

VORLAGE · TOMORIS TOOLBOX

Security Awareness: Jahresplan für Schulung und Sensibilisierung

Themen je Quartal, Zielgruppen, Formate, Schulung der Leitungsorgane und Nachweis, nach NIST SP 800-50 Rev. 1, BSI ORP.3 und NISG 2026

STAND

25.10.2026

UMFANG

PDF, 8 Seiten

ONLINE

tomoris.com/downloads/security-awareness-jahresplan

AUF EINEN BLICK

§ 31

NISG 2026: Schulungen für Leitung und Mitarbeitende

3

Zielgruppen nach NIST, von allen bis zu Sicherheitsrollen

4

Quartale im Jahresplan zum Ausfüllen

Okt.

Europäischer Monat der Cybersicherheit

FÜR WEN

- Geschäftsführung, die Schulungen freigibt und selbst an Schulungen teilnimmt
- Informationssicherheitsbeauftragte, die das Programm planen und auswerten
- Personalabteilung, die neue Mitarbeitende und Nachweise betreut
- Führungskräfte, die Sicherheitsregeln vorleben und einfordern

WORUM ES GEHT

Ein einzelner Pflichtvortrag im Jahr verändert wenig. Wirksame Sensibilisierung läuft über das ganze Jahr, erreicht jede Zielgruppe mit passenden Inhalten und wird gemessen. Diese Vorlage hilft Ihnen, einen Jahresplan aufzustellen: Zielgruppen festlegen, Themen auf vier Quartale verteilen, Formate wählen, die Schulung der Leitungsorgane einplanen und Teilnahme und Wirksamkeit nachweisen. Sie stützt sich auf NIST SP 800-50 Rev. 1, den Baustein ORP.3 des BSI IT-Grundschutz-Kompendiums und für NIS2-pflichtige Einrichtungen auf § 31 NISG 2026 und Anhang Nr. 8 der DVO (EU) 2024/2690.

Diese Vorlage ist an Ihr Unternehmen, Ihre Risiken und Ihre Werkzeuge anzupassen; Themen, Formate und Rhythmus sind Empfehlungen von TOMORIS. Sie ersetzt keine Rechtsberatung. Für Einrichtungen unter dem NISG 2026 maßgeblich sind der Gesetzestext, die NISV 2026 und die DVO (EU) 2024/2690 in der geltenden Fassung. Stimmen Sie Phishing-Übungen und Auswertungen vorab mit Betriebsrat und Datenschutz ab.

Nutzung: Diese Vorlage dürfen Sie für den eigenen Gebrauch anpassen; weitergeben dürfen Sie sie nur in unveränderter Form.

INHALT

01	Was gefordert ist	2
02	Zielgruppen festlegen	4
03	Formate: sensibilisieren, üben, schulen	4
04	Jahresplan zum Ausfüllen	5
05	Schulung der Leitungsorgane	6
06	Nachweis und Wirksamkeit	7
07	Häufige Fehler	8
08	Quellen	8

01

Was gefordert ist

Pflichten nach NISG 2026 und DVO, Empfehlungen von BSI und NIST

Für wesentliche und wichtige Einrichtungen ist Schulung Pflicht: Die Leitungsorgane müssen an für sie spezifisch gestalteten Cybersicherheitsschulungen teilnehmen, und die Einrichtungen haben den Mitarbeitenden regelmäßig entsprechende Schulungen anzubieten (§ 31 Abs. 2 NISG 2026, Umsetzung von Art. 20 Abs. 2 NIS-2-Richtlinie). Wer das nicht vorsieht, begeht eine Verwaltungsübertretung (§ 45 Abs. 1 Z 1 und 2 NISG 2026); für Stellen der öffentlichen Verwaltung gilt stattdessen § 46. Für alle anderen Unternehmen beschreiben BSI und NIST, wie ein gutes Programm aussieht.

§ 31 Abs. 2 NISG 2026

Leitungsorgane nehmen an spezifisch gestalteten Cybersicherheitsschulungen teil. Die Einrichtung bietet den Mitarbeitenden regelmäßig entsprechende Schulungen an, damit sie Risiken erkennen und bewerten können und Managementpraktiken der Cybersicherheit und deren Auswirkungen auf die Dienste der Einrichtung kennen.

DVO (EU) 2024/2690, Anhang Nr. 8.1

Sensibilisierungsprogramm für Mitarbeitende, Mitglieder der Leitungsorgane und soweit angemessen direkte Anbieter: zeitlich so geplant, dass Maßnahmen wiederholt werden und neue Mitarbeitende erreichen; mit Cyberbedrohungen, bestehenden Maßnahmen, Kontaktstellen und Verfahren der Cyberhygiene. Wirksamkeit soweit angemessen testen, Programm in geplanten Abständen aktualisieren.

