

# DIN ISO/IEC 27002:2008-09 (D)

## Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management (ISO/IEC 27002:2005)

---

Inhalt	Seite
Nationales Vorwort .....	6
0 Einleitung .....	7
0.1 Was ist Informationssicherheit? .....	7
0.2 Warum ist Informationssicherheit notwendig? .....	7
0.3 Festlegung der Sicherheitsanforderungen .....	8
0.4 Einschätzung der Sicherheitsrisiken .....	8
0.5 Auswahl von Maßnahmen .....	9
0.6 Ausgangspunkt für Informationssicherheit .....	9
0.7 Entscheidende Erfolgsfaktoren .....	10
0.8 Entwicklung eigener Richtlinien .....	11
1 Anwendungsbereich .....	12
2 Begriffe .....	12
3 Aufbau dieser Norm .....	14
3.1 Abschnitte .....	14
3.2 Wesentliche Sicherheitskategorien .....	15
4 Risikoeinschätzung und -behandlung .....	15
4.1 Einschätzung der Sicherheitsrisiken .....	15
4.2 Umgang mit Sicherheitsrisiken .....	16
5 Sicherheitsleitlinie .....	17
5.1 Informationssicherheitsleitlinie .....	17
5.1.1 Leitlinie zur Informationssicherheit .....	17
5.1.2 Überprüfung der Informationssicherheitsleitlinie .....	18
6 Organisation der Informationssicherheit .....	20
6.1 Interne Organisation .....	20
6.1.1 Engagement des Managements für Informationssicherheit .....	20
6.1.2 Koordination der Informationssicherheit .....	22
6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit .....	22
6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen .....	23
6.1.5 Vertraulichkeitsvereinbarungen .....	23
6.1.6 Kontakt zu Behörden .....	24
6.1.7 Kontakt zu speziellen Interessengruppen .....	25
6.1.8 Unabhängige Überprüfung der Informationssicherheit .....	26
6.2 Externe .....	26
6.2.1 Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern .....	27
6.2.2 Adressieren von Sicherheit im Umgang mit Kunden .....	29
6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten .....	30
7 Management von organisationseigenen Werten .....	33
7.1 Verantwortung für organisationseigene Werte (Assets) .....	33
7.1.1 Inventar der organisationseigenen Werte (Assets) .....	33
7.1.2 Eigentum von organisationseigenen Werten (Assets) .....	34
7.1.3 Zulässiger Gebrauch von organisationseigenen Werten (Assets) .....	35
7.2 Klassifizierung von Informationen .....	36
7.2.1 Regelungen für die Klassifizierung .....	36
7.2.2 Kennzeichnung von und Umgang mit Informationen .....	37
8 Personalsicherheit .....	38
8.1 Vor der Anstellung .....	38

