rules for secure IT use at [Company]

1. Accounts, passwords, MFA	Your account is personal: never share credentials, not even with supposed IT staff. Use a separate, hard-to-guess password from [password manager] for each system, and multi-factor authentication for [email, remote access, cloud services]. If you suspect a problem, change the password immediately and report it. Basis: ORP.4.A8; § 32 para. 4 lit. j NISG 2026.
2. Updates	Install offered updates and restart when prompted; postpone for no longer than [period]. Automatic updates stay turned on. Use software without vendor support only after approval by [IT department]. Basis: SYS.2.1.A3, OPS.1.1.3.A15.
3. Email and phishing	Senders can be spoofed. Don't open unexpected attachments, don't reply to suspicious messages, and don't follow their links. Report them via [report button address] and then delete them. If you have already clicked or entered data, report it immediately. Basis: APP.5.3.A7, APP.5.3.A8.
4. Storing data	Store business data only in the approved locations: [e.g., file server, SharePoint]. [Private cloud services and private email accounts are not permitted for this.] Connect only approved USB storage devices and keep confidential documents locked away. Basis: CON.3.A5, APP.5.3.A6, SYS.2.1.A24, INF.7.A7.
5. Devices and workplace	Lock your screen or device as soon as you leave your workplace; protect smartphones and tablets with a lock code. Don't turn off protective software. Don't leave confidential documents lying around. Basis: SYS.2.1.A1, SYS.3.2.1.A4, SYS.2.1.A6, INF.7.A6.
6. Mobile working	When traveling and at home, work only on approved information: [rule]. Never leave devices and documents unattended, use a privacy screen when traveling, and don't work on business data on other people's devices. Access internal systems only via [VPN approved access]. Basis: INF.9.A2, INF.9.A3, INF.9.A4, INF.9.A12.
7. Reporting incidents	Report immediately to [reporting office, phone, email], and outside working hours to [emergency number]: suspicious messages or calls, devices behaving unusually, your own mistakes, and lost or stolen devices and documents. Even a mere suspicion counts. Basis: DER.2.1.A3, DER.2.1.A9, INF.9.A5, SYS.3.2.1.A7.
8. Confidentiality	Business information is intended for internal use, including after working hours and outside the company. Share it only with authorized persons. When you leave the company, return documents, keys, devices, and ID badges. Basis: ORP.2.A14, ORP.2.A2.

Acknowledgment: I have read the basic rules and will comply with them. I will direct questions to [contact person, contact details]. New employees confirm before their first IT use; all users confirm again regularly or after major changes (ORP.1.A16). The “Basis” references can be omitted in your version.

Acknowledgment of receipt

NAME	DEPARTMENT	DATE	SIGNATURE
_____	_____	_____	_____
_____	_____	_____	_____

06

Implementation Checklist

Twelve items from management's mandate to the next review date.

- ☐ Management has commissioned the work and appointed an information security officer with adequate resources (BSI Standard 200-2, chapter 3.4; ISMS.1.A4).
- ☐ If the role cannot be filled internally, an external information security officer has been engaged; the contract governs tasks, rights, obligations, confidentiality, and the handover at the end (ISMS.1.A5; BSI Standard 200-2, chapter 4.11).
- ☐ IT operations, business units, data protection, HR, and employee representatives have contributed to the draft (BSI Standard 200-2, chapter 3.4.1).
- ☐ The scope fully covers the business processes under consideration (BSI Standard 200-2, chapter 3.4.3).
- ☐ All placeholders are replaced; the objectives are derived from business objectives, laws, customer contracts, and threats (BSI Standard 200-1, chapter 7.1).
- ☐ NIS2 entities: the risk analysis takes technological, human, supply chain, and location-related risks into account (§ 3 NISV 2026); compensating measures are documented with reasons (§ 4).
- ☐ The information security officer reports directly to management, has a deputy, and is not also an active administrator (ISMS.1.A4, ISMS.1.A6; BSI Standard 200-2, chapter 4.4).
- ☐ Management has given formal written approval, and the approval date is in the document (BSI Standard 200-2, chapter 3.4.4; Annex point 1.1.1(k) IR 2024/2690).
- ☐ The policy has been communicated to everyone and is easily accessible; it is explained to new employees before their first IT access (BSI Standard 200-2, chapter 3.4.4).

