Muster

Cyber-Luftsicherheitsprogramm

**für reglementierte Beauftragte, bekannte Versender und reglementierte Lieferanten**

Version 1.0

# Abkürzungsverzeichnis

|  |  |
| --- | --- |
| Grundsätze | *„Grundsätze zur Anwendung der Cybersicherheitsmaßnahmen der Verordnung (EU) 2015/1998 der Kommission zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit im Zuständigkeitsbereich des Bundesministeriums für Digitales und Verkehr (§§ 9 und 9a LuftSiG)“* |
| KIKS | *Kritische informations- und kommunikationstechnische Systeme* ***und Daten*** *(Definition siehe* ***„****Grundsätze zur Anwendung der Cybersicherheitsmaßnahmen der Verordnung (EU) 2015/1998 der Kommission zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit im Zuständigkeitsbereich des Bundesministeriums für Digitales und Verkehr (§§ 9 und 9a LuftSiG)“ Punkt 1.2.2)* |
| BSI | *Das* ***B****undesamt für* ***S****icherheit in der* ***I****nformationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland. (*[*https://www.bsi.bund.de/*](https://www.bsi.bund.de/)*)* |

Inhalt

[Abkürzungsverzeichnis 2](#_Toc184135136)

[0 Cybersicherheitsbeauftragte/r 4](#_Toc184135137)

[1 Grundsätzliches 5](#_Toc184135138)

[1.4 Melde- und Informationswesen 5](#_Toc184135139)

[2 Risikomanagement 6](#_Toc184135140)

[2.1 Ermittlung kritischer informations- und kommunikationstechnischer Systeme und Daten 6](#_Toc184135141)

[2.2 Risikobeurteilung - Risk assessment 7](#_Toc184135142)

[2.3 Risikobehandlung – Risk treatment 9](#_Toc184135143)

[2.4 Überwachung – Monitoring 9](#_Toc184135144)

[2.5 Cybersicherheitsreaktionsplan 10](#_Toc184135145)

[3 Personalangelegenheiten 11](#_Toc184135146)

[3.1 Zuverlässigkeitsüberprüfung 11](#_Toc184135147)

[3.2 Eignung 11](#_Toc184135148)

[3.3 Schulung 12](#_Toc184135149)

Die Nummerierung der Kapitel orientiert sich an den entsprechenden Kapiteln der Anwendungsgrundsätze zu §§9 und 9a LuftSiG.

# Cybersicherheitsbeauftragte/r

Die Person der/des „*Cybersicherheitsbeauftragten*“ ist identisch mit der Person der/des „(Luft-)Sicherheitsbeauftragten“.

Die folgende Person übernimmt die Rolle der/des „*Cybersicherheitsbeauftragten*“:

Name: Klicken oder tippen Sie hier, um Text einzugeben.

Telefon: Klicken oder tippen Sie hier, um Text einzugeben.

E-Mail: Klicken oder tippen Sie hier, um Text einzugeben.

# Grundsätzliches

## Melde- und Informationswesen

### Melde- und Informationsportal des BSI

Wir haben uns bislang nicht im Melde- und Informationsportal des BSI registriert.

|  |  |
| --- | --- |
|  | *Hinweis*:  *Über das Melde- und Informationsportal des BSI (*[*https://mip2.bsi.bund.de/*](https://mip2.bsi.bund.de/)*) sollten Störungen der Informationssicherheit gemeldet werden. Zudem erhalten die registrierten Unternehmen neben aktuellen Tageslageberichten und Cybersicherheitswarnungen, auch weiterführende Informationen zu gemeldeten Cybersicherheitsvorfällen und ggf. Hinweise bzgl. notwendiger Sicherheitsmaßnahmen.*  *Eine Registrierung wird empfohlen.* |

Wir haben uns bereits im Melde- und Informationsportal des BSI registriert.

