ePrivacyseal NIS-2

ePrivacyseal GmbH

Kriterienkatalog 1.0

10.03.2026

Das NIS-2 Cybersecurity Gütesiegel der ePrivacyseal zertifiziert dem jeweiligen Antragsteller, dass sein Unternehmen mit den im nachfolgenden Kriterienkatalog näher spezifizierten Mindestanforderungen an Governance, Risikomanagement und technische/organisatorische Maßnahmen im Einklang steht, die sich an der NIS-2 Richtlinie (EU) 2022/2555 und dem Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Stärkung der Cybersicherheit (NIS-2-Umsetzungsgesetz) orientieren.

Hinweis: Die NIS2-Richtlinie und das nationale Umsetzungsgesetz sehen sektorspezifische Anforderungen vor, die in diesem Katalog nicht abschließend abgebildet sind. Eine unternehmens- und sektorspezifische Anpassung ist daher unerlässlich.

I. Grundsätze der Informationssicherheit

1. Sicherheitsrichtlinie und Sicherheitsziele

- Sind formale Informationssicherheitsrichtlinien vorhanden, die den Umgang mit Vertraulichkeit, Integrität und Verfügbarkeit regeln?
- Ist sichergestellt, dass die Schutzbedarfe (z. B. vertrauliche Geschäftsdaten, Personendaten) systematisch erfasst und klassifiziert werden?
- Ist sichergestellt, dass durch technische und organisatorische Maßnahmen die Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme und Daten angemessen, verhältnismäßig und risikoorientiert gewahrt wird?

2. Organisation und Verantwortlichkeiten

- Sind Rollen, Zuständigkeiten und Berichtslinien für Informationssicherheit verbindlich festgelegt, dokumentiert und kommuniziert?
- Gibt es einen benannten Informationssicherheitsbeauftragten (oder ein vergleichbares Gremium) mit klar definierten Aufgaben?
- Ist die oberste Leitung nachweislich in Entscheidungen zur Informationssicherheit eingebunden (z. B. Genehmigung der Sicherheitsstrategie, Überwachung der Umsetzung)?
- Existiert eine Richtlinie zur Informationssicherheit, die von der Leitungsebene verabschiedet und mindestens jährlich sowie anlassbezogen überprüft wird?

3. Einhaltung rechtlicher Vorgaben

- Werden bei der Planung und Umsetzung von Sicherheitsmaßnahmen alle einschlägigen gesetzlichen Anforderungen (z. B. NIS-2, IT-Sicherheitsgesetze, Datenschutzvorgaben) systematisch identifiziert, dokumentiert und umgesetzt?
- Ist im Risikomanagement geregelt, dass neben technischen Risiken auch rechtliche und regulatorische Risiken (Compliance-Risiken) ermittelt und bewertet werden?

II. Rechtmäßigkeit und Risikomanagement

1. Risikomanagementprozess

- Ist ein dokumentierter Risikomanagementprozess etabliert, der systematisch Risiken für Netz- und Informationssysteme erfasst, analysiert, bewertet und dokumentiert?
- Werden Gefährdungen und Bedrohungen regelmäßig ermittelt sowie Eintrittswahrscheinlichkeit und potenzielle Schäden nachvollziehbar erfasst?
- Werden bei Auswahl und Priorisierung von Sicherheitsmaßnahmen Art, Ausmaß und Eintrittswahrscheinlichkeit der Risiken sowie mögliche Schäden und gesellschaftliche Auswirkungen berücksichtigt?
- Werden technische und organisatorische Maßnahmen in Bezug auf Stand der Technik und anerkannte Normen (z. B. ISO/IEC 27001, IT-Grundschutz) ausgerichtet?
- Gibt es eine dokumentierte Bewertung der Verhältnismäßigkeit der Maßnahmen unter Berücksichtigung von Risikoexposition, Unternehmensgröße, Kosten und Auswirkungen (gemäß § 30 BSIG)?

- Erfolgt die Risikobehandlung in Form von Vermeidung, Verminderung, Übertragung oder Akzeptanz, wobei alle akzeptierten Restrisiken mit Begründung dokumentiert und von der Leitungsebene freigegeben sind?
- Werden identifizierte Risiken dokumentiert, priorisiert und behandelt (z. B. durch technische/organisatorische Maßnahmen)?
- Ist für erkannte Risiken, die aus bestimmten Gründen nicht mit Maßnahmen gemindert werden, eine formalisierte Risikoakzeptanzentscheidung vorhanden und dokumentiert?
- Werden Zwischenergebnisse des Risikomanagements (Risk Register, Maßnahmenpläne) regelmäßig berichtspflichtig gemacht, überwacht und aktualisiert?

