SECURITY QUESTIONNAIRE

Antwortmuster für Security-Fragebögen von Primes und Beschaffern.

Die Vorlage folgt der Struktur von ISO 27001 Anhang A. Sie umfasst zehn Kernbereiche und liefert Referenzantworten, die als Ausgangspunkt für die Bearbeitung individueller Fragebögen dienen. Die Antworten sind sachlich, ohne Auftragsspezifika.

STRUKTUR	UMFANG	BAUSTEIN	STAND
ISO 27001 Anhang A	10 Bereiche	04 von 06	1 / 2026

Auftraggeber im wehrtechnischen und im behördlichen Kontext versenden typischerweise mehrseitige Security Questionnaires, bevor eine tiefere Zusammenarbeit beginnt. Diese Fragebögen unterscheiden sich in Länge und Detailtiefe, folgen aber in den Bereichen einer wiederkehrenden Struktur.

Die folgenden zehn Bereiche entsprechen den zentralen Domänen von ISO 27001 Anhang A und decken die Prüf-Themen ab, die in den meisten Fragebögen vorkommen. Zu jedem Bereich formulieren wir eine Referenzantwort, wie new direction sie in einem Erstkontakt liefert.

A.5

Informationssicherheitsrichtlinien

Verfügt Ihr Unternehmen über eine dokumentierte Informationssicherheits-Richtlinie? Wer verantwortet sie? Wann wurde sie zuletzt überarbeitet?

REFERENZANTWORT

Ja. Verabschiedet und regelmäßig überprüft durch die Geschäftsführung, letzte Überarbeitung im Rahmen der TISAX-Auditierung 2025. Kernrichtlinie ergänzt durch spezifische Verfahrensanweisungen für Entwicklung, Zugriff und Vorfallsmanagement.

A.6

Organisation der Informationssicherheit

Wer trägt die operative Verantwortung für Informationssicherheit? Wie sind Rollen und Trennung von Aufgaben geregelt?

REFERENZANTWORT

Benannter Informationssicherheitsbeauftragter mit direkter Berichtslinie an die Geschäftsführung. Trennung von operativen und prüfenden Rollen. Externe Auditbegleitung durch TISAX-akkreditierten Prüfdienstleister.

A.7

Personalsicherheit

Wie werden Beschäftigte und externe Kräfte vor Aufnahme der Tätigkeit geprüft? Wie erfolgt Onboarding und Offboarding hinsichtlich Zugängen und Verpflichtungen?

REFERENZANTWORT

Führungs- und polizeiliche Führungszeugnisse für sicherheitsrelevante Rollen. Sicherheitsüberprüfungen für Personal in klassifizierten Mandaten. Achtstündiges Sicherheits-Onboarding für alle neuen Kräfte. Automatisierte Offboarding-Prozedur mit Zugangswiderruf am Tag des Ausscheidens.

A.8

Asset-Management

Wie werden Informationswerte identifiziert, klassifiziert und dem Verantwortlichen zugeordnet? Wie werden Klassifizierungsstufen technisch umgesetzt?

REFERENZANTWORT

Zentraler Asset-Katalog mit Klassifizierung nach Vertraulichkeit, Integrität, Verfügbarkeit. Klassifizierung folgt den Anforderungen der Auftraggeber. Umsetzung in Zugriffsrechten, Verschlüsselung und Backup-Regimen.

A.9

Zugriffskontrolle

Wie wird der Zugriff auf Systeme und Informationen gewährt und regelmäßig geprüft? Wie sind privilegierte Zugriffe kontrolliert?

REFERENZANTWORT

Rollenbasierte Zugriffssteuerung. Mehrfaktor-Authentisierung für alle kritischen Systeme. Quartalsweise Rezertifizierung der Berechtigungen. Privilegierte Zugriffe zeitlich befristet und protokolliert.

A.10

Kryptographie

Welche kryptographischen Verfahren werden eingesetzt? Wie erfolgt Schlüsselmanagement?

