

ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN ISO/IEC 27002:2017

Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor

Technologies de l'information -
Techniques de sécurité - Code de bonne
pratique pour le management de la
sécurité de l'information (ISO/IEC

Information technology - Security
techniques - Code of practice for
information security controls (ISO/IEC
27002:2013 including Cor 1:2014 and Cor

02/2017



Nationales Vorwort

Diese Europäische Norm EN ISO/IEC 27002:2017 wurde als luxemburgische Norm ILNAS-EN ISO/IEC 27002:2017 übernommen.

Alle interessierten Personen, welche Mitglied einer luxemburgischen Organisation sind, können sich kostenlos an der Entwicklung von luxemburgischen (ILNAS), europäischen (CEN, CENELEC) und internationalen (ISO, IEC) Normen beteiligen:

- Inhalt der Normen beeinflussen und mitgestalten
- Künftige Entwicklungen vorhersehen
- An Sitzungen der technischen Komitees teilnehmen

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

DIESES WERK IST URHEBERRECHTLICH GESCHÜTZT

Kein Teil dieser Veröffentlichung darf ohne schriftliche Einwilligung weder vervielfältigt noch in sonstiger Weise genutzt werden - sei es elektronisch, mechanisch, durch Fotokopien oder auf andere Art!

Deutsche Fassung

Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015)

Information technology - Security techniques - Code of
practice for information security controls (ISO/IEC
27002:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information - Techniques de sécurité -
Code de bonne pratique pour le management de la
sécurité de l'information (ISO/IEC 27002:2013 y
compris Cor 1:2014 et Cor 2:2015)

Diese Europäische Norm wurde vom CEN am 26. Januar 2017 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

Inhalt

	Seite
Europäisches Vorwort	6
Vorwort	7
0 Einleitung	8
1 Anwendungsbereich.....	11
2 Normative Verweisungen.....	11
3 Begriffe	11
4 Aufbau dieser Norm.....	11
4.1 Abschnitte.....	11
4.2 Maßnahmenkategorien.....	11
5 Informationssicherheitsrichtlinien.....	12
5.1 Vorgaben der Leitung für Informationssicherheit.....	12
5.1.1 Informationssicherheitsrichtlinien.....	12
5.1.2 Überprüfung der Informationssicherheitsrichtlinien	14
6 Organisation der Informationssicherheit	14
6.1 Interne Organisation	14
6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten.....	14
6.1.2 Aufgabentrennung	15
6.1.3 Kontakt mit Behörden	16
6.1.4 Kontakt mit speziellen Interessensgruppen	16
6.1.5 Informationssicherheit im Projektmanagement.....	17
6.2 Mobilgeräte und Telearbeit.....	17
6.2.1 Richtlinie zu Mobilgeräten.....	17
6.2.2 Telearbeit.....	19
7 Personalsicherheit.....	20
7.1 Vor der Beschäftigung.....	20
7.1.1 Sicherheitsüberprüfung.....	20
7.1.2 Beschäftigungs- und Vertragsbedingungen.....	21
7.2 Während der Beschäftigung	22
7.2.1 Verantwortlichkeiten der Leitung.....	22
7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung.....	23
7.2.3 Maßregelungsprozess.....	24
7.3 Beendigung und Änderung der Beschäftigung	25
7.3.1 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung.....	25
8 Verwaltung der Werte	26
8.1 Verantwortlichkeit für Werte	26
8.1.1 Inventarisierung der Werte.....	26
8.1.2 Zuständigkeit für Werte.....	26
8.1.3 Zulässiger Gebrauch von Werten.....	27
8.1.4 Rückgabe von Werten	27
8.2 Informationsklassifizierung.....	28
8.2.1 Klassifizierung von Information	28
8.2.2 Kennzeichnung von Information	29
8.2.3 Handhabung von Werten.....	30

