

VORLAGE · TOMORIS TOOLBOX

IT-Sicherheitsrichtlinie: Vorlage für kleine und mittlere Unternehmen

Mustertext für die Leitlinie zur Informationssicherheit und Grundregeln für alle Mitarbeitenden, mit Fundstellen in BSI IT-Grundschutz, NISG 2026 und NISV 2026

STAND

25.10.2026

UMFANG

PDF, 10 Seiten

ONLINE

tomoris.com/downloads/it-sicherheitsrichtlinie-vorlage

AUF EINEN BLICK

2 Teile

Leitlinie und Grundregeln für alle Mitarbeitenden

8

Grundregeln vom Passwort bis zur Vorfallsmeldung

1× im Jahr

Überprüfung durch die Leitung bei NIS2-Einrichtungen

§ 31

NISG 2026: Leitung stellt Risikomanagement sicher

FÜR WEN

- Geschäftsführung und Leitungsorgane kleiner und mittlerer Unternehmen
- Informationssicherheitsbeauftragte und IT-Leitung, die eine Leitlinie erstellen oder überarbeiten
- Unternehmen, die als wesentliche oder wichtige Einrichtung unter das NISG 2026 fallen oder sich darauf vorbereiten

WURUM ES GEHT

Eine IT-Sicherheitsrichtlinie, beim BSI Leitlinie zur Informationssicherheit genannt, hält fest, warum ein Unternehmen Informationen schützt, welche Ziele es verfolgt und wer wofür verantwortlich ist. Diese Vorlage enthält einen Mustertext mit Platzhaltern, Grundregeln für alle Mitarbeitenden und eine Checkliste zur Einführung. Sie zeigt, welche Inhalte BSI-Standard 200-2 und der IT-Grundschutz-Baustein ISMS.1 verlangen und was seit Oktober 2026 für wesentliche und wichtige Einrichtungen nach NISG 2026 und NISV 2026 gilt.

Diese Vorlage ist an Ihr Unternehmen anzupassen und ersetzt keine Rechtsberatung. Maßgeblich sind NISG 2026, NISV 2026 und die Durchführungsverordnung (EU) 2024/2690 in der jeweils geltenden Fassung. Klären Sie arbeitsrechtliche Fragen, etwa zum Umgang mit Verstößen, mit Ihrer Rechtsberatung.

INHALT

01	Was eine IT-Sicherheitsrichtlinie regelt	2
02	Was hineingehört: BSI und EU-Verordnung	3
03	Was das NISG 2026 von der Leitung verlangt	4
04	Mustertext Teil A: Leitlinie zur Informationssicherheit	5
05	Mustertext Teil B: Grundregeln für alle Mitarbeitenden	7
06	Checkliste zur Einführung	8
07	Häufige Fehler	9
08	Quellen	10

01

Was eine IT-Sicherheitsrichtlinie regelt

Das oberste Dokument der Informationssicherheit: Begriffe bei BSI und EU und der Aufbau dieser Vorlage.

Die IT-Sicherheitsrichtlinie ist das oberste Dokument der Informationssicherheit. Das BSI nennt sie Leitlinie zur Informationssicherheit, englisch Information Security Policy (BSI-Standard 200-1, Kapitel 7.1); die Durchführungsverordnung (EU) 2024/2690 spricht vom Konzept für die Sicherheit von Netz- und Informationssystemen (Anhang Nr. 1.1). Sie beschreibt allgemein verständlich, für welche Zwecke, mit welchen Mitteln und Strukturen Informationssicherheit hergestellt werden soll, und enthält Sicherheitsziele und Strategie (BSI-Standard 200-2, Kapitel 3.4). Sie ist das sichtbare Bekenntnis der Leitung zu ihrer Strategie (BSI-Standard 200-1, Kapitel 3.1).

Aufbau dieser Vorlage: Teil A ist die Leitlinie, die die Geschäftsführung genehmigt. Teil B enthält Grundregeln für alle Mitarbeitenden, wie sie das BSI für eine Richtlinie zur sicheren IT-Nutzung vorsieht: Ziele, Rollen, Ansprechperson und einzuhaltende Maßnahmen (ORP.1.A16). Die Trennung empfiehlt TOMORIS, damit die Leitlinie kurz bleibt und die Grundregeln sich leichter anpassen lassen.

