Informationssicherheitsrichtlinie für Betreiber und Entwickler von IT-Systemen (ISEC-Richtlinie BE)

- Lizenzfrei -

(Diese Richtlinie enthält lediglich die Überschriften der geforderten Controls ohne Umsetzungsmaßnahmen. Die vollständige Richtlinie erhalten Sie, wenn Sie eine gültige Lizenz für die DIN EN ISO/IEC 27001/2 Normreihe besitzen)

V1.01

Verantwortlich: Informationssicherheitsbeauftragter der FMG (Alexander Cmarits)

Vertraulichkeit: Dienstlich

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Änderungsverzeichnis

Version	Datum	Status	Änderungen
V1.0	01.07.2019	Final	Erstellung ISEC-Richtlinie BE auf Basis CoPiP 3.2, Abgleich mit ISO 27001 und ISO 27002; Integration der FMG-Konzern-spezifischen Vorgaben aus ITSS-B und ITSS-E
V1.01	01.08.2020	Final	Diverse kleinere Anpassungen

Mitgeltende Dokumente

Dokument	Speicherort/Veröffentlichung
Begriffe und Abkürzungen des FMG-Konzerns zur Informationssicherheit (Glossar)	eMotion
Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen	eMotion
Richtlinie für die sichere Nutzung von Informations- und Kommunikationssystemen im FMG Konzern	eMotion
ISEC-Richtlinie für Extern & Ausschreibungen	eMotion
Meldung von Abweichungen zur ISEC-Richtlinie BE	eMotion

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Inhalt

© Flughafen München

Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

0 Einleitung

Die vorliegende Informationssicherheitsrichtlinie (ISEC-Richtlinie) des FMG-Konzerns für Betreiber und Entwickler von IT-Systemen (ISEC-Richtlinie BE) basiert auf dem Informationssicherheits-Standard des Bundesverbandes der deutschen Luftverkehrswirtschaft (BDL), Arbeitsgruppe Informationssicherheit (Code of Practice in Practice V3.2. (CoPiP)), sowie der darin referenzierten aktuellsten ISO 27xxx Standards.

Die Schreibweisen der Informationssicherheits-Begriffe in diesem Dokument orientieren sich an der Schreibweise der Standards ISO 27001 und ISO 27002 und können daher von der bekannten und üblicherweise verwendeten Schreibweise im FMG-Konzern abweichen.

1 Anwendungsbereich

1.1 Zielsetzung

Die ISEC-Richtlinie BE des FMG-Konzerns definiert verbindliche Sicherheits-Mindestvorgaben für die Entwicklung, die Einführung, den Betrieb, die Außerbetriebnahme und die Entsorgung von informationsverarbeitenden Systemen im FMG-Konzern. Bei kritischen Geschäftsprozessen sind gegebenenfalls zusätzliche Maßnahmen zu ergreifen.
Die ISEC-Richtlinie BE ist Bestandteil des FMG-Konzern-Informationssicherheitsrahmenwerks (ISEC-Framework), aus dessen Vorgaben Sicherheitskonzepte und -maßnahmen so abgeleitet werden, dass stets ein angemessener Schutz gewährleistet ist.
Die ISEC-Richtlinie BE beschreibt nicht die Umsetzung der Sicherheits-Mindestvorgaben. Diese muss jeweils projekt- bzw. bereichsspezifisch erarbeitet werden.
Neben der vorliegenden „ISEC-Richtlinie BE“ existiert für die Beauftragung von externen Systemen das Dokument „ISEC-Richtlinie für Externe & Ausschreibungen“ (ITSS-X).

1.2 Geltungsbereich und Gültigkeit

Die ISEC-Richtlinie BE gilt verbindlich und ortsunabhängig für alle Bereiche und Beteiligungsgesellschaften des FMG-Konzerns und für Auftraggeber sowie Auftragnehmer, die direkt oder indirekt bei der Entwicklung, der Einführung, dem Betrieb sowie der Außerbetriebnahme und Entsorgung von Anwendungen und informationsverarbeitenden Systemen im FMG-Konzern beteiligt sind.
Als Entwicklung ist die systematische Herstellung von Computerprogrammen (Software) definiert. Im Gegensatz zur reinen Programmierung beinhaltet die Entwicklung den gesamten Softwareentwicklungsprozess. Neben der eigentlichen Programmierarbeit gehört dazu auch das Erarbeiten der Anforderungen an die Software sowie das Erstellen einer sicheren Softwarearchitektur und die Planung der Umsetzung.
Die ISEC-Richtlinie BE gilt somit auch für die Neuentwicklung und Änderung von Software-Anwendungen und informationsverarbeitenden Systemen, die im Auftrag des FMG-Konzerns sowie dessen Beteiligungsgesellschaften entwickelt werden. Dies gilt analog auch für die Anpassung von Standard-Softwareprodukten.
Die vorliegende ISEC-Richtlinie BE tritt mit Wirkung zum 01.08.2020 in Kraft und ist verbindlich für alle ab diesem Zeitpunkt neu eingeführten IT-Systeme/Anwendungen einzuhalten.
Für zum Stichtag bereits im Einsatz bzw. in Realisierung befindliche IT-Systeme/Anwendungen sind die Vorgaben nicht verpflichtend, sollten aber soweit wie möglich berücksichtigt werden.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

1.3 Rollen und Verantwortlichkeiten

FMG-Informationssicherheitsbeauftragter

Die ISEC-Richtlinie BE wird vom FMG-Konzern ISEC-Beauftragten erarbeitet und in Kraft gesetzt. Er wird im Intranet des FMG-Konzerns veröffentlicht. Die ISEC-Richtlinie BE wird jährlich oder bei Bedarf überprüft und den aktuellen organisatorischen Bedingungen, neuen IT-Entwicklungen und Bedrohungen der Informationssicherheit angepasst.
Die Rollen des ISEC-Managements des FMG-Konzerns sind in der Informationssicherheitsleitlinie (ISEC-Leitlinie) beschrieben. Eine wichtige Rolle hier ist die Rolle Information Security Assurance.

Information Security Assurance

Zur ISEC-Richtlinie BE können durch Information Security Assurance noch zusätzliche technische Vorgaben erstellt werden. Die security relevanten Logfiles werden durch Information Security Assurance analysiert.

Auftraggeber und Betreiber

Zusätzliche Rollen innerhalb der ISEC-Richtlinie BE sind die des Auftraggebers und des Betreibers. Mit dem Begriff „Betreiber" sind alle Betreiber (operativer Betrieb) von Informationssystemen gemeint. Mit dem Begriff „Auftraggeber" ist der für ein System Verantwortliche gemeint. Im Sinne der ISEC-Richtlinie BE ist dies der Unternehmensteil, der das System in Auftrag gegeben hat, selbst betreibt oder durch einen Dritten betreiben lässt.
Der Auftraggeber hat dafür zu sorgen, dass die Einhaltung der ISEC-Richtlinie BE durch ihn oder die von ihm beauftragten Betreiber sichergestellt ist. Das beinhaltet, dass die vom Betreiber zu gewährleistenden ISEC-Regelungen vertraglich klar fixiert sind.
Innerhalb des betreffenden Unternehmensteils (Auftraggeber) tragen die personalverantwortlichen Führungskräfte die Verantwortung für die Einhaltung der ISEC-Richtlinie BE.

Informationsverantwortlicher

Der Informationsverantwortliche ist verantwortlich für die Klassifizierung von Informationen in seinem Verantwortungsbereich (siehe hierzu: "Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen"). Typischerweise gehört er der ersten oder zweiten Führungsebene an oder hat bereichsübergreifende Aufgaben (z.B. Revision, Beihilfe, ISEC-Beauftragter, Arbeitsschutz, Datenschutz). Bei Aufgaben- und Funktionsänderungen passt er die Berechtigungen entsprechend an. Die Verantwortlichkeit zur Klassifizierung von Informationen kann durch ihn auch an andere Mitarbeiter delegiert werden

Projekt-/Produktverantwortlichen

Der Projekt-/Produktverantwortliche ist verantwortlich für die Umsetzung der Vorgaben der ISEC-Richtlinie BE bei der Entwicklung, Einführung, Änderung sowie Aussonderung und Entsorgung von IT-Systemen sowie Anwendungen/Software.

1.4 Ausnahmeregelung

Abweichungen von der ISEC-Richtlinie BE sind durch den Auftraggeber bzw. durch den Betreiber oder Projekt-/Produktverantwortlichen, soweit vertraglich in seiner Verantwortung, beim FMG-Konzern-ISEC-Beauftragten mit Angabe von Gründen schriftlich mit dem bereitgestellten Formular zu melden.
Können einzelne Regeln der ISEC-Richtlinie BE nachweislich technisch nicht realisiert werden (z.B. Virenschutz auf Switches), so kann auf diese Meldungen verzichtet werden.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

1.5 Überwachung

Die Umsetzung der ISEC-Richtlinie BE wird stichprobenartig in Form von Audits durch den ISEC-Beauftragten des FMG-Konzerns überprüft.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

2 Referenzen

Die folgenden Empfehlungen und internationalen Standards enthalten Bestimmungen, die – soweit auf sie im vorliegenden Standard referenziert wird – anwendbare Bestimmungen dieses Standards sind.

- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management.
- ISO/IEC 27005:2018
- BDL B3S Branchenspezifischer Sicherheitsstandard im Luftverkehr, Version 1.20, 2019 (eingereicht)
- CoPiP 3.2, Version 2019

3 Begriffe & Abkürzungen

Hier wird auf das eigenständige Dokument **„Begriffe & Abkürzungen des FMG-Konzerns zur Informationssicherheit“** verwiesen sowie auf ISO/IEC 27000.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

4 Informationssicherheitsmanagement in der Luftfahrt

4.1 Struktur dieses Standards und Anwendungen dieses Standards

Dieser Standard ist gemäß der CoPiP Version 3.2 sowie der ISO/IEC 27002 aufgebaut.

- Maßnahmen aus dem CoPiP Version 3.2 bzw. der ISO/IEC 27002, soweit sie für diesen Standard zutreffen, sind im vorliegenden Standard schwarz markiert und müssen durch geeignete Verfahren erfüllt werden.
- Ergänzende Maßnahmen/Anforderungen zu den in der ISO/IEC 27002 genannten Maßnahmen, die spezifisch für den FMG Konzern gelten, sind im vorliegenden Standard blau markiert und sind als Mindestanforderungen einzuhalten.
- Ergänzende luftfahrtspezifische Maßnahmen gemäß CoPiP 3.2 (BDL), sind im vorliegenden Standard grün markiert und müssen für KRITIS-relevante Systeme als Mindestanforderungen eingehalten werden.

4.2 Analyse & Bewertung von Informationssicherheitsrisiken (ISEC-Risiken)

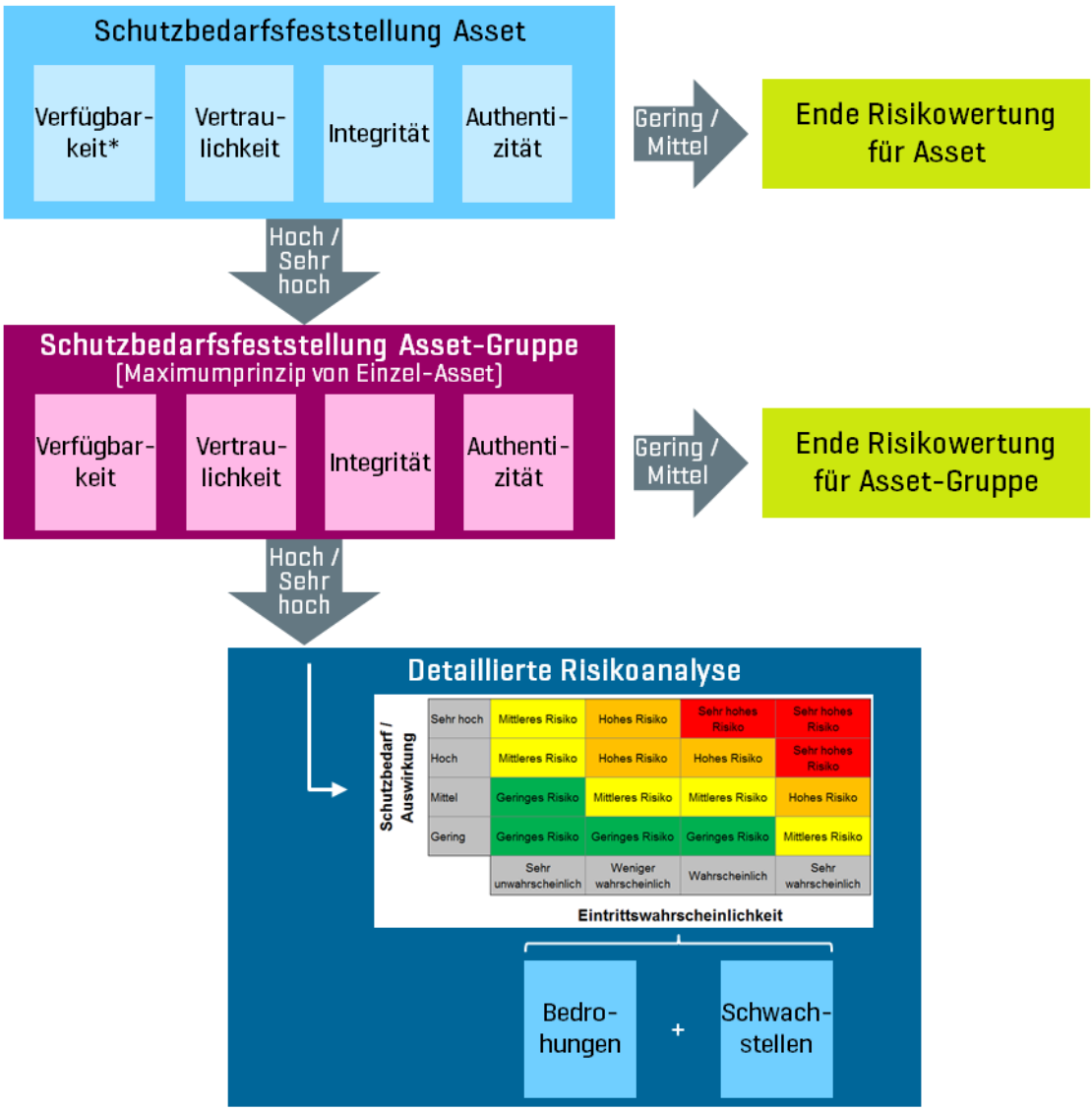
4.2.1 Einführung Informationssicherheitsrisikomanagement (ISEC-Risikomanagement)

Die in ISO/IEC 27002 Kapitel 4 aufgeführten Maßnahmenziele und Inhalte sollten entsprechend angewendet werden. Das ISEC-Risikomanagement sollte gemäß ISO/IEC 27005 erfolgen.
Beim ISEC-Risikomanagement sollten alle Assets (Informationen, Anwendungen, Systeme) berücksichtigt werden.

4.2.2 Anwendung ISEC-Risikomanagement

Grundlegende Vorgehensweise
Das ISEC-Risikomanagement beim FMG-Konzern wird entsprechend der nachstehenden Vorgehensweise durchgeführt:

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion



*) einschließlich maximal hinnehmbare Zeitspanne für Datenverlust (RPO) und maximal tolerierbare Ausfallzeit

Die Dokumentation erfolgt mit Hilfe des aktuell beim FMG-Konzern freigegebenen und veröffentlichten Tools für ISEC-Risikomanagement.
Im Rahmen der Risikobewertung werden folgende Aktivitäten durchgeführt:

Schritt 1: Schutzbedarfsfeststellung Asset
Für ein ausgewähltes Asset wird der Schutzbedarf anhand der Informationssicherheitsaspekte mit vordefinierten Abstufungen bestimmt. Diese Aspekte sind:

a) **Verfügbarkeit**: Sicherstellung, dass Daten und Systeme präsent und innerhalb einer definierten Zeit nutzbar sind.
   Die **maximal tolerierbare Ausfallzeit (MTA)** gibt den Zeitraum an, innerhalb dessen bei einem Ausfall die betroffenen Systeme wieder in einem funktionsfähigen Zustand sein müssen.
   Mit der Definition der **maximal hinnehmbaren Zeitspanne für Datenverlust (RPO)** wird festgelegt, für welchen zurückliegenden Zeitraum Daten bei einem Ausfall unwiederbringlich verloren sein dürfen, d.h. in welchem Intervall Backups der Daten erfolgen müssen.
b) **Vertraulichkeit**: Sicherstellung, dass Systeme und Daten nur für berechtigte Personen zugänglich/einsehbar sind.
c) **Integrität**: Sicherstellung, dass Systeme und Daten vollständig und richtig zur Verfügung stehen.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

d) **Authentizität**: Sicherstellung, dass die Datenherkunft nachgewiesen werden kann und die Glaubwürdigkeit der Daten gesichert ist.

Der Gesamt-Schutzbedarf des Assets wird dabei vom höchsten Wert eines Aspektes bestimmt (Maximumprinzip).
Die Einstufung erfolgt anhand folgender Kriterien:

Aspekt	Gering	Mittel	Hoch	Sehr hoch
Verfügbarkeit	Gering	Mittel	Hoch	Sehr hoch
Vertraulichkeit	Offen	Dienstlich	Vertraulich	Streng vertraulich
Integrität	n/a	Normal	Hoch	n/a
Authentizität	n/a	Normal	Hoch	n/a

Sofern als maximaler Wert für den Schutzbedarf Gering oder Mittel ermittelt wurde, kann auf eine weitergehende Schutzbedarfsfeststellung des Assets bzw. im nächsten Schritt auf eine detaillierte Risikoanalyse verzichtet werden.

