

E DIN ISO/IEC 17799:2007-02 (D)

Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management (ISO/IEC 17799:2005)

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	8
0.6 Ausgangspunkt für Informationssicherheit.....	9
0.7 Entscheidende Erfolgsfaktoren	9
0.8 Entwicklung eigener Richtlinien	10
1 Anwendungsbereich	11
2 Begriffe	11
3 Aufbau dieser Norm	13
3.1 Abschnitte	13
3.2 Wesentliche Sicherheitskategorien.....	13
4 Risikoeinschätzung und –behandlung.....	14
4.1 Einschätzung der Sicherheitsrisiken	14
4.2 Umgang mit Sicherheitsrisiken.....	14
5 Sicherheitsleitlinie.....	15
5.1 Informationssicherheitsleitlinie	15
5.1.1 Leitlinie zur Informationssicherheit.....	16
5.1.2 Überprüfung der Informationssicherheitsleitlinie.....	16
6 Organisation der Informationssicherheit.....	18
6.1 Interne Organisation	18
6.1.1 Engagement des Managements für Informationssicherheit.....	18
6.1.2 Koordination der Informationssicherheit.....	19
6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit.....	19
6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen	20
6.1.5 Vertraulichkeitsvereinbarungen	20
6.1.6 Kontakt zu Behörden	21
6.1.7 Kontakt zu speziellen Interessengruppen	21
6.1.8 Unabhängige Überprüfung der Informationssicherheit	22
6.2 Externe	23
6.2.1 Identifizierung von Risiken in Zusammenhang mit Externen.....	23
6.2.2 Adressieren von Sicherheit im Umgang mit Kunden	24
6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten	26
7 Management von organisationseigenen Werte.....	28
7.1 Verantwortung für organisationseigene Werte (Assets).....	28
7.1.1 Inventar der organisationseigenen Werte (Assets)	28
7.1.2 Eigentum von organisationseigenen Werten (Assets).....	29
7.1.3 Zulässiger Gebrauch von organisationseigenen Werten (Assets)	29
7.2 Klassifizierung von Informationen	30
7.2.1 Regelungen für die Klassifizierung	30
7.2.2 Kennzeichnung von und Umgang mit Informationen.....	31
8 Personalsicherheit	32
8.1 Vor der Anstellung	32