ILNAS-EN ISO/IEC 27002:2017 - Preview only Copy via ILNAS e-Shop

8.3	Handhabung von Datenträgern.....	30
8.3.1	Handhabung von Wechseldatenträgern	30
8.3.2	Entsorgung von Datenträgern	31
8.3.3	Transport von Datenträgern.....	32
9	Zugangssteuerung.....	33
9.1	Geschäftsanforderungen an die Zugangsteuerung	33
9.1.1	Zugangssteuerungsrichtlinie	33
9.1.2	Zugang zu Netzwerken und Netzwerkdiensten.....	34
9.2	Benutzerzugangsverwaltung	35
9.2.1	Registrierung und Deregistrierung von Benutzern.....	35
9.2.2	Zuteilung von Benutzerzugängen.....	36
9.2.3	Verwaltung privilegierter Zugangsrechte.....	36
9.2.4	Verwaltung geheimer Authentisierungsinformation von Benutzern.....	37
9.2.5	Überprüfung von Benutzerzugangsrechten	38
9.2.6	Entzug oder Anpassung von Zugangsrechten	39
9.3	Benutzerverantwortlichkeiten	40
9.3.1	Gebrauch geheimer Authentisierungsinformation	40
9.4	Zugangssteuerung für Systeme und Anwendungen	41
9.4.1	Informationszugangsbeschränkung.....	41
9.4.2	Sichere Anmeldeverfahren	41
9.4.3	System zur Verwaltung von Kennwörtern.....	42
9.4.4	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	43
9.4.5	Zugangssteuerung für Quellcode von Programmen.....	44
10	Kryptographie	45
10.1	Kryptographische Maßnahmen	45
10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen	45
10.1.2	Schlüsselverwaltung	46
11	Physische und umgebungsbezogene Sicherheit	48
11.1	Sicherheitsbereiche.....	48
11.1.1	Physische Sicherheitsperimeter.....	48
11.1.2	Physische Zutrittssteuerung	49
11.1.3	Sichern von Büros, Räumen und Einrichtungen	50
11.1.4	Schutz vor externen und umweltbedingten Bedrohungen	50
11.1.5	Arbeiten in Sicherheitsbereichen.....	50
11.1.6	Anlieferungs- und Ladebereiche.....	51
11.2	Geräte und Betriebsmittel.....	51
11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln.....	51
11.2.2	Versorgungseinrichtungen	52
11.2.3	Sicherheit der Verkabelung.....	53
11.2.4	Instandhaltung von Geräten und Betriebsmitteln	53
11.2.5	Entfernen von Werten	54
11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	55
11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	56
11.2.8	Unbeaufsichtigte Benutzergeräte.....	56
11.2.9	Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren.....	57
12	Betriebssicherheit.....	58
12.1	Betriebsabläufe und -verantwortlichkeiten.....	58
12.1.1	Dokumentierte Betriebsabläufe	58
12.1.2	Änderungssteuerung.....	59
12.1.3	Kapazitätssteuerung	59
12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen.....	60
12.2	Schutz vor Schadsoftware	61
12.2.1	Maßnahmen gegen Schadsoftware	61
12.3	Datensicherung	63