Schritt 2: Schutzbedarfsfeststellung Asset-Gruppe

Dieser Schritt soll dabei helfen, Assets mit identischem Schutzbedarf bzw. vergleichbaren Bedrohungen als Asset-Gruppe zusammenzufassen. Der Schutzbedarf für die Asset-Gruppe ergibt sich aus dem jeweils höchsten Wert eines darin enthaltenen Assets (Maximumprinzip). Die Gruppierung kann auch dazu führen, dass der Schutzbedarf für die Asset-Gruppe höher ist als für die einzelnen Assets.
Für die Einstufung der unterschiedlichen Aspekte kommen dieselben Werte wie bei
Schritt 1 (siehe vorstehende Tabelle) zum Einsatz.
Sofern für eine Asset-Gruppe ein Schutzbedarf Gering oder Mittel festgestellt wurde, kann auf eine detaillierte Risikoanalyse für diese Asset-Gruppe verzichtet werden. Sofern der Gesamt-Schutzbedarf jedoch bei Hoch oder Sehr hoch liegt, muss eine detaillierte Risikoanalyse gemäß Schritt 3 erfolgen.

Schritt 3: Identifikation Umsetzung erforderliche Sicherheitsmaßnahmen

Die vorgeschriebenen – insbesondere in der vorliegenden Richtlinie aufgestellten – Sicherheitsmaßnahmen stellen grundsätzlich ein ausreichendes Sicherheitsniveau zur Gewährleistung des jeweiligen Schutzbedarfs dar. Aus diesem Grund ist in diesem Schritt festzustellen, inwieweit die Vorgaben umgesetzt sind bzw. eingehalten werden und wo ggf. noch Handlungsbedarf besteht.
Dabei können folgende Konstellationen als ausreichend im Sinne eines angemessenen Schutzes hinsichtlich Informationssicherheit betrachtet werden:

- Für das Asset/die Asset-Gruppe wurden alle Sicherheitsmaßnahmen gemäß den aktuellen Vorgaben unter Berücksichtigung des Schutzbedarfs umgesetzt bzw. werden eingehalten.
- Für nicht umgesetzte Sicherheitsmaßnahmen gemäß den aktuellen Vorgaben existiert eine gültige Ausnahmegenehmigung.

Sofern keine der beiden Konstellationen zutrifft, muss für das betreffende Asset/die Asset-Gruppe eine detaillierte Risikoanalyse durchgeführt werden, um eine Identifikation der bestehenden Risiken zu gewährleisten.

Schritt 4: Detaillierte Risikoanalyse

Der in Schritt 1 bzw. 2 ermittelte Schutzbedarf entspricht dem potenziellen Schaden und damit der Y-Achse der Informationssicherheitsrisikomatrix. Im Rahmen der detaillierten Risikoanalyse muss der Wert der X-Achse, der sogenannten Eintrittswahrscheinlichkeit, einer Kombination aus Bedrohung und Schwachstelle möglicher Szenarien bestimmt werden.
Dabei werden zunächst die für das betreffende Asset relevanten Bedrohungen aus folgenden Kategorien ausgewählt:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

- Technisches Versagen
- Vorsätzliche Handlungen

Die Bedrohungen sind anhand der allgemeinen Gegebenheiten (wie häufig/verbreitet ist sie) und der FMG-Konzern-spezifischen Exponiertheit (besonderes „Ziel" aufgrund z.B. geografischer Gegebenheiten, Geschäftstätigkeit etc.) mit einer Wahrscheinlichkeit zu bestimmen.
Zu den Bedrohungen gilt es, jeweils eine oder mehrere Schwachstellen, also mögliche konkrete Verwundbarkeiten, zu identifizieren und unter Berücksichtigung existierender oder eben nicht existierender Sicherheitsmaßnahmen mit einem Wert für die Ausnutzbarkeit zu versehen.
Aus der Kombination der Bedrohung und Schwachstelle ergibt sich gemäß nachfolgender Matrix die potenzielle Eintrittswahrscheinlichkeit:

Ausnutzbarkeit Schwachstelle	Nicht vorhanden	Sehr selten	Selten	Häufig/regelmäßig	Permanent
Sehr leicht	sehr unwahrscheinlich	weniger wahrscheinlich	wahrscheinlich	sehr wahrscheinlich	sehr wahrscheinlich
Leicht	sehr unwahrscheinlich	weniger wahrscheinlich	weniger wahrscheinlich	wahrscheinlich	sehr wahrscheinlich
Schwierig	sehr unwahrscheinlich	sehr unwahrscheinlich	weniger wahrscheinlich	weniger wahrscheinlich	wahrscheinlich
Sehr schwierig	sehr unwahrscheinlich	sehr unwahrscheinlich	sehr unwahrscheinlich	weniger wahrscheinlich	weniger wahrscheinlich
Nicht vorhanden	sehr unwahrscheinlich	sehr unwahrscheinlich	sehr unwahrscheinlich	sehr unwahrscheinlich	sehr unwahrscheinlich

Wahrscheinlichkeit Bedrohung

In Kombination mit dem ermittelten Schutzbedarf ergibt die Eintrittswahrscheinlichkeit das festgestellte ISEC-Risiko entsprechend der nachstehenden Informationssicherheitsrisikomatrix:

Schutzbedarf / Auswirkung	Sehr unwahrscheinlich	Weniger wahrscheinlich	Wahrscheinlich	Sehr wahrscheinlich
Sehr hoch	Mittleres Risiko	Hohes Risiko	Sehr hohes Risiko	Sehr hohes Risiko
Hoch	Mittleres Risiko	Hohes Risiko	Hohes Risiko	Sehr hohes Risiko
Mittel	Geringes Risiko	Mittleres Risiko	Mittleres Risiko	Hohes Risiko
Gering	Geringes Risiko	Geringes Risiko	Geringes Risiko	Mittleres Risiko

Eintrittswahrscheinlichkeit

Risiken der Stufe Hohes Risiko bzw. Sehr hohes Risiko müssen – soweit möglich und wirtschaftlich sinnvoll – entweder mit entsprechenden Maßnahmen behandelt werden (Reduzierung, Transfer, Vermeidung) oder von einer hierfür zuständigen Stelle im Management bewusst akzeptiert werden. Dies ist in entsprechender Weise und für Dritte nachvollziehbar zu dokumentieren, ebenso wie das (voraussichtlich) verbleibende Restrisiko nach Umsetzung der vorgesehenen Risikobehandlungs-Maßnahmen.

4.2.3 Risikobehandlung

Für die analysierten Risiken sind die entsprechenden Maßnahmen durch die beteiligten Verantwortlichen einvernehmlich festzulegen und zu dokumentieren.

4.3 Auswahl von Maßnahmen

Gemäß den Ergebnissen der ISEC-Risikoanalyse müssen die in Kapitel 4.1 näher erläuterten Maßnahmen ausgewählt und umgesetzt werden.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

4.4 Umgang mit und Dokumentation von Ausnahmen

Bei folgenden besonderen Umständen können Ausnahmen gemacht werden:
Es sind Ersatzmaßnahmen (Maßnahmen, die nicht unter 4.3 aufgeführt sind) realisiert, die zumindest die gleiche Effizienz und den gleichen Schutzwert aufweisen.
Aufgrund von objektbezogenen Risikobewertungen wird nachgewiesen, dass Ersatzmaßnahmen mit einem geringeren Schutzwert bzw. der Wegfall einer Maßnahme akzeptiert werden können.
Die Ausnahmen sind umfassend zu dokumentieren. Der Verantwortliche muss die Abweichungen anhand einer Risikoanalyse bewerten und die Ergebnisse dem ISM schriftlich mitteilen.

4.5 Levels of Trust

Da die Leistungserbringung im Luftverkehr stark von der Zusammenarbeit der einzelnen Teilnehmer geprägt ist, hängt das ISM einer Organisation wesentlich vom ISM der Organisationen ab, mit denen man in der Leistungserbringung zusammenarbeitet.
Die Gewährleistung der Sicherheit der Informationen und der informationsverarbeitenden Systeme einzelner Organisationen im gemeinsamen Geschäftsprozess sowie der dahinter stehenden eigenen Geschäftsprozesse ist mit einem hohen Aufwand an individuellen Vereinbarungen und Überprüfungen verbunden.
Gemäß CoPiP 3.2 wurde vereinbart, dass überprüfte Vertrauensstellungen (aus der 1:1-Beziehung zweier Organisation oder durch die Überprüfung durch Externe) in weiteren gemeinsamen Geschäftsprozessen (auch mit dritten Organisationen) anerkannt werden.
Die Vertrauensstufe bzw. „Level-of-Trust der Organisation" (abgekürzt LoT) bezieht sich grundsätzlich auf die jeweilige Organisation. Die Einstufung bezieht sich dabei immer auf den Teil des Kernflugprozesses, der der jeweiligen Organisation erbracht wird. Hierbei sind v.a. potentielle ISEC-Risiken, die durch Koppelung der Geschäftsprozesse für die jeweiligen Organisationen entstehen können, zu berücksichtigen.
Die Einstufung gemäß LoT der einzelnen im Folgenden näher beschriebenen Controls für den FMG-Konzern inklusive Einbeziehung des Schutzbedarfs hinsichtlich Vertraulichkeit und Verfügbarkeit findet sich in der Übersichtstabelle im Anhang 2.
Nach der in diesem Kapitel beschriebenen Risikobewertung werden die umzusetzenden technischen und organisatorischen Maßnahmen gemäß der unten stehenden Kriterien identifiziert:

- IT-Abhängigkeit ist vorhanden. Es existieren keine technischen Redundanzen bzw. keine Substituierbarkeit durch NON-IT-Maßnahmen:
  ⇨ Maßnahmen aus CoPiP gemäß LT1 sind umzusetzen
  (gemäß Tabelle Annex B in Verbindung mit den Kapiteln 5 – 18)
- IT-Abhängigkeit ist vorhanden. Es existieren technische Redundanzen, aber keine Substituierbarkeit durch NON-IT-Maßnahmen:
  ⇨ Maßnahmen aus CoPiP gemäß LT2 sind umzusetzen
  (gemäß Tabelle Annex B in Verbindung mit den Kapiteln 5 – 18)
- IT-Abhängigkeit ist vorhanden. Es existieren zudem technische Redundanzen und eine Substituierbarkeit durch NON-IT-Maßnahmen:
  ⇨ Maßnahmen aus CoPiP gemäß LT3 sind umzusetzen
  (gemäß Tabelle Annex B in Verbindung mit den Kapiteln 5 – 18)
- Es ist keine IT-Abhängigkeit vorhanden:
  ⇨ Keine Vorgabe konkreter Maßnahmen

Dabei ist zu beachten, dass die Möglichkeit der Risikoakzeptanz oder Übertragbarkeit gem. CoPiP nur unter der Voraussetzung von §8a BSIG (Verhältnis Aufwand zu Folgen eines Ausfalls/einer Beeinträchtigung) erfolgen kann.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

5 Sicherheitsleitlinie

5.1 Informationssicherheitsleitlinie

Ziel: Vorgaben und Unterstützung für die Informationssicherheit sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt.

5.1.1 Vorgaben der Leitung für Informationssicherheit

Luftverkehrsspezifische Umsetzungsvorgaben

Die Leitlinie zur Informationssicherheit sollte mit den vielfältigen Sicherheitsanforderungen in anderen Bereichen des Luftverkehrs (z. B. physische Absicherung von Sicherheitsbereichen) abgestimmt werden. Die Abgrenzungen und gegenseitigen Abhängigkeiten zwischen den einzelnen Bereichen sollten in der Leitlinie oder einem gesonderten Dokument dokumentiert werden.

5.1.2 Überprüfung der Informationssicherheitsrichtlinien

5.2 Führung

a) Das Management sollte den Bedarf an Beratung durch interne oder externe Fachleute für Informationssicherheit identifizieren und die Ergebnisse daraus überprüfen und organisationsweit die sich daraus ergebenden Aktivitäten koordinieren.
b) Je nach Größe der Organisation kann diese Verantwortung von einem eigenen Managementforum oder einem bereits vorhandenen Managementgremium, wie dem Vorstand, wahrgenommen werden.

5.2.1 Führung und Verpflichtung

Die oberste Leitung muss in Bezug auf das Informationssicherheitsmanagementsystem Führung und Verpflichtung zeigen, indem sie:

a) sicherstellt, dass die Informationssicherheitspolitik und die Informationssicherheitsziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbart sind;
b) sicherstellt, dass die Anforderungen des Informationssicherheitsmanagementsystems in die Geschäftsprozesse der Organisation integriert werden;
c) sicherstellt, dass die für das Informationssicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;
d) die Bedeutung eines wirksamen Informationssicherheitsmanagements sowie die Wichtigkeit der Erfüllung der Anforderungen des Informationssicherheitsmanagementsystems vermittelt;
e) sicherstellt, dass das Informationssicherheitsmanagementsystem sein beabsichtigtes Ergebnis bzw. seine beabsichtigten Ergebnisse erzielt
f) Personen anleitet und unterstützt, damit diese zur Wirksamkeit des Informationssicherheitsmanagementsystems beitragen können;
g) fortlaufende Verbesserungen fördert und
h) andere relevante Führungskräfte unterstützt, um deren Führungsrolle in deren jeweiligen Verantwortungsbereichen deutlich zu machen.

5.2.2 Politik

Die oberste Leitung muss eine Informationssicherheitspolitik festlegen, die:

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

a) Für den Zweck der Organisation angemessen ist;
b) Informationssicherheitsziele (siehe ISO 27001, Kap. 6.2.) beinhaltet oder den Rahmen zum Festlegen von Informationssicherheitszielen bietet;
c) eine Verpflichtung zur Erfüllung zutreffender Anforderungen mit Bezug zur Informationssicherheit enthält und
d) eine Verpflichtung zur fortlaufenden Verbesserung des Informationssicherheitsmanagementsystems enthält.

5.2.3 Managementbewertung

Die oberste Leitung muss das Informationssicherheitsmanagementsystem der Organisation in geplanten Abständen bewerten, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.
Die Managementbewertung muss folgende Aspekte behandeln:
a) den Status von Maßnahmen vorheriger Managementbewertungen;
b) Veränderungen bei externen und internen Themen, die das Informationssicherheitsmanagementsystem betreffen;
c) Rückmeldungen über die Informationssicherheitsleistungen, einschließlich Entwicklungen bei:
    1) Nichtkonformität und Korrekturmaßnahmen;
    2) Ergebnissen von Überwachungen und Messungen;
    3) Auditierergebnissen und
    4) Erreichung von Informationssicherheitszielen.
d) Rückmeldung von interessierten Parteien
e) Ergebnisse der Risikobeurteilung und Status des Plans für die Risikobehandlung und
f) Möglichkeit zur fortlaufenden Verbesserung.

Die Ergebnisse der Managementbewertung müssen Entscheidungen zu Möglichkeiten der fortlaufenden Verbesserung sowie zu jeglichem Änderungsbedarf am Informationssicherheitssystem enthalten.
Die Organisation muss dokumentierte Informationen als Nachweis der Ergebnisse der Managementbewertung aufbewahren.

5.2.4 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

Die oberste Leitung muss sicherstellen, dass die Verantwortlichkeiten und Befugnisse für Rollen mit Bezug zur Informationssicherheit zugewiesen und bekannt gemacht werden.
Die oberste Leitung muss die Verantwortlichkeiten und Befugnisse zuweisen für:
a) Das Sicherstellen, dass das Informationssicherheitsmanagementsystem die Anforderungen dieser internationalen Norm erfüllt und
b) Das Berichten an die oberste Leitung über die Leistung des Informationssicherheitsmanagementsystems.

Anmerkung: Die oberste Leitung darf auch Verantwortlichkeiten und Befugnisse für das Berichten der Leistung des Informationssicherheitsmanagementsystems innerhalb der Organisation zuweisen.

5.2.5 Überwachung, Messung, Analyse & Bewertung

Die Organisation muss die Informationssicherheitsleistung und die Wirksamkeit des Informationssicherheitsmanagementsystems bewerten.
Die Organisation muss bestimmen:
a) was überwacht und gemessen werden muss, einschließlich der Informationssicherheitsprozesse und Maßnahmen;
b) die Methode zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen;

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Anmerkung: die ausgewählten Methoden sollten zu vergleichbaren und reproduzierbaren Ergebnissen führen, damit sie als gültig zu betrachten sind.

c) wann die Überwachung und Messung durchzuführen ist;
d) wer überwachen und messen muss;
e) wann die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind und
f) wer diese Ergebnisse analysieren und bewerten muss.

Die Organisation muss geeignete dokumentierte Informationen als Nachweis der Ergebnisse aufbewahren.

5.2.6 Dokumentierte Information

Allgemeines

Das Informationssicherheitsmanagementsystem der Organisation muss beinhalten:

a) Die von dieser internationalen Norm geforderte dokumentierte Information und
b) Dokumentierte Information, welche die Organisation als notwendig für die Wirksamkeit des Managementsystems bestimmt hat.

Anmerkung: Der Umfang dokumentierter Information für ein Informationssicherheitsmanagementsystem kann sich von Organisation zu Organisation unterscheiden und zwar aufgrund

1) Der Größe der Organisation und der Art ihrer Tätigkeiten, Prozesse, Produkte und Dienstleistungen;
2) Der Komplexität der Prozesse und deren Wechselwirkungen und
3) Der Kompetenz der Personen.

Erstellen und Aktualisieren

Beim Erstellen und Aktualisieren dokumentierter Information muss die Organisation:

a) Angemessene Kennzeichnung und Beschreibung (z.B. Titel, Datum, Autor oder Referenznummer);
b) Angemessenes Format (z.B. Sprache, Softwareversion, Grafiken) und Medium (z.B. Papier, elektronisches Medium) und
c) Angemessene Überprüfung und Genehmigung im Hinblick auf Eignung und Angemessenheit

sicherstellen.

Lenkung dokumentierter Information

Die für das Informationssicherheitsmanagementsystem erforderliche und von dieser Internationalen Norm geforderte dokumentierte Information muss gelenkt werden, um sicherzustellen, dass sie

a) Verfügbar und für die Verwendung geeignet ist, wo und wann sie benötigt wird und
b) Angemessen geschützt wird (z.B. vor Verlust der Vertraulichkeit, unsachgemäßem Gebrauch oder Verlust der Integrität).