02

Was hineingehört: BSI und EU-Verordnung

Inhalte nach BSI-Standard 200-2 und ISMS.1.A3 neben den Pflichtinhalten aus Anhang Nr. 1.1 der DVO (EU) 2024/2690.

Mindestinhalte nennen BSI-Standard 200-2 (Kapitel 3.4.3) und die Anforderung ISMS.1.A3 des IT-Grundschutz-Kompendiums. Für wesentliche und wichtige Einrichtungen verbindlich sind die Inhalte nach Anhang Nr. 1.1.1 lit. a bis k der Durchführungsverordnung (EU) 2024/2690. Sie konkretisiert Art. 21 Abs. 2 lit. a der NIS-2-Richtlinie und gilt für Anbieter wie Cloud- und verwaltete Dienste unmittelbar, über § 2 NISV 2026 für alle übrigen wesentlichen und wichtigen Einrichtungen. Wo das BSI einen Inhalt nicht für die Leitlinie selbst verlangt, nennt die Tabelle die verwandte Anforderung in Klammern.

Inhalte der Leitlinie mit Fundstelle bei BSI und in Anhang Nr. 1 der DVO (EU) 2024/2690

INHALT	BSI	DVO 2024/2690
Geltungsbereich	ISMS.1.A3; 200-2, Kap. 3.4.3	in Nr. 1.1.1 nicht genannt
Stellenwert der Informationssicherheit, Ansatz des Sicherheitsmanagements	ISMS.1.A3; 200-2, Kap. 3.4.3	Nr. 1.1.1 lit. a
Sicherheitsziele mit Bezug zu Geschäftszielen und Strategie	ISMS.1.A3	Nr. 1.1.1 lit. b, c
Zusage der Leitung zu Durchsetzung und Ressourcen	Durchsetzung: 200-2, Kap. 3.4.3 (Ressourcen: ISMS.1.A1)	Ressourcen: Nr. 1.1.1 lit. e
Rollen, Verantwortlichkeiten, Organisationsstruktur	ISMS.1.A3	Nr. 1.1.1 lit. g, Nr. 1.2
Liste der themenspezifischen Regelungen	nicht verlangt (zielgruppengerechte Richtlinien: ISMS.1.A16)	Nr. 1.1.1 lit. i
Verbesserung, Erfolgskontrolle, Kennzahlen	Erfolgskontrolle: 200-2, Kap. 3.4.3; Verbesserung: ISMS.1.A11	Nr. 1.1.1 lit. d, j
Aufzubewahrende Unterlagen und Dauer	nicht verlangt (Dokumentation: ISMS.1.A13)	Nr. 1.1.1 lit. h
Bekanntgabe an Mitarbeitende und externe Beteiligte	ISMS.1.A3	Nr. 1.1.1 lit. f, mit Anerkennung
Genehmigung durch die Leitung, mit Datum	schriftlich, formell zugestimmt: 200-2, Kap. 3.4.4	Nr. 1.1.1 lit. k

Überprüfung

200-2, Kap. 3.4.5: spätestens alle zwei Jahre

Nr. 1.1.2: mindestens jährlich und anlassbezogen

03

Was das NISG 2026 von der Leitung verlangt

§ 31 Governance, § 32 Risikomanagement und die NISV 2026: was seit Oktober 2026 für wesentliche und wichtige Einrichtungen gilt.

Für wesentliche und wichtige Einrichtungen gilt seit 1. Oktober 2026 das NISG 2026 (BGBl. I Nr. 94/2025, § 51 Abs. 2). Ihre Leitungsorgane, also die nach Gesetz, Satzung oder Vertrag zur Führung der Geschäfte berufenen Personen oder Organe (§ 3 Z 11), haben die Einhaltung der Risikomanagementmaßnahmen nach § 32 sicherzustellen und zu beaufsichtigen (§ 31 Abs. 1). Sie müssen an für sie gestalteten Cybersicherheits-schulungen teilnehmen; den Mitarbeitern sind regelmäßig entsprechende Schulungen anzubieten (§ 31 Abs. 2). Zu den Mindestinhalten des Risikomanagements zählen Konzepte für Risikoanalyse und Sicherheit der Informationssysteme (§ 32 Abs. 4 lit. a).