2. Lieferketten- und Drittanbieter-Sicherheit

- Werden Cyber-Sicherheitsrisiken in der Lieferkette (IT-/OT-Drittanbieter, Zulieferer) bewertet und in das Risikomanagement einbezogen (Lieferantencheck)?
- Sind in Lieferverträgen spezifische Sicherheitsanforderungen (z. B. Security-Standards, Zertifizierungen, Meldepflichten bei Sicherheitsvorfällen) festgelegt?
- Werden Zertifikate, Auditberichte oder Prüfnachweise der Dienstleister eingeholt und bewertet?
- Werden regelmäßige Überprüfungen der Sicherheitspraktiken und der Produktqualität (z. B. secure-by-design, Schwachstellenmanagement) bei Drittanbietern durchgeführt?
- Wird die Einhaltung der vertraglichen Sicherheitsmaßnahmen regelmäßig kontrolliert und bei Verstößen nach einem definierten Eskalationsverfahren behandelt?

III. Geschäftsleitungsverantwortung und Managementsysteme

1. Führungs- und Kontrollverantwortung

- Ist die Geschäftsleitung eingebunden in das Informationssicherheits-Management (Freigabe von Maßnahmen, regelmäßige Reviews)?
- Erfolgt ein regelmäßiges Reporting an die oberste Leitung über den Stand des Informationssicherheitsmanagementsystems (ISMS) und erkannte Risiken auf Basis definierter Kennzahlen (KPIs)?
- Sind Informationssicherheitsziele definiert, strategisch geplant und werden deren Erreichung gemessen?

- Gibt es ein festgelegtes Kontroll- und Revisionsprogramm (z. B. regelmäßige Prüfungen, interne Audits) zur Überwachung der Umsetzung der Sicherheitsmaßnahmen?

2. Schulungen und Sensibilisierung

- Werden Leitungsorgane sowie alle Mitarbeitenden in festgelegten Abständen zu Cyber-Risiken und Sicherheitsmaßnahmen geschult?
- Enthalten Schulungsprogramme die Fähigkeit zur Erkennung von Risiken, Bedrohungen und Phishing-Attacken sowie die Mitwirkung im Sicherheitsprozess?
- Erfolgt eine Wirksamkeitskontrolle der Schulungen (z. B. Testverfahren, Nachweis der Teilnahme) und Auswertung mit Blick auf notwendige Anpassungen der Inhalte?

3. Managementsystem (ISMS)

- Existiert ein formales Informationssicherheits-Managementsystem, dessen Aufbau, Implementierung und kontinuierliche Verbesserung dokumentiert ist?
- Ist sichergestellt, dass das ISMS alle relevanten Geschäftsprozesse, Anwendungen und IT-Systeme erfasst?
- Werden Managementbewertungen (Management-Reviews) über die Effektivität des ISMS mindestens einmal jährlich durchgeführt?
- Ist ein Verfahren zur Behandlung von Abweichungen und Verbesserungsvorschlägen im ISMS etabliert (Change- und Korrekturprozess) inkl. Fristen und Verantwortlichkeiten?

IV. Technische und organisatorische Sicherheitsmaßnahmen

1. Allgemeine Maßnahmen

- Ist ein fortlaufendes Sicherheitskonzept („Informationssicherheitskonzept“) für die IT-Systeme und -Prozesse vorhanden und wird es regelmäßig aktualisiert?
- Werden alle im Rahmen des Risikomanagements festgelegten technischen und organisatorischen Maßnahmen umgesetzt und dokumentiert (z. B. als Teil des ISMS)?
- Werden regelmäßige Risikoanalysen und Penetrationstests oder Systemüberprüfungen durchgeführt, um Sicherheitslücken zu identifizieren und zu beheben?
- Ist eine Endpoint Protection (z. B. EDR, Antivirus) für alle Systeme implementiert?