Zur Lenkung dokumentierter Informationen muss die Organisation, falls zutreffend, folgende Tätigkeiten berücksichtigen:

c) Verteilung, Zugriff, Auffindung und Verwendung
d) Ablage/Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit;
e) Überwachung von Änderungen (z.B. Versionskontrolle) und
f) Aufbewahrung und Verfügung über den weiteren Verbleib.

Dokumentierte Information externer Herkunft, die von der Organisation als notwendig für die Planung und den Betrieb des Informationssicherheitsmanagementsystems bestimmt wurde, muss angemessen gekennzeichnet und gelenkt werden.

Anmerkung: Zugriff kann eine Entscheidung voraussetzen, mit der die Erlaubnis erteilt wird, dokumentierte Information lediglich zu lesen, oder die Erlaubnis und Befugnis zum Lesen und Ändern dokumentierter Information usw.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

6 Organisation der Informationssicherheit

6.1 Interne Organisation

Ziel: Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der Informationssicherheit in der Organisation eingeleitet und gesteuert werden kann, ist eingerichtet.

6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

a) Die konkrete Zuweisung der Verantwortlichkeiten einzelner Komponenten/Aspekte ist für jedes System gemäß der Tabelle (Anhang 1) zu dokumentieren.
b) Die Verantwortlichkeiten müssen den Schutz von Werten vor unberechtigtem Zugriff, Offenlegung, Veränderung, Zerstörung oder Beeinträchtigung beinhalten.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte einen Verantwortlichen benennen, der als Ansprechpartner für strategische Fragen zur Informationssicherheit Dritten zur Verfügung steht (z. B. für Planung und Umsetzung gemeinsamer Maßnahmen usw.).

6.1.2 Aufgabentrennung

Die Aufteilung von Rollen und Verantwortlichkeiten muss in Form eines dokumentierten Konzepts vorliegen.

6.1.3 Kontakt mit Behörden

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte mit den entsprechenden Fach- und Aufsichtsbehörden, insbesondere in den Bereichen IT-Sicherheit und Strafverfolgung und anderen kritischen Infrastrukturen zusammenarbeiten.
Das umfasst Kontakte zu Behörden, die sich mit dem Schutz kritischer Infrastrukturen auf nationaler und europäischer Ebene beschäftigen.

6.1.4 Kontakt mit speziellen Interessensgruppen

Weitere für die Luftfahrt spezifische Informationen

Die Organisation sollte sich außerdem der Kritikalität ihrer Dienstleistungen auf regionaler, nationaler und internationaler Ebene bewusst sein. Sie darf sich deshalb in Verbänden und Zusammenschlüssen engagieren und sich an nationalen und internationalen Programmen beteiligen, um die Sicherheit im Luftverkehr umfassend zu unterstützen.
Aufgrund der besonderen Art der Bedrohungen für den Luftverkehr, kann es für die Organisation notwendig sein, mit anderen Luftverkehrsorganisationen zusammenzuarbeiten, um nach außen eine einmütige Position zu vertreten. Ein solcher gemeinsamer Auftritt sollte die Grundlage für die Auswahl angemessener Schutzmaßnahmen und reaktiver Maßnahmen sein:

- Sicherstellung der Interoperabilität der ausgewählten Maßnahmen;
- Unterstützung der Zusammenarbeit bei der Alarmierung bei auftretenden IT-Krisen, die mehrere Organisationen betreffen, sowie bei der Krisen-Bewältigung;
- auf der Grundlage gemeinsam gezogener Lehren aus bereits aufgetretenen Sicherheitsvorfällen.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

6.1.5 Informationssicherheit im Projektmanagement

6.2 Mobilgeräte und Telearbeit

Ziel: Die Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten ist sichergestellt.
(Mobilgeräte umfassen mobile Geräte jeder Art (Smartphones, Tablets, Laptops, Netbooks usw.).)

6.2.1 Richtlinie zu Mobilgeräten

Für den Einsatz von mobilen Geräten sind Regelungen und Verfahren zu erstellen, die mindestens folgende Aspekte berücksichtigen:

a) Physischer Schutz
b) Zugangskontrollen
c) Kryptographische Maßnahmen
d) Backup
e) Virenschutz

Mobile Geräte sind vor unbefugter Nutzung bzw. die darauf gespeicherten Daten vor unberechtigter Einsichtnahme zu schützen. Hierzu zählen insbesondere folgende Maßnahmen:

a) Authentifizierungsmechanismen
b) Verschlüsselung der gespeicherten Informationen
c) Sperrung des Geräts nach einer definierten Zeit
d) Löschung der Daten nach einer definierten Anzahl fehlerhafter Anmeldeversuche

6.2.2 Telearbeit

Es sind Regelungen und Verfahren für die Arbeit außerhalb des FMG-Konzern-Standortes mit Remote Access zu einem FMG-Netzwerk umzusetzen. Diese müssen folgende Aspekte berücksichtigen:

a) Berechtigte Geräte (Geräte des FMG-Konzerns, private Geräte etc.)
b) Authentifizierungsverfahren
c) Voraussetzungen für Verbindung mit dem FMG-Netzwerk
d) Management von remote betriebenen Geräten
e) Schutz der Ausstattung und Informationen durch firmenfremde Personen
f) Rückgabe von Ausstattung bzw. Rücknahme von Zugangs-/Zugriffsberechtigungen bei Beendigung der Telearbeit.

7 Personalsicherheit

7.1 Vor der Beschäftigung

Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Rollen geeignet sind.

7.1.1 Sicherheitsüberprüfung

Bei der Überprüfung sind in Abhängigkeit der vorgesehenen Tätigkeit die nachfolgenden Aspekte zu berücksichtigen:

a) Überprüfung des Lebenslaufs des Mitarbeiters (auf Vollständigkeit und Richtigkeit);
b) unabhängige Identitätsprüfung (Reisepass oder ähnliches Dokument);

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

c) weiterführende Prüfungen (z. B. Überprüfung der Kreditwürdigkeit, Prüfung auf Vorstrafen im Rahmen eines polizeilichen Führungszeugnisses, Durchführung einer Luftsicherheitsüberprüfung).

Luftverkehrsspezifische Umsetzungsvorgaben

Im Falle mehrerer Partnerorganisationen sollte sichergestellt sein, dass von Partnerorganisationen Hintergrundüberprüfungen auf einem angemessenen Niveau durchgeführt werden, um sicherzustellen, dass der Zugriff auf Daten/Informationen, die von den Partnerorganisationen gemeinsam genutzt werden, die nationalen und geschäftlichen Interessen aller Beteiligten berücksichtigen.

7.1.2 Beschäftigungs- und Vertragsbedingungen

Die Vereinbarungen mit Mitarbeitern und externen Dienstleistern müssen mindestens die nachfolgenden Inhalte berücksichtigen:

a) Unterzeichnung einer Vertraulichkeitsvereinbarung, bevor Zugang zu informationsverarbeitenden Einrichtungen gewährt wird;
b) Verantwortlichkeiten für die Handhabung von Informationen, die von anderen Firmen oder Externen bereitgestellt wurden;
c) Bericht von Sicherheitsvorfällen oder potentiellen Sicherheitsvorfällen sowie anderen Sicherheitsrisiken für die Organisation.

Es ist sicherzustellen, dass Angestellte und externe Dienstleister die relevanten Vertragsklauseln für Informationssicherheit akzeptieren.

7.2 Während der Anstellung

Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer sich ihrer Verantwortlichkeiten bezüglich der Informationssicherheit bewusst sind und diesen nachkommen.

7.2.1 Verantwortlichkeiten der Leitung

Das Management hat sicherzustellen, dass Mitarbeiter sowie externe Dienstleister im Rahmen ihrer Beschäftigung

a) zur Wahrnehmung ihrer Informationssicherheitsaufgaben und –verantwortlichkeiten richtig instruiert sind, bevor ihnen Zugang zu sensitiven Informationen oder Informationssystemen gegeben wird;
b) die erforderlichen Fähigkeiten und Qualifikationen haben und beibehalten.

7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Anforderung an die Personalentwicklung:

a) Mitarbeiter und externe Dienstleister sind in regelmäßigen Abständen auf relevante Bereiche der Sicherheitsrichtlinien des Unternehmens zu schulen.
b) Mitarbeiter und externe Dienstleister müssen die nötige Fachkunde zur Ausführung ihrer Tätigkeiten besitzen und sich regelmäßig gemäß aktuellen technischen Standards fortbilden.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Herausbildung des Bewusstseins der Angestellten, ihre Ausbildung und Schulung sollten insbesondere in Übereinstimmung mit den maßgeblichen Sicherheitsfestlegungen der Abkommensanhänge und anderer Dokumente der Internationalen Zivilluftfahrtorganisation (ICAO) erfolgen.
Die Organisation sollte sicherstellen, dass Anwendungsentwickler über Fähigkeiten verfügen, die es ihnen ermöglichen, sichere Anwendungen umzusetzen.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

7.2.3 Maßregelungsprozess

7.3 Beendigung und Änderung der Beschäftigung

Ziel: Der Schutz der Interessen der Organisation ist Teil des Prozesses der Änderung oder Beendigung einer Beschäftigung.

7.3.1 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung

Die Verantwortlichkeiten sind im Rahmen eines dokumentierten Prozesses für Austritte zu beschreiben, in dem alle relevanten Schritte enthalten sind.

8 Verwaltung der Werte

8.1 Verantwortlichkeit für Werte

Ziel: Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz sind festgelegt.

8.1.1 Inventarisierung der Werte

Es ist ein Verzeichnis für mindestens die nachfolgenden Assets zu führen:
a) Systeme
b) installierte Software pro System
c) Informationen mit zugehöriger Vertraulichkeitseinstufung
Die Aushändigung relevanter Assets an Angestellte oder externe Dienstleister ist zu dokumentieren.

8.1.2 Zuständigkeit für Werte

Der Eigentümer eines Wertes muss verantwortlich sein, dass
a) Informationen und Systeme entsprechend den Vorgaben klassifiziert werden;
b) eine Definition und regelmäßige Überprüfung der Zugangs-/Zugriffsbeschränkungen und Klassifikation der Werte, unter Berücksichtigung der anwendbaren Zugangskontrollpolitiken, erfolgt.

Luftverkehrsspezifische Umsetzungsvorgaben

Wenn Werte in Geschäftsprozessen verwendet werden, an denen mehrere Organisationen beteiligt sind, sollten die Interessen der anderen Organisationen von den Eigentümern der Werte berücksichtigt werden.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

8.1.3 Zulässiger Gebrauch von Werten

8.1.4 Rückgabe von Werten

8.2 Informationsklassifizierung

Ziel: Es ist sichergestellt, dass Information ein angemessenes Schutzniveau entsprechend ihrer Bedeutung für die Organisation erhält.

8.2.1 Klassifizierung von Information

Bei der Klassifizierung von Informationen sind gesetzliche, aufsichtsrechtliche sowie vertragliche Anforderungen zu berücksichtigen.

Luftverkehrsspezifische Umsetzungsvorgaben

Um eine organisationsübergreifende Vergleichbarkeit sicherzustellen, sollte die Organisation Informationen, die in übergreifenden Geschäftsprozessen benutzt werden, so klassifizieren, dass diese Klassifizierung für alle am Geschäftsprozess beteiligten Partner annehmbar ist und sie dieser Klassifizierung zustimmen. Derartige Informationen sollten klassifiziert werden, um sicherzustellen, dass nationale und geschäftliche Interessen in angemessener Weise geschützt werden.

Vertraulichkeitsklassen:

Die Zuordnung von Informationen zu einer Vertraulichkeitsklasse sollte auf der Grundlage des zu erwartenden Schadens für den Geschäftsprozess, falls die Information Unberechtigten zur Kenntnis gelangt, erfolgen.
Öffentlich: Informationen, deren Bekanntwerden keinen Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich zieht
Intern: Informationen, deren Bekanntwerden einen geringen bis mittleren Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich zieht
Vertraulich: Informationen, deren Bekanntwerden einen großen Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich ziehen kann
Streng Vertraulich: Informationen, deren Bekanntwerden einen erheblichen bis existenziellen Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich ziehen kann
Allgemein sollte die gemeinsame Nutzung von Informationen nach dem „Need-to-know-Prinzip" erfolgen.

Weitere für die Luftfahrt spezifische Informationen

Geschäftliche Bedürfnisse und die geschäftlichen Auswirkungen in Zusammenhang mit diesen Bedürfnissen können das öffentliche Interesse an einer sicheren und schnellen Erbringung der Dienstleistung einschließen wie auch geschäftliche Interessen von einzelnen Beteiligten.

8.2.2 Kennzeichnung von Information

a) Beim Ausdrucken von Informationen muss eine explizite Kennzeichnung möglich sein.
b) Beim Datenexport müssen die exportierten Daten explizit gekennzeichnet werden können.
c) Festplatten von mobilen Geräten wie Notebooks bzw. Datenspeicher von Smartphones oder Tablets, auf denen vertrauliche Informationen gespeichert sind, müssen verschlüsselt werden. Dies gilt auch für Datenträger wie z. B. CDs, DVDs, USB-Sticks oder externe Festplatten.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

d) Vertrauliche oder streng vertrauliche Informationen müssen bei Übertragung in oder durch öffentliche Netze verschlüsselt werden. Hierzu müssen Lösungen verwendet werden, die auf dem aktuellen Stand der Technik basieren.
e) Eine Speicherung von vertraulichen bzw. streng vertraulichen Daten (z. B. Datenbank-Kennwörtern) im Klartext im Code bzw. Konfigurationsdateien ist nicht zulässig.
f) Auf mobilen Geräten muss eine Verschlüsselung der lokalen Daten aktiviert sein.
g) Vertrauliche bzw. streng vertrauliche Daten dürfen nicht auf unverschlüsselten Clientrechnern abgelegt werden.

8.2.3 Handhabung von Werten

Bezüglich des Umgangs mit vertraulichen Informationen muss beim FMG-Konzern und von ihm beauftragten Dienstleistern die „Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen" eingehalten werden.

8.3 Handhabung von Datenträgern

Ziel: Die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Information, die auf Datenträgern gespeichert ist, wird unterbunden.

8.3.1 Handhabung von Wechseldatenträgern

Bezüglich des Umgangs mit vertraulichen Informationen muss beim FMG-Konzern und von ihm beauftragten Dienstleistern die „Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen" eingehalten werden.

8.3.2 Entsorgung von Datenträgern

Es müssen Maßnahmen zur sicheren Löschung oder Entsorgung von Datenträgern zur Verfügung gestellt oder alternative organisatorische/vertragliche Maßnahmen zur sicheren Löschung/Entsorgung von Datenträgern ergriffen werden.
Dies beinhaltet die Anwendung von angemessenen Löschverfahren einschließlich der Nachvollziehbarkeit der ordnungsgemäßen Durchführung.
Der Schutz der Informationen muss gewährleistet werden, auch wenn IT-Systeme bzw. darin enthaltene Datenspeicher nicht länger verwendet werden, nicht länger innerhalb des FMG-Konzerns verwendbar sind oder wenn sie zu einem anderen Zweck verwendet werden.

8.3.3 Transport von Datenträgern

Sofern Datenspeicher transportiert werden, müssen die darauf gespeicherten Daten mit einem Verfahren entsprechend dem aktuellen Stand der Technik verschlüsselt sein.
Die für die Entschlüsselung erforderlichen Informationen müssen auf einem anderen Kommunikationsweg zum Empfänger übermittelt werden wie der Datenspeicher.
Der Transport von Medien mit Informationen der Klasse „Vertraulich" oder „Streng vertraulich" muss dokumentiert werden. Es muss sichergestellt sein, dass der Aufenthaltsort des Datenspeichers zu jeder Zeit bekannt ist (z. B. Carrier mit Paket-Tracking).

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

9 Zugangssteuerung

9.1 Geschäftsanforderungen an die Zugangssteuerung

Ziel: Der Zugang zu Informationen und informationsverarbeitenden Einrichtungen ist eingeschränkt.

9.1.1 Zugangssteuerungsrichtlinie

Es ist ein Regelwerk zur Zugangskontrolle für IT-Systeme zu erstellen, welches mindestens die nachfolgenden Anforderungen erfüllt, um sicherzustellen, dass unbefugte Nutzung ausgeschlossen wird.
Jedes IT-System muss über angemessene Authentifizierungsmechanismen verfügen, welches für alle Nutzer gültig ist.
Der Informationsverantwortliche bzw. von diesen autorisierte Mitarbeiter legen in enger Abstimmung mit dem Produktmanager fest, welche Personen Zugangsberechtigung zu einem IT-System erhalten.
Einem Nutzer dürfen nur genau die Zugangs- und Zugriffsrechte eingeräumt werden, die er zum Erfüllen seiner Aufgaben benötigt.
Die Genehmigung, Umsetzung und Verwaltung von Zugangs- und Zugriffsrechten sollte nach dem Prinzip der Trennung von Verantwortlichkeiten („Separation of Duties" oder „Vier-Augen-Prinzip") ausgeführt werden.
Trennung der Rollen und Funktionen für die Erteilung von Zugangsrechten in Bezug auf Genehmigung und Rechteverwaltung.

9.1.2 Zugang zu Netzwerken und Netzwerkdiensten

Es ist ein Regelwerk für die Nutzung von Netzen und Netzdiensten zu erstellen, welches mindestens die nachfolgenden Punkte beinhaltet:

a) die Netze und Netzdienste, auf die zugegriffen werden darf,
b) Berechtigungsverfahren, um festzustellen, wer auf welche Netze und Netzdienste zugreifen darf,
c) Administrations-Maßnahmen und Prozeduren, um den Zugang zu Netzen und Netzdiensten zu schützen.

9.2 Benutzerzugangsverwaltung

Ziel: Es ist sichergestellt, dass befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird.