8.1.1	Aufgaben und Verantwortlichkeiten .....	38
8.1.2	Überprüfung .....	39
8.1.3	Arbeitsvertragsklauseln .....	40
8.2	Während der Anstellung .....	41
8.2.1	Verantwortung des Managements .....	41
8.2.2	Sensibilisierung, Ausbildung und Schulung für Informationssicherheit .....	42
8.2.3	Disziplinarverfahren .....	43
8.3	Beendigung oder Änderung der Anstellung .....	43
8.3.1	Verantwortlichkeiten bei der Beendigung .....	43
8.3.2	Rückgabe von organisationseigenen Werten .....	44
8.3.3	Zurücknahme von Zugangsrechten .....	45
9	Physische und umgebungsbezogene Sicherheit .....	46
9.1	Sicherheitsbereiche .....	46
9.1.1	Sicherheitszonen .....	46
9.1.2	Zutrittskontrolle .....	47
9.1.3	Sicherung von Büros, Räumen und Einrichtungen .....	48
9.1.4	Schutz vor Bedrohungen von außen und aus der Umgebung .....	48
9.1.5	Arbeiten in Sicherheitszonen .....	48
9.1.6	Öffentlicher Zugang, Anlieferungs- und Ladezonen .....	49
9.2	Sicherheit von Betriebsmitteln .....	50
9.2.1	Platzierung und Schutz von Betriebsmitteln .....	50
9.2.2	Unterstützende Versorgungseinrichtungen .....	51
9.2.3	Sicherheit der Verkabelung .....	52
9.2.4	Instandhaltung von Gerätschaften .....	52
9.2.5	Sicherheit von außerhalb des Standorts befindlicher Ausrüstung .....	53
9.2.6	Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln .....	54
9.2.7	Entfernung von Eigentum .....	54
10	Betriebs- und Kommunikationsmanagement .....	55
10.1	Verfahren und Verantwortlichkeiten .....	55
10.1.1	Dokumentierte Betriebsprozesse .....	55
10.1.2	Änderungsverwaltung .....	56
10.1.3	Aufteilung von Verantwortlichkeiten .....	57
10.1.4	Trennung von Entwicklungs-, Test- und Produktiveinrichtungen .....	57
10.2	Management der Dienstleistungserbringung von Dritten .....	58
10.2.1	Erbringung von Dienstleistungen .....	58
10.2.2	Überwachung und Überprüfung der Dienstleistungen von Dritten .....	59
10.2.3	Management von Änderungen an Dienstleistungen von Dritten .....	60
10.3	Systemplanung und Abnahme .....	60
10.3.1	Kapazitätsplanung .....	61
10.3.2	Systemabnahme .....	61
10.4	Schutz vor Schadsoftware und mobilem Programmcode .....	62
10.4.1	Maßnahmen gegen Schadsoftware .....	62
10.4.2	Schutz vor mobiler Software (mobilen Agenten) .....	64
10.5	Backup .....	64
10.5.1	Backup von Informationen .....	64
10.6	Management der Netzsicherheit .....	66
10.6.1	Maßnahmen für Netze .....	66
10.6.2	Sicherheit von Netzdiensten .....	66
10.7	Handhabung von Speicher- und Aufzeichnungsmedien .....	67
10.7.1	Verwaltung von Wechselmedien .....	67
10.7.2	Entsorgung von Medien .....	68
10.7.3	Umgang mit Informationen .....	69
10.7.4	Sicherheit der Systemdokumentation .....	70
10.8	Austausch von Informationen .....	70
10.8.1	Leitlinien und Verfahren zum Austausch von Informationen .....	70
10.8.2	Vereinbarungen zum Austausch von Informationen .....	72
10.8.3	Transport physischer Medien .....	73
10.8.4	Elektronische Mitteilungen/Nachrichten (Messaging) .....	74
10.8.5	Geschäftsinformationssysteme .....	75
10.9	E-Commerce-Anwendungen .....	76
10.9.1	E-Commerce .....	76

