

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