12.3.1	Sicherung von Information	63
12.4	Protokollierung und Überwachung	64
12.4.1	Ereignisprotokollierung	64
12.4.2	Schutz der Protokollinformation.....	65
12.4.3	Administratoren- und Bedienerprotokolle	65
12.4.4	Uhrensynchronisation	66
12.5	Steuerung von Software im Betrieb.....	66
12.5.1	Installation von Software auf Systemen im Betrieb.....	66
12.6	Handhabung technischer Schwachstellen.....	67
12.6.1	Handhabung von technischen Schwachstellen.....	67
12.6.2	Einschränkungen von Softwareinstallation	69
12.7	Audits von Informationssystemen	70
12.7.1	Maßnahmen für Audits von Informationssystemen.....	70
13	Kommunikationssicherheit.....	70
13.1	Netzwerksicherheitsmanagement	70
13.1.1	Netzwerksteuerungsmaßnahmen.....	70
13.1.2	Sicherheit von Netzwerkdiensten	71
13.1.3	Trennung in Netzwerken.....	72
13.2	Informationsübertragung	73
13.2.1	Richtlinien und Verfahren für die Informationsübertragung.....	73
13.2.2	Vereinbarungen zur Informationsübertragung.....	74
13.2.3	Elektronische Nachrichtenübermittlung.....	75
13.2.4	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	75
14	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	77
14.1	Sicherheitsanforderungen an Informationssysteme	77
14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen.....	77
14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	78
14.1.3	Schutz der Transaktionen bei Anwendungsdiensten	79
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen.....	80
14.2.1	Richtlinie für sichere Entwicklung.....	80
14.2.2	Verfahren zur Verwaltung von Systemänderungen	81
14.2.3	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	82
14.2.4	Beschränkung von Änderungen an Softwarepaketen.....	83
14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	83
14.2.6	Sichere Entwicklungsumgebung.....	84
14.2.7	Ausgegliederte Entwicklung.....	85
14.2.8	Testen der Systemsicherheit.....	85
14.2.9	Systemabnahmetest.....	86
14.3	Testdaten.....	86
14.3.1	Schutz von Testdaten	86
15	Lieferantenbeziehungen.....	87
15.1	Informationssicherheit in Lieferantenbeziehungen	87
15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	87
15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen	88
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie.....	89
15.2	Steuerung der Dienstleistungserbringung von Lieferanten.....	91
15.2.1	Überwachung und Überprüfung von Lieferantendienstleistungen.....	91
15.2.2	Handhabung der Änderungen von Lieferantendienstleistungen	92
16	Handhabung von Informationssicherheitsvorfällen.....	93
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen.....	93
16.1.1	Verantwortlichkeiten und Verfahren	93
16.1.2	Meldung von Informationssicherheitsereignissen	94
16.1.3	Meldung von Schwächen in der Informationssicherheit	95
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse.....	95

16.1.5	Reaktion auf Informationssicherheitsvorfälle	95
16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen	96
16.1.7	Sammeln von Beweismaterial	97
17	Informationssicherheitsaspekte beim Business Continuity Management	98
17.1	Aufrechterhalten der Informationssicherheit.....	98
17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit.....	98
17.1.2	Umsetzung der Aufrechterhaltung der Informationssicherheit.....	98
17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit	99
17.2	Redundanzen	100
17.2.1	Verfügbarkeit von informationsverarbeitenden Einrichtungen.....	100
18	Compliance	101
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	101
18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	101
18.1.2	Geistige Eigentumsrechte.....	101
18.1.3	Schutz von Aufzeichnungen	102
18.1.4	Privatsphäre und Schutz von personenbezogener Information.....	103
18.1.5	Regelungen bezüglich kryptographischer Maßnahmen.....	104
18.2	Überprüfungen der Informationssicherheit	104
18.2.1	Unabhängige Überprüfung der Informationssicherheit.....	104
18.2.2	Einhaltung von Sicherheitsrichtlinien und -standards	105
18.2.3	Überprüfung der Einhaltung von technischen Vorgaben	106
	Literaturhinweise.....	107

Europäisches Vorwort

Der Text von ISO/IEC 27002:2013 + Cor. 1:2014 + Cor. 2:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 27002:2017 übernommen.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis August 2017, und etwaige entgegenstehende nationale Normen müssen bis August 2017 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27002:2013 + Cor. 1:2014 + Cor. 2:2015 wurde von CEN als EN ISO/IEC 27002:2017 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Regeln nach ISO/IEC Direktive, Teil 2 erarbeitet.

ISO/IEC 27002 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“, Unterkomitee SC 27 „IT Security techniques“, erarbeitet.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 27002:2005), welche technisch überarbeitet wurde.