E DIN ISO/IEC 27002:2014-02 (D)

Erscheinungsdatum: 2014-01-10

Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management (ISO/IEC FDIS 27002:2013)

Inhalt

Seite

Nationales Vorwort 4

Nationaler Anhang NA (informativ) Literaturhinweise 5

0 ..... Einleitung 6
0.1 Hintergrund und Zusammenhänge 6
0.2 Anforderungen an Informationssicherheit 7
0.3 Auswahl von Sicherheitsmaßnahmen 7
0.4 Entwicklung eigener Richtlinien 7
0.5 Berücksichtigung von Lebenszyklen 8
0.6 Zugehörige Normen 8

1 Anwendungsbereich 9

2 Normative Verweisungen 9

3 Begriffe 9

4 Aufbau dieser Norm 9
4.1 Abschnitte 9
4.2 Kategorien von Sicherheitsmaßnahmen 10

5 Sicherheitsleitlinien 10
5.1 Managementausrichtung zur 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 Anstellung 18
7.2 Während der Anstellung 20
7.3 Beendigung und Wechsel der Anstellung 22

8 Management von organisationseigenen Werten 23
8.1 Verantwortung für organisationseigene Werte 23
8.2 Klassifizierung von Informationen 25
8.3 Handhabung von Speicher- und Aufzeichnungsmedien 28

9 Zugriffskontrolle 30
9.1 Geschäftliche Anforderungen in Bezug auf die Zugriffskontrolle 30
9.2 Benutzerverwaltung 32
9.3 Benutzerverantwortung 37
9.4 Kontrolle des Zugangs zu Systemen und Anwendungen 38

10 Kryptographie 42
10.1 Kryptographische Maßnahmen 42

11 Schutz vor physischem Zugang und Umwelteinflüssen 44
11.1 Sicherheitsbereiche 44
11.2 Sicherheit von Betriebsmitteln 48

12 Betriebssicherheit 54
12.1 Betriebsverfahren und Zuständigkeiten 54
12.2 Schutz vor Malware 57
12.3 Backup 59
12.4 Protokollierung und Überwachung 60
12.5 Kontrolle von Betriebssoftware 62

12.6 Technisches Schwachstellenmanagement....64
12.7 Auswirkungen von Audits auf Informationssysteme....66

13 Sicherheit in der Kommunikation....67
13.1 Netzwerksicherheitsmanagement....67
13.2 Informationsübertragung....69

14 Anschaffung, Entwicklung und Instandhaltung von Systemen....73
14.1 Sicherheitsanforderungen für Informationssysteme....73
14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen....76
14.3 Prüfdaten....82

15 Lieferantenbeziehungen....82
15.1 Informationssicherheit bei Lieferantenbeziehungen....82
15.2 Management der Dienstleistungserbringung durch Lieferanten....86

16 Management von Informationssicherheitsvorfällen....88
16.1 Management von Informationssicherheitsvorfällen und Verbesserungen....88

17 Informationssicherheitsaspekte des Betriebskontinuitätsmanagements....93
17.1 Aufrechterhaltung der Informationssicherheit....93
17.2 Redundanzen....95

18 Richtlinienkonformität....96
18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen....96
18.2 Informationssicherheitsprüfungen....99

Literaturhinweise....102