

E DIN EN ISO/IEC 27010:2020-02 (D/E)

Erscheinungsdatum: 2020-01-17

Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagement für
sektor- und organisationsübergreifende Kommunikation (ISO/IEC 27010:2015);
Deutsche und Englische Fassung prEN ISO/IEC 27010:2020

Information technology - Security techniques - Information security management for
inter-sector and inter-organizational communications (ISO/IEC 27010:2015); German
and English version prEN ISO/IEC 27010:2020

Inhalt	Seite
Europäisches Vorwort.....	5
Vorwort.....	6
Einleitung.....	7
1 Anwendungsbereich.....	8
2 Normative Verweisungen.....	8
3 Begriffe.....	8
4 Begriffe und Erläuterung.....	8
4.1 Einleitung.....	8
4.2 Informationsaustauschende Gemeinschaften.....	9
4.3 Verwaltung von Gemeinschaften.....	9
4.4 Unterstützende Stellen.....	9
4.5 Sektorübergreifende Kommunikation.....	10
4.6 Konformität.....	10
4.7 Kommunikationsmodell.....	11
5 Informationssicherheitsrichtlinien.....	12
5.1 Vorgaben der Leitung für Informationssicherheit.....	12
5.1.1 Informationssicherheitsrichtlinien.....	12
5.1.2 Überprüfung der Informationssicherheitsrichtlinien.....	12
6 Organisation der Informationssicherheit.....	12
7 Personalsicherheit.....	12
7.1 Vor der Beschäftigung.....	12
7.1.1 Sicherheitsüberprüfung.....	12
7.1.2 Beschäftigungs- und Vertragsbedingungen.....	13
7.2 Während der Beschäftigung.....	13
7.3 Beendigung und Änderung der Beschäftigung.....	13
8 Verwaltung der Werte.....	13
8.1 Verantwortlichkeit für Werte.....	13
8.1.1 Inventarisierung der Werte.....	13
8.1.2 Zuständigkeit für Werte.....	13
8.1.3 Zulässiger Gebrauch von Werten.....	13
8.1.4 Rückgabe von Werten.....	13
8.2 Informationsklassifizierung.....	14
8.2.1 Klassifizierung von Informationen.....	14
8.2.2 Kennzeichnung von Informationen.....	14
8.2.3 Handhabung von Werten.....	14
8.3 Handhabung von Datenträgern.....	14
8.4 Schutz des Informationsaustauschs.....	15

8.4.1	Weitergabe von Informationen	15
8.4.2	Haftungsausschluss für Informationen.....	15
8.4.3	Glaubwürdigkeit von Informationen.....	16
8.4.4	Verringerung der Sensibilität von Informationen.....	16
8.4.5	Schutz von anonymen Quellen.....	16
8.4.6	Schutz von anonymen Empfängern	17
8.4.7	Berechtigung zur weiteren Weitergabe.....	17
9	Zugangssteuerung.....	17
10	Kryptographie	18
10.1	Kryptographische Maßnahmen.....	18
10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen	18
10.1.2	Schlüsselverwaltung	18
11	Physische und umgebungsbezogene Sicherheit.....	18
12	Betriebssicherheit	18
12.1	Betriebsabläufe und -verantwortlichkeiten.....	18
12.2	Schutz vor Schadsoftware.....	18
12.2.1	Maßnahmen gegen Schadsoftware.....	18
12.3	Datensicherung.....	18
12.4	Protokollierung und Überwachung.....	19
12.4.1	Ereignisprotokollierung	19
12.4.2	Schutz der Protokollinformation	19
12.4.3	Administratoren- und Bedienerprotokolle	19
12.4.4	Uhrensynchronisation.....	19
12.5	Steuerung von Software im Betrieb	19
12.6	Handhabung technischer Schwachstellen.....	19
12.7	Audits von Informationssystemen.....	19
12.7.1	Maßnahmen für Audits von Informationssystemen	19
12.7.2	Auditberechtigungen in der Gemeinschaft.....	19
13	Kommunikationssicherheit.....	20
13.1	Netzwerksicherheitsmanagement.....	20
13.2	Informationsübertragung	20
13.2.1	Richtlinien und Verfahren für die Informationsübertragung	20
13.2.2	Vereinbarungen zur Informationsübertragung.....	20
13.2.3	Elektronische Nachrichtenübermittlung.....	20
13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen.....	20
14	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	20
15	Lieferantenbeziehungen	21
15.1	Informationssicherheit in Lieferantenbeziehungen	21
15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	21
15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen.....	21
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie.....	21
15.2	Steuerung der Dienstleistungserbringung von Lieferanten	21
16	Handhabung von Informationssicherheitsvorfällen	21
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen.....	21
16.1.1	Verantwortlichkeiten und Verfahren	21
16.1.2	Meldung von Informationssicherheitsereignissen	21
16.1.3	Meldung von Schwächen in der Informationssicherheit.....	22
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	22
16.1.5	Reaktion auf Informationssicherheitsvorfälle	22
16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen.....	22
16.1.7	Sammeln von Beweismaterial.....	22
16.1.8	Frühwarnsystem	23
17	Informationssicherheitsaspekte beim Business Continuity Management.....	23

