E DIN EN 16495:2018-07 (D/E)

Erscheinungsdatum: 2018-06-08

Flugverkehrsmanagement - Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt; Deutsche und Englische Fassung prEN 16495:2018

Air Traffic Management - Information security for organisations supporting civil aviation operations; German and English version prEN 16495:2018

Inhalt	Seite
Europäisches Vorwort.....	6
Einleitung	7
1 Anwendungsbereich.....	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Informationssicherheitsmanagement in der Luftfahrt.....	9
4.1 Aufbau dieser Europäischen Norm.....	9
4.2 Auf ISO/IEC 27001:2013 bezogene luftverkehrsspezifische Anforderungen.....	9
5 Informationssicherheitsleitlinien.....	10
5.1 Managementausrichtung zur Informationssicherheit.....	10
5.1.1 Informationssicherheitsleitlinien.....	10
5.1.2 Überprüfung der Informationssicherheitsrichtlinien.....	10
6 Organisation der Informationssicherheit	11
6.1 Interne Organisation	11
6.1.1 Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit	11
6.1.2 Aufgabentrennung	11
6.1.3 Kontakt zu Behörden	11
6.1.4 Kontakt mit Interessengruppen	11
6.1.5 Informationssicherheit im Projektmanagement.....	12
6.2 Mobilgeräte und Telearbeit	12
7 Personalsicherheit.....	12
7.1 Vor der Anstellung	12
7.1.1 Überprüfung.....	12
7.1.2 Arbeitsvertragsklauseln	12
7.2 Während der Anstellung.....	12
7.2.1 Verantwortung des Managements.....	12
7.2.2 Sensibilisierung, Aus- und Weiterbildung zur Informationssicherheit	12
7.2.3 Disziplinarverfahren.....	13
7.3 Beendigung und Wechsel der Anstellung.....	13
8 Management von organisationseigenen Werten	13
8.1 Verantwortung für organisationseigene Werte	13
8.1.1 Inventar der organisationseigenen Werte.....	13
8.1.2 Eigentum von organisationseigenen Werten.....	13
8.1.3 Zulässiger Gebrauch von organisationseigenen Werten.....	13
8.1.4 Rückgabe von organisationseigenen Werten.....	13
8.2 Klassifizierung von Informationen.....	13
8.2.1 Klassifizierung von Informationen.....	13
8.2.2 Kennzeichnung von Informationen.....	14
8.2.3 Handhabung von organisationseigenen Werten.....	14
8.3 Handhabung von Speicher- und Aufzeichnungsmedien.....	14