DVO (EU) 2024/2690, Anhang Nr. 8.2

Mitarbeitende, deren Rollen sicherheitsrelevante Fähigkeiten erfordern, ermitteln und regelmäßig schulen: sichere Konfiguration und Betrieb einschließlich mobiler Geräte, bekannte Cyberbedrohungen, Verhalten bei sicherheitsrelevanten Ereignissen; Wirksamkeit bewerten, Schulung auch bei Wechsel in eine solche Rolle.

§ 2 NISV 2026

Erklärt den Anhang der DVO auch für die Einrichtungsarten der Anlagen 1 und 2 des NISG 2026 für anwendbar, die die DVO selbst nicht erfasst; Nummer 8 gilt damit für alle wesentlichen und wichtigen Einrichtungen.

BSI IT-Grundschutz, ORP.3

Baustein Sensibilisierung und Schulung zur Informationssicherheit (Edition 2023): Institutionsleitung sensibilisieren und Unterstützung einholen (A1), Personal in den sicheren Umgang mit IT einweisen (A3), zielgruppenorientiertes Programm (A4), Schulung nach Aufgaben (A6), Lernerfolg messen (A8).

Art. 4 KI-Verordnung

Seit der Änderung durch die VO (EU) 2026/1744 ergreifen Anbieter und Betreiber von KI-Systemen Maßnahmen, um die Entwicklung der KI-Kompetenz ihres Personals zu unterstützen; ein bestimmtes Kompetenzniveau müssen sie nicht garantieren.

Die Themen, Formate und der Jahresrhythmus in dieser Vorlage sind Empfehlungen von TOMORIS. Gesetzlich vorgegeben sind für NIS2-pflichtige Einrichtungen die genannten Inhalte von § 31 NISG 2026 und Anhang Nr. 8 der DVO; einen bestimmten Takt in Monaten schreiben sie nicht vor.

02

Zielgruppen festlegen

Wer welche Inhalte braucht, von allen Mitarbeitenden bis zur Leitung

NIST teilt die Teilnehmenden in drei sich überschneidende Gruppen: alle Benutzerinnen und Benutzer, Inhaber privilegierter Konten und Personen mit wesentlichen Aufgaben in Cybersicherheit oder Datenschutz (SP 800-50 Rev. 1, Abschnitt 2.5). Das BSI empfiehlt eine Zielgruppenanalyse und ein darauf ausgerichtetes Programm (Standard-Anforderung ORP.3.A4).

Zielgruppen und Schwerpunkte

ZIELGRUPPE	SCHWERPUNKT	GRUNDLAGE
Alle Mitarbeitenden	Regeln zur Nutzung, Erkennen von Angriffen, Meldeweg, Cyberhygiene; laufend aufgefrischt	§ 31 Abs. 2 NISG 2026; DVO Nr. 8.1; ORP.3.A3; NIST 2.5.1
Leitungsorgane	Für die Leitung gestaltete Schulung zu Pflichten, Risiken und Entscheidungen	§ 31 Abs. 2 NISG 2026; ORP.3.A1
Privilegierte Konten	Zusätzliche Schulung zu Rechten und Risiken administrativer Konten	NIST 2.5.2
Sicherheitsrollen	Rollenbezogene Schulung: sichere Konfiguration, Bedrohungen, Verhalten bei Ereignissen	DVO Nr. 8.2; NIST 2.5.3
Neue Mitarbeitende und Rollenwechsel	Regeln für die Systeme, auf die sie zugreifen werden; Schulung bei neuer Rolle	DVO Nr. 8.1.2 lit. a und 8.2.4; NIST 3.1.2.2
Externe und Anbieter	Einweisung externer Benutzender, soweit angemessen auch direkte Anbieter	ORP.3.A3; DVO Nr. 8.1.2
Besonders exponierte Personen	Vertiefung zu gezielten Angriffen und Vorsichtsmaßnahmen (erhöhter Schutzbedarf)	ORP.3.A9

03

Formate: sensibilisieren, üben, schulen

Die drei Bausteine eines Programms und wie Sie sie mischen

Sensibilisierung	Laufend über das Jahr, als Kampagne oder anlassbezogen, z. B. Hinweise auf dem Anmeldebildschirm, Beiträge im Newsletter, Plakate, Aktionstage im Oktober, kurze E-Mails mit Tipps oder nach einem Vorfall (NIST 2.7.1).
Übung	Praktische Szenarien, die Ereignisse nachstellen: Phishing-, Smishing- oder Vishing-Simulationen, Quiz, Planspiele am Tisch, Übungen zu Notfall und Wiederanlauf (NIST 2.7.2).

Schulung

Vermittelt Wissen und Fertigkeiten, als Präsenz- oder Onlinekurs, Demonstration oder szenariobasierte Übung; rollenbezogen für Personen mit Sicherheitsaufgaben (NIST 2.5.3, 2.7.3).