Am 1. Oktober 2026 wurde die NISV 2026 kundgemacht (BGBl. II Nr. 290/2026); sie trat mit Ablauf dieses Tages in Kraft (§ 9). Ihr § 2 erklärt die Anforderungen der Durchführungsverordnung (EU) 2024/2690 samt Anhang auch für die übrigen Arten wesentlicher und wichtiger Einrichtungen der Anlagen 1 und 2 NISG 2026 für anwendbar. Für die Leitlinie heißt das: Inhalte nach Anhang Nr. 1.1.1, Datum der förmlichen Genehmigung durch die Leitungsorgane (lit. k), Überprüfung durch sie mindestens jährlich und nach erheblichen Vorfällen oder wesentlichen Änderungen mit dokumentiertem Ergebnis (Nr. 1.1.2), dazu mindestens eine Person, die den Leitungsorganen direkt verantwortlich ist (Nr. 1.2.3).

Kann eine Einrichtung einzelne Anforderungen vorübergehend oder wegen ihrer Größe nicht erfüllen, setzt sie kompensierende Maßnahmen um, dokumentiert sie begründet und prüft ihre Wirksamkeit mindestens jährlich; ausgenommen sind Anforderungen, die nur soweit angemessen, anwendbar oder durchführbar gelten (§ 4 NISV 2026). Wer die Schulungspflichten verletzt, begeht eine Verwaltungsübertretung; ebenso, wer Risikomanagementmaßnahmen nicht umsetzt, sofern die Behörde davon nicht nur durch die Selbstdeklaration erfahren hat (§ 45 Abs. 1 Z 1 bis 3). Der Strafraum beträgt bis zu 10 Mio. Euro oder 2 % des weltweiten Vorjahresumsatzes für wesentliche, bis zu 7 Mio. Euro oder 1,4 % für wichtige Einrichtungen, jeweils der höhere Betrag (§ 45 Abs. 2 und 3).

Die NIS-2-Richtlinie verlangt, dass Leitungsorgane die Maßnahmen billigen, ihre Umsetzung überwachen und verantwortlich gemacht werden können (Art. 20 Abs. 1); in Österreich maßgeblich ist der Wortlaut von § 31 NISG 2026. Ob Ihr Unternehmen betroffen ist, regeln §§ 24 bis 26 samt Anlagen 1 und 2. Für alle anderen sind die Inhalte dieser Vorlage Empfehlungen nach BSI.

04 —

Mustertext Teil A: Leitlinie zur Informationssicherheit

Acht Abschnitte mit Platzhaltern in eckigen Klammern, dazu Rollen und Unterschriftenfeld der Geschäftsführung.

Ersetzen Sie jeden Platzhalter in eckigen Klammern, streichen Sie, was nicht zutrifft, und leiten Sie die Ziele aus Ihren Geschäftszielen und Ihrer Risikoanalyse ab. Die acht Abschnitte decken alle Zeilen der Tabelle in Abschnitt 2 ab; NIS2-Einrichtungen streichen dort nichts ohne Prüfung.

1 Zweck und Geltungsbereich

Diese Leitlinie legt fest, warum und wie [Unternehmen] Informationen schützt. Sie gilt für [das gesamte Unternehmen | Standorte, Bereiche], für Geschäftsführung, Führungskräfte und alle Mitarbeitenden, für externe Personen, die für [Unternehmen] tätig sind, und für Informationen in jeder Form: auf Papier, in IT-Systemen, in Cloud-Diensten und auf mobilen Geräten.

2 Stellenwert und Sicherheitsziele

Unsere wichtigsten Geschäftsprozesse sind [z. B. Auftragsabwicklung, Produktion]; sie hängen ab von [z. B. ERP-System, E-Mail]. Ein Ausfall oder Abfluss dieser Informationen gefährdet [z. B. Lieferfähigkeit, Kundenvertrauen]. Wir schützen deshalb Vertraulichkeit, Integrität und Verfügbarkeit, wie es dem Risiko angemessen ist. Unsere Ziele: [z. B. Kundendaten sind nur Berechtigten zugänglich; die Auftragsabwicklung läuft nach einem Ausfall binnen [Stunden] wieder; gesetzliche und vertragliche Pflichten werden eingehalten].