8.1.1	Aufgaben und Verantwortlichkeiten	32
8.1.2	Überprüfung	32
8.1.3	Arbeitsvertragsklauseln	33
8.2	Während der Anstellung	34
8.2.1	Verantwortung des Managements	34
8.2.2	Sensibilisierung, Ausbildung und Schulung für Informationssicherheit	35
8.2.3	Disziplinarverfahren	35
8.3	Beendigung oder Änderung der Anstellung	36
8.3.1	Verantwortlichkeiten bei der Beendigung	36
8.3.2	Rückgabe von organisationseigenen Werten	36
8.3.3	Zurücknahme von Zugangsrechten	37
9	Physische und umgebungsbezogene Sicherheit	38
9.1	Sicherheitsbereiche	38
9.1.1	Sicherheitszonen	38
9.1.2	Zutrittskontrolle	39
9.1.3	Sicherung von Büros, Räumen und Einrichtungen	39
9.1.4	Schutz vor Bedrohungen von Außen und aus der Umgebung	40
9.1.5	Arbeiten in Sicherheitszonen	40
9.1.6	Öffentlicher Zugang, Anlieferungs- und Ladezonen	40
9.2	Sicherheit von Betriebsmitteln	41
9.2.1	Platzierung und Schutz von Betriebsmitteln	41
9.2.2	Unterstützende Versorgungseinrichtungen	42
9.2.3	Sicherheit der Verkabelung	42
9.2.4	Instandhaltung von Gerätschaften	43
9.2.5	Sicherheit von außerhalb des Standorts befindlicher Ausrüstung	44
9.2.6	Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln	44
9.2.7	Entfernung von Eigentum	44
10	Betriebs- und Kommunikationsmanagement	45
10.1	Verfahren und Verantwortlichkeiten	45
10.1.1	Dokumentierte Betriebsprozesse	45
10.1.2	Änderungsverwaltung	46
10.1.3	Aufteilung von Verantwortlichkeiten	46
10.1.4	Trennung von Entwicklungs-, Test- und Produktiveinrichtungen	47
10.2	Management der Dienstleistungs-Erbringung von Dritten	48
10.2.1	Erbringung von Dienstleistungen	48
10.2.2	Überwachung und Überprüfung der Dienstleistungen von Dritten	48
10.2.3	Management von Änderungen an Dienstleistungen von Dritten	49
10.3	Systemplanung und Abnahme	50
10.3.1	Kapazitätsplanung	50
10.3.2	System Abnahme	50
10.4	Schutz vor Schadsoftware und mobilem Programmcode	51
10.4.1	Maßnahmen gegen Schadsoftware	51
10.4.2	Schutz vor mobiler Software (mobilen Agenten)	52
10.5	Backup	53
10.5.1	Backup von Informationen	53
10.6	Management der Netzsicherheit	54
10.6.1	Maßnahmen für Netze	54
10.6.2	Sicherheit von Netzdiensten	55
10.7	Handhabung von Speicher- und Aufzeichnungsmedien	55
10.7.1	Verwaltung von Wechselmedien	55
10.7.2	Entsorgung von Medien	56
10.7.3	Umgang mit Informationen	56
10.7.4	Sicherheit der Systemdokumentation	57
10.8	Austausch von Informationen	57
10.8.1	Regelwerke und Verfahren zum Austausch von Informationen	58
10.8.2	Vereinbarungen zum Austausch von Informationen	59
10.8.3	Transport physischer Medien	60
10.8.4	Elektronische Mitteilungen/Nachrichten (Messaging)	60
10.8.5	Geschäftsinformationssysteme	61
10.9	E-Commerce-Anwendungen	62

10.9.1	E-Commerce	62
10.9.2	Online Transaktionen.....	63
10.9.3	Öffentlich verfügbare Informationen.....	63
10.10	Überwachung.....	64
10.10.1	Auditprotokolle.....	64
10.10.2	Überwachung der Systemnutzung	65
10.10.3	Schutz von Protokollinformationen.....	66
10.10.4	Administrator- und Betreiberprotokolle.....	67
10.10.5	Fehlerprotokolle	67
10.10.6	Zeitsynchronisation	68
11	Zugangskontrolle	68
11.1	Geschäftsanforderungen für Zugangskontrolle	68
11.1.1	Regelwerk zur Zugangskontrolle.....	68
11.2	Benutzerverwaltung	69
11.2.1	Benutzerregistrierung.....	69
11.2.2	Verwaltung von Sonderrechten	70
11.2.3	Verwaltung von Benutzerpasswörtern.....	71
11.2.4	Überprüfung von Benutzerberechtigungen.....	71
11.3	Benutzerverantwortung	72
11.3.1	Passwortverwendung	72
11.3.2	Unbeaufsichtigte Benutzerausstattung	73
11.3.3	Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms.....	73
11.4	Zugangskontrolle für Netze	74
11.4.1	Regelwerk zur Nutzung von Netzdiensten.....	74
11.4.2	Benutzerauthentisierung für externe Verbindungen	74
11.4.3	Geräteidentifikation in Netzen.....	75
11.4.4	Schutz der Diagnose- und Konfigurationsports	75
11.4.5	Trennung in Netzen.....	76
11.4.6	Kontrolle von Netzverbindungen.....	77
11.4.7	Routingkontrolle für Netze	77
11.5	Zugriffskontrolle auf Betriebssysteme.....	78
11.5.1	Verfahren für sichere Anmeldung	78
11.5.2	Benutzeridentifikation und Authentisierung	79
11.5.3	Systeme zur Verwaltung von Passwörtern.....	79
11.5.4	Verwendung von Systemwerkzeugen.....	80
11.5.5	Session Time-out.....	81
11.5.6	Begrenzung der Verbindungszeit.....	81
11.6	Zugangskontrolle zu Anwendungen und Information.....	81
11.6.1	Einschränkung von Informationszugriffen	82
11.6.2	Isolation sensibler Systeme	82
11.7	Mobile Computing und Telearbeit	83
11.7.1	Mobile Computing und Kommunikation	83
11.7.2	Telearbeit.....	84
12	Beschaffung, Entwicklung und Wartung von Informationssystemen	85
12.1	Sicherheitsanforderungen von Informationssystemen.....	85
12.1.1	Analyse und Spezifikation von Sicherheitsanforderungen	85
12.2	Korrekte Verarbeitung in Anwendungen	86
12.2.1	Überprüfung von Eingabedaten.....	86
12.2.2	Kontrolle der internen Verarbeitung.....	87
12.2.3	Integrität von Nachrichten.....	88
12.2.4	Überprüfung von Ausgabedaten	88
12.3	Kryptographische Maßnahmen.....	89
12.3.1	Leitlinie zur Anwendung von Kryptographie.....	89
12.3.2	Verwaltung kryptographischer Schlüssel	90
12.4	Sicherheit von Systemdateien	92
12.4.1	Kontrolle von Software im Betrieb	92
	Seite	
12.4.2	Schutz von Test-Daten.....	93
12.4.3	Zugangskontrolle zu Quellcode.....	93
12.5	Sicherheit bei Entwicklungs- und Unterstützungsprozessen	94

