# DIN EN ISO/IEC 27002:2024-01 (D)

## Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022); Deutsche Fassung EN ISO/IEC 27002:2022

## Inhalt

Seite


Europäisches Vorwort ..... 5

Vorwort ..... 6

Einleitung ..... 7

1 Anwendungsbereich ..... 10

2 Normative Verweisungen ..... 10

3 Begriffe und Abkürzungen ..... 10
3.1 Begriffe ..... 10
3.2 Abkürzungen ..... 16

4 Aufbau dieses Dokuments ..... 17
4.1 Abschnitte ..... 17
4.2 Themen und Attribute ..... 18
4.3 Maßnahmengestaltung ..... 19

5 Organisatorische Maßnahmen ..... 20
5.1 Informationssicherheitspolitik und -richtlinien ..... 20
5.2 Informationssicherheitsrollen und -verantwortlichkeiten ..... 22
5.3 Aufgabentrennung ..... 23
5.4 Verantwortlichkeiten der Leitung ..... 25
5.5 Kontakt mit Behörden ..... 26
5.6 Kontakt mit speziellen Interessengruppen ..... 27
5.7 Informationen über die Bedrohungslage ..... 27
5.8 Informationssicherheit im Projektmanagement ..... 29
5.9 Inventar der Informationen und anderer damit verbundener Werte ..... 31
5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten ..... 33
5.11 Rückgabe von Werten ..... 35
5.12 Klassifizierung von Informationen ..... 36
5.13 Kennzeichnung von Informationen ..... 38
5.14 Informationsübermittlung ..... 39
5.15 Zugangssteuerung ..... 42
5.16 Identitätsmanagement ..... 45
5.17 Authentisierungsinformationen ..... 46
5.18 Zugangsrechte ..... 49
5.19 Informationssicherheit in Lieferantenbeziehungen ..... 51
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen ..... 53
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette ..... 56
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen ..... 58
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten ..... 60
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen ..... 63
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse ..... 65
5.26 Reaktion auf Informationssicherheitsvorfälle ..... 66
5.27 Erkenntnisse aus Informationssicherheitsvorfällen ..... 67
5.28 Sammeln von Beweismaterial ..... 68
5.29 Informationssicherheit bei Störungen ..... 69
5.30 IKT-Bereitschaft für Business-Continuity ..... 70

**5.31 Juristische, gesetzliche, regulatorische und vertragliche Anforderungen ..... 71**
**5.32 Geistige Eigentumsrechte ..... 73**
**5.33 Schutz von Aufzeichnungen ..... 75**
**5.34 Datenschutz und Schutz personenbezogener Daten (pbD) ..... 77**
**5.35 Unabhängige Überprüfung der Informationssicherheit ..... 78**
**5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit ..... 79**
**5.37 Dokumentierte Betriebsabläufe ..... 80**

**6 Personenbezogene Maßnahmen ..... 82**
**6.1 Sicherheitsüberprüfung ..... 82**
**6.2 Beschäftigungs- und Vertragsbedingungen ..... 83**
**6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung ..... 85**
**6.4 Maßregelungsprozess ..... 87**
**6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung ..... 88**
**6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen ..... 89**
**6.7 Remote-Arbeit ..... 90**
**6.8 Meldung von Informationssicherheitsereignissen ..... 92**

**7 Physische Maßnahmen ..... 93**
**7.1 Physische Sicherheitsperimeter ..... 93**
**7.2 Physischer Zutritt ..... 94**
**7.3 Sichern von Büros, Räumen und Einrichtungen ..... 96**
**7.4 Physische Sicherheitsüberwachung ..... 97**
**7.5 Schutz vor physischen und umweltbedingten Bedrohungen ..... 98**
**7.6 Arbeiten in Sicherheitsbereichen ..... 100**
**7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren ..... 101**
**7.8 Platzierung und Schutz von Geräten und Betriebsmitteln ..... 102**
**7.9 Sicherheit von Werten außerhalb der Räumlichkeiten ..... 103**
**7.10 Speichermedien ..... 104**
**7.11 Versorgungseinrichtungen ..... 106**
**7.12 Sicherheit der Verkabelung ..... 107**
**7.13 Instandhaltung von Geräten und Betriebsmitteln ..... 108**
**7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln ..... 109**

**8 Technologische Maßnahmen ..... 111**
**8.1 Endpunktgeräte des Benutzers ..... 111**
**8.2 Privilegierte Zugangsrechte ..... 113**
**8.3 Informationszugangsbeschränkung ..... 115**
**8.4 Zugriff auf den Quellcode ..... 117**
**8.5 Sichere Authentisierung ..... 118**
**8.6 Kapazitätssteuerung ..... 120**
**8.7 Schutz gegen Schadsoftware ..... 122**
**8.8 Handhabung von technischen Schwachstellen ..... 124**
**8.9 Konfigurationsmanagement ..... 128**
**8.10 Löschung von Informationen ..... 130**
**8.11 Datenmaskierung ..... 132**
**8.12 Verhinderung von Datenlecks ..... 134**
**8.13 Sicherung von Informationen ..... 135**
**8.14 Redundanz von informationsverarbeitenden Einrichtungen ..... 137**
**8.15 Protokollierung ..... 138**
**8.16 Überwachung von Aktivitäten ..... 142**
**8.17 Uhrensynchronisation ..... 144**
**8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten ..... 145**
**8.19 Installation von Software auf Systemen in Betrieb ..... 146**
**8.20 Netzwerksicherheit ..... 148**
**8.21 Sicherheit von Netzwerkdiensten ..... 149**
**8.22 Trennung von Netzwerken ..... 150**
**8.23 Webfilterung ..... 152**
**8.24 Verwendung von Kryptographie ..... 153**

**8.25 Lebenszyklus einer sicheren Entwicklung ... 155**
**8.26 Anforderungen an die Anwendungssicherheit ... 156**
**8.27 Sichere Systemarchitektur und Entwicklungsgrundsätze ... 159**
**8.28 Sichere Codierung ... 161**
**8.29 Sicherheitsprüfung bei Entwicklung und Abnahme ... 164**
**8.30 Ausgegliederte Entwicklung ... 166**
**8.31 Trennung von Entwicklungs-, Test- und Produktionsumgebungen ... 167**
**8.32 Änderungssteuerung ... 169**
**8.33 Testdaten ... 170**
**8.34 Schutz der Informationssysteme während Tests im Rahmen von Audits ... 171**

**Anhang A (informativ) Verwendung von Attributen ... 173**
**A.1 Allgemeines ... 173**
**A.2 Organisatorische Sichten ... 191**

**Anhang B (informativ) Übereinstimmung von ISO/IEC 27002:2022 (dieses Dokument) mit ISO/IEC 27002:2013 ... 193**

**Literaturhinweise ... 201**