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

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

Inha	alt	Seite
Natio	nales Vorwort	4
Natio	naler Anhang NA (informativ) Literaturhinweise	5
0	Einleitung	6
1	Anwendungsbereich	
2	Normative Verweisungen	Ç
3	Begriffe	
4	Aufbau dieser Norm	
4.1	Abschnitte	
4.2	Maßnahmenkategorien	g
5	Informationssicherheitsrichtlinien	
5.1	Vorgaben der Leitung für Informationssicherheit	10
6	Organisation der Informationssicherheit	
6.1 6.2	Interne OrganisationMobilgeräte und Telearbeit	
	o a constant of the constant o	
7 7.1	PersonalsicherheitVor der Beschäftigung	
7.2	Während der Beschäftigung	
7.3	Beendigung und Änderung der Beschäftigung	23
8	Verwaltung der Werte	
8.1 8.2	Verantwortlichkeit für WerteInformationsklassifizierung	
8.3	Handhabung von Datenträgern	
9	Zugangssteuerung	3(
9.1	Geschäftsanforderungen an die Zugangsteuerung	
9.2	Benutzerzugangsverwaltung	
9.3 9.4	BenutzerverantwortlichkeitenZugangssteuerung für Systeme und Anwendungen	
10	Kryptographie	
10.1	Kryptographische Maßnahmen	
11	Physische und umgebungsbezogene Sicherheit	
11.1	Sicherheitsbereiche	45
11.2	Geräte und Betriebsmittel	49
12	Betriebssicherheit	55
12.1 12.2	Betriebsabläufe und -verantwortlichkeitenSchutz vor Schadsoftware	
12.3	Datensicherung	
12.4	Protokollierung und Überwachung	
12.5 12.6	Steuerung von Software im Betrieb	
	HANNIANNIN IELININ NEL ALIWALIN PUPU	n-

12.7	Audits von Informationssystemen	67
13	Kommunikationssicherheit	
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	
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
Litera	turhinweise	105