12.5.1	Änderungskontrollverfahren	94
12.5.2	Technische Kontrolle von Anwendungen nach Änderungen am Betriebssystem.....	95
12.5.3	Einschränkung von Änderungen an Softwarepaketen.....	96
12.5.4	Ungewollte Preisgabe von Informationen.....	96
12.5.5	Ausgelagerte Softwareentwicklung	97
12.6	Umgang mit Schwachstellen	97
12.6.1	Kontrolle technischer Schwachstellen.....	97
13	Umgang mit Informationssicherheitsvorfällen	99
13.1	Melden von Informationssicherheitsereignissen und Schwachstellen	99
13.1.1	Melden von Informationssicherheitsereignissen	99
13.1.2	Melden von Sicherheitsschwachstellen.....	100
13.2	Umgang mit Informationssicherheitsvorfällen und Verbesserungen	101
13.2.1	Verantwortlichkeiten und Verfahren.....	101
13.2.2	Lernen von Informationssicherheitsvorfällen	102
13.2.3	Sammeln von Beweisen.....	102
14	Sicherstellung des Geschäftsbetriebs (Business Continuity Management).....	104
14.1	Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management).....	104
14.1.1	Einbeziehung der Informationssicherheit in den Prozess zur Sicherstellung des Geschäftsbetriebs.....	104
14.1.2	Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung.....	105
14.1.3	Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten	105
14.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs.....	106
14.1.5	Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung des Geschäftsbetriebs.....	107
15	Einhaltung von Vorgaben (Compliance)	109
15.1	Einhaltung gesetzlicher Vorgaben.....	109
15.1.1	Identifikation der anwendbaren Gesetze.....	109
15.1.2	Rechte an geistigem Eigentum	109
15.1.3	Schutz von organisationseigenen Aufzeichnungen	110
15.1.4	Datenschutz und Vertraulichkeit von personenbezogenen Informationen	111
15.1.5	Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen	112
15.1.6	Regelungen zu kryptographischen Verfahren.....	112
15.2	Einhaltung von Sicherheitsregelungen und -standards, und technischer Vorgaben	113
15.2.1	Einhaltung von Sicherheitsregelungen und -standards.....	113
15.2.2	Prüfung der Einhaltung technischer Vorgaben.....	113
15.3	Überlegungen zu Revisionsprüfungen von Informationssystemen.....	114
15.3.1	Maßnahmen für Audits von Informationssystemen.....	114
15.3.2	Schutz von Revisionswerkzeugen für Informationssysteme.....	115
	Literaturhinweise	116