9.2.1 Registrierung und Deregistrierung von Benutzern

Um eine Nachvollziehbarkeit zu gewährleisten, müssen Zugangs- und Zugriffsrechte sowie deren Erteilung und Entzug in geeigneter Weise dokumentiert sein.
Bei Beendigung des Arbeitsverhältnisses muss ein sofortiger Entzug der vorhandenen Zugangs- und Zugriffsrechte gemäß den Vorgaben des Personalbereichs sichergestellt werden.
Bei der Vergabe von Zugangsberechtigungen ist darauf zu achten, dass ausschließlich eindeutige Benutzerkennungen vergeben werden, um sicherzustellen, dass Benutzer einer Benutzerkennung zuordenbar sind. Die Verwendung von Gruppenkennungen ist nur dann zulässig, wenn dies aus betrieblichen oder geschäftlichen Gründen notwendig ist und dies genehmigt sowie dokumentiert wurde.
Anonyme Administrations-Accounts (z. B. Windows: Administrator oder Unix: Root) müssen grundsätzlich durch persönliche Administrations-Accounts ersetzt werden, die eindeutig einer bestimmten Person zugeordnet werden können. Sofern dies für sicherheitskritische IT-Systeme nicht möglich ist, muss die Nutzung von anonymen Administrations-Accounts protokolliert werden.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Darüber hinaus ist sicherzustellen, dass die Passwörter für anonyme Administrations-Accounts mindestens einmal jährlich sowie unverzüglich bei Ausscheiden eines Nutzers dieser Accounts geändert werden. Für sicherheitskritische Systeme sind die Zugangsdaten dieser Accounts in einem versiegelten Umschlag in einem abschließbaren Schrank (oder einem Safe) aufzubewahren. Der Zugriff auf diese Informationen muss geregelt und dokumentiert werden.

9.2.2 Zuteilung von Benutzerzugängen

Es müssen Benutzerkonten mit den geringsten möglichen Privilegien und Zugriffsrechten auf Systemebene verwendet werden. Dazu gehören beispielsweise Zugriffsrechte auf Dateien, Ordner, Geräte im Netz, Datenbankobjekte oder Ereignisprotokolle.
Es ist ein Verfahren für die Reaktivierung gesperrter Accounts sowie die Rücksetzung von Passwörtern zu etablieren.
Bei internen Versetzungen bzw. Neuzuordnungen von Aufgaben muss eine zeitnahe Änderung von Zugangs- und Zugriffsrechten sichergestellt werden.
Zugangsrechte sind in Abhängigkeit des Nutzerstatus unbefristet (interne Mitarbeiter) oder befristet (z. B. externe Mitarbeiter, Geschäftspartner, Auszubildende, Werkstudenten, Praktikanten) zu erteilen.

9.2.3 Verwaltung privilegierter Zugangsrechte

Es ist sicherzustellen, dass privilegierte Zugangsrechte nur bei tatsächlichem Bedarf vergeben werden.
Die mit jeder Systemkomponente (z. B. Betriebssysteme, Datenbanken und Anwendungen) verbundenen Sonderrechte und die Benutzer, denen diese Sonderrechte zugeteilt werden, müssen dokumentiert sein.
Sonderrechte dürfen nur einer von der normalen Benutzerkennung für den Alltagsgebrauch getrennten Benutzerkennung zugewiesen werden.

9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern

Passwörter von privilegierten Kennungen (z. B. Administratoren) müssen für Notfälle einem definierten Vertreterkreis zugänglich sein und an einem besonders geschützten Ort aufbewahrt werden.
Standardpasswörter der Hersteller müssen nach der Installation von Systemen oder Software geändert werden.
Ein Passwort- bzw. PIN-Schutz muss auch auf mobilen Geräten vorhanden sein, sobald ein Zugriff auf Informationen des FMG-Konzerns erfolgt.
Benutzer müssen grundsätzlich mit einem individuellen Initialpasswort versorgt werden, welches bei der Erstanmeldung geändert werden muss.
Passwörter dürfen ausschließlich dem jeweiligen Accountinhaber auf sichere Art und Weise mitgeteilt werden.
Passwörter dürfen nur durch geeignete Maßnahmen (z. B. Hashing) geschützt gespeichert werden.
Die Rücksetzung von Passwörtern darf nur unter Einhaltung eines genehmigten Verfahrens zur Identitätsprüfung erfolgen.

9.2.5 Überprüfung von Benutzerzugangsrechten

Der Informationsverantwortliche muss sicherstellen, dass eine Prüfung
a) der eingerichteten Zugangs- und Zugriffsberechtigungen mindestens einmal im Jahr,
b) der erteilten Sonderrechte mindestens halbjährlich
erfolgt.
Die durchgeführte Prüfung ist in geeigneter Weise zu dokumentieren.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

9.2.6 Entzug oder Anpassung von Zugangsrechten

Eine zeitnahe Umsetzung der Änderung unter Berücksichtigung der Kritikalität der betroffenen Systeme bzw. Informationen ist sicherzustellen.
Dabei muss bedarfsweise unterschieden werden, wie, aus welchem Grund bzw. durch wen die Beendigung oder Änderung eingeleitet wurde.

9.2.7 Digitales Identitätsmanagement

Anleitung zur Umsetzung (gem. CoPiP 3.2):

Quellendatenbanken (z. B. LDAP-Verzeichnisse, Active Directory, dezentrale Datenbanken wie SAP usw.) des Identitätsmanagementsystems sollten eine eindeutige Beziehung zwischen einer Identität und einer Entität des zentralen Identitätsmanagementsystems herstellen.
Die folgenden Hauptprozesse zur Verwaltung digitaler Identitäten sollten umgesetzt werden:

- Erzeugung digitaler Identitäten;
- Änderung (Anpassung, Erweiterung, Löschung) von Merkmalen einer digitalen Identität;
- Deaktivierung/Löschung digitaler Identitäten; systematische Bereitstellung digitaler Identitätsinformationen (einschließlich Authentisierungsdaten) für angeschlossene Systeme;
- Verarbeitung von Informationen (aus der Personalverwaltung und dem Organisationsmanagement) zur automatisierten Verwaltung von Benutzergruppen, Rollen und Rechten (Autorisierungsprofile);
- systematische Bereitstellung von Benutzergruppen, Rollen und Rechten in angeschlossenen Systemen.

Jeder der vorgenannten Prozesse im Zusammenhang mit dem digitalen Identitäts-Management sollte dokumentiert werden und rückverfolgbar sein.
Die Gültigkeit sollte durch ein angeschlossenes Personalmanagementsystem oder über ein verbundenes Unternehmensverzeichnis umgesetzt werden.
Sofern manuelle Prozesse angewendet werden müssen, sollte die Gültigkeitsdauer ein Jahr nicht überschreiten. Die Festlegung einer neuen Gültigkeitsdauer sollte einmal jährlich durch eine Überprüfung erfolgen.

9.2.8 Organisationsübergreifende eindeutige Darstellung von Entitäten

Anleitung zur Umsetzung (gem. CoPiP 3.2):

Im organisationsübergreifenden Identitätsmanagement sollten folgende Entitäten betrachtet werden:

- Menschen
- Organisationseinheiten und organisatorische Rollen (Departments)
- Systeme.

Jede Entität der Organisation sollte im zentralen Identitätsmanagementsystem durch eine eindeutige digitale Identität dargestellt werden.

Weitere Informationen

Ein einheitliches System zur organisationsübergreifenden Darstellung von Entitäten stellt die Kompatibilität und Interoperabilität im Identitätsmanagement sicher.

9.3 Benutzerverantwortlichkeiten

Ziel: Benutzer sind für den Schutz Ihrer Authentisierungsinformation verantwortlich gemacht.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

9.3.1 Gebrauch geheimer Authentisierungsinformation

Benutzer müssen ihre Passwörter umgehend ändern, wenn deren Vertraulichkeit in irgendeiner Form gefährdet wurde.
Für IT-Systeme, bei denen eine vermutete oder festgestellte Kompromittierung vorliegt, ist sicherzustellen, dass die Passwörter sämtlicher betroffenen bzw. potenziell betroffenen Benutzerkonten umgehend geändert werden.
Passwörter für Administrations-Accounts dürfen nicht für andere Zwecke verwendet werden.
Es ist sicherzustellen, dass Passwörter nicht im Klartext in Dokumentationen enthalten sind.
Als Schutzmaßnahme gegen Social Engineering Angriffe dürfen Administratoren generell nie die Passwörter von Nutzern erfragen, sondern müssen diese im Supportfall technisch zurücksetzen.

9.4 Zugangssteuerung für Systeme und Anwendungen

Ziel: Unbefugter Zugang zu Systemen und Anwendungen ist unterbunden.

9.4.1 Informationszugangsbeschränkung

Zugriffsberechtigungen auf Dateien müssen in allen IT-Systemen standardmäßig so gesetzt werden, dass nicht autorisierten Personen der Zugriff verwehrt wird.
Die Zugriffsrechte von Benutzern oder anderen Anwendungen sind gemäß den geschäftlichen Anforderungen einzuschränken und zu kontrollieren.

9.4.2 Sichere Anmeldeverfahren

Um zu vermeiden, dass Passwörter erraten werden, ist nur eine maximale Anzahl von 10 fehlerhaften Versuchen bei der Eingabe von Passwörtern zuzulassen.
Wird diese Grenze überschritten, muss der Account gesperrt werden und darf anschließend nur gemäß dem festgelegten Prozess zum Entsperren von Accounts wieder freigeschaltet werden.
Wenn ein Teil der Anmeldung an einem IT-System fehlschlägt, darf der Benutzer lediglich darüber informiert werden, dass der Anmeldevorgang insgesamt fehlgeschlagen ist. Er darf nicht darüber informiert werden, welcher Teil der Anmeldung (Benutzername oder Passwort) fehlgeschlagen ist.
Das eingegebene Passwort darf standardmäßig nicht vollständig bei der Eingabe angezeigt werden.

9.4.3 System zur Verwaltung von Kennwörtern

Regelung für alle Systeme außer mobile Endgeräte:
Soweit technisch möglich, muss erzwungen werden, dass nur sichere Passwörter gewählt werden. Für sichere Passwörter auf allen Systemen (ausgeschlossen mobile Endgeräte) sollten grundsätzlich folgende Anforderungen beachtet werden:

- Mindestlänge 12 Zeichen
- Komplexität: 3 aus 4
- History: 12
- Änderungsintervall: 180 Tage
- Account Lockout: Auto lockout für 30 Min
- keine Trivial-Ersetzung (a=@, i=1)
- keine Verwendung von Worten aus Wörterbüchern (Sommer2019)
- Passwörter werden bei Änderungen nicht hochgezählt (Sommer2020)
- Mindestalter 1 Tag

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Regelung für mobile Endgeräte:
Soweit technisch möglich, muss erzwungen werden, dass nur sichere Passwörter gewählt werden. Für sichere Passwörter auf mobilen Endgeräte sollten grundsätzlich folgende Anforderungen beachtet werden:

- Mindestlänge 6 Zeichen
- History: 10
- Änderungsintervall: 180 Tage
- Account Lockout: Auto lockout für 30 Min
- Mindestalter 1 Tag
- Maximale Anzahl an Fehlversuche: 6

Für besondere Berechtigungen (Funktionskonten, privilegierte und hoch privilegierte Konten) müssen soweit technisch möglich höhere Sicherheitsanforderungen (z. B. längere Passwörter, kürzeres Änderungsintervall, höhere Komplexität, MFA) erzwungen werden.

9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten

9.4.5 Zugangssteuerung für Quellcode von Programmen

9.4.6 Web-Application Firewalls

Anleitung zur Umsetzung (gem. CoPiP 3.2):

- Um versuchte Angriffe auf Web-Anwendungen vorausschauend erkennen, protokollieren und abblocken zu können, sollte die nachstehende Anleitung für die Umsetzung befolgt werden: eine Basis von Signaturen (oder Regeln), die verbreitete Angriffe wie z. B. seitenübergreifendes Scripting (XSS) und SQL-Einschleusung abdecken, sollte angewendet und auf dem aktuellen Stand gehalten werden;
- Angriff-Signaturen (oder Regeln) sollten für jede Web-Anwendung angepasst werden und bei Änderungen an den Anwendungen auf dem aktuellen Stand gehalten werden.

Weitere Informationen

Eine Application Firewall ist eine Art Firewall, die den Eintritt, Austritt und/oder den Zugang von, zu oder durch eine Anwendung oder einen Dienst steuert. Sie funktioniert durch Überwachung und möglicherweise Blockierung des Eintritts, Austritts oder von System Service Calls, die nicht mit der konfigurierten Leitlinie übereinstimmen. Die Web-Application-Firewall-Technik verfügt speziell über die Fähigkeit, eine Reihe von Regeln auf HTTP/HTTPS-Nachrichtenübermittlungen anzuwenden, um viele Angriffsversuche erkennen und blockieren zu können.

10 Kryptographie

10.1 Kryptographische Maßnahmen

Ziel: Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt.

10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

Es ist eine Kryptoleitlinie zu erstellen und weiterzuentwickeln, die mindestens die nachfolgenden Punkte berücksichtigt:

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

a) Anwendung von Verschlüsselung zum Schutz sensitiver Informationen, die auf Endgeräten, mobilen Datenträgern oder über Kommunikationsverbindungen transportiert werden,
b) Auswirkungen, die eine Verwendung verschlüsselter Informationen auf Maßnahmen hat, die von der Untersuchung des Inhalts von Informationen abhängig sind (z. B. Virenscanner),
c) Ansatz zur Schlüsselverwaltung, inklusive Methoden, um kryptographische Schlüssel zu schützen und verschlüsselte Informationen zurückzugewinnen, falls der Schlüssel verloren, kompromittiert oder beschädigt wurde.
d) Für die Nutzung von Kryptografie müssen die bewährten Kryptographie services oder Bibliotheken, die im Betriebssystem oder in der Laufzeitumgebung enthalten sind, verwendet werden. Es dürfen keine eigenen Verfahren entwickelt werden.
e) Daten müssen so lange wie möglich verschlüsselt belassen werden.
f) Klartextdaten sind in so wenig Variablen wie möglich abzuspeichern.

Passende Algorithmen und erforderliche Schlüssellängen müssen entsprechend den Sicherheitsanforderungen gewählt werden. Sicherheit steigt mit der Schlüssellänge. Empfohlen ist eine AES-basierte Verschlüsselung.

10.1.2 Schlüsselverwaltung

Für Kryptografie dürfen ausschließlich anerkannte Verschlüsselungsverfahren eingesetzt werden (z. B. AES, RSA)
Bei den kryptografischen Verfahren sind folgende Mindestschlüssellängen zu gewährleisten:
a) bei symmetrischen Verfahren mindestens 256 bit
b) bei asymmetrischen Verfahren mindestens 2048 bit

Eine Veröffentlichung von geheimen Schlüsseln an Dritte ist nicht gestattet. Ebenso dürfen Passwörter, die ggf. den Zugang zu Schlüsselmaterial gewähren, nicht weitergegeben werden.
Die Verteilung von kryptografischen Schlüsseln muss auf einem sicheren Weg erfolgen.
Öffentliche Schlüssel sind in einem zentralen Verzeichnis direkt oder indirekt zugänglich für alle Nutzer des Dienstes abzulegen.
Private Schlüssel sind ausschließlich dem entsprechenden Benutzer zugänglich zu machen. Dies kann auch mittelbar über eine Software erfolgen.
Von allen Schlüsseln sind seitens IT Sicherungskopien vorzuhalten. Administratoren mit Zugriff auf diese Sicherungskopien dürfen keinen Zugriff auf verschlüsselte Daten erhalten (Funktionstrennung).
Bei Erzeugung von Schlüsseln soll – soweit technisch und rechtlich möglich – die Verwendung eines Generalschlüssels implementiert werden. Der Generalschlüssel kann dann alle verschlüsselten Daten aller Anwender des Dienstes entschlüsseln.
Die Nutzung eines Generalschlüssels darf nicht einer einzelnen Person möglich sein.
Der Zugriff auf private Schlüssel von Nutzern sowie auf Generalschlüssel durch Administratoren ist grundsätzlich nicht erlaubt.
In begründeten Ausnahmefällen kann IT auf private Schlüssel eines Nutzers oder auf den Generalschlüssel zugreifen und Daten eines Nutzers entschlüsseln, ohne den Nutzer vorab zu informieren. Ein begründeter Ausnahmefall liegt insbesondere vor bei:
a) Unvorhergesehenem Ausscheiden aus dem Unternehmen (z. B. fristlose Kündigung, Tod)
b) Voraussichtlich längerer Abwesenheit vom Arbeitsplatz ohne Möglichkeit des Kontakts mit dem Betroffenen (z. B. Erkrankung, Unfall), bei unaufschiebbarer Erforderlichkeit des Zugriffs auf verschlüsselte Daten
c) Soweit in einem behördlichen oder gerichtlichen Verfahren zur Wahrung der Interessen des FMG-Konzerns erforderlich.

Dieser unangekündigte Zugriff auf verschlüsselte Daten eines Nutzers unterliegt einem besonderen Verfahren, in dem die Verhältnismäßigkeit der Maßnahme durch Einbeziehung des Datenschutzbeauftragten und eines Mitglieds der jeweils zuständigen Arbeitnehmervertretung überprüft wird.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Betroffene Nutzer sind über den Zugriff auf die verschlüsselten Daten in den beschriebenen Fällen unverzüglich in Kenntnis zu setzen, sobald Natur und Zweck der Maßnahme dies gestatten.

11 Physische und umgebungsbezogene Sicherheit

11.1 Sicherheitsbereiche

Ziel: Unbefugter Zutritt, die Beschädigung und die Beeinträchtigung von Information und informationsverarbeitenden Einrichtungen der Organisation sind verhindert.

11.1.1 Physische Sicherheitsperimeter

11.1.2 Physische Zutrittssteuerung

Personen ohne eigene Zutrittsberechtigung zur jeweiligen Zone müssen grundsätzlich während ihres Aufenthaltes durch einen Angestellten begleitet werden.
Mitarbeiter externer Firmen müssen durch den Vertragspartner vorab benannt werden. Alternativ muss er eine Identifikation als Mitarbeiter oder Dienstleister der externen Firma vorlegen können.

