DIN EN ISO/IEC 27017:2021-11 (D)

Informationstechnik - Sicherheitsverfahren - Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste (ISO/IEC 27017:2015); Deutsche Fassung EN ISO/IEC 27017:2021

Inhalt

Seite

Europäisches Vorwort 4

Vorwort 5

Einleitung 6

1 Anwendungsbereich 7

2 Normative Verweisungen 7
2.1 Identische Empfehlungen | Internationale Normen 7
2.2 Zusätzliche Verweisungen 7

3 Begriffe und Abkürzungen 7
3.1 An anderer Stelle definierte Begriffe 7
3.2 Abkürzungen 8

4 Für den Cloud-Sektor spezifische Konzepte 8
4.1 Übersicht 8
4.2 Lieferantenbeziehungen bei Cloud-Diensten 9
4.3 Beziehungen zwischen Cloud-Dienstleistungskunden und Cloud-Dienstleistern 9
4.4 Umgang mit Informationssicherheitsrisiken bei Cloud-Diensten 10
4.5 Gliederung dieser Norm 10

5 Informationssicherheitsrichtlinien 11
5.1 Vorgaben der Leitung für Informationssicherheit 11

6 Organisation der Informationssicherheit 12
6.1 Interne Organisation 12
6.2 Mobilgeräte und Telearbeit 14

7 Personalsicherheit 14
7.1 Vor der Beschäftigung 14
7.2 Während der Beschäftigung 14
7.3 Beendigung und Änderung der Beschäftigung 15

8 Verwaltung der Werte 15
8.1 Verantwortlichkeit für Werte 15
8.2 Informationsklassifizierung 16
8.3 Handhabung von Datenträgern 17

9 Zugangssteuerung 17
9.1 Geschäftsanforderungen an die Zugangsteuerung 17
9.2 Benutzerzugangsverwaltung 18
9.3 Benutzerverantwortlichkeiten 20
9.4 Zugangssteuerung für Systeme und Anwendungen 20

10 Kryptographie 21
10.1 Kryptographische Maßnahmen 21

11 Physische und umgebungsbezogene Sicherheit 23
11.1 Sicherheitsbereiche 23
11.2 Geräte und Betriebsmittel 24

12 Betriebssicherheit **25**
12.1 Betriebsabläufe und -verantwortlichkeiten **25**
12.2 Schutz vor Schadsoftware **27**
12.3 Datensicherung **27**
12.4 Protokollierung und Überwachung **28**
12.5 Steuerung von Software im Betrieb **30**
12.6 Handhabung technischer Schwachstellen **30**
12.7 Audit von Informationssystemen **31**

13 Kommunikationssicherheit **31**
13.1 Netzwerksicherheitsmanagement **31**
13.2 Informationsübertragung **32**

14 Anschaffung, Entwicklung und Instandhaltung von Systemen **32**
14.1 Sicherheitsanforderungen an Informationssysteme **32**
14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen **33**
14.3 Testdaten **34**

15 Lieferantenbeziehungen **34**
15.1 Informationssicherheit in Lieferantenbeziehungen **34**
15.2 Steuerung der Dienstleistungserbringung von Lieferanten **36**

16 Handhabung von Informationssicherheitsvorfällen **36**
16.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen **36**

17 Informationssicherheitsaspekte beim Business Continuity Management **39**
17.1 Aufrechterhalten der Informationssicherheit **39**
17.2 Redundanzen **39**

18 Compliance **39**
18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen **39**
18.2 Überprüfungen der Informationssicherheit **41**

Anhang A Erweiterungssatz von Maßnahmen für Cloud-Dienste **43**

Anhang B Verweisungen zum Informationssicherheitsrisiko im Zusammenhang mit Cloud Computing **49**

Literaturhinweise **51**