17.1	Aufrechterhalten der Informationssicherheit.....	23
17.1.1	Planung der Aufrechterhaltung der Informationssicherheit.....	23
17.1.2	Umsetzung der Aufrechterhaltung der Informationssicherheit.....	23
17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit.....	23
17.2	Redundanzen	23
18	Compliance	24
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	24
18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	24
18.1.2	Geistige Eigentumsrechte	24
18.1.3	Schutz von Aufzeichnungen	24
18.1.4	Privatsphäre und Schutz von personenbezogenen Informationen	24
18.1.5	Regelungen bezüglich kryptographischer Maßnahmen.....	24
18.1.6	Haftung gegenüber der informationsaustauschenden Gemeinschaft.....	24
18.2	Überprüfungen der Informationssicherheit.....	25
Anhang A (informativ)	Teilen von sensiblen Informationen.....	26
A.1	Einleitung.....	26
A.2	Herausforderungen	27
A.3	Möglicher Nutzen.....	28
A.4	Anwendbarkeit	28
A.5	Definition und Betrieb einer informationsaustauschenden Gemeinschaft	28
A.6	Vereinbarungen zum Informationsaustausch	30
A.7	Erfolgsfaktoren	31
A.8	Anwendungsbereich des ISMS für eine informationsaustauschende Gemeinschaft.....	31
Anhang B (informativ)	Schaffen von Vertrauen in den Informationsaustausch	32
B.1	Vertrauen in Aussagen.....	32
B.2	Technologische Unterstützung	32
B.2.1	Einleitung.....	32
B.2.2	Anonymität und Pseudoanonymität	33
B.2.3	Reputations-Engines	34
B.3	Beurteilung der Vertrauenswürdigkeit von Informationen	35
Anhang C (informativ)	Das Ampelprotokoll.....	38
Anhang D (informativ)	Modelle für die Organisation einer informationsaustauschenden Gemeinschaft	39
D.1	Einleitung.....	39
D.2	Vertrauenswürdige Einheiten zur Informationsverbreitung (TICE)	39
D.2.1	Einleitung.....	39
D.2.2	Organisatorische Aspekte von TICE	40
D.2.3	Kerndienstleistungen und optionale Dienstleistungen einer TICE	41
D.2.4	Zusammenfassung	42
D.3	Warn-, Hinweis- und Meldestellen.....	42
D.3.1	Einleitung.....	42
D.3.2	Funktionen von WARPs.....	43
D.3.3	WARP-Dienstleistungen.....	43
D.3.4	Vorteile von WARPs.....	44
D.3.5	Zusammenfassung	45
Literaturhinweise		46