11.1.3 Sichern von Büros, Räumen und Einrichtungen

11.1.4 Schutz vor externen und umweltbedingten Bedrohungen

Materialien mit hoher Brandlast (z. B. leicht entzündliche Stoffe, Papier) dürfen nicht in Info- oder Serverräumen sowie Rechenzentren gelagert werden.
Geeignete Ausstattung zur Brandbekämpfung ist bereitzustellen und adäquat zu platzieren.

11.1.5 Arbeiten in Sicherheitsbereichen

11.1.6 Anlieferungs- und Ladebereiche

11.2 Geräte und Betriebsmittel

Ziel: Verlust, Beschädigung, Diebstahl oder Gefährdung von Werten und die Unterbrechung von Organisationstätigkeiten sind unterbunden.

11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln

Luftverkehrsspezifische Umsetzungsvorgaben

Ausrüstungen, die in öffentlich zugänglichen Bereichen eingesetzt werden, sollten gegen unberechtigten Zugriff geschützt werden, z. B. durch feststehende und abzusperrende Gehäuse für PCs, physische und/oder logische Absicherung von Netzwerkdosen usw.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

11.2.2 Versorgungseinrichtungen

11.2.3 Sicherheit der Verkabelung

11.2.4 Instandhaltung von Geräten und Betriebsmitteln

Die Erfordernis und der Umfang von Instandhaltungs- und Wartungsmaßnahmen für relevante Gerätschaften sind zu überprüfen und festzulegen.

11.2.5 Entfernen von Werten

Betriebsmittel, Informationen oder Software dürfen nicht unberechtigt aus dem Standort entfernt werden. Mitarbeiter, Vertragspartner und Externe, die die Mitnahme von Betriebsmitteln genehmigen dürfen, müssen eindeutig festgelegt sein.

11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten

Systeme und Datenträger, die außerhalb des Standortes mitgenommen werden, dürfen in der Öffentlichkeit nicht unbeaufsichtigt sein.

11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

11.2.8 Unbeaufsichtigte Benutzergeräte

Es sind geeignete Maßnahmen zum Schutz unbeaufsichtigter IT-Systeme vor unbefugtem Zugriff zu etablieren (z. B. Abmeldung vom System, aktive Sperrung des Gerätes, Aktivierung eines Bildschirmschoners mit automatischer Sperre des betreffenden IT-Systems nach einer definierten Zeitspanne).
Darüber hinaus sind Maßnahmen zum physischen Schutz von IT-Systemen in öffentlich zugänglichen Bereichen zu ergreifen.

11.2.9 Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

12 Betriebssicherheit

12.1 Betriebsabläufe und –verantwortlichkeiten

Ziel: Der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

12.1.1 Dokumentierte Betriebsabläufe

Der Produktmanager ist verantwortlich für die Erstellung und Pflege einer Betriebsdokumentation für sämtliche IT-Systeme seines Zuständigkeitsbereichs. Diese muss auf einer hohen Abstraktionsebene die Komponenten und Voraussetzungen der jeweiligen IT-Systeme beschreiben, die für einen zuverlässigen Betrieb erforderlich sind.
Die Betriebsdokumentation muss mindestens die nachfolgenden sicherheitsrelevanten Themen enthalten:

a) Betrieb und Wartung
b) Umgang mit Informationssicherheitsereignissen/-vorfällen
c) Änderungsmanagement und Freigabeprozesse
d) Verantwortlichkeiten
e) Logging & Monitoring
f) Externe Partner (Dienstleister, Lieferanten etc.)

12.1.2 Änderungssteuerung

Eine geregelte Durchführung beinhaltet eine für Dritte nachvollziehbare Dokumentation.
Ein Change Management Prozess muss eingerichtet sein, um sicherzustellen, dass Änderungen an den IT-Systemen durch die verantwortlichen Teams in einer ordnungsgemäßen Art und Weise durchgeführt und mögliche Auswirkungen der Änderungen identifiziert werden.
Bevor Änderungen an IT-Systemen vorgenommen werden, sind diese hinsichtlich Funktionsfähigkeit und Wechselwirkungen mit anderen Systemen zu testen. Soweit möglich, ist dies auf entsprechenden Testsystemen vorzunehmen.
Jede Änderung muss kategorisiert werden und Aufschluss darüber geben, welche Änderungen als wichtige Änderung (major change) eingestuft sind.
Alle wichtigen Änderungen müssen dokumentiert und mindestens sechs Monate lang rückverfolgbar sein.
Diese Dokumentation kann in Form der Protokollierung mit Tools, über die Verwendung von Tickets oder in manueller Form erfolgen.

12.1.3 Kapazitätssteuerung

12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Es ist eine Trennung in Form dedizierter Rollen oder Serversysteme zu gewährleisten.

12.2 Schutz vor Schadsoftware

Ziel: Information und informationsverarbeitende Einrichtungen sind vor Schadsoftware geschützt.

12.2.1 Maßnahmen gegen Schadsoftware

Prinzipiell ist jedes IT-System in geeigneter Weise vor Schadsoftware zu schützen. Dabei sind folgende Aspekte zwingend zu berücksichtigen:

a) Mehrstufiges Sicherheitskonzept (mindestens auf Netzwerk-, E-Mail- und Datei-Level)
b) Zentrales Management von Software und Virenpattern durch eine definierte verantwortliche Einheit
c) Prozesse zur Alarmierung von Anwendern und Administratoren bei Virenbefall
d) Protokollierung von Ereignissen in Bezug auf Schadsoftware
e) Umgang mit verschlüsselten Daten

Von der grundsätzlichen Implementierung kann unter folgenden Voraussetzungen abgewichen werden wenn:

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

a) der Hersteller des IT-Systems oder -Verbunds explizit den Einsatz einer Software zum Schutz vor Schadsoftware verbietet oder
b) der Einsatz der Software zum Schutz vor Schadsoftware drastische Performance-Einbußen bzw. Instabilitäten erzeugt oder
c) durch sonstige Maßnahmen sichergestellt ist, dass keinerlei Schadsoftware auf die Systeme ohne Schutz gelangen kann.

Die Software zum Schutz vor Schadsoftware muss regelmäßig, mindestens einmal täglich aktualisiert werden und folgende Merkmale aufweisen:

a) Prüfung aller Dateien, die auf elektronischen Medien bereitgestellt oder über Netze empfangen wurden;
b) Überprüfung von E-Mail-Anhängen und Downloads vor deren Verwendung;

Mindestens einmal pro Monat muss ein Komplett-Scan durchgeführt werden.
Es muss sichergestellt werden, dass durch infizierte Dateien kein weiterer Schaden verursacht werden kann (Löschen der Dateien; Verschieben in Quarantäne).

12.3 Datensicherung

Ziel: Daten sind vor Verlust geschützt.

12.3.1 Sicherung von Information

Es muss ein Datensicherungskonzept erarbeitet und umgesetzt werden, das die Anforderungen der Geschäftsprozesse berücksichtigt.
Die Funktionsfähigkeit von Backup und Restore – einschließlich der Prüfung der Backup-Logs, regelmäßiger Restore-Tests – muss sichergestellt werden.
Vor Inbetriebnahme eines Systems muss mindestens ein Restoretest durchgeführt werden.
Eine Archivierung muss entsprechend der aktuell gültigen gesetzlichen Regelungen bzw. entsprechend den Anforderungen der Geschäftsprozesse durchgeführt werden.
Sämtliche relevanten Informationen müssen auf Basis der Verfügbarkeitsanforderungen gesichert werden.
Das angewandte Sicherungsverfahren muss für jedes IT-System dokumentiert werden. Die Dokumentation muss dabei Angaben zur Technik, zu Backupintervallen, zu Art und Umfang der Backups sowie zu Aufbewahrungszeiten der Backupmedien enthalten.
Jeder Backupvorgang ist zu protokollieren. Die Protokolle müssen regelmäßig auf Vorhandensein und Vollständigkeit sowie hinsichtlich des Backupergebnisses überprüft werden.
Backups sind in regelmäßigen Abständen zu überprüfen. Hierzu zählen auch die Überprüfung des Inhalts der Backupmedien und die Wiederherstellung der Backupinformationen (Restore) auf einem geeigneten Prüfsystem.
Alle Backupmedien sind an einem sicheren und für die jeweiligen Medien geeigneten Ort, getrennt vom Betriebsort (unter Berücksichtigung von Brandschutzmaßnahmen), aufzubewahren. Bei Transport und Aufbewahrung sind die Backupmedien entsprechend des Schutzbedarfs der darauf gespeicherten Informationen in geeigneter Weise zu schützen.

12.4 Protokollierung und Überwachung

Ziel: Ereignisse sind aufgezeichnet und Nachweise sind erzeugt.

12.4.1 Ereignisprotokollierung

Die Aufbewahrungsdauer von Protokolldaten ist in Abstimmung mit dem Datenschutz-Beauftragten und dem Betriebsrat festzulegen und sollte mindestens 90 Tage betragen.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Die nachfolgenden Aktivitäten und Transaktionen sind zu protokollieren:
a) Anmeldeversuche
b) Verwendung administrativer Funktionen (z. B. Benutzerwechsel)
Vertrauliche Daten, wie z. B. Passwörter, dürfen nicht protokolliert werden.
Es sind Protokollierungsmechanismen für eigenen Code zu verwenden und die entsprechenden Funktionen der Produkte, die eingesetzt werden (Web-Server, Anwendungsserver, Datenbank, Betriebssystem usw.) sind zu aktivieren.
Interne Systemmeldungen (Log-Files) müssen auf erkennbare Missbrauchsversuche (z. B. Passwortraten) überwacht werden.

12.4.2 Schutz der Protokollinformation

Die Protokolldateien müssen gegen ein Überschreiben (z. B. durch Überlauf) innerhalb des Aufbewahrungszeitraums geschützt werden.

12.4.3 Administratoren- und Bedienerprotokolle

Die Protokolle von Systemadministratoren oder Betreibern sind regelmäßig zu kontrollieren.
Die Überwachung muss mindestens die nachfolgenden Ereignisse umfassen:
a) genehmigter Zugang
b) alle privilegierten Operationen
c) unbefugte Zugriffsversuche
d) Systemalarme und Fehler
e) Änderungen oder der Versuch von Änderungen an den Sicherheitseinstellungen des Systems oder an dessen Sicherheitsmaßnahmen.

12.4.4 Uhrensynchronisation

12.5 Steuerung von Software im Betrieb

Ziel: Die Integrität von Systemen im Betrieb ist sichergestellt.

12.5.1 Installation von Software auf Systemen im Betrieb

Es sind Härtungsmaßnahmen vor Inbetriebnahme einer Anwendung oder eines Systems durchzuführen, die insbesondere folgende Punkte beinhalten:
a) die Deaktivierung sämtlicher nicht erforderlicher Dienste,
b) die Deaktivierung oder Deinstallation sämtlicher nicht erforderlicher Anwendungen sowie
c) die Berücksichtigung von herstellerspezifischen Hinweisen zur sicheren Konfiguration der Anwendungen und Systeme.
Anwendungen und Betriebssystemsoftware sollten nur nach ausgiebigen und erfolgreichen Tests eingespielt werden. Die Tests sollten Benutzbarkeit, Sicherheit, Nebenwirkungen auf andere Systeme beinhalten und auf separaten Systemen (siehe auch14.2.8) durchgeführt werden.

12.6 Handhabung technischer Schwachstellen

Ziel: Die Ausnutzung technischer Schwachstellen ist verhindert.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

12.6.1 Handhabung von technischen Schwachstellen

Es ist sicherzustellen, dass eine Überwachung und ggf. Überprüfung von Schwachstellen und die entsprechenden Bereitstellungen von Patches und Fixes erfolgt und eine zeitnahe Bekanntgabe für angemessene Tests und Überprüfungen stattfindet.
Es ist sicherzustellen, dass ein Patch-Prozess etabliert ist, der mindestens die nachfolgenden Aspekte enthält:

a) Identifikation der zu überwachenden und zu patchenden Anwendungen und Systeme.
b) Definition von Verantwortlichkeiten für die Überwachung und Risikobewertung von Schwachstellen sowie die Durchführung und Prüfung von Aktualisierungen
c) Patches sind vor dem Rollout auf Funktionsfähigkeit und Wechselwirkungen mit relevanten Anwendungen und Systemen zu testen.
d) Patches sind in Abhängigkeit der Kritikalität des Patches und der betroffenen Systeme (Vertraulichkeits-, Integritäts- sowie Verfügbarkeitsanforderungen) zeitnah zu installieren.
e) Der aktuelle Patch-Level sowie fehlende Patches müssen zu jeder Zeit für jedes System nachvollziehbar sein.

Ports, Dienste und ähnliche Einrichtungen, die auf einem Computer oder in einer anderen Komponente vorhanden und für den Betrieb nicht unbedingt erforderlich sind, müssen deaktiviert, entfernt oder anderweitig geschützt werden.

12.6.2 Einschränkungen von Softwareinstallation

12.7 Audits von Informationssystemen

Ziel: Die Auswirkung von Audittätigkeiten auf Systeme im Betrieb ist minimiert.

12.7.1 Maßnahmen für Audits von Informationssystemen

12.7.2 Penetrationsprüfungen von Anwendungen

Luftverkehrsspezifische Umsetzungsvorgaben (gem. CoPiP 3.2)

Regelmäßige Penetrationsprüfungen von Anwendungen sollten bei geschäftskritischen Anwendungen jedes Jahr festgelegt sein. Außerdem sollten Penetrationsprüfungen nach jeder wesentlichen Aktualisierung oder Änderung einer Anwendung erfolgen (z. B. wenn der Umgebung eine neue Anwendung hinzugefügt wurde, wenn eine wesentliche Funktion in eine Anwendung eingefügt wurde usw.).
Die Häufigkeit und der Grad der Prüfungen sollten dem Grad entsprechen, in dem die Anwendungen organisationsübergreifend eingesetzt sind. Im Allgemeinen dürfen automatische Sicherheitsscanner verwendet werden, aber die Scan-Ergebnisse müssen durch eine manuelle Überprüfung eingefügt werden (um falschpositive und falschnegative Ergebnisse zu entfernen) sowie über genaue Prüfungen auf der Grundlage einer formellen methodischen Vorgehensweise.
Die Arbeitsgruppe, die die Penetrationsprüfungen durchführt, darf aus externen oder organisationsinternen Personen zusammengesetzt sein. Ihre Mitglieder sollten über nachgewiesene Erfahrungen auf dem Gebiet der vorausschauenden Sicherheit verfügen und sollten regelmäßige Sicherheitsschulungen besuchen, um umsetzbare Ergebnisse sicherzustellen.

Weitere Informationen

Eine Penetrationsprüfung ist ein vorausschauender Sicherheitsdienst, der die Ausführung vollständiger ethischer Hacking-Prüfungen umfasst. Sie beruht auf intelligenten Angriffstechniken, die dazu dienen, Schwachstellen zu identifizieren, die allein mittels automatischer Sicherheitsscanner nicht entdeckt werden können.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Sofern die Penetrationsprüfungen von Anwendungen ordnungsgemäß durchgeführt werden, führen sie zu einer objektiven und wiederholbaren Beurteilung der Sicherheitslage von Anwendungen. Somit können sie Sicherheitsschwachstellen bezüglich der Konstruktion, Umsetzung und Konfiguration aufdecken.

12.7.3 Penetrationsprüfungen von Infrastrukturen

Luftverkehrsspezifische Umsetzungsvorgaben (gem. CoPiP 3.2)

Regelmäßige Penetrationsprüfungen sollten jedes Jahr durchgeführt werden. Außerdem sollten Penetrationsprüfungen nach jeder wesentlichen Aktualisierung oder Änderung der Infrastruktur erfolgen (z. B. Aktualisierung des Betriebssystems, wenn ein neues Subnetz in die Netzwerkumgebung eingefügt wurde usw.).
Der Grad der Prüfungen sollte dem Grad entsprechen, in dem das System und das Netz organisationsübergreifend eingesetzt sind. Im Allgemeinen dürfen automatische Sicherheitsscanner verwendet werden, aber die Scan-Ergebnisse müssen durch eine manuelle Überprüfung eingefügt werden (um falschpositive und falschnegative Ergebnisse zu entfernen) sowie über genaue Prüfungen auf der Grundlage einer formellen methodischen Vorgehensweise. Anschlussstellen nach außen sollten regelmäßig nach aktuellen Normen auf Sicherheitsschwachstellen geprüft werden. Die Arbeitsgruppe, die die Penetrationsprüfungen durchführt, darf aus externen oder organisationsinternen Personen zusammengesetzt sein. Ihre Mitglieder sollten über nachgewiesene Erfahrungen auf dem Gebiet der vorausschauenden Sicherheit verfügen und sollten regelmäßige Sicherheitsschulungen besuchen, um umsetzbare Ergebnisse sicherzustellen.

Weitere Informationen

Eine Penetrationsprüfung ist ein vorausschauender Sicherheitsdienst, der die Ausführung vollständiger ethischer Hacking-Prüfungen umfasst. Sie beruht auf intelligenten Angriffstechniken, die dazu dienen, Schwachstellen zu identifizieren, die allein mittels automatischer Sicherheitsscanner nicht entdeckt werden können. Sofern die Penetrationsprüfungen von Infrastrukturen ordnungsgemäß durchgeführt werden, führen sie zu einer objektiven und wiederholbaren Beurteilung der Sicherheitslage von Systemen und Netzen im Allgemeinen. Eine der verbreitetsten methodischen Vorgehensweisen für Penetrationsprüfungen ist das Open Source Security Testing Methodology Manual (siehe www.osstmm.org).

13 Kommunikationssicherheit

13.1 Netzwerksicherheitsmanagement

Ziel: Der Schutz von Information in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen ist sichergestellt.