- Gibt es ein Notfall- und Backup-Konzept für kritische Systeme, das Wiederanlauf- und Krisenmanagement umfasst?
- Ist ein Prozess zur Vorfallsbewältigung etabliert, der Detektion, Meldung und Beseitigung von Sicherheitsvorfällen sowie Wiederherstellungsschritte definiert?
- Werden die Lieferkettenbeziehungen nach Risiko bewertet und enthält die IT-Beschaffung Sicherheitsanforderungen (z. B. sichere Entwicklung, Vulnerability Disclosure)?
- Gibt es Verfahren zur Bewertung der Wirksamkeit der Sicherheitsmaßnahmen (z. B. interne Audits, Überprüfung von KPIs)?
- Werden Mitarbeiter regelmäßig zu Informationssicherheit und Cyber-Hygiene geschult und sensibilisiert?
- Werden Richtlinien für die Nutzung von IT-Systemen (Bring-your-own-Device, Kennwortregeln, mobile Sicherheit, externe Datenträger) verbindlich vorgegeben und technisch unterstützt (z. B. MDM, Richtlinienerzwingung)?
- Ist ein Verschlüsselungskonzept vorhanden, das den Einsatz von Kryptografie und Verschlüsselung für Datenübertragung und -speicherung regelt?
- Werden Zugriffsrechte strikt nach dem Need-to-know-Prinzip vergeben und verwaltet (Identity- und Access-Management)?
- Ist die Identitätsprüfung verstärkt (z. B. durch Mehr-Faktor-Authentifizierung, Passwortregeln, biometrische Verfahren) und für besonders schützenswerte Zugänge verpflichtend?
- Werden alle sicherheitsrelevanten Systeme (Netzwerk, Server, Anwendungen) gegen unerlaubte Kommunikation geschützt (Firewall, IDS/IPS, Netzwerksegmentierung)?
- Ist der Betrieb von IKT-Systemen durch kontinuierliche Überwachung (Monitoring) und Intrusion-Detection-Systeme abgesichert?
- Werden Notfallkommunikationssysteme vorgehalten (z. B. gesicherte Kanäle) für den Krisenfall?

2. Branchenspezifische Anforderungen

2.1 Energieversorgung (Strom, Gas, Fernwärme)

- Sind die Energieerzeugungs- und Energieverteilungssysteme (z. B. Kraftwerke, Netze, Substationen) durch spezielle Zutritts- und Netzwerksicherheitsmaßnahmen geschützt?
- Werden industrielle Steuerungssysteme (SCADA/ICS) und Smart-Grid-Komponenten segmentiert und vor unbefugtem Zugriff abgesichert?

- Existiert ein Patches- und Update-Management für Betreiber-leitsysteme nach Branchenstandards (z. B. IEC 62443)?
- Gibt es Maßnahmen zur Redundanz (z. B. parallele Kontrollräume, Notfallschaltungen) bei kritischen Anlagen?

2.2 Transport und Verkehr (Bahn, Luftfahrt, Straße, Schifffahrt)

- Werden Betriebs- und Leittechniksysteme im Verkehrssektor (z. B. Signaltechnik, Flugverkehrsführungssysteme) durch Zutrittskontrollen und Netzwerksegmentierung geschützt?
- Ist für sicherheitskritische Anwendungen (z. B. Zugsicherung, Fluglotsenkommunikation) eine besondere Ausfallsicherheit vorgesehen?
- Gibt es konzernweite Security-Standards, die für alle Verkehrsträger gelten, und sind diese implementiert und kontrolliert?

2.3 Finanz- und Versicherungswesen

- Werden Transaktionssysteme (Zahlungsverkehr, Handelssysteme) durch End-to-End-Verschlüsselung und Trennung der Netze gegen Manipulation gesichert?
- Gibt es ein striktes Monitoring von Finanztransaktionen und sofortige Alarmschwellen bei unüblichen Aktivitäten?
- Werden Kontrollen wie Vier-Augen-Prinzip und Segregation of Duties in kritischen Finanzprozessen umgesetzt und dokumentiert?

2.4 Gesundheitswesen (Krankenhäuser, Pflegeeinrichtungen)

- Sind Patienten- und Gesundheitsdaten besonders geschützt (z. B. Verschlüsselung von Datenträgern, strenge Zutrittskontrollen zu Systemen)?
- Werden medizinische Geräte (z. B. Bildgebende Systeme, Implantat Programmierungen) in eigene, geschützte Netze eingebunden?
- Existiert ein Konzept für den Schutz von Telematik- und Notfallsystemen (z. B. Rettungsleitstellen, elektronische Patientenakte) gegen IT-Angriffe?

2.5 Wasserversorgung und Abwasserentsorgung

- Werden die Steuerungs- und Leitstände in Wasserwerken durch separate Kontrollnetzwerke und Zugriffskontrollen abgesichert?
- Ist ein Schutzkonzept für kritische Infrastruktur im Wasserbereich vorhanden (z. B. Trennung von Produktions- und Verwaltungsnetz)?
- Werden Sensordaten und Fernsteuerungssignale in der Wasserversorgung vor Manipulation geschützt?