3 Verantwortung der Geschäftsführung

Die Geschäftsführung trägt die Gesamtverantwortung für die Informationssicherheit. Sie genehmigt diese Leitlinie, setzt sie durch, lebt die Regeln vor und stellt Personal, Budget, Verfahren und Technik bereit. Sie lässt sich mindestens [halbjährlich] über Stand, Risiken und Vorfälle berichten und entscheidet über den Umgang mit Restrisiken.

4 Rollen und Organisation

Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter (ISB) ist [Name, Funktion], Vertretung [Name, Funktion]. Die oder der ISB koordiniert die Informationssicherheit, berät die Geschäftsführung, berichtet ihr direkt und wird bei größeren Projekten und neuen IT-Systemen frühzeitig beteiligt. Weitere Rollen nennt die Tabelle unten; die Geschäftsführung überprüft sie [jährlich] und nach erheblichen Vorfällen oder Änderungen.

5 Regelungen und Schulung

Das Sicherheitskonzept legt auf Grundlage einer Risikoanalyse die Maßnahmen fest. Für einzelne Themen gelten eigene, mit dieser Leitlinie vereinbare Regelungen: [z. B. Grundregeln (Teil B), Zugriffskontrolle, Datensicherung, Sicherheitsvorfälle, Lieferanten], freigegeben von [Funktion]. Alle Mitarbeitenden werden vor der ersten IT-Nutzung eingewiesen und mindestens [jährlich] geschult, die Geschäftsführung in eigens für sie gestalteten Schulungen.

6

Verstöße und Ausnahmen

Verstöße können [Unternehmen], Kunden und Partnern schaden; die Mitarbeitenden werden über mögliche Konsequenzen aufgeklärt. Wie ein Verstoß behandelt wird, entscheidet [Funktion] im Einzelfall nach Arbeitsvertrag, [Betriebsvereinbarung] und geltendem Recht. Ausnahmen von Regeln sind nur begründet, befristet und nach Genehmigung durch [Funktion] zulässig; [ISB] führt darüber eine Übersicht.

7

Überprüfung, Kennzahlen und Dokumentation

Wir verbessern die Informationssicherheit fortlaufend. Die Geschäftsführung überprüft diese Leitlinie mindestens [jährlich] und nach erheblichen Vorfällen oder wesentlichen Änderungen und dokumentiert das Ergebnis. Den Fortschritt messen wir an [Kennzahlen, z. B. Schulungsquote, Zeit bis zur Installation kritischer Updates]. [ISB] bewahrt [Unterlagen, z. B. Risikoanalyse, Berichte, Schulungsnachweise, Vorfallsprotokolle] [Dauer] auf.

8

Inkraftsetzung

Die Geschäftsführung hat diese Leitlinie am [Datum] genehmigt. Sie tritt am [Datum] in Kraft, ersetzt [frühere Fassung | keine] und wird allen Mitarbeitenden sowie den betroffenen externen Partnern bekannt gegeben, die ihre Kenntnis bestätigen. Nächste Überprüfung spätestens am [Datum].

Rollen in der Informationssicherheit (zu Abschnitt 4)

ROLLE	AUFGABEN	WER
Geschäftsführung	Gesamtverantwortung, Ressourcen, regelmäßige Berichte (ISMS.1.A1, ISMS.1.A12)	_____
ISB	koordiniert, berät die Leitung, berichtet direkt, untersucht Vorfälle, koordiniert Schulungen (ISMS.1.A4; 200-2, Kap. 4.4)	_____
Vertretung ISB	übernimmt bei Abwesenheit, ebenso qualifiziert (ISMS.1.A6; 200-2, Kap. 4.4)	_____
IT-Betrieb	setzt technische Maßnahmen um, etwa Updates und Berechtigungen (OPS.1.1.3.A15, ORP.4.A2); möglichst nicht zugleich ISB (200-2, Kap. 4.4)	_____
Führungskräfte	gehen mit gutem Beispiel voran und weisen auf die Regeln hin (ORP.3.A1)	alle
Mitarbeitende und Externe	Sicherheit am eigenen Arbeitsplatz (200-1, Kap. 7.2); Dritte wenden die Regeln an (DVO 2024/2690, Anhang Nr. 1.2.2)	alle