REFERENZANTWORT

Ausschließlich Verfahren nach BSI TR-02102 und aktuellen Empfehlungen. Symmetrisch AES-256, asymmetrisch RSA-4096 oder elliptische Kurven. Zentrales Schlüsselmanagement mit dokumentiertem Lebenszyklus.

A.11

Physische Sicherheit

Wie ist die physische Sicherheit der Betriebsstätten organisiert? Zugangskontrollen, Videoüberwachung, Besucherregelung?

REFERENZANTWORT

Sicherheitsüberprüfter Standort in Augsburg mit Zugangskontrolle, dokumentierter Besucherregelung, Videoüberwachung öffentlicher Bereiche. Serverräume separat gesichert. Reinigungspersonal unter Verschwiegenheitsverpflichtung.

A.12

Betriebssicherheit

Wie erfolgen Patch-Management, Malware-Schutz und Sicherung? Welche Logs werden geführt und wie lange aufbewahrt?

REFERENZANTWORT

Automatisiertes Patch-Management, kritische Sicherheits-Patches innerhalb definierter Fristen. Endpoint-Protection auf allen Systemen. Backup-Konzept nach 3-2-1-Regel mit Offline-Kopie. Log-Aufbewahrung mindestens ein Jahr, sicherheitsrelevante Ereignisse länger.

A.14

Anwendungssicherheit

Wie ist Security in den Entwicklungsprozess integriert? Code-Reviews, statische Analyse, Testabdeckung, Freigabeprozesse?

REFERENZANTWORT

Security by Design als Prozessvorgabe. Vier-Augen-Prinzip bei Code-Reviews. Statische Analyse in der CI-Pipeline. Dependency-Scanning für Open-Source-Komponenten. Test-Coverage nach Kritikalität, dokumentierte Freigabepfade für Releases.

A.16

Vorfallsmanagement

Wie werden Sicherheitsvorfälle erkannt, gemeldet und bearbeitet? Welche Meldefristen gelten gegenüber Auftraggebern?

REFERENZANTWORT

Dokumentierter Incident-Response-Prozess. Meldung an Auftraggeber innerhalb der vertraglich vereinbarten Fristen, in der Regel innerhalb von 24 Stunden bei sicherheitsrelevanten Vorfällen. Post-Incident-Reviews mit Ableitung von Maßnahmen.

A.17

Business Continuity

Welche Vorkehrungen bestehen für den Fortbestand der Leistungsfähigkeit? Recovery-Ziele, Redundanzen, Insolvenz-Vorsorge?

REFERENZANTWORT

Dokumentiertes Business-Continuity-Konzept. Redundante Entwicklungsumgebungen. Recovery-Ziele nach Auftrag definiert. Quellcode-Escrow in Vorbereitung. Betriebsfähigkeit 90 Tage nach Insolvenzanmeldung dokumentiert.

A.18

Compliance

Welche gesetzlichen und vertraglichen Anforderungen werden systematisch überwacht? Wie erfolgt der Nachweis?

REFERENZANTWORT

Compliance-Register mit den relevanten Vorschriften (DSGVO, EU 2021/821, AWG, TISAX-Vorgaben, branchenspezifische Standards). Regelmäßige interne Prüfungen. Externe Audits durch TISAX und EcoVadis. Compliance-Ansprechpartner: compliance@newdirection.de.

ANWENDUNG DIESER VORLAGE

Diese Antwortvorlage ist Ausgangspunkt, kein fertiger Fragebogen.

Jeder Auftraggeber verwendet einen eigenen Fragebogen mit spezifischen Formulierungen und Zusatzfragen. Die Referenzantworten dieser Vorlage dienen als Baseline, die auf die konkrete Fragestellung angepasst werden muss. Für auftragsspezifische Anpassungen, insbesondere bei klassifizierten Mandaten, sind wir unter getintouchwith@newdirection.de erreichbar.

COMPLIANCE-ANSPRECHPARTNER
compliance@newdirection.de

BESCHAFFER-POSTFACH
getintouchwith@newdirection.de