

DIN EN ISO/IEC 27011:2021-10 (D)

Informationstechnik - Sicherheitsverfahren - Leitfaden für
Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für
Telekommunikationsorganisationen (ISO/IEC 27011:2016); Deutsche Fassung EN
ISO/IEC 27011:2020

Inhalt	Seite
Europäisches Vorwort.....	5
Vorwort.....	6
Einleitung.....	7
1 Anwendungsbereich.....	9
2 Normative Verweisungen.....	9
3 Begriffe und Abkürzungen.....	9
3.1 Begriffe.....	9
3.2 Abkürzungen.....	11
4 Übersicht.....	12
4.1 Aufbau dieser Empfehlung Internationalen Norm.....	12
4.2 Informationssicherheits-Managementsysteme in Telekommunikationsorganisationen.....	12
4.2.1 Ziel.....	12
4.2.2 Sicherheitsbetrachtungen in der Telekommunikation.....	13
4.2.3 Zu schützende Informationswerte.....	14
4.2.4 Einrichtung des Informationssicherheitsmanagements.....	15
5 Informationssicherheitsrichtlinien.....	16
6 Organisation der Informationssicherheit.....	16
6.1 Interne Organisation.....	16
6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten.....	16
6.1.2 Aufgabentrennung.....	16
6.1.3 Kontakt mit Behörden.....	16
6.1.4 Kontakt mit speziellen Interessensgruppen.....	17
6.1.5 Informationssicherheit im Projektmanagement.....	17
6.2 Mobilgeräte und Telearbeit.....	17
7 Personalsicherheit.....	17
7.1 Vor der Beschäftigung.....	17
7.1.1 Sicherheitsüberprüfung.....	17
7.1.2 Beschäftigungs- und Vertragsbedingungen.....	18
7.2 Während der Beschäftigung.....	18
7.3 Beendigung oder Änderung der Beschäftigung.....	18
8 Verwaltung der Werte.....	19
8.1 Verantwortlichkeit für Werte.....	19
8.1.1 Inventarisierung der Werte.....	19
8.1.2 Zuständigkeit für Werte.....	19
8.1.3 Zulässiger Gebrauch von Werten.....	19
8.1.4 Rückgabe von Werten.....	19
8.2 Informationsklassifizierung.....	19
8.2.1 Leitlinien für die Klassifizierung.....	19
8.2.2 Kennzeichnung von Information.....	20
8.2.3 Handhabung von Werten.....	20