### Informationsquellen

Die folgenden Quellen für Informationen zur Cybersicherheit in der zivilen Luftfahrt sind uns bekannt:

* Die Bausteine des BSI-Grundschutz auf der Webseite des BSI[[1]](#footnote-1) i. V. m. der Kreuzreferenztabelle zum IT-Grundschutz-Kompendium[[2]](#footnote-2)
* Informationen zu aktuellen Warnungen zu spezifischen IT-System-Elementen von der Allianz für Cyber-Sicherheit des BSI auf deren Webseite[[3]](#footnote-3)
* Aktuelle allgemeine Lagebilder der Bereiche IT-Sicherheit und Cybercrime vom BSI bzw. dem Bundeskriminalamt von deren Webseiten[[4]](#footnote-4)

# Risikomanagement

Wir haben einen Risikomanagementprozess unter Berücksichtigung der folgenden Unterabschnitte etabliert.[[5]](#footnote-5)

## Ermittlung kritischer informations- und kommunikationstechnischer Systeme und Daten

### Methodik

Wie wurden KIKS identifiziert?[[6]](#footnote-6)

Klicken oder tippen Sie hier, um Text einzugeben.

Welche Mitarbeitenden und Informationen wurden bei der Identifizierung einbezogen?

Klicken oder tippen Sie hier, um Text einzugeben.

### Auflistung KIKS

Basierend auf den Begriffsbestimmungen in Abschnitt 1.2 der *Grundsätze* haben wir die

* durch uns und/oder
* auftragsgemäß für uns durch einen Dienstleister bzw. Auftragnehmer

betriebenen informations- und kommunikationstechnischen Systeme und Daten ermittelt[[7]](#footnote-7), welche

1. aufgrund ihrer Bedeutung oder ihres Einflusses auf die Luftsicherheit als kritisch zu bewerten sind und
2. in der Bundesrepublik Deutschland einer Interaktion zugeführt werden oder unter der deutschen Gerichtsbarkeit oder Zugehörigkeit stehen.

Die Erhebung erfolgte unabhängig des Umstandes, ob bereits Sicherheitsmaßnahmen etabliert wurden.   
In den folgenden Anlagen sind neben dem *Zugang zur Unionsdatenbank/KSDA2* als Anlage 1 alle ermittelten KIKS aufgeführt[[8]](#footnote-8):

|  |  |
| --- | --- |
| **Anlagennummer** | **Bezeichnung des KIKS** |
| 1 | Zugang zur Unionsdatenbank/KSDA2 |
| 2 | … |

## Risikobeurteilung - Risk assessment

* + 1. **Gefährdungsübersicht – Risk identification[[9]](#footnote-9)**
       1. **Methodik**

Wie wurden die Gefährdungen ermittelt und welche Informationsquellen wurden genutzt?

Klicken oder tippen Sie hier, um Text einzugeben.

### Auflistung Gefährdungen

Zu den ermittelten KIKS wurde jeweils eine Gefährdungsübersicht erstellt.

Die ermittelten Gefährdungen sind im unmittelbaren Zusammenhang mit den KIKS in den Anlagen gemäß Kapitel 2.2 angegeben.

Die ermittelten Gefährdungen sind in folgenden Anlagen aufgeführt:

|  |  |
| --- | --- |
| **Anlagennummer** | **Bezeichnung der Gefährdung** |
| … | … |
| … | … |

* + 1. **Risikoeinschätzung – Risk analysis[[10]](#footnote-10)**

Die konkretisierten Gefährdungen wurden einer Risikoeinschätzung unterzogen und hinsichtlich der Eintrittshäufigkeit und der Schadenshöhe betrachtet.

Die Eintrittshäufigkeiten und die Schadenshöhen sind im unmittelbaren Zusammenhang mit den konkretisierten Gefährdungen der KIKS in den Anlagen gemäß Kapitel 2.3.1.2 angegeben*.*

Die Eintrittshäufigkeiten und die Schadenshöhen sind in folgenden Anlagen aufgeführt:

|  |  |
| --- | --- |
| **Anlagennummer** | **Bezeichnung des Risikos** |
| … | … |
| … | … |

* + 1. **Risikobewertung – Risk evaluation[[11]](#footnote-11)**

#### Methodik

Auf Grundlage der Risikoeinschätzung wurde eine Risikobewertung durchgeführt. Hierfür wurde die folgende qualitative Risikomatrix verwendet[[12]](#footnote-12):

Klicken oder tippen Sie hier, um Text einzugeben.