Phishing-Übungen sind Lerngelegenheiten: NIST empfiehlt, zuerst die Ausgangs-Klickrate je Gruppe zu ermitteln, und betont, dass solche Übungen nicht bestrafen sollen und niemand für seine Reaktion bloßgestellt werden soll (Abschnitt 2.7.2). Klären Sie Simulationen vorab mit Betriebsrat und Datenschutz.

04

Jahresplan zum Ausfüllen

Themen auf vier Quartale verteilt, mit Zielgruppe, Format und Termin

Die Themen sind ein Vorschlag von TOMORIS und decken die Inhalte ab, die Anhang Nr. 8.1.2 lit. c der DVO nennt: Cyberbedrohungen, bestehende Maßnahmen, Kontaktstellen und Verfahren der Cyberhygiene. Passen Sie Reihenfolge und Themen an Ihre Risiken, Vorfälle und Werkzeuge an und tragen Sie Termin und Verantwortliche ein.

Jahresplan [Jahr] für [Unternehmen] (Vorschlag von TOMORIS)

ZEITRAUM	THEMA	ZIELGRUPPE	FORMAT	TERMIN, ZUSTÄNDIG
Q1	Auftakt: Ziele, Regeln, Meldeweg für Vorfälle	alle	Kurzschulung	_____
Q1	Schulung der Leitungsorgane	Leitung	Workshop	_____
Q1	Passwörter, Passwortmanager, MFA	alle	Onlinekurs	_____
Q2	Phishing und Social Engineering	alle	Schulung	_____
Q2	Phishing-Übung mit Auswertung	alle	Simulation	_____
Q2	Umgang mit Daten und Datenschutz	alle	Onlinekurs	_____
Q3	Mobiles Arbeiten, Geräte, Updates	alle	Kurzschulung	_____
Q3	Notfall: Wer tut was?	Leitung, IT	Planspiel	_____
Q3	Administrative Konten sicher nutzen	Admins	Schulung	_____
Q4	Oktober: Aktionen im Cybersicherheitsmonat	alle	Kampagne	_____
Q4	KI-Werkzeuge sicher nutzen	alle	Schulung	_____
Q4	Auswertung und Plan für das Folgejahr	ISB, Leitung	Besprechung	_____
laufend	Einweisung neuer Mitarbeitender	Neue	Einweisung	_____
laufend	Warnhinweise zu aktuellen Angriffen	alle	E-Mail	_____

Im Oktober läuft der Europäische Monat der Cybersicherheit, eine jährliche Kampagne der EU, die ENISA gemeinsam mit der Europäischen Kommission unterstützt. Eigene Aktionen in diesem Monat verbinden sich gut mit öffentlichem Material.

05

Schulung der Leitungsorgane

Was eine für die Leitung gestaltete Schulung abdecken sollte

Die Leitungsorgane wesentlicher und wichtiger Einrichtungen haben die Einhaltung der Risikomanagementmaßnahmen sicherzustellen und zu beaufsichtigen (§ 31 Abs. 1 NISG 2026). Die Schulung nach § 31 Abs. 2 sollte sie dazu befähigen. Auch das BSI verlangt, die Institutionsleitung ausreichend zu sensibilisieren und ihre Unterstützung einzuholen, bevor ein Programm beginnt (ORP.3.A1). Inhalte, Empfehlung von TOMORIS:

- ☐ Pflichten der Leitung: sicherstellen und beaufsichtigen (§ 31 Abs. 1), selbst an Schulungen teilnehmen (§ 31 Abs. 2).
- ☐ Die Mindestinhalte der Risikomanagementmaßnahmen nach § 32 Abs. 4 lit. a bis j NISG 2026 im Überblick, von Risikoanalyse bis Multi-Faktor-Authentifizierung.
- ☐ Meldepflichten bei erheblichen Vorfällen: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht spätestens einen Monat danach (§ 34 Abs. 2 NISG 2026).
- ☐ Selbstdeklaration und Nachweis der Maßnahmen gegenüber der Cybersicherheitsbehörde (§ 33 NISG 2026).
- ☐ Strafraumen: für wesentliche Einrichtungen bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes, für wichtige bis 7 Mio. Euro oder 1,4 %, je nachdem, welcher Betrag höher ist (§ 45 Abs. 2 und 3 NISG 2026); für Stellen der öffentlichen Verwaltung Feststellungsbescheid statt Geldstrafe (§ 46).
- ☐ Die aktuelle Bedrohungslage und die Risiken des eigenen Unternehmens (DVO Nr. 8.1.3).
- ☐ Die eigene Rolle im Notfall: Entscheidungen, Erreichbarkeit, Kommunikation.
- ☐ Vorbildwirkung: Führungskräfte setzen Sicherheitsvorgaben um und weisen ihre Mitarbeitenden auf die Einhaltung hin (ORP.3.A1).