13.1.1 Netzwerksteuerungsmaßnahmen

Öffentlich zugängliche Systeme müssen mit Sicherheitsmechanismen ausgestattet werden, die eine Verbindung nur zu erlaubten Systemen zulassen.
Eine angemessene Protokollierung und Überwachung muss angewandt werden.
Fremdsysteme dürfen nur über entsprechende Schutzmechanismen (Firewall, Proxy etc.) an die IT-Systeme des FMG-Konzerns angeschlossen werden.
Ausnahmen dürfen vom Betreiber des internen Netzes nur genehmigt werden, wenn sichergestellt ist, dass diese Systeme vor Verbindungsaufbau umfassend und aktuell auf Viren und bösartige oder nicht erwünschte Anwendungen überprüft werden und somit keine Gefährdungen für die IT-Systeme des FMG-Konzerns darstellen. Eine Prüfung kann erfolgen durch

a) den Betreiber des internen Netzes

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

b) den Bediener des Fremdsystems, sofern vom Eigentümer vertraglich zugesichert ist, dass das System ISEC-Richtlinien-konform betrieben wird

Ausnahmen dürfen vom Betreiber des internen Netzes nur genehmigt werden, wenn sichergestellt ist, dass diese Systeme vor Verbindungsaufbau umfassend und aktuell auf Viren und bösartige oder nicht erwünschte Anwendungen überprüft werden und somit keine Gefährdungen für die IT-Systeme des FMG-Konzerns darstellen. Eine Prüfung kann erfolgen durch

a) den Betreiber des internen Netzes
b) den Bediener des Fremdsystems, sofern vom Eigentümer vertraglich zugesichert ist, dass das System ISEC-Richtlinien-konform betrieben wird

Alle relevanten Informationen (z. B. Netzwerkpläne, IP-Adressbereiche) zu den bei bzw. explizit für den FMG-Konzern betriebenen Netzwerken sind in einem zentralen Bestandsverzeichnis zu pflegen.
Bei der Planung und Umsetzung von Maßnahmen für Netzwerke sind die Anforderungen

a) an die Verfügbarkeit,
b) an Vertraulichkeit und Integrität (insbesondere bei Informationsaustausch über öffentliche Netzwerke)

zu berücksichtigen.

13.1.2 Sicherheit von Netzwerkdiensten

Informationen über Netzwerkdesign und Maßnahmen zum Schutz von Netzdiensten sind mindestens als „Vertraulich“ einzustufen und in entsprechender Weise zu schützen.
Das FMG-Konzern-System ist regelmäßig auf nicht autorisierte verbundene Netzwerke (z. B. nicht von IT bereitgestellte WLANs) zu überprüfen und diese ggf. außer Betrieb zu nehmen.
Systeme oder Netze, die für Remote-Zugriffe genutzt werden, müssen gegen unbefugten Zugriff geschützt werden. Sie müssen mit einer sicheren Konfiguration inkl. Virenschutz und sicherer Authentifizierung ausgerüstet werden.
Remote-Zugriffsverbindungen müssen von Produktionsnetzwerken durch Firewall-Mechanismen getrennt werden.
Remote-Zugriffe über öffentliche Netze (z. B. Internet) müssen durch den Einsatz eines verschlüsselten VPNs abgesichert werden. Bei einer ISDN-Verbindung mit vordefiniertem Rückruf (predefinied callback) oder einer Verbindung über eine private Standleitung (ISDN, ATM) ist keine VPN-Verschlüsselung notwendig.
Remote-Zugriffe über Transfernetze müssen generell verschlüsselt werden, es sei denn, der Betreiber des Fremd-Netzwerkes betreibt dieses konform zu den Anforderungen dieser Richtlinie.
Die Verbindungsdaten von Remote-Zugriffssitzungen müssen protokolliert werden.
Die Remote-Zugriffsysteme und das Netz, in dem sie sich befinden, müssen in Übereinstimmung mit den Anforderungen dieses Standards betrieben werden.
Der Zugriff auf Remote Services ist durch eine 2-Faktor-Authentifizierung zu schützen. Ausgenommen hiervon ist ein Zugriff auf:

- von der FMG bereitgestellte bzw. im Auftrag der FMG betriebene Webservices,
- Geschäftsinformationen über öffentliche Netze von mobilen Geräten, sofern hierfür eine Identifikation und Authentisierung unter Anwendung angemessener Zugangskontrollmechanismen erforderlich ist.

13.1.3 Trennung in Netzwerken

a) Alle Verbindungen zwischen dem internen Netzwerk des FMG-Konzerns und externen Netzwerken (z. B. dem Internet und Netzwerken von Lieferanten oder Partnern des FMG-Konzerns) müssen durch technische Maßnahmen (z. B. Firewall) und Zugriffskontrollmechanismen gesichert werden.
b) Zugänge zu FMG-Konzern-Netzwerken (z. B. Netzwerkdosen, Netzwerkkabel) in physisch öffentlich zugänglichen Bereichen sind zu vermeiden. Sofern erforderlich müssen diese durch geeignete physische (z. B. Absperren) oder logische (z. B. ACL, Netzwerkzugangskontrollsysteme) Sicherheitsmaßnahmen vor unberechtigter Nutzung geschützt werden.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

c) Drahtlose Netze müssen von internen und privaten Netzen getrennt werden, falls keine starke Authentifizierung wie beispielsweise WPA2 beim Zugriff auf das Netzwerk stattfindet.

13.2 Informationsübertragung

Ziel: Die Sicherheit von übertragener Information, sowohl innerhalb einer Organisation als auch mit jeglicher externen Stelle, ist aufrechterhalten.

13.2.1 Richtlinien und Verfahren für die Informationsübertragung

Bezüglich des Umgangs mit vertraulichen Informationen muss beim FMG-Konzern und von ihm beauftragten Dienstleistern die „Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen“ eingehalten werden.

13.2.2 Vereinbarungen zur Informationsübertragung

Bezüglich des Umgangs mit vertraulichen Informationen muss beim FMG-Konzern und von ihm beauftragten Dienstleistern die „Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen“ eingehalten werden.

13.2.3 Elektronische Nachrichtenübermittlung

Bezüglich des Umgangs mit vertraulichen Informationen muss beim FMG-Konzern von ihm beauftragten Dienstleistern die „Richtlinie zum Umgang mit Informationen unterschiedlicher Vertraulichkeitsklassen“ eingehalten werden.

13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

a) In einem direkten Auftraggeber-/Auftragnehmerverhältnis muss die FMG-Konzern-spezifische Vertraulichkeitsvereinbarung verwendet werden.
b) Zwischen Auftraggeber und Auftragnehmer muss eine Vertraulichkeitsvereinbarung vorliegen.
c) Anpassungen bzw. fremde Vertraulichkeitsvereinbarungen müssen durch die Rechtsabteilung des FMG-Konzerns freigegeben werden.

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

14.1 Sicherheitsanforderungen an Informationssysteme

Ziel: Es ist sichergestellt, dass Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus von Informationssystemen ist. Dies beinhaltet auch die Anforderungen an Informationssysteme, die Dienste über öffentliche Netze bereitstellen.

14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen

Bei der Definition von Sicherheitsanforderungen sind folgende Punkte zu berücksichtigen:
a) Durchführung einer frühzeitigen Schutzbedarfsanalyse der betroffenen Systeme/Informationen,

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

b) Durchführung einer Gefährdungsanalyse mit Bedrohungen und Schwachstellen,
c) Definition und Abfrage von Sicherheitsanforderungen an den möglichen Lieferanten sowie das zu beauftragende System im Rahmen der Auftragsbeschreibung,
d) Erstellung eines Sicherheitskonzeptes für Systeme mit hohem oder sehr hohem Schutzbedarf.
e) Die Verpflichtung zur Durchführung eines Vulnerability Scans mit definiertem Umfang/Scope vor Inbetriebnahme von Systemen und Anwendungen, die aus dem Internet erreichbar sind.
f) Die Freigabe neuer Systeme muss durch das Management erfolgen.
g) Das Management muss festlegen, in welchem Rahmen die Wartung und Erfüllung der Sicherheitsanforderungen erfolgt und wer für diese verantwortlich ist.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Sicherheitsanforderungen und -maßnahmen sollten die Sicherheitsanforderungen der betroffenen externen Organisationen, die an gemeinsamen Geschäftsprozessen beteiligt sind, berücksichtigen.

14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken

Ein Sicherheitskonzept für E-Commerce-Anwendungen muss erstellt werden. Dieses muss mindestens die folgenden Punkte enthalten:
a) Eindeutige Authentisierung der relevanten Parteien
b) die Sicherstellung der Vertraulichkeit, Integrität sowie der Nichtabstreitbarkeit jeglicher Bestelltransaktion, Zahlungsinformation, Lieferadresse sowie der Bestätigung von Rechnungen
c) Die Aufrufbarkeit der Geschäftsbedingungen bei Vertragsabschluss.

Bei Systemen, die Kreditkartendaten speichern, sind zwingend die Vorgaben des PCI DSS einzuhalten.
Bevor Informationen öffentlich bereitgestellt werden, muss deren Veröffentlichung durch den Informationsverantwortlichen genehmigt werden.
Die Integrität öffentlich zugänglicher Informationen muss durch geeignete Maßnahmen (z. B. Absicherung von Webservern und Applikationen) gegen unberechtigte Veränderungen geschützt werden.
Das öffentlich zugängliche System ist auf Schwachstellen und Fehler zu untersuchen, bevor dort Informationen bereitgestellt werden.
Es ist sicherzustellen, dass der Zugriff auf das Veröffentlichungssystem keinen unbeabsichtigten bzw. unerlaubten Zugriff auf Netze ermöglicht, die an das System angeschlossen sind.

14.1.3 Schutz der Transaktionen bei Anwendungsdiensten

14.1.4 Richtlinie für Webanwendungen/Web-Services

Die folgenden Regelungen für Genehmigungsverfahren bei neuen informationsverarbeitenden Einrichtungen (insbesondere neue Technologien) müssen betrachtet werden:
a) Die Freigabe neuer Systeme muss durch das Management erfolgen.
b) Das Management muss festlegen, in welchem Rahmen die Wartung und Erfüllung der Sicherheitsanforderungen erfolgt und wer für diese verantwortlich ist.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Leitlinie sollte insbesondere die Authentizität und Integrität der in Web-Anwendungen verwendeten Informationen abdecken.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

Ziel: Es ist sichergestellt, dass Informationssicherheit im Entwicklungszyklus von Informationssystemen geplant und umgesetzt ist.

14.2.1 Richtlinie für sichere Entwicklung

14.2.2 Verfahren zur Verwaltung von Systemänderungen

Die Einführung von neuen Systemen und größeren Änderungen an bestehenden Systemen muss einem formalen Prozess folgen, der eine Risikobetrachtung, Dokumentation, Spezifikation, Tests, Qualitätskontrolle und Maßnahmen für eine kontrollierte Umsetzung beinhaltet.
Es ist sicherzustellen, dass Änderungen nur von befugten Benutzern eingereicht oder durchgeführt werden.
Es ist klar zu regeln, unter welchen Voraussetzungen Änderungen durchgeführt werden und mit wem diese im Vorfeld abzustimmen sind.
Bei wesentlichen Änderungen muss die Möglichkeit zum Rollback auf den vorherigen Zustand gegeben sein.
Es ist sicherzustellen, dass die Implementierung von Änderungen zu einem mit den betroffenen Bereichen abgestimmten Zeitpunkt erfolgt.

14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform

Es ist sicherzustellen, dass relevante Änderungen auch in den Business-Continuity-Plänen (siehe Abschnitt 17) berücksichtigt werden.

14.2.4 Beschränkung von Änderungen an Softwarepaketen

14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme

- Benutzer dürfen nur die absolut notwendigen technischen Informationen in der Fehlermeldung erhalten. Inkonsistenzen, die zur unbeabsichtigten Offenlegung von Informationen führen oder Angriffe begünstigen könnten, sind durch das Abdecken
  aller Ausnahmen, die in der Anwendung bzw. dem Framework und den APIs (Application Programming Interfaces) vorkommen, zu vermeiden.
- Ausführliche Fehlermeldungen sind im Fehlerprotokoll festzuhalten und sollten eine Fehler-ID enthalten. Mit dieser Fehler-ID kann eine Fehlermeldung, welche dem Benutzer angezeigt wird, die detaillierte (technische) Fehlermeldung referenzieren.
- Die Behandlung und Verbreitung von Fehlern und Ausnahmen innerhalb der Anwendung ist sorgfältig zu planen.
- Bei der Planung und Realisierung von Anwendungen und Systemen ist zu berücksichtigen, dass diese keine vertraulichen Daten preisgeben, die einem Angreifer eventuelle Schwachstellen in der Anwendung aufzeigen (z. B. detaillierte Versionsnummern, Patchstände etc.).

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

14.2.6 Sichere Entwicklungsumgebung

14.2.7 Ausgegliederte Entwicklung

14.2.8 Testen der Systemsicherheit

14.2.9 Systemabnahmetest

Luftverkehrsspezifische Umsetzungsvorgaben

Die Abnahme von Systemen, die in organisationsübergreifenden Prozessen eingesetzt werden, sollte einen formalen Prozess beinhalten, der sicherstellt, dass die Systemabnahme-Anforderungen und -kriterien mit der in Abschnitt 4 beschriebenen gemeinsamen Risikobewertung in Einklang stehen.

14.2.10 Entwicklung von Anwendungen

Luftverkehrsspezifische Umsetzungsvorgaben

Die folgenden Schlüsselbereiche bei der Entwicklung von Webanwendungen sollten abgedeckt sein:

- Sicherheitsarchitektur;
- Authentisierung;
- Verwaltung von Sitzungen;
- Zugangskontrolle;
- Validierung von Eingabedaten;
- Ausgabecodierung/Escaping;
- Kryptografie;
- Fehlerbehandlung und Ereignisprotokollierung;
- Datenschutz;
- Kommunikationssicherheit;
- HTTP Sicherheit;
- Sicherheitskonfiguration.

Für jede spezielle Webanwendung sollten die maßgeblichen Sicherheitsmaßnahmen umgesetzt werden.

Weitere Informationen:

Die Entwicklungsleitlinie des OWASP erklärt, wie Webanwendungen anzulegen sind, damit sie die Anforderungen an die Verifizierungsstufen für Anwendungssicherheit, die in der Application Security Verification Standard (ASVS) des OWASP festgelegt sind, erfüllen oder übererfüllen. Die Verifizierungsstufen für Anwendungssicherheit konzentrieren sich auf die Analyse von Bauteilen, die die Anwenderebene des OSI-Modells darstellen. Die Leitlinie wurde mit folgenden Zielen entwickelt:

- Verwendung als Bezug;
- Verwendung, um Design-Entscheidungen zu treffen;
- Verwendung als Anleitung.

14.2.11 Code-Reviews

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte Code-Reviews entweder durch Anwendung von Werkzeugen für eine automatische statische Codeanalyse, durch manuelle Überprüfung oder beides durchführen.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Weitere Informationen

Ein Code-Review ist eine systematische Überprüfung des Quellcodes. Es wird damit beabsichtigt, Fehler zu erkennen und zu beheben, die in der anfänglichen Entwicklungsphase übersehen wurden, wodurch sich sowohl die Gesamtqualität der Software als auch die Fähigkeiten der Entwickler verbessern.

14.3 Testdaten

Ziel: Der Schutz von Daten, die für das Testen verwendet werden, ist sichergestellt.

14.3.1 Schutz von Testdaten

Produktivdaten oder Teile von Produktivdaten, die zu Testzwecken genutzt werden sollen, müssen grundsätzlich durch geeignete Verfahren (z. B. Scrambling, Pseudonymisierung) verfremdet werden. Sofern dies nicht möglich ist, sind Maßnahmen zum Schutz dieser Daten in Abhängigkeit ihrer Vertraulichkeit zu gewährleisten.

15 Lieferantenbeziehungen

15.1 Informationssicherheit in Lieferantenbeziehungen

Ziel: Für Lieferanten zugängliche Werte des Unternehmens sind geschützt.

15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen

Bei bereichsübergreifenden Geschäftsprozessen muss vertraglich eine genaue Abgrenzung der Verantwortlichkeiten für die Sicherheit von Assets (Services, Systeme etc.) festgelegt werden (Beispieltabelle zur Zuordnung von Mindestverantwortlichkeiten siehe Anhang 1).

Luftverkehrsspezifische Umsetzungsvorgaben

Die Offenlegung von Identitäten gegenüber Partnern sollte Teil der Vereinbarungen sein. In den Vereinbarungen sollten die Bedingungen für die Offenlegung eindeutig festgelegt sein. Bei Geschäftsprozessen, die mehrere Organisationen betreffen, sollte vertraglich eine genaue Abgrenzung der Verantwortlichkeiten für die Sicherheit von Werten (Assets) (siehe Abschnitt 8) festgelegt werden.

15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen

a) Externe müssen die Vertraulichkeitsvereinbarung (NDA) unterschreiben, bevor ihnen der Zugriff auf Informationen gewährt wird.
b) Die Verpflichtung zur Einhaltung der FMG-Richtlinien muss durch einen zeichnungsberechtigten Vertreter der externen Firma erfolgen und die Verpflichtung zur Weitergabe der Verpflichtung an alle für FMG tätigen Mitarbeiter und beauftragte Dienstleister beinhalten.
c) Bei der Definition von Sicherheitsanforderungen ist die ISEC-Richtlinie BE in der jeweils gültigen Fassung zu verwenden.
d) Es ist sicherzustellen, dass zu jedem Zeitpunkt der Zusammenarbeit mit Lieferanten Sicherheitsaspekte definiert und verbindlich vereinbart sind.
e) Dies beinhaltet insbesondere:
   - den Abschluss von Vertraulichkeitsvereinbarungen,

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

- die Verpflichtung des Lieferanten zur Information aller an der Auftragserfüllung beteiligten Personen über einzuhaltende Verpflichtungen/Sicherheitsaspekte,
- die Verpflichtung zur Meldung sämtlicher Ereignisse mit möglichen sicherheitsrelevanten Auswirkungen auf den Auftraggeber,
- die Verpflichtung des Lieferanten, die Einhaltung aller an ihn gestellten Sicherheitsanforderungen gegenüber Subunternehmen und Erfüllungsgehilfen sicherzustellen sowie
- die Vereinbarung des Rechts zur Prüfung von Sicherheitsanforderungen (Auditrecht)

15.1.3 Lieferkette für Informations- und Kommunikationstechnologie

15.2 Steuerung der Dienstleistungserbringung von Lieferanten

Ziel: Ein vereinbartes Niveau der Informationssicherheit und der Dienstleistungserbringung ist im Einklang mit Lieferantenverträgen aufrechterhalten.