- ☐ The basic rules are confirmed in writing; everyone knows the contact person and the reporting channel for incidents (ORP.1.A15, ORP.1.A16, DER.2.1.A3).
- ☐ Training for management and employees is scheduled (ORP.3.A4; for NIS2 entities § 31 para. 2 NISG 2026).
- ☐ The next review date is set: according to the BSI, after two years at the latest (BSI Standard 200-2, chapter 3.4.5), and for NIS2 entities at least annually (Annex point 1.1.2 IR 2024/2690).

This checklist is a TOMORIS recommendation based on BSI Standard 200-2. For essential and important entities, §§ 31 and 32 NISG 2026 and the requirements of Implementing Regulation (EU) 2024/2690, which § 2 NISV 2026 declares applicable, are mandatory by law.

07

Common Mistakes

What makes policies ineffective in practice, and what the BSI and the EU regulation require instead.

- Too long and too technical: according to the BSI, more than 20 pages has not proven effective (BSI Standard 200-2, chapter 3.4.3). Specific measures belong in the security concept (ISMS.1.A10).
- An active administrator as information security officer, or the role in the IT department: the BSI advises against this because of the risk of role and interest conflicts (BSI Standard 200-2, chapter 4.4).
- Signed but not communicated: all employees should know the content, new employees before their first IT access (BSI Standard 200-2, chapter 3.4.4).
- No deputy: there must be effective deputy arrangements for all important functions of the security organization (ISMS.1.A6).
- No resources: resources must be planned so that the agreed security level can actually be achieved (BSI Standard 200-1, chapter 7.2).
- Adopted once, never reviewed: NIS2 entities must review at least annually and document the result (Annex point 1.1.2 IR 2024/2690).
- Template adopted unchanged: objectives with no connection to your own company do not meet ISMS.1.A3, because the policy must explain how the security objectives relate to the business objectives.

The policy is followed by the security concept: it derives specific measures from the security objectives, protection requirements, and risk assessment (ISMS.1.A10). Plan it together with the policy.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 applicability check (German)

tomoris.com/tools/nis2-check

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

08

Sources

All statements are supported by sources. Legislation applies in its current version.

- NISG 2026, BGBl. I No. 94/2025, current version in the RIS**
§ 3 no. 11, §§ 24 to 26, 31, 32, § 45 para. 1 to 3, § 51 para. 2; version as of October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=105061000
- NISV 2026, BGBl. II No. 290/2026, authentic promulgation in the RIS**
§§ 2, 3, 4, and 9, promulgated on October 1, 2026, accessed October 25, 2026
www.ris.bka.gv.at/eli/bgbli/II/2026/290
- Implementing Regulation (EU) 2024/2690, Annex no. 1 Policy on the security of network and information systems**
Annex points 1.1 and 1.2; OJ L of October 18, 2024
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- Directive (EU) 2022/2555 (NIS2 Directive), Art. 20 governance and Art. 21**
Art. 20(1), Art. 21(2)(a); OJ L 333 of December 27, 2022
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- BSI Standard 200-1: Information Security Management Systems (ISMS)**
Chapters 3.1, 7.1, and 7.2; version 1.0, October 2017
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschrift/BSI_Sta...
- BSI Standard 200-2: IT-Grundschrift Methodology**
Chapter 3.4 creating a policy, 4.4 information security officers, 4.11 external security experts
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschrift/BSI_Sta...
- BSI IT-Grundschrift Compendium, 2023 edition**
ISMS.1, ORP.1 to ORP.5, CON.3, OPS.1.1.3, DER.2.1, APP.5.3, SYS.2.1, SYS.3.2.1, INF.7, INF.9; accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschrift/IT-GS-K...