

DIN ISO/IEC 27002:2016-11 (D)

Informationstechnologie - IT-Sicherheitsverfahren - Leitfaden für Informationssicherheits-Maßnahmen (ISO/IEC 27002:2013 + Cor. 1:2014 + Cor. 2:2015)

Inhalt	Seite
Nationales Vorwort	4
Nationaler Anhang NA (informativ) Literaturhinweise	5
0 Einleitung.....	6
1 Anwendungsbereich.....	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Aufbau dieser Norm.....	9
4.1 Abschnitte	9
4.2 Maßnahmenkategorien.....	9
5 Informationssicherheitsrichtlinien.....	10
5.1 Vorgaben der Leitung für Informationssicherheit	10
6 Organisation der Informationssicherheit	12
6.1 Interne Organisation	12
6.2 Mobilgeräte und Telearbeit	15
7 Personalsicherheit.....	18
7.1 Vor der Beschäftigung.....	18
7.2 Während der Beschäftigung	20
7.3 Beendigung und Änderung der Beschäftigung	23
8 Verwaltung der Werte	23
8.1 Verantwortlichkeit für Werte	23
8.2 Informationsklassifizierung	26
8.3 Handhabung von Datenträgern	28
9 Zugangssteuerung.....	30
9.1 Geschäftsanforderungen an die Zugangsteuerung.....	30
9.2 Benutzerzugangsverwaltung.....	33
9.3 Benutzerverantwortlichkeiten	37
9.4 Zugangssteuerung für Systeme und Anwendungen.....	38
10 Kryptographie	42
10.1 Kryptographische Maßnahmen	42
11 Physische und umgebungsbezogene Sicherheit.....	45
11.1 Sicherheitsbereiche	45
11.2 Geräte und Betriebsmittel	49
12 Betriebssicherheit.....	55
12.1 Betriebsabläufe und -verantwortlichkeiten	55
12.2 Schutz vor Schadsoftware.....	58
12.3 Datensicherung.....	60
12.4 Protokollierung und Überwachung.....	61
12.5 Steuerung von Software im Betrieb.....	63
12.6 Handhabung technischer Schwachstellen.....	65

12.7	Audits von Informationssystemen.....	67
13	Kommunikationssicherheit.....	67
13.1	Netzwerksicherheitsmanagement.....	67
13.2	Informationsübertragung	70
14	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	74
14.1	Sicherheitsanforderungen an Informationssysteme.....	74
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	77
14.3	Testdaten	83
15	Lieferantenbeziehungen	84
15.1	Informationssicherheit in Lieferantenbeziehungen	84
15.2	Steuerung der Dienstleistungserbringung von Lieferanten	88
16	Handhabung von Informationssicherheitsvorfällen	90
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen.....	90
17	Informationssicherheitsaspekte beim Business Continuity Management.....	95
17.1	Aufrechterhalten der Informationssicherheit.....	95
17.2	Redundanzen.....	97
18	Compliance	98
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	98
18.2	Überprüfungen der Informationssicherheit	102
	Literaturhinweise	105