15.2.1 Überwachung und Überprüfung von Lieferantendienstleistungen

Die Erfordernis sowie Art und Umfang von Überprüfungen der bei Lieferanten umgesetzten Sicherheitsmaßnahmen sind für die erteilten Aufträge festzulegen. Die Durchführung ist durch geeignete Personen vorzunehmen und zu dokumentieren.

15.3 Handhabung der Änderungen von Lieferantendienstleistungen

16 Handhabung von Informationssicherheitsvorfällen

16.1 Handhabung von Informationssicherheitsvorfällen und –verbesserungen

Ziel: Eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen einschließlich der Benachrichtigung über Sicherheitsereignisse und Schwächen ist sichergestellt.

16.1.1 Verantwortlichkeiten und Verfahren

Sicherheitsrelevante Vorfälle müssen analysiert und bewertet werden. Wenn im Rahmen der Bewertung Handlungsbedarf ermittelt wird, müssen entsprechende Maßnahmen ergriffen werden.

16.1.2 Melden von Informationssicherheitsereignissen

Jeder sicherheitsrelevante Vorfall muss dokumentiert und dem zuständigen Ansprechpartner gemeldet werden. Die Dokumentation muss mindestens die folgenden Punkte beinhalten:

a) Beschreibung des Vorfalls
b) Auswirkungen des Vorfalls
c) Reaktive Maßnahmen zur Schadensbeseitigung
d) Vorschlag für zukünftige proaktive Maßnahmen

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Allen Angestellten, Auftragnehmern und Drittbenutzern muss die Verpflichtung zur Meldung sicherheitsrelevanter Vorfälle bekannt sein. Dies beinhaltet auch die Kenntnis des Meldeverfahrens und des betreffenden Ansprechpartners.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte eine Arbeitsgruppe zur Reaktion auf Sicherheitsvorfälle einrichten, die entsprechend ausgebildet ist und über die Fertigkeiten verfügt, umgehend auf Sicherheitsvorfälle zu reagieren und die notwendigen Maßnahmen umzusetzen. Wenn ein Geschäftsprozess organisationsübergreifend betrieben wird, so sollten die einzelnen eingesetzten Arbeitsgruppen zur Reaktion auf Sicherheitsvorfälle – entsprechend den Anforderungen und der Risikobewertung für diesen Geschäftsprozess – aufeinander abgestimmt werden, oder es sollte gegebenenfalls eine gemeinsame Arbeitsgruppe zur Reaktion auf Sicherheitsvorfälle von den beteiligten Organisationen eingesetzt werden. Die Organisation sollte dazu einen Verantwortlichen für Fragen zum Umgang mit Sicherheitsvorfällen und die Kontakte für die operative Durchführung des Managements von Sicherheitsvorfällen benennen.
Die Organisation sollte darüber hinaus an vorhandenen organisationsübergreifenden Managementsystemen für Sicherheitsvorfälle teilnehmen, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden.
Eine angemessene Reaktionszeit der Arbeitsgruppe sollte sichergestellt sein.

16.1.3 Meldung von Schwächen in der Informationssicherheit

Jede Sicherheitsschwachstelle muss dem zuständigen Ansprechpartner gemeldet werden, um sicherheitsrelevante Vorfälle zu vermeiden.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte erkannte Sicherheitsschwachstellen bei Geschäftsprozessen, die mehrere Organisationen betreffen, umgehend an die anderen beteiligten Organisationen melden.
Die Organisation sollte in bereits vorhandenen übergreifenden Gremien und Foren, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden, mitarbeiten, um Informationen über Sicherheitsschwachstellen untereinander – soweit notwendig und für Dritte interessant – auszutauschen.

16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse

16.1.5 Reaktion auf Informationssicherheitsvorfälle

16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen

Verantwortliche Rollen: Auftraggeber/Projektmanager extern, IS-Beauftragter/Bereichs-IS-Beauftragter
Die Informationen, die durch die Auswertung von Informationssicherheitsvorfällen erhalten wurden, sollten dazu dienen, um sich wiederholende Vorfälle oder Vorfälle mit großer Auswirkung zu identifizieren.
Die Auswertung von Informationssicherheitsvorfällen kann den Bedarf für verbesserte oder zusätzliche Maßnahmen aufzeigen, um die Häufigkeit, den Schaden und die Kosten bei zukünftigen Vorfällen zu begrenzen, oder um im Überprüfungsprozess für die Sicherheitsleitlinie berücksichtigt zu werden (siehe 5.1.2).

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte in bereits vorhandenen Organisationen mitarbeiten, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden, um insbesondere für allgemeine Geschäftsprozesse gemeinsam aus Sicherheitsvorfällen zu lernen und entsprechende Maßnahmen abzuleiten.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

16.1.7 Sammeln von Beweismaterial

Für die Sammlung gerichtlich verwertbarer Beweise müssen interne Verfahren entwickelt und befolgt werden. Diese müssen u.a. die nachfolgenden Aspekte berücksichtigen:

a) Bei Papierdokumenten: Das Original wird sicher verwahrt, und es wird aufgezeichnet, wer es gefunden hat, wo es gefunden wurde, wann es gefunden wurde und wer Zeuge bei der Entdeckung war; Untersuchungen müssen sicherstellen, dass die Originale nicht verfälscht wurden;
b) Bei Informationen auf Computermedien: Zur Sicherstellung, dass Informationen verfügbar sind, müssen Spiegelungen oder Kopien aller mobilen Datenträger, Informationen auf Festplatten oder im Speicher erstellt werden; das Protokoll aller Tätigkeiten während des Kopierprozesses muss aufbewahrt und der Prozess von einem Zeugen beobachtet werden; das Original des Datenträgers und das Protokoll (falls dies nicht möglich ist, dann zumindest eine Spiegelung oder Kopie) müssen sicher verwahrt werden und unangetastet bleiben.

Jegliche forensische Arbeit darf nur an Kopien des Beweismaterials durchgeführt werden.

Luftverkehrsspezifische Umsetzungsvorgaben

Die Organisation sollte mit Organisationen, die Informationen sammeln und gemeinsam nutzen, zusammenarbeiten, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden.

17 Informationssicherheitsaspekte beim Business Continuity Management

17.1 Aufrechterhalten der Informationssicherheit

Ziel: Die Aufrechterhaltung der Informationssicherheit sollte in das Business Continuity Managementsystem der Organisation eingebettet sein.

17.1.1 Planung zur Aufrechterhaltung der Informationssicherheit

Risikoeinschätzungen zur Sicherstellung des Geschäftsbetriebs müssen unter voller Einbeziehung der Eigentümer von Geschäftsressourcen und Prozessen durchgeführt werden.
Die Einschätzung muss die Risiken identifizieren, quantifizieren und nach Kriterien und Zielen priorisieren, die für die Organisation wichtig sind.
Abhängig von den Ergebnissen der Risikoeinschätzung muss eine Strategie zur Sicherstellung des Geschäftsbetriebs entwickelt werden, um den Gesamtansatz der Sicherstellung des Geschäftsbetriebs festzulegen. Diese Strategie ist vom Management freizugeben, und es ist daraus resultierend ein Plan zur Umsetzung dieser Strategie zu erstellen.

Luftverkehrsspezifische Umsetzungsvorgaben

Die an einem gemeinsamen Geschäftsprozess beteiligten Organisationen sollten für den gesamten Vorgang eine Geschäftsauswirkungsanalyse durchführen.

Weitere luftverkehrsspezifische Informationen

Die Geschäftsauswirkungsanalyse sollte folgende Schritte nach ISO/IEC 27031:2011 enthalten:

- Auswahl der einzubeziehenden Organisationseinheiten und (Einzel-)Prozesse;
- Kritikalitätsanalyse für die betreffenden Werte (Assets);
- Festlegung von Kritikalitätskategorien und Schadensszenarien;

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

- Festlegung der zu betrachtenden Bewertungszeiträume;
- besondere Termine und Ereignisse;
- Kritikalitätsanalyse;
- Priorisierung der einzelnen Prozesse;
- Übersicht über Ressourcen für Normal- und Notbetrieb;
- Kritikalität und Wiederanlaufzeiten der Ressourcen;
- Berichterstattung.

Werden im laufenden Prozess Werte (Assets) ausgetauscht, so dass Änderungen in der Geschäftsauswirkungsanalyse nicht ausgeschlossen werden können, sollte die Geschäftsauswirkungsanalyse wiederholt werden. Die am Geschäftsprozess beteiligten Partner sollten umgehend darüber informiert werden.

17.1.2 Umsetzung der Aufrechterhaltung der Informationssicherheit

17.1.3 Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit

Notfallpläne müssen regelmäßig durch die beteiligten Organisationen getestet werden. Die daraus gewonnenen Ergebnisse müssen Input für die Verbesserung und Aktualisierung der Notfallpläne sein. Die Tests müssen dokumentiert werden. Um das Funktionieren der Notfallpläne sicherzustellen, müssen die beteiligten Organisationen folgendes durchführen:

a) Test und Abnahme der Notfallpläne vor Inbetriebnahme des Systems
b) Test und Abnahme der Notfallpläne bei kritischen System- und Prozessänderungen
c) Regelmäßiger Test aller Notfallpläne

Art und Umfang der Tests müssen sich an der Kritikalität des Geschäftsprozesses orientieren.
Die Verantwortung für regelmäßige Überprüfungen der Pläne zur Sicherstellung des Geschäftsbetriebs muss geregelt sein.
Verlauf und Ergebnisse der Tests müssen aufgezeichnet werden, und bei Bedarf sind Maßnahmen zu ergreifen und die Pläne zu optimieren.

Luftverkehrsspezifische Umsetzungsvorgaben

Das Rahmenwerk für Kontinuitätspläne sollte einen Terminplan für die Überprüfung und Aktualisierung der Kontinuitätspläne enthalten.
Kontinuitätspläne sollten regelmäßig durch die beteiligten Organisationen gemeinsam geprüft werden. Die daraus gewonnenen Informationen sollten als Eingabe für die Verbesserung und Aktualisierung der Kontinuitätspläne dienen. Die Prüfungen sollten dokumentiert werden. Um das ordnungsgemäße Funktionieren der Kontinuitäts-Kontingenzpläne sicherzustellen, sollten die beteiligten Organisationen folgende Maßnahmen durchführen:
Die Prüfung und Abnahme der Pläne sollte vor

- Inbetriebnahme des Systems/des Geschäftsprozesses,
- kritischen System- und Prozessänderungen erfolgen.
- Der Anwendungsbereich der Prüfungen sollte sich an der Kritikalität des Geschäftsprozesses orientieren.

17.1.4 Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs

Anforderung

- Der Prozess für ein Business Continuity Management muss mindestens die nachfolgenden Punkte enthalten:
  a) Identifikation aller organisationseigenen Werte (Assets), die zu kritischen Geschäftsprozessen gehören

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

b) Verstehen der Auswirkungen, die Informationssicherheitsvorfälle wahrscheinlich auf das Geschäft haben werden sowie Festlegung der Organisationsziele für Anwendungen und Systeme
c) Identifikation von zusätzlichen vorbeugenden und schadensmildernden Maßnahmen und Überlegungen zu deren Umsetzung
d) Formulierung und Dokumentation von Plänen zur Sicherstellung des Geschäftsbetriebs, die die Informationssicherheitsanforderungen in Übereinstimmung mit der vereinbarten Strategie zur Sicherstellung des Geschäftsbetriebs behandeln
e) regelmäßige Tests und Aktualisierungen der etablierten Pläne und Prozesse

- Auf Basis der Risikoeinschätzung müssen die beteiligten Bereiche einen Notfallplan erstellen. Dieser muss zumindest beinhalten:
  a) Verantwortlichkeiten
  b) Notfall-Situationen
  c) Ausweichmaßnahmen, alternative Betriebsverfahren
  d) Detaillierte Beschreibung der relevanten Notfallmaßnahmen
  e) Regelungen zu Prüfungen und Aktualisierungen der Notfallpläne

- Der Rahmen für die Pläne zur Sicherstellung des Geschäftsbetriebs muss die identifizierten Informationssicherheitsanforderungen behandeln und die folgenden Elemente berücksichtigen:
  a) die Bedingungen zum Inkrafttreten der Pläne, die den zu befolgenden Prozess beschreiben, bevor jeder Plan in Kraft tritt;
  b) Notfall-Verfahren, die die Aktionen beschreiben, die nach einem Vorfall zu ergreifen sind, der Geschäftsabläufe gefährdet;
  c) Ausweichmaßnahmen, die die Aktionen beschreiben, die zu ergreifen sind, um wichtige Geschäftsaktivitäten oder unterstützende Dienste vorübergehend zu alternativen Standorten umzusiedeln, und um Geschäftsprozesse innerhalb des geforderten Zeitraums wieder zum Laufen zu bringen;
  d) ein Wartungsplan, welcher spezifiziert, wie und wann der Plan getestet wird, und der Prozess zur Pflege des Plans;
  e) Maßnahmen zur Sensibilisierung, Ausbildung und Schulung, die entwickelt wurden, um Verständnis für die Prozesse zur Sicherstellung des Geschäftsbetriebs zu schaffen, und um sicherzustellen, dass die Prozesse weiterhin wirksam bleiben;
  f) die Verantwortung einzelner Personen, mit einer Beschreibung, wer für die Ausführung welcher Komponente des Plans verantwortlich ist. Vertreter sollten je nach Bedarf benannt sein.

Luftverkehrsspezifische Umsetzungsvorgaben

Die beteiligten Organisationen sollten einen organisationsübergreifenden Rahmen für den Plan zur Sicherstellung des Geschäftsbetriebs erstellen, der auf der Geschäftsauswirkungsanalyse beruht. Folgendes sollte darin mindestens enthalten sein:

- Personen in verantwortlichen Positionen bezüglich der gemeinschaftlichen Entscheidungsfindung;
- Notfallszenarien, die mehrere Organisationen betreffen,
- alternative Maßnahmen;
- alternative Betriebsverfahren;
- Aufbau der Kontinuitätspläne.

Aufgrund der geforderten hohen Verfügbarkeit von Geschäftsprozessen in der Luftfahrt sollte die Organisation in ihren Betriebsprozessen die Umstände dokumentieren, unter denen Kontinuitäts- oder Krisenpläne aktiviert werden.

17.2 Redundanzen

Ziel: Die Verfügbarkeit von informationsverarbeitenden Einrichtungen ist sichergestellt.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen

18 Compliance

18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

Ziel: Verstöße gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Verpflichtungen mit Bezug auf Informationssicherheit und gegen jegliche Sicherheitsanforderungen sind vermieden.

18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen

Luftverkehrsspezifische Umsetzungsvorgaben

Verpflichtungen zum Schutz kritischer Infrastrukturen auf nationaler und Europäischer Ebene könnten betrachtet werden.

18.1.2 Geistige Eigentumsrechte

Die Mitarbeiter sind in Bezug auf die Leitlinie zu sensibilisieren.
Die Beschaffung von Software darf nur über seriöse Anbieter erfolgen, um sicherzustellen, dass das Urheberrecht nicht verletzt wird.
Es ist sicherzustellen, dass zu jeder Zeit geeignete Nachweise für den Erwerb von Nutzungsrechten/Lizenzen erbracht werden können.
Es sind Maßnahmen zu etablieren, die garantieren, dass die Nutzungsrechte des Herstellers eingehalten werden.
Es sind regelmäßige Überprüfungen des eingesetzten Softwarebestandes vorzunehmen, um zu gewährleisten, dass nur genehmigte Software und lizenzierte Produkte installiert sind.

18.1.3 Schutz von Aufzeichnungen

Es sind Regelungen für die Aufbewahrung, Speicherung, Handhabung und Entsorgung von Aufzeichnungen und Informationen zu erstellen.
Ein Aufbewahrungsverzeichnis muss erstellt werden, das die Aufzeichnungen und die erforderlichen Aufbewahrungsfristen festlegt.
Es sind angemessene Maßnahmen umzusetzen, die Aufzeichnungen und Informationen vor Verlust, Zerstörung und Fälschung schützen. Dabei ist sicherstellen, dass verschlüsselte Informationen innerhalb des erforderlichen Zeitraums wieder entschlüsselt werden können.

18.1.4 Privatsphäre und Schutz von personenbezogener Information

Es ist eine Datenschutz- und Vertraulichkeitsleitlinie zu entwickeln und umzusetzen. Diese Leitlinie ist allen Personen bekannt zu machen, die an der Verarbeitung personenbezogener Daten beteiligt sind.
Die Verantwortung für den Umgang mit personenbezogenen Daten ist in Übereinstimmung mit den geltenden Gesetzen und Vorschriften zu definieren.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

18.1.5 Regelungen bezüglich kryptographischer Maßnahmen

Es sind Verfahren/Regelungen für die Nutzung von kryptografischen Maßnahmen zu etablieren, die mindestens die nachstehenden Aspekte berücksichtigen. Bei der Erstellung ist juristischer Rat einzuholen, um sicherzustellen, dass die Einhaltung der entsprechenden Gesetze gewährleistet ist.

a) Einschränkungen bezüglich des Imports und/oder Exports von Hard- und Software, die kryptographische Funktionen ausführen
b) Einschränkungen bezüglich des Imports und/oder Exports von Hard- und Software, die so gestaltet ist, dass kryptographische Funktionen hinzugefügt werden können
c) Einschränkungen bezüglich des Gebrauchs von Verschlüsselungsverfahren
d) Einschränkungen bei der Einführung verschlüsselter Systeme in bestimmte Länder

18.2 Überprüfungen der Informationssicherheit

Ziel: Informationssicherheit ist in Übereinstimmung mit den Richtlinien und Verfahren der Organisation umgesetzt und wird entsprechend angewendet.