2.6 Digitale Infrastruktur und Telekommunikation

- Sind Cloud-Dienste, Rechenzentren und Content-Delivery-Netzwerke durch besondere Sicherheitsstandards (z. B. physische Absicherung, Redundanz, Zugangskontrollen) geschützt?
- Verfügen Domain-Name-Registry-Anbieter (TLD, DNS) über Mehrfachausfallkonzepte und spezielle Integritätsschutzmaßnahmen?
- Werden Managed Service Provider und Telekommunikationsdienste nach branchenspezifischen Regelwerken (z. B. EK-MT-Protokolle, 5G Security) betrieben?

2.7 Produktion und Industrie (Fertigung, Chemie, Lebensmittel)

- Sind Produktionsanlagen und Anlagensteuerungen (OT) vom IT-Bereich getrennt und nach Industriestandards (z. B. OPC-UA-Sicherheitsprofile) abgesichert?
- Werden im Produktionsprozess eingesetzte Maschinen und Roboter gegen Sabotage geschützt (z. B. manipulierte Steuerbefehle)?
- Existiert eine besondere Härtung kritischer Industrie-Komponenten (z. B. SPS/PPS) gegen Cyberangriffe?

2.8 Weitere kritische Bereiche

- (Sofern zutreffend) Bestehen für sonstige „kritische Einrichtungen“ (z. B. Raumfahrt, zentrale Behörden) branchenspezifische Sicherheitsrichtlinien, die umgesetzt werden?

V. Überwachung, Nachweise, Auditierung, Meldung von Sicherheitsvorfällen

1. Monitoring und Nachweisführung

- Sind Sicherheitsrelevante Ereignisse (z. B. Login-Versuche, Konfigurationsänderungen) zentral protokolliert und vor Manipulation geschützt (Audit-Trails)?
- Werden Netzwerke und Systeme mit Echtzeitüberwachung (z. B. SIEM, IDS/IPS) beobachtet und ungewöhnliche Aktivitäten gemeldet?
- Existiert ein Dokumentationssystem (Log-Management) zur Nachverfolgung von Änderungen an sicherheitsrelevanten Konfigurationen?
- Werden nach Bedarf Reports über Kennzahlen der Informationssicherheit (z. B. Anzahl Schwachstellen, Ergebnis Audits) erstellt und ausgewertet?

2. Auditierung und Kontrolle

- Finden regelmäßige interne und/oder externe Audits statt, um die Einhaltung des Informationssicherheits-Managementsystems zu überprüfen?
- Ist dokumentiert, wie Abweichungen (Non-Compliance) aus Audits identifiziert, behandelt und behoben werden?
- Werden Änderungen in der Bedrohungslage (z. B. neue Risiken) in die Sicherheitsstrategie einbezogen?
- Werden externe Prüfungen (z. B. ISO/IEC-27001-Zertifizierung, Grundschutzaudit) als Nachweis der Konformität eingeholt?

3. Meldepflichten bei Sicherheitsvorfällen

- Wird jeder erhebliche IT-Sicherheitsvorfall unverzüglich (innerhalb von 24 Stunden nach Kenntniserlangung) an das BSI (mittels BSI-Portal) gemeldet, sofern eine Meldepflicht nach NIS-2 / NIS-2-Umsetzungsgesetz besteht?
- Wird bei einem IT-Sicherheitsvorfall sichergestellt, dass nach der Erstmeldung eine vollständige Folgemeldung innerhalb von 72 Stunden und eine Abschlussmeldung spätestens nach einem Monat erstellt wird?
- Ist sichergestellt, dass die Meldung alle relevanten Informationen enthält (Schweregrad, Art des Vorfalls, betroffene Systeme, ergriffene Maßnahmen)?
- Verfügt das Unternehmen über ein definiertes Vorfalls Management mit klaren Meldewegen intern und extern?
- Werden auch interne Sicherheitsvorfälle und Beinahe-Vorfälle dokumentiert und bei kritischer Relevanz gemäß Meldeprozess behandelt?

VI. Sonstiges

1. Datenschutz (DSGVO-relevante Aspekte)

- Werden Datenübermittlungen in Drittländer nur unter Einhaltung der Art. 44–49 DSGVO durchgeführt (z. B. Standardvertragsklauseln)?
- Sind Verträge mit Auftragsverarbeitern nach Art. 28 DSGVO gestaltet (inkl. Unterauftragsverarbeiter)?
- Werden Pseudonymisierung und Datenminimierung wo möglich umgesetzt?
- Werden sensible personenbezogene Daten separiert oder pseudonymisiert?
- Gibt es Zugriffsschutz und Protokollierung bei personenbezogenen Daten?
- Sind technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO umgesetzt und in das Informationssicherheits-Managementsystem integriert?