Genehmigung (zu Abschnitt 8)

FUNKTION	NAME	DATUM	UNTERSCHRIFT
Geschäftsführung	_____	_____	_____
ISB, zur Kenntnis	_____	_____	_____

Fundstellen zum Mustertext: Abschnitt 3 nach ISMS.1.A1 und ISMS.1.A12. Abschnitt 4 nach ISMS.1.A4, ISMS.1.A6 und Anhang Nr. 1.2 DVO 2024/2690. Abschnitt 5 nach ISMS.1.A7 und ORP.3.A3. Abschnitt 6 nach ISMS.1.A8 und ORP.5.A5. Abschnitt 7 nach ISMS.1.A11, ISMS.1.A13 und Anhang Nr. 1.1.1 lit. d, h, j sowie Nr. 1.1.2. Abschnitt 8 nach BSI-Standard 200-2, Kapitel 3.4.4, und Anhang Nr. 1.1.1 lit. f, k.

05

Mustertext Teil B: Grundregeln für alle Mitarbeitenden

Acht Regeln für den Arbeitsalltag mit Platzhaltern, dazu die schriftliche Bestätigung der Kenntnisnahme.

Grundregeln zur sicheren IT-Nutzung bei [Unternehmen]

1. Konten, Passwörter, MFA

Ihr Konto ist persönlich: Geben Sie Zugangsdaten nie weiter, auch nicht an angebliche IT-Mitarbeitende. Nutzen Sie für jedes System ein eigenes, schwer zu erratendes Passwort aus [Passwort-Manager] und die Multi-Faktor-Authentifizierung für [E-Mail, Fernzugriff, Cloud-Dienste]. Bei Verdacht ändern Sie das Passwort sofort und melden es. Grundlage: ORP.4.A8; § 32 Abs. 4 lit. j NISG 2026.

2. Updates

Installieren Sie angebotene Updates und starten Sie neu, wenn Sie dazu aufgefordert werden; verschieben Sie höchstens [Frist]. Automatische Updates bleiben eingeschaltet. Software ohne Herstellerunterstützung nutzen Sie nur nach Freigabe durch [IT-Abteilung]. Grundlage: SYS.2.1.A3, OPS.1.1.3.A15.

3. E-Mail und Phishing

Absender lassen sich fälschen. Öffnen Sie keine unerwarteten Anhänge, antworten Sie nicht auf verdächtige Nachrichten und folgen Sie deren Links nicht. Melden Sie sie über [Meldeknopf | Adresse] und löschen Sie sie danach. Haben Sie schon geklickt oder Daten eingegeben, melden Sie das sofort. Grundlage: APP.5.3.A7, APP.5.3.A8.

4. Daten ablegen

Speichern Sie dienstliche Daten nur an den freigegebenen Orten: [z. B. Fileserver, SharePoint]. [Private Cloud-Dienste und private E-Mail-Konten sind dafür nicht erlaubt.] Schließen Sie nur freigegebene USB-Speicher an und bewahren Sie vertrauliche Unterlagen verschlossen auf. Grundlage: CON.3.A5, APP.5.3.A6, SYS.2.1.A24, INF.7.A7.

5. Geräte und Arbeitsplatz

Sperren Sie Bildschirm oder Gerät, sobald Sie den Platz verlassen; Smartphones und Tablets schützen Sie mit einem Sperrcode. Schalten Sie Schutzprogramme nicht ab. Lassen Sie keine vertraulichen Unterlagen offen liegen. Grundlage: SYS.2.1.A1, SYS.3.2.1.A4, SYS.2.1.A6, INF.7.A6.