9	Zugangskontrolle	14
9.1	Geschäftsanforderungen für Zugangskontrolle	14
9.2	Benutzerverwaltung	14
9.2.1	An- und Abmeldung von Benutzern	14
9.2.2	Zugangsbereitstellung für Benutzer	15
9.2.3	Verwaltung von Sonderzugangsrechten	15
9.2.4	Verwaltung geheimer Authentisierungsdaten von Benutzern.....	15
9.2.5	Überprüfung von Benutzerberechtigungen	15
9.2.6	Entziehung oder Anpassung von Zugangsrechten.....	15
9.2.7	Digitales Identitätsmanagement.....	15
9.2.8	Organisationsübergreifende eindeutige Darstellung von Entitäten	16
9.3	Benutzerverantwortung	16
9.4	Kontrolle des Zugangs zu Systemen und Anwendungen	16
9.4.1	Einschränkung von Informationszugriffen.....	16
9.4.2	Verfahren für sichere Anmeldung	16
9.4.3	Systeme zur Verwaltung von Passwörtern	17
9.4.4	Verwendung von Systemwerkzeugen.....	17
9.4.5	Zugangskontrolle zum Programmquellcode.....	17
9.4.6	Web Application Firewalls	17
10	Kryptografie.....	17
10.1	Kryptografische Maßnahmen	17
10.1.1	Leitlinie für die Anwendung kryptografischer Maßnahmen	17
10.1.2	Verwaltung kryptografischer Schlüssel.....	18
11	Physische und umgebungsbezogene Sicherheit.....	18
11.1	Sicherheitsbereiche.....	18
11.1.1	Physische Sicherheitszonen.....	18
11.1.2	Physische Zutrittskontrollen.....	18
11.1.3	Sicherung von Büros, Räumen und Einrichtungen.....	18
11.1.4	Schutz vor Bedrohungen von außen und aus der Umgebung.....	18
11.1.5	Arbeiten in Sicherheitsbereichen	18
11.1.6	Anlieferungs- und Ladezonen	19
11.2	Betriebsmittel	19
11.2.1	Platzierung und Schutz von Betriebsmitteln	19
11.2.2	Unterstützende Versorgungseinrichtungen.....	19
11.2.3	Sicherheit der Verkabelung.....	19
11.2.4	Instandhaltung von Gerätschaften	19
11.2.5	Entfernung von Werten	19
11.2.6	Sicherheit von Betriebsmitteln und Werten außerhalb der Betriebsgebäude.....	19
11.2.7	Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln	19
11.2.8	Unbeaufsichtigte Benutzerausstattung.....	19
11.2.9	Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms.....	19
12	Betriebssicherheit	20
12.1	Betriebliche Verfahren und Verantwortlichkeiten.....	20
12.2	Schutz vor Malware	20
12.3	Backup	20
12.3.1	Datensicherungen	20
12.4	Protokollierung und Überwachung.....	20
12.4.1	Ereignisprotokollierung	20
12.4.2	Schutz von Protokollinformationen.....	20
12.4.3	Administrator- und Betreiberprotokolle	20
12.4.4	Zeitsynchronisierung.....	20
12.5	Kontrolle von Software im Betrieb.....	20
12.6	Umgang mit technischen Schwachstellen.....	20
12.7	Überlegungen zu Audits von Informationssystemen	21
13	Sicherheit in der Kommunikation	21
13.1	Management der Netzsicherheit	21

13.1.1	Maßnahmen für Netze	21
13.1.2	Sicherheit von Netzdiensten	21
13.1.3	Trennung in Netzwerken	21
13.2	Informationsübertragung	21
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	21
14.1	Sicherheitsanforderungen von Informationssystemen	21
14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen	21
14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzen	22
14.1.3	Schutz von Transaktionen im Zusammenhang mit Anwendungsdiensten	22
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	22
14.2.1	Leitlinie für sichere Entwicklung	22
14.2.2	Änderungskontrollverfahren	22
14.2.3	Technische Prüfung von Anwendungen nach Wechseln der Betriebsplattform	22
14.2.4	Einschränkung von Änderungen an Softwarepaketen	22
14.2.5	Leitlinien zur sicheren Systementwicklung	22
14.2.6	Sichere Entwicklungsumgebung	22
14.2.7	Ausgelagerte Entwicklung	22
14.2.8	Systemsicherheitsprüfungen	22
14.2.9	Systemabnahmeprüfung	23
14.3	Prüfdaten	23
15	Lieferantenbeziehungen	23
15.1	Informationssicherheit bei Lieferantenbeziehungen	23
15.1.1	Informationssicherheitsleitlinie für Lieferantenbeziehungen	23
15.1.2	Sicherheitsthemen in Lieferantenverträgen	23
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie	23
15.2	Management der Dienstleistungserbringung durch Lieferanten	23
16	Umgang mit Informationssicherheitsvorfällen	24
16.1	Umgang mit Informationssicherheitsvorfällen und Verbesserungen	24
16.1.1	Verantwortlichkeiten und Verfahren	24
16.1.2	Melden von Informationssicherheitsereignissen	24
16.1.3	Meldung von Informationssicherheitschwachstellen	24
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	24
16.1.5	Reaktion auf Informationssicherheitsvorfälle	24
16.1.6	Lernen von Informationssicherheitsvorfällen	25
16.1.7	Sammeln von Beweisen	25
17	Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs	25
17.1	Aufrechterhaltung der Informationssicherheit	25
17.1.1	Planung der Aufrechterhaltung der Informationssicherheit	25
17.1.2	Implementierung von Verfahren zur Aufrechterhaltung der Informationssicherheit	26
17.1.3	Überprüfung, Überarbeitung und Auswertung von Maßnahmen zur Aufrechterhaltung der Informationssicherheit	26
17.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs	26
17.2	Redundanzen	26
18	Einhaltung von Vorgaben	27
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	27
18.1.1	Feststellung anwendbarer Gesetze und vertraglicher Anforderungen	27
18.1.2	Rechte an geistigem Eigentum	27
18.1.3	Schutz von Aufzeichnungen	27
18.1.4	Privatsphäre und Schutz von personenbezogenen Informationen	27
18.1.5	Leitlinien zu kryptografischen Maßnahmen	27
18.2	Informationssicherheitsprüfungen	27
18.2.1	Unabhängige Überprüfung der Informationssicherheit	27
18.2.2	Einhaltung von Sicherheitsleitlinien und -standards	27
18.2.3	Technische Konformitätsprüfung	27
Anhang A (informativ) Zusätzliche, auf das Flugverkehrsmanagement bezogene Anleitung		28