10.9.2	Online-Transaktionen.....	77
10.9.3	Öffentlich verfügbare Informationen.....	78
10.10	Überwachung.....	79
10.10.1	Auditprotokolle.....	79
10.10.2	Überwachung der Systemnutzung.....	80
10.10.3	Schutz von Protokollinformationen.....	82
10.10.4	Administrator- und Betreiberprotokolle.....	82
10.10.5	Fehlerprotokolle.....	83
10.10.6	Zeitsynchronisation.....	83
11	Zugangskontrolle.....	84
11.1	Geschäftsanforderungen für Zugangskontrolle.....	84
11.1.1	Leitlinie zur Zugangskontrolle.....	84
11.2	Benutzerverwaltung.....	86
11.2.1	Benutzerregistrierung.....	86
11.2.2	Verwaltung von Sonderrechten.....	87
11.2.3	Verwaltung von Benutzerpasswörtern.....	88
11.2.4	Überprüfung von Benutzerberechtigungen.....	88
11.3	Benutzerverantwortung.....	89
11.3.1	Passwortverwendung.....	89
11.3.2	Unbeaufsichtigte Benutzerausstattung.....	90
11.3.3	Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms.....	91
11.4	Zugangskontrolle für Netze.....	92
11.4.1	Regelwerk zur Nutzung von Netzdiensten.....	92
11.4.2	Benutzerauthentisierung für externe Verbindungen.....	92
11.4.3	Geräteidentifikation in Netzen.....	93
11.4.4	Schutz der Diagnose- und Konfigurationsports.....	94
11.4.5	Trennung in Netzen.....	94
11.4.6	Kontrolle von Netzverbindungen.....	95
11.4.7	Routingkontrolle für Netze.....	96
11.5	Zugriffskontrolle auf Betriebssysteme.....	97
11.5.1	Verfahren für sichere Anmeldung.....	98
11.5.2	Benutzeridentifikation und Authentisierung.....	99
11.5.3	Systeme zur Verwaltung von Passwörtern.....	100
11.5.4	Verwendung von Systemwerkzeugen.....	101
11.5.5	Session Time-out.....	102
11.5.6	Begrenzung der Verbindungszeit.....	102
11.6	Zugangskontrolle zu Anwendungen und Information.....	103
11.6.1	Einschränkung von Informationszugriffen.....	103
11.6.2	Isolation sensibler Systeme.....	103
11.7	Mobile Computing und Telearbeit.....	104
11.7.1	Mobile Computing und Kommunikation.....	104
11.7.2	Telearbeit.....	106
12	Beschaffung, Entwicklung und Wartung von Informationssystemen.....	107
12.1	Sicherheitsanforderungen von Informationssystemen.....	107
12.1.1	Analyse und Spezifikation von Sicherheitsanforderungen.....	107
12.2	Korrekte Verarbeitung in Anwendungen.....	108
12.2.1	Überprüfung von Eingabedaten.....	108
12.2.2	Kontrolle der internen Verarbeitung.....	109
12.2.3	Integrität von Nachrichten.....	111
12.2.4	Überprüfung von Ausgabedaten.....	111
12.3	Kryptographische Maßnahmen.....	111
12.3.1	Leitlinie zur Anwendung von Kryptographie.....	112
12.3.2	Verwaltung kryptographischer Schlüssel.....	113
12.4	Sicherheit von Systemdateien.....	115
12.4.1	Kontrolle von Software im Betrieb.....	115
12.4.2	Schutz von Test-Daten.....	116
12.4.3	Zugangskontrolle zu Quellcode.....	117
12.5	Sicherheit bei Entwicklungs- und Unterstützungsprozessen.....	118
12.5.1	Änderungskontrollverfahren.....	118
12.5.2	Technische Kontrolle von Anwendungen nach Änderungen am Betriebssystem.....	119
12.5.3	Einschränkung von Änderungen an Softwarepaketen.....	120

12.5.4	Ungewollte Preisgabe von Informationen.....	120
12.5.5	Ausgelagerte Softwareentwicklung.....	121
12.6	Umgang mit Schwachstellen.....	121
12.6.1	Kontrolle technischer Schwachstellen.....	122
13	Umgang mit Informationssicherheitsvorfällen.....	123
13.1	Melden von Informationssicherheitsereignissen und Schwachstellen.....	123
13.1.1	Melden von Informationssicherheitsereignissen.....	123
13.1.2	Melden von Sicherheitsschwachstellen.....	125
13.2	Umgang mit Informationssicherheitsvorfällen und Verbesserungen.....	126
13.2.1	Verantwortlichkeiten und Verfahren.....	126
13.2.2	Lernen von Informationssicherheitsvorfällen.....	127
13.2.3	Sammeln von Beweisen.....	128
14	Sicherstellung des Geschäftsbetriebs (Business Continuity Management).....	129
14.1	Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management).....	129
14.1.1	Einbeziehung der Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs.....	129
14.1.2	Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung.....	130
14.1.3	Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten.....	131
14.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs.....	132
14.1.5	Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs.....	133
15	Einhaltung von Vorgaben (Compliance).....	134
15.1	Einhaltung gesetzlicher Vorgaben.....	135
15.1.1	Identifikation der anwendbaren Gesetze.....	135
15.1.2	Rechte an geistigem Eigentum.....	135
15.1.3	Schutz von organisationseigenen Aufzeichnungen.....	136
15.1.4	Datenschutz und Vertraulichkeit von personenbezogenen Informationen.....	138
15.1.5	Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen.....	138
15.1.6	Leitlinien zu kryptographischen Verfahren.....	139
15.2	Einhaltung von Sicherheitsleitlinien und -standards, und technischer Vorgaben.....	140
15.2.1	Einhaltung von Sicherheitsleitlinien und -standards.....	140
15.2.2	Prüfung der Einhaltung technischer Vorgaben.....	141
15.3	Überlegungen zu Revisionsprüfungen von Informationssystemen.....	142
15.3.1	Maßnahmen für Audits von Informationssystemen.....	142
15.3.2	Schutz von Revisionswerkzeugen für Informationssysteme.....	142
	Literaturhinweise.....	144