6. Mobiles Arbeiten

Unterwegs und zu Hause bearbeiten Sie nur freigegebene Informationen: [Regel]. Lassen Sie Geräte und Unterlagen nie unbeaufsichtigt, nutzen Sie unterwegs einen Sichtschutz und bearbeiten Sie keine dienstlichen Daten auf fremden Geräten. Auf interne Systeme greifen Sie nur über [VPN | freigegebenen Zugang] zu. Grundlage: INF.9.A2, INF.9.A3, INF.9.A4, INF.9.A12.

7. Vorfälle melden

Melden Sie sofort an [Meldestelle, Telefon, E-Mail], außerhalb der Arbeitszeit an [Notfallnummer]: verdächtige Nachrichten oder Anrufe, auffällige Geräte, eigene Fehler sowie verlorene oder gestohlene Geräte und Unterlagen. Auch ein bloßer Verdacht zählt. Grundlage: DER.2.1.A3, DER.2.1.A9, INF.9.A5, SYS.3.2.1.A7.

8. Vertraulichkeit

Dienstliche Informationen sind für den internen Gebrauch bestimmt, auch nach Dienstschluss und außerhalb des Unternehmens. Geben Sie sie nur an Berechtigte weiter. Beim Austritt geben Sie Unterlagen, Schlüssel, Geräte und Ausweise zurück. Grundlage: ORP.2.A14, ORP.2.A2.

Bestätigung: Ich habe die Grundregeln gelesen und halte sie ein. Fragen richte ich an [Ansprechperson, Kontakt]. Neue Mitarbeitende bestätigen vor der ersten IT-Nutzung, alle Benutzenden regelmäßig oder nach größeren Änderungen erneut (ORP.1.A16). Die Angaben „Grundlage“ können in Ihrer Fassung entfallen.

Bestätigung der Kenntnisnahme

NAME	ABTEILUNG	DATUM	UNTERSCHRIFT
_____	_____	_____	_____
_____	_____	_____	_____

06

Checkliste zur Einführung

Zwölf Punkte vom Auftrag der Geschäftsführung bis zum nächsten Überprüfungstermin.

- ☐ Die Geschäftsführung hat die Erarbeitung beauftragt und eine oder einen ISB mit angemessenen Ressourcen benannt (BSI-Standard 200-2, Kapitel 3.4; ISMS.1.A4).
- ☐ Ist die Rolle intern nicht zu besetzen, ist eine externe ISB beauftragt; der Vertrag regelt Aufgaben, Rechte, Pflichten, Vertraulichkeit und die Übergabe am Ende (ISMS.1.A5; BSI-Standard 200-2, Kapitel 4.11).
- ☐ IT-Betrieb, Fachbereiche, Datenschutz, Personalabteilung und Personalvertretung haben am Entwurf mitgewirkt (BSI-Standard 200-2, Kapitel 3.4.1).
- ☐ Der Geltungsbereich umfasst die betrachteten Geschäftsprozesse vollständig (BSI-Standard 200-2, Kapitel 3.4.3).
- ☐ Alle Platzhalter sind ersetzt; die Ziele leiten sich aus Geschäftszielen, Gesetzen, Kundenverträgen und Bedrohungen ab (BSI-Standard 200-1, Kapitel 7.1).
- ☐ NIS2-Einrichtungen: Die Risikoanalyse berücksichtigt technologische, menschliche, Lieferketten- und standortbezogene Risiken (§ 3 NISV 2026); kompensierende Maßnahmen sind begründet dokumentiert (§ 4).

- ☐ Die oder der ISB berichtet direkt an die Geschäftsführung, hat eine Vertretung und ist nicht zugleich aktiver Administrator (ISMS.1.A4, ISMS.1.A6; BSI-Standard 200-2, Kapitel 4.4).
- ☐ Die Geschäftsführung hat formell und schriftlich zugestimmt, das Genehmigungsdatum steht im Dokument (BSI-Standard 200-2, Kapitel 3.4.4; Anhang Nr. 1.1.1 lit. k DVO 2024/2690).
- ☐ Die Leitlinie ist allen bekannt gegeben und leicht zugänglich; neuen Mitarbeitenden wird sie vor dem ersten IT-Zugang erläutert (BSI-Standard 200-2, Kapitel 3.4.4).
- ☐ Die Grundregeln sind schriftlich bestätigt; Ansprechperson und Meldeweg für Vorfälle sind allen bekannt (ORP.1.A15, ORP.1.A16, DER.2.1.A3).
- ☐ Schulungen für Geschäftsführung und Mitarbeitende sind terminiert (ORP.3.A4; für NIS2-Einrichtungen § 31 Abs. 2 NISG 2026).
- ☐ Der nächste Überprüfungstermin steht fest: laut BSI spätestens nach zwei Jahren (BSI-Standard 200-2, Kapitel 3.4.5), für NIS2-Einrichtungen mindestens jährlich (Anhang Nr. 1.1.2 DVO 2024/2690).