18.2.1 Unabhängige Überprüfung der Informationssicherheit

a) Die Überprüfung muss die Untersuchung von Möglichkeiten zur Verbesserung und Untersuchungen des Bedarfs für Änderungen am generellen Ansatz für Sicherheit, einschließlich der Leitlinie und der Maßnahmenziele beinhalten.
b) Die Ergebnisse der unabhängigen Überprüfung müssen aufgezeichnet und dem Management berichtet werden.
c) Die Abarbeitung der identifizierten Maßnahmen muss regelmäßig überprüft werden.

18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards

Manager müssen regelmäßig die Einhaltung der in ihrem Verantwortungsbereich stattfindenden Informationsverarbeitung mit anwendbaren Sicherheitsleitlinien, -standards und allen anderen Sicherheitsanforderungen überprüfen.
Sofern im Rahmen der Überprüfungen Abweichungen festgestellt werden, muss der Manager sicherstellen, dass

a) der Bedarf für Maßnahmen bewertet wird, um sicherzustellen, dass die Abweichung nicht wieder auftritt
b) angemessene Korrekturmaßnahmen festgelegt und umsetzt werden
c) die ergriffenen Korrekturmaßnahmen überprüft werden

18.2.3 Überprüfung der Einhaltung von technischen Vorgaben

Prüfungen der Einhaltung technischer Standards sollten entweder manuell (falls nötig mit Unterstützung geeigneter Software-Tools) durch einen erfahrenen Systemingenieur und/oder mit Hilfe von automatisierten Tools durchgeführt werden, die einen technischen Bericht erzeugen, der anschließend durch einen technischen Spezialisten interpretiert wird.
Falls Penetrationstests oder Schwachstellenanalysen durchgeführt werden, so sollten diese mit Vorsicht geschehen, da solche Aktivitäten die Sicherheit des Systems gefährden könnten. Solche Tests sollten geplant und dokumentiert werden und wiederholbar sein. Alle Prüfungen der Einhaltung technischer Standards sollten nur durch kompetente, berechtigte Mitarbeiter oder unter der Aufsicht solcher Experten erfolgen.

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

Anhang 1: Beispieltabelle zur Zuordnung von Mindestverantwortlichkeiten der Informationssicherheit

Wert	Verantwortliche	Prozesse
Zugangsweg (z.B. WLAN, UMTS, Ethernet)		
Zone (z.B. internes Netz, eigenes VPN, externes Netz)		
Informationsverantwortlicher (Festlegung: Vertraulichkeit, Verfügbarkeit, Berechtigungen)		
Applikation		
Genutzte Applikationen (z.B. Apache, Tomcat)		
Runtime (z.B. Applikationsserver, Netframework, Java)		
Datenbank		
Middleware		
OS		
Virtueller Server		
Virtualisierungslösung		
Physikalische Server / Device		
Firewall		
Netzwerk		
Physikalischer Zugang (z.B. zum jeweiligen Server, Inforaum, Büro, RZ)		

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

20 Anhang 2: Zuordnung Controls zu Level of Trust, Vertraulichkeit und Verfügbarkeit

Die folgende Tabelle gibt einen Überblick über die zu erfüllenden Controls beim jeweiligen Level of Trust (LT). Zusätzlich stellt sie den jeweiligen Schutzbedarf aus Vertraulichkeits- bzw. Verfügbarkeits-Gesichtspunkt dar, ab dem das betreffende Controls ebenfalls umzusetzen ist.

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
5 Sicherheitsleitlinie					
5.1 Informationssicherheitsleitlinie					
5.1.1 Vorgaben der Leitung für Informationssicherheit	X	X	X	**dienstlich**	**mittel**
5.1.2 Überprüfung der Informationssicherheitsrichtlinien	X	X	X	**dienstlich**	**mittel**

CoPiP Controls aus ISO27001:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
5.2 Führung					
5.2.1 Führung und Verpflichtung (Referenz Kapitel 5.1)	X	X	X	**dienstlich**	**mittel**
5.2.2 Politik (Referenz Kapitel 5.2)	X	X	X	**dienstlich**	**mittel**
5.2.3 Managementbewertung (Referenz Kapitel 9.3)	X	X		**vertraulich**	**hoch**
5.2.4 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation (Referenz Kapitel 5.3)	X	X	X	**dienstlich**	**mittel**
5.2.5 Überwachung, Messung, Analyse & Bewertung (Referenz Kapitel 9.1)	X	X		**vertraulich**	**hoch**
5.2.6 Dokumentierte Information (Referenz Kapitel 7.5)	X	X		**vertraulich**	**hoch**

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
6 Organisation der Informationssicherheit					
6.1 Interne Organisation					
6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten	X	X	X	**dienstlich**	**mittel**
6.1.2 Aufgabentrennung	X			**streng vertraulich**	**sehr hoch**
6.1.3 Kontakt mit Behörden	X			**streng vertraulich**	**sehr hoch**
6.1.4 Kontakt mit speziellen Interessensgruppen	X			**streng vertraulich**	**sehr hoch**
6.1.5 Informationssicherheit im Projektmanagement	X			**streng vertraulich**	**sehr hoch**
6.2 Mobilgeräte und Telearbeit					

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
6.2.1 Richtlinie zu Mobilgeräten	X	X		vertraulich	hoch
6.2.2 Telearbeit	X	X		vertraulich	hoch
7 Personalsicherheit					
7.1 Vor der Beschäftigung					
7.1.1 Sicherheitsüberprüfung	X	X		vertraulich	hoch
7.1.2 Beschäftigungs- und Vertragsbedingungen	X			streng vertraulich	sehr hoch
7.2 Während der Anstellung					
7.2.1 Verantwortlichkeiten der Leitung	X	X		vertraulich	hoch
7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung	X	X	X	dienstlich	mittel
7.2.3 Maßregelungsprozess	X			streng vertraulich	sehr hoch
7.3 Beendigung und Änderung der Beschäftigung					
7.3.1 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	X			streng vertraulich	sehr hoch
8 Verwaltung der Werte					
8.1 Verantwortlichkeit für Werte					
8.1.1 Inventarisierung der Werte	X	X	X	dienstlich	mittel
8.1.2 Zuständigkeit für Werte	X	X		vertraulich	hoch
8.1.3 Zulässiger Gebrauch von Werten	X			streng vertraulich	sehr hoch
8.1.4 Rückgabe von Werten	X	X		vertraulich	hoch
8.2 Informationsklassifizierung					
8.2.1 Klassifizierung von Information	X	X	X	dienstlich	mittel
8.2.2 Kennzeichnung von Information	X	X		vertraulich	hoch
8.2.3 Handhabung von Werten	X	X		vertraulich	hoch
8.3 Handhabung von Datenträgern					
8.3.1 Handhabung von Wechseldatenträgern	X			streng vertraulich	sehr hoch
8.3.2 Entsorgung von Datenträgern	X			streng vertraulich	sehr hoch
8.3.3 Transport von Datenträgern					
9 Zugangssteuerung					
9.1 Geschäftsanforderungen an die Zugangssteuerung					
9.1.1 Zugangssteuerungsrichtlinie	X	X	X	dienstlich	mittel
9.1.2 Zugang zu Netzwerken und Netzwerkdiensten	X			streng vertraulich	sehr hoch
9.2 Benutzerzugangsverwaltung					

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
9.2.1 Registrierung und Deregistrierung von Benutzern	X	X	X	dienstlich	mittel
9.2.2 Zuteilung von Benutzerzugängen	X	X		vertraulich	hoch
9.2.3 Verwaltung privilegierter Zugangsrechte	X	X	X	dienstlich	mittel
9.2.4 Verwaltung geheimer Authentisierungs-information von Benutzern	X	X		vertraulich	hoch
9.2.5 Überprüfung von Benutzerzugangsrech-ten	X	X		vertraulich	hoch
9.2.6 Entzug oder Anpassung von Zugangs-rechten	X	X	X	dienstlich	mittel
9.2.7 Digitales Identitätsmanagement (Zusätz-liches CoPiP Control)	X			streng vertrau-lich	sehr hoch
9.2.8 Organisationsübergreifende eindeutige Darstellung von Entitäten (Zusätzliches CoPiP Control)	X			streng vertrau-lich	sehr hoch
9.3 Benutzerverantwortlichkeiten					
9.3.1 Gebrauch geheimer Authentisierungsin-formation	X	X	X	dienstlich	mittel
9.4 Zugangssteuerung für Systeme und An-wendungen					
9.4.1 Informationszugangsbeschränkung	X	X	X	dienstlich	mittel
9.4.2 Sichere Anmeldeverfahren	X	X	X	dienstlich	mittel
9.4.3 System zur Verwaltung von Kennwörtern	X	X		vertraulich	hoch
9.4.4 Gebrauch von Hilfsprogrammen mit privi-legierten Rechten					
9.4.5 Zugangssteuerung für Quellcode von Pro-grammen	X			streng vertrau-lich	sehr hoch
9.4.6 Web-Application Firewalls (Zusätzliches CoPiP Control)	X			streng vertrau-lich	sehr hoch
10 Kryptographie					
10.1 Kryptographische Maßnahmen					
10.1.1 Richtlinie zum Gebrauch von kryptogra-phischen Maßnahmen	X			streng vertrau-lich	sehr hoch
10.1.2 Schlüsselverwaltung	X			streng vertrau-lich	sehr hoch
11 Physische und umgebungsbezogene Si-cherheit					
11.1 Sicherheitsbereiche					
11.1.1 Physische Sicherheitsperimeter	X	X	X	dienstlich	mittel
11.1.2 Physische Zutrittssteuerung	X	X	X	dienstlich	mittel
11.1.3 Sichern von Büros, Räumen und Einrich-tungen	X			streng vertrau-lich	sehr hoch

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
11.1.4 Schutz vor externen und umweltbedingten Bedrohungen	X			streng vertraulich	sehr hoch
11.1.5 Arbeiten in Sicherheitsbereichen					
11.1.6 Anlieferungs- und Ladebereiche	X			streng vertraulich	sehr hoch
11.2 Geräte und Betriebsmittel					
11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln	X	X		vertraulich	hoch
11.2.2 Versorgungseinrichtungen	X	X	X	dienstlich	mittel
11.2.3 Sicherheit der Verkabelung	X			streng vertraulich	sehr hoch
11.2.4 Instandhaltung von Geräten und Betriebsmitteln	X			streng vertraulich	sehr hoch
11.2.5 Entfernen von Werten	X			streng vertraulich	sehr hoch
11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	X			streng vertraulich	sehr hoch
11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	X			streng vertraulich	sehr hoch
11.2.8 Unbeaufsichtigte Benutzergeräte	X	X	X	dienstlich	mittel
11.2.9 Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	X			streng vertraulich	sehr hoch
12 Betriebssicherheit					
12.1 Betriebsabläufe und -verantwortlichkeiten					
12.1.1 Dokumentierte Betriebsabläufe	X	X		vertraulich	hoch
12.1.2 Änderungssteuerung	X	X		vertraulich	hoch
12.1.3 Kapazitätssteuerung					
12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen	X			streng vertraulich	sehr hoch
12.2 Schutz vor Schadsoftware					
12.2.1 Maßnahmen gegen Schadsoftware	X	X	X	dienstlich	mittel
12.3 Datensicherung					
12.3.1 Sicherung von Information	X	X		vertraulich	hoch
12.4 Protokollierung und Überwachung					
12.4.1 Ereignisprotokollierung	X			streng vertraulich	sehr hoch
12.4.2 Schutz der Protokollinformation	X			streng vertraulich	sehr hoch
12.4.3 Administratoren- und Bedienerprotokolle	X	X		vertraulich	hoch

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
12.4.4 Uhrensynchronisation	X			streng vertraulich	sehr hoch
12.5 Steuerung von Software im Betrieb					
12.5.1 Installation von Software auf Systemen im Betrieb	X			streng vertraulich	sehr hoch
12.6 Handhabung technischer Schwachstellen					
12.6.1 Handhabung von technischen Schwachstellen	X	X	X	dienstlich	mittel
12.6.2 Einschränkungen von Softwareinstallation	X			streng vertraulich	sehr hoch
12.7 Audits von Informationssystemen					
12.7.1 Maßnahmen für Audits von Informationssystemen	X	X		vertraulich	hoch
12.7.2 Penetrationsprüfungen von Anwendungen (Zusätzliches CoPiP Control)	X	X	X	dienstlich	mittel
12.7.3 Penetrationsprüfungen von Infrastrukturen (Zusätzliches CoPiP Control)	X	X	X	dienstlich	mittel
13 Kommunikationssicherheit					
13.1 Netzwerksicherheitsmanagement					
13.1.1 Netzwerksteuerungsmaßnahmen	X	X	X	dienstlich	mittel
13.1.2 Sicherheit von Netzwerkdiensten	X	X		vertraulich	hoch
13.1.3 Trennung in Netzwerken	X	X		vertraulich	hoch
13.2 Informationsübertragung					
13.2.1 Richtlinien und Verfahren für die Informationsübertragung	X	X		vertraulich	hoch
13.2.2 Vereinbarungen zur Informationsübertragung	X			streng vertraulich	sehr hoch
13.2.3 Elektronische Nachrichtenübermittlung					
13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen	X	X	X	dienstlich	mittel
14 Anschaffung, Entwicklung und Instandhaltung von Systemen					
14.1 Sicherheitsanforderungen an Informationssysteme					
14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen	X			streng vertraulich	sehr hoch
14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	X	X		vertraulich	hoch
14.1.3 Schutz der Transaktionen bei Anwendungsdiensten	X	X		vertraulich	hoch

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
14.1.4 Richtlinie für Webanwendungen/Web-Services	X			streng vertraulich	sehr hoch
14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen					
14.2.1 Richtlinie für sichere Entwicklung	X			streng vertraulich	sehr hoch
14.2.2 Verfahren zur Verwaltung von Systemänderungen	X			streng vertraulich	sehr hoch
14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	X			streng vertraulich	sehr hoch
14.2.4 Beschränkung von Änderungen an Softwarepaketen					
14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	X			streng vertraulich	sehr hoch
14.2.6 Sichere Entwicklungsumgebung	X			streng vertraulich	sehr hoch
14.2.7 Ausgegliederte Entwicklung					
14.2.8 Testen der Systemsicherheit	X			streng vertraulich	sehr hoch
14.2.9 Systemabnahmetest	X			streng vertraulich	sehr hoch
14.2.10 Entwicklung von Anwendungen (Zusätzliches CoPiP Control)	X			streng vertraulich	sehr hoch
14.2.11 Code-Reviews (Zusätzliches CoPiP Control)	X			streng vertraulich	sehr hoch
14.3 Testdaten					
14.3.1 Schutz von Testdaten					
15 Lieferantenbeziehungen					
15.1 Informationssicherheit in Lieferantenbeziehungen					
15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen	X	X		vertraulich	hoch
15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen	X	X		vertraulich	hoch
15.1.3 Lieferkette für Informations- und Kommunikationstechnologie	X			streng vertraulich	sehr hoch
15.2 Steuerung der Dienstleistungserbringung von Lieferanten					
15.2.1 Überwachung und Überprüfung von Lieferantendienstleistungen	X			streng vertraulich	sehr hoch
15.2.2 Handhabung der Änderungen von Lieferantendienstleistungen	X			streng vertraulich	sehr hoch
16 Handhabung von Informationssicherheitsvorfällen					

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
16.1 Handhabung von Informationssicherheitsvorfällen und –verbesserungen					
16.1.1 Verantwortlichkeiten und Verfahren	X			**streng vertraulich**	**sehr hoch**
16.1.2 Melden von Informationssicherheitsereignissen	X	X		**vertraulich**	**hoch**
16.1.3 Meldung von Schwächen in der Informationssicherheit	X			**streng vertraulich**	**sehr hoch**
16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse	X	X		**vertraulich**	**hoch**
16.1.5 Reaktion auf Informationssicherheitsvorfälle	X	X		**vertraulich**	**hoch**
16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen	X			**streng vertraulich**	**sehr hoch**
16.1.7 Sammeln von Beweismaterial	X			**streng vertraulich**	**sehr hoch**
17 Informationssicherheitsaspekte beim Business Continuity Management					
17.1 Aufrechterhalten der Informationssicherheit					
17.1.1 Planung zur Aufrechterhaltung der Informationssicherheit	X			**streng vertraulich**	**sehr hoch**
17.1.2 Umsetzung der Aufrechterhaltung der Informationssicherheit	X			**streng vertraulich**	**sehr hoch**
17.1.3 Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit					
17.1.4 Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs (Zusätzliches CoPiP Control)	X			**streng vertraulich**	**sehr hoch**
17.2 Redundanzen					
17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen	X			**streng vertraulich**	**sehr hoch**
18 Compliance					
18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen					
18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	X			**streng vertraulich**	**sehr hoch**
18.1.2 Geistige Eigentumsrechte					
18.1.3 Schutz von Aufzeichnungen					
18.1.4 Privatsphäre und Schutz von personenbezogener Information	X	X	X	**dienstlich**	**mittel**
18.1.5 Regelungen bezüglich kryptographischer Maßnahmen					

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion

CoPiP Controls aus ISO27002:2013	LT1	LT2	LT3	Vertraulichkeit	Verfügbarkeit
18.2 Überprüfungen der Informationssicherheit					
18.2.1 Unabhängige Überprüfung der Informationssicherheit	X			**streng vertraulich**	**sehr hoch**
18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards	X	X	X	**dienstlich**	**mittel**
18.2.3 Überprüfung der Einhaltung von technischen Vorgaben	X	X	X	**dienstlich**	**mittel**

© Flughafen München
Information: Gedrucktes Dokument wird nicht überwacht, kein Änderungsdienst! Aktuelle Version: eMotion