06 —

Nachweis und Wirksamkeit

Teilnahme belegen, Lernerfolg messen, Programm verbessern

Teilnahmezahlen allein genügen nicht: NIST verlangt, über die bloße Erfüllung von Vorgaben hinaus auch Wirkung auf Fähigkeiten, Haltung und Verhalten zu messen (Abschnitt 2.4.1). Das BSI empfiehlt, den Lernerfolg zielgruppenbezogen quantitativ und qualitativ zu messen und die Ergebnisse in das Angebot einfließen zu lassen (ORP.3.A8).

- ☐ Teilnahme je Person dokumentiert: Datum, Thema, Format, Dauer, Bestätigung.
- ☐ Unterlagen jeder Schulung mit Stand archiviert, damit nachvollziehbar ist, was vermittelt wurde.
- ☐ Neue Mitarbeitende vor dem ersten Zugriff eingewiesen und das dokumentiert (Empfehlung von TOMORIS, vgl. NIST 3.1.2.2; das Programm muss neue Mitarbeitende erreichen, DVO Nr. 8.1.2 lit. a).
- ☐ Wirksamkeit gemessen, z. B. Quiz mit Bestehensgrenze, praktische Prüfung, Klickrate bei Phishing-Übungen (NIST 2.7.2 und 3.2, ORP.3.A8).
- ☐ Ergebnisse mit Personalabteilung und Datenschutz besprochen (ORP.3.A8).
- ☐ Programm in geplanten Abständen aktualisiert (DVO Nr. 8.1.3, 8.2.5; ORP.3.A4), zusätzlich nach Vorfällen (NIST 2.5.1).
- ☐ Für NIS2-pflichtige Einrichtungen: Nachweis über die Schulung der Leitungsorgane griffbereit.

Teilnahmenachweis (Muster)

DATUM	THEMA	NAME	FORMAT, DAUER	BESTÄTIGUNG
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

07 —

Häufige Fehler

Woran Awareness-Programme in der Praxis scheitern

- Nur ein Pflichttermin im Jahr. NIST beschreibt Sensibilisierung als laufende Aktivität über das ganze Jahr (Abschnitt 2.7.1).
- Die Leitung fehlt. Ohne ihre Unterstützung soll ein Programm laut BSI gar nicht beginnen (ORP.3.A1); NIS2-pflichtige Leitungsorgane müssen selbst teilnehmen.
- Alle bekommen dasselbe. Administratoren und Sicherheitsrollen brauchen zusätzliche, rollenbezogene Schulung (NIST 2.5.2, 2.5.3; DVO Nr. 8.2).
- Phishing-Übungen werden zum Pranger. NIST rät ausdrücklich zu einem Ansatz ohne Strafe und ohne Bloßstellung (Abschnitt 2.7.2).
- Gemessen wird nur die Teilnahmequote, nicht die Wirkung auf das Verhalten (NIST 2.4.1, ORP.3.A8).
- Neue Mitarbeitende und Externe werden vergessen (DVO Nr. 8.1.2, ORP.3.A3).

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

Link-Prüfer

tomoris.com/tools/link-check

E-Mail-Header-Analyse

tomoris.com/tools/mail-header-analyse

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

08 —

Quellen

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

- 1 NIST SP 800-50 Rev. 1: Building a Cybersecurity and Privacy Learning Program (September 2024)
Abschnitte 2.4.1, 2.5, 2.7, 3.1 und 3.2, gelesen am 25.10.2026
doi.org/10.6028/NIST.SP.800-50r1
- 2 BSI IT-Grundschutz-Kompendium, Baustein ORP.3 Sensibilisierung und Schulung zur Informationssicherheit (Edition 2023)
Anforderungen A1, A3, A4, A6, A8, A9, gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 3 NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS
§§ 31 bis 34, 45 und 46, gelesen am 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 4 NISV 2026, BGBl. II Nr. 290/2026
§ 2 Anwendbarkeit der DVO, gelesen am 25.10.2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 5 Durchführungsverordnung (EU) 2024/2690, deutsche Fassung auf EUR-Lex
Anhang Nr. 8.1 und 8.2, gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu
- 6 Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), deutsche Fassung auf EUR-Lex
Art. 20 Abs. 2, gelesen am 25.10.2026
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- 7 Verordnung (EU) 2026/1744 (Digital-Omnibus-Verordnung zur KI), ABL. L vom 24.7.2026
Art. 1 Nr. 5, neue Fassung von Art. 4 KI-VO, gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg/2026/1744/oj/deu
- 8 ENISA: European Cybersecurity Month
Beschreibung der Kampagne, gelesen am 25.10.2026
www.enisa.europa.eu/topics/cyber-hygiene/european-cybersecurity...