

E DIN EN ISO/IEC 27002:2022-08 (D/E)

Erscheinungsdatum: 2022-07-15

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

Information security, cybersecurity and privacy protection - Information security
controls (ISO/IEC 27002:2022); German and English version prEN ISO/IEC 27002:2022

Inhalt	Seite
Europäisches Vorwort.....	5
Vorwort	6
Einleitung	8
1 Anwendungsbereich.....	11
2 Normative Verweisungen	11
3 Begriffe und Abkürzungen	11
3.1 Begriffe	11
3.2 Abkürzungen	17
4 Aufbau dieses Dokuments	18
4.1 Abschnitte	18
4.2 Themen und Attribute	19
4.3 Maßnahmengestaltung.....	20
5 Organisatorische Maßnahmen.....	21
5.1 Informationssicherheitsrichtlinien.....	21
5.2 Informationssicherheitsrollen und -verantwortlichkeiten.....	23
5.3 Aufgabentrennung	24
5.4 Verantwortlichkeiten der Leitung.....	26
5.5 Kontakt mit Behörden	27
5.6 Kontakt mit speziellen Interessensgruppen	28
5.7 Bedrohungsintelligenz	28
5.8 Informationssicherheit im Projektmanagement.....	30
5.9 Inventar der Informationen und anderen damit verbundenen Werten	32
5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten.....	34
5.11 Rückgabe von Werten	36
5.12 Klassifizierung von Information.....	37
5.13 Kennzeichnung von Information.....	39
5.14 Informationsübertragung.....	40
5.15 Zugangssteuerung.....	43
5.16 Identitätsmanagement	46
5.17 Informationen zur Authentifizierung.....	47
5.18 Zugangsrechte	50
5.19 Informationssicherheit in Lieferantenbeziehungen.....	52
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen	54
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette	57
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	59
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten.....	61
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen.....	64
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse.....	66
5.26 Reaktion auf Informationssicherheitsvorfälle	67

5.27	Erkenntnisse aus Informationssicherheitsvorfällen.....	68
5.28	Sammeln von Beweismaterial.....	69
5.29	Informationssicherheit bei Störungen.....	70
5.30	IKT-Bereitschaft für Business Continuity.....	71
5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	72
5.32	Geistige Eigentumsrechte.....	74
5.33	Schutz von Aufzeichnungen.....	76
5.34	Datenschutz und Schutz personenbezogener Daten (pBD).....	78
5.35	Unabhängige Überprüfung der Informationssicherheit.....	79
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit.....	80
5.37	Dokumentierte Betriebsabläufe.....	81
6	Personenbezogene Maßnahmen.....	83
6.1	Sicherheitsüberprüfung.....	83
6.2	Beschäftigungs- und Vertragsbedingungen.....	84
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung.....	86
6.4	Maßregelungsprozess.....	88
6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung.....	89
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	90
6.7	Telearbeit.....	91
6.8	Meldung von Informationssicherheitsereignissen	93
7	Physische Maßnahmen.....	94
7.1	Physische Sicherheitsperimeter	94
7.2	Physischer Zutritt.....	95
7.3	Sichern von Büros, Räumen und Einrichtungen	97
7.4	Physische Sicherheitsüberwachung.....	98
7.5	Schutz vor physischen und umweltbedingten Bedrohungen	99
7.6	Arbeiten in Sicherheitsbereichen	101
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren.....	102
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	103
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten.....	104
7.10	Speichermedien.....	105
7.11	Versorgungseinrichtungen	107
7.12	Sicherheit der Verkabelung.....	108
7.13	Instandhaltung von Geräten und Betriebsmitteln	109
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	110
8	Technologische Maßnahmen.....	112
8.1	Endpunktgeräte des Benutzers	112
8.2	Privilegierte Zugangsrechte	114
8.3	Informationszugangsbeschränkung	116
8.4	Zugriff auf den Quellcode.....	118
8.5	Sichere Authentifizierung.....	119
8.6	Kapazitätssteuerung	121
8.7	Schutz gegen Schadsoftware.....	123
8.8	Handhabung von technischen Schwachstellen.....	125
8.9	Konfigurationsmanagement.....	129
8.10	Löschung von Informationen	131
8.11	Datenmaskierung.....	133
8.12	Verhinderung von Datenlecks	135
8.13	Sicherung von Information	136
8.14	Redundanz von informationsverarbeitenden Einrichtungen	138
8.15	Protokollierung	139
8.16	Überwachung von Aktivitäten	142
8.17	Uhrensynchronisation.....	145
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	146
8.19	Installation von Software auf Systemen im Betrieb.....	147
8.20	Netzwerksicherheit	148

8.21	Sicherheit von Netzwerkdiensten.....	150
8.22	Trennung von Netzwerken.....	151
8.23	Webfilterung.....	152
8.24	Verwendung von Kryptographie.....	153
8.25	Lebenszyklus einer sicheren Entwicklung.....	156
8.26	Anforderungen an die Anwendungssicherheit.....	157
8.27	Sichere Systemarchitektur und technische Grundsätze.....	160
8.28	Sicheres Coding.....	162
8.29	Sicherheitsprüfung in Entwicklung und Abnahme.....	165
8.30	Ausgegliederte Entwicklung.....	167
8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen.....	168
8.32	Änderungssteuerung.....	170
8.33	Prüfinformationen.....	171
8.34	Schutz der Informationssysteme während der Überwachungsprüfung.....	172
Anhang A (informativ) Verwendung von Attributen.....		174
A.1	Allgemeines.....	174
A.2	Organisatorische Sichten.....	192
Anhang B (informativ) Übereinstimmung von ISO/IEC 27002:2022 (dieses Dokument) mit ISO/IEC 27002:2013.....		194
Literaturhinweise.....		202