A.1	Bewertung von Informationssicherheitsrisiken.....	28
A.1.1	Internes Informationssicherheitsrisiko-Management	28
A.2	Probleme der Interoperabilität von Risikobewertungen	32
A.2.1	Allgemeines.....	32
A.2.2	Management der Informationssicherheit für mehrere Organisationen	32
A.2.3	Anpassung des Sicherheits- und Sicherheitsrisikomanagements.....	33
A.3	Auswahl von Maßnahmen	33
A.4	Vertrauensstufen	33
A.4.1	Einleitung.....	33
A.4.2	Skala der Vertrauensstufen	34
A.4.3	Klassifizierungskriterien.....	35
A.5	Bericht über die Anwendbarkeit.....	35
A.6	Messung und Auditierung der Sicherheit.....	35
Anhang B (informativ) Beispiele für die Umsetzung.....		36
B.1	Allgemeines.....	36
B.2	Sicherheit von Informationen in Webanwendungen und Webdiensten (LoT-A-WEB)	37
B.2.1	Allgemeines.....	37
B.2.2	Parameter für die Vertrauensstufe einer Webanwendung/eines Webdienstes	37
B.2.3	Ermittlung der Vertrauensstufe der Webanwendung/des Webdienstes (LoT-A-WEB)	37
B.2.4	Folgen.....	38
B.3	Organisationsübergreifende Verbindungen/externe Verbindungen (LoT-A-NET)	39
B.3.1	Ermittlung der notwendigen Schutzmaßnahmen	39
B.3.2	Auswirkungen der Kopplung von Netzwerken	44
B.4	Zertifikate/Public-Key-Infrastruktur (LoT-A-PKI)	45
B.4.1	Parameter für die Vertrauensstufe des Zertifikatsmanagements	45
B.4.2	Ermittlung der Vertrauensstufe des Zertifikatsmanagements (LoT-A-PKI).....	45
B.4.3	Auswirkungen: Anerkennung von Zertifikaten/PKI	45
B.5	Identitätsmanagement (LoT-A-IDM)	46
B.5.1	Parameter für die Bestimmung der Vertrauensstufe des Identitätsmanagements	46
B.5.2	Ermittlung der Vertrauensstufe des Identitätsmanagements (LoT-A-IDM)	46
B.5.3	Auswirkungen: Anerkennung von Identitäten	47
Anhang C (informativ) Vertrauensstufe — Beispiel für die Umsetzung		48
Anhang D (informativ) Anwendung von Maßnahmen in einer Kontrollübersicht — Beispiel für die Umsetzung.....		64
Literaturhinweise		69