Die Checkliste ist eine Empfehlung von TOMORIS auf Grundlage von BSI-Standard 200-2. Gesetzlich vorgegeben sind für wesentliche und wichtige Einrichtungen §§ 31 und 32 NISG 2026 sowie die Anforderungen der Durchführungsverordnung (EU) 2024/2690, die § 2 NISV 2026 für anwendbar erklärt.

07 —

Häufige Fehler

Was Leitlinien in der Praxis unwirksam macht, und was BSI und EU-Verordnung stattdessen verlangen.

- Zu lang und zu technisch: Mehr als 20 Seiten haben sich laut BSI nicht bewährt (BSI-Standard 200-2, Kapitel 3.4.3). Konkrete Maßnahmen gehören in das Sicherheitskonzept (ISMS.1.A10).
- Ein aktiver Administrator als ISB oder die Rolle in der IT-Abteilung: Das BSI rät davon ab, weil Rollen- und Interessenkonflikte drohen (BSI-Standard 200-2, Kapitel 4.4).
- Unterschrieben, aber nicht bekannt gegeben: Alle Mitarbeitenden sollen die Inhalte kennen, neue vor dem ersten IT-Zugang (BSI-Standard 200-2, Kapitel 3.4.4).
- Keine Vertretung: Für alle wichtigen Funktionen der Sicherheitsorganisation muss es wirksame Vertretungsregelungen geben (ISMS.1.A6).
- Keine Mittel: Die Ressourcen müssen so geplant sein, dass das beschlossene Sicherheitsniveau tatsächlich erreicht werden kann (BSI-Standard 200-1, Kapitel 7.2).
- Einmal beschlossen, nie überprüft: NIS2-Einrichtungen müssen mindestens jährlich überprüfen und das Ergebnis dokumentieren (Anhang Nr. 1.1.2 DVO 2024/2690).
- Vorlage unverändert übernommen: Ziele ohne Bezug zum eigenen Unternehmen erfüllen ISMS.1.A3 nicht, denn die Leitlinie muss den Bezug der Sicherheitsziele zu den Geschäftszielen erläutern.

Auf die Leitlinie folgt das Sicherheitskonzept: Es leitet aus Sicherheitszielen, Schutzbedarf und Risikobewertung konkrete Maßnahmen ab (ISMS.1.A10). Planen Sie es gemeinsam mit der Leitlinie.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck

tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

08

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§ 3 Z 11, §§ 24 bis 26, 31, 32, § 45 Abs. 1 bis 3, § 51 Abs. 2; Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=1051257
- NISV 2026, BGBl. II Nr. 290/2026, authentische Kundmachung im RIS**
§§ 2, 3, 4 und 9, kundgemacht am 1.10.2026, gelesen am 25.10.2026
www.ris.bka.gv.at/eli/bgbli/II/2026/290
- Durchführungsverordnung (EU) 2024/2690, Anhang Nr. 1 Konzept für die Sicherheit von Netz- und Informationssystemen**
Anhang Nr. 1.1 und 1.2; ABL L vom 18.10.2024
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), Art. 20 Governance und Art. 21**
Art. 20 Abs. 1, Art. 21 Abs. 2 lit. a; ABL L 333 vom 27.12.2022
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)**
Kapitel 3.1, 7.1 und 7.2; Version 1.0, Oktober 2017
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Sta...
- BSI IT-Grundschutz-Kompodium, Edition 2023**
ISMS.1, ORP.1 bis 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; gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...