8.3	Handhabung von Datenträgern	20
9	Zugangssteuerung.....	20
9.1	Geschäftsanforderungen an die Zugangsteuerung.....	20
9.1.1	Zugangssteuerungsrichtlinie.....	20
9.1.2	Zugang zu Netzwerken und Netzwerkdiensten.....	21
9.2	Benutzerzugangsverwaltung.....	21
9.3	Benutzerverantwortlichkeiten.....	21
9.4	Zugangssteuerung für Systeme und Anwendungen.....	21
10	Kryptographie	21
11	Physische und umgebungsbezogene Sicherheit.....	21
11.1	Sicherheitsbereiche.....	21
11.1.1	Physische Sicherheitsperimeter	21
11.1.2	Physische Zutrittssteuerung.....	22
11.1.3	Sichern von Büros, Räumen und Einrichtungen	22
11.1.4	Schutz vor externen und umweltbedingten Bedrohungen.....	22
11.1.5	Arbeiten in Sicherheitsbereichen	23
11.1.6	Anlieferungs- und Ladebereiche	23
11.2	Geräte und Betriebsmittel.....	23
11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln	23
11.2.2	Versorgungseinrichtungen	23
11.2.3	Sicherheit der Verkabelung.....	24
11.2.4	Instandhaltung von Geräten und Betriebsmitteln	24
11.2.5	Entfernen von Werten	24
11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	24
11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	24
11.2.8	Unbeaufsichtigte Benutzergeräte	24
11.2.9	Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	24
12	Betriebssicherheit	25
12.1	Betriebsabläufe und -verantwortlichkeiten.....	25
12.1.1	Dokumentierte Betriebsabläufe.....	25
12.1.2	Änderungssteuerung.....	25
12.1.3	Kapazitätssteuerung	25
12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen.....	26
12.2	Schutz vor Schadsoftware.....	26
12.3	Datensicherung.....	26
12.4	Protokollierung und Überwachung.....	26
12.4.1	Ereignisprotokollierung	26
12.4.2	Schutz der Protokollinformation	27
12.4.3	Administratoren- und Bedienerprotokolle	27
12.4.4	Uhrensynchronisation.....	27
12.5	Steuerung von Software im Betrieb	27
12.5.1	Installation von Software auf Systemen im Betrieb.....	27
12.6	Handhabung technischer Schwachstellen.....	28
12.6.1	Handhabung von technischen Schwachstellen.....	28
12.6.2	Einschränkungen von Softwareinstallation	28
12.7	Audits von Informationssystemen.....	28
13	Kommunikationssicherheit.....	28
13.1	Netzwerksicherheitsmanagement.....	28
13.1.1	Netzwerksteuerungsmaßnahmen	28
13.1.2	Sicherheit von Netzwerkdiensten.....	29
13.1.3	Trennung in Netzwerken.....	29
13.2	Informationsübertragung	30
13.2.1	Richtlinien und Verfahren für die Informationsübertragung	30
13.2.2	Vereinbarungen zur Informationsübertragung.....	30
13.2.3	Elektronische Nachrichtenübermittlung.....	30

13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	30
14	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	30
14.1	Sicherheitsanforderungen an Informationssysteme.....	30
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen.....	30
14.3	Testdaten	30
15	Lieferantenbeziehungen	30
15.1	Informationssicherheit in Lieferantenbeziehungen.....	30
15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	30
15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen	31
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie.....	31
15.2	Steuerung der Dienstleistungserbringung von Lieferanten.....	32
16	Handhabung von Informationssicherheitsvorfällen	32
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen.....	32
16.1.1	Verantwortlichkeiten und Verfahren	32
16.1.2	Meldung von Informationssicherheitsereignissen	33
16.1.3	Meldung von Schwächen in der Sicherheit	33
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	34
16.1.5	Reaktion auf Informationssicherheitsvorfälle	34
16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen	34
16.1.7	Sammeln von Beweismaterial.....	35
17	Informationssicherheitsaspekte beim Business Continuity Management.....	35
17.1	Aufrechterhalten der Informationssicherheit.....	35
17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit.....	35
17.1.2	Umsetzung der Aufrechterhaltung der Informationssicherheit.....	35
17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit	36
17.2	Redundanzen	36
17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen	36
18	Compliance	36
	Anhang A (normativ) Telekommunikationsspezifischer Maßnahmenkatalog	37
	TEL.9 Zugangssteuerung.....	37
	TEL.9.5 Steuerung des Netzwerkzugangs.....	37
	TEL.11 Physische und umgebungsbezogene Sicherheit.....	38
	TEL.11.1 Sicherheitsbereiche	38
	TEL.11.3 Sicherheit im Verantwortungsbereich von Dritten	41
	TEL.13 Kommunikationssicherheit	42
	TEL.13.1 Netzwerksicherheitsmanagement	42
	TEL.18 Compliance	45
	TEL.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen.....	45
	Anhang B (informativ) Weitere Leitlinien für die Netzwerksicherheit	49
	B.1 Sicherheitsmaßnahmen zum Schutz vor Netzwerkangriffen	49
	B.1.1 Schutz vor Netzwerkangriffen.....	49
	B.1.2 Anwender informieren.....	50
	B.2 Netzwerksicherheitsmaßnahmen zum Schutz vor Netzwerküberlastung.....	50
	B.2.1 Sammeln von Informationen	50
	B.2.2 Maßnahmen gegen Netzwerküberlastungen	50
	Literaturhinweise	52