#### Auflistung Risikowerte

Die Ergebnisse der Risikobewertung sind im unmittelbaren Zusammenhang mit den konkretisierten Gefährdungen in den Anlagen gemäß Kapitel 2.3.1.2 angegeben*.*

Die Ergebnisse der Risikobewertung sind in folgenden Anlagen aufgeführt:

|  |  |
| --- | --- |
| **Anlagennummer** | **Bezeichnung des Risikos** |
| … | … |
| … | … |

## Risikobehandlung – Risk treatment[[13]](#footnote-13)

Die **Schutzmaßnahmen** (Maßnahmen zur Risikobehandlung), welche zur Reduzierung der im Rahmen der Risikobewertung ermittelten inakzeptablen Risiken[[14]](#footnote-14) beitragen, sind mit dem jeweiligen Bezugsrisiko verknüpft. Weiterhin sind auch die Auswirkungen der Schutzmaßnahmen auf den restlichen Risikowert dargestellt.

Die Schutzmaßnahmen sind mit ihren Auswirkungen auf die Risikowerte der konkretisierten Gefährdungen zu den KIKS in den Anlagen gemäß Kapitel 2.3.3.2 angegeben.

Die Schutzmaßnahmen sind in folgenden Anlagen aufgeführt:

|  |  |
| --- | --- |
| **Anlagennummer** | **Bezeichnung des KIKS** |
| … | … |
| … | … |

## Überwachung – Monitoring[[15]](#footnote-15)

Die folgenden Qualitätskontrollmaßnahmen werden zur Überwachung der Risikobeurteilung (siehe Abschnitt 2.3 der *Grundsätze*) und der Risikobehandlung (siehe Abschnitt 2.4 der *Grundsätze*) angewandt:

Klicken oder tippen Sie hier, um Text einzugeben.

## Cybersicherheitsreaktionsplan[[16]](#footnote-16)

Ein Cybersicherheitsreaktionsplan der mindestens die Anforderungen des Abschnitts 2.6 Absatz 1 der *Grundsätze* erfüllt, wurde entwickelt und umgesetzt.

Die im Abschnitt 2.6 Absatz 2 der *Grundsätze* geforderten Informationen sind in den folgenden Anlagen ausgeführt*.*

|  |  |
| --- | --- |
| **Anlagennummer** | **Bezeichnung** |
| … | … |
| … | … |

Die im Abschnitt 2.6 Absatz 2 der *Grundsätze* geforderten Informationen sind in der Folge ausgeführt:

Klicken oder tippen Sie hier, um Text einzugeben.

# Personalangelegenheiten

## Zuverlässigkeitsüberprüfung

Das folgende Verfahren für die Einstellung und Überprüfung, einschließlich der Zuverlässigkeitsüberprüfung und der Vorbeschäftigungsprüfungen des im Folgenden angegebenen Personals wird

wie im Sicherheitsprogramm beschrieben umgesetzt.

wie im Folgenden beschrieben umgesetzt:

Klicken oder tippen Sie hier, um Text einzugeben.

## Eignung

Für die Personen, welche die Maßnahmen nach Abschnitt 2.4 (Risikobehandlung) umsetzen, wird mithilfe des im Sicherheitsprogramm beschriebenen Konzepts gewährleistet, dass sie über die erforderlichen Fähigkeiten und Fertigkeiten verfügen.

## Schulung

Zur funktionsangemessenen Bestimmung der Schulungserfordernisse sind die Rollen und Tätigkeitsprofile der Mitarbeitenden wie folgt den Personengruppen gemäß Punkt 3.3.1 der *Grundsätze* zugeordnet:

**Personengruppe a)**

Klicken oder tippen Sie hier, um Text einzugeben.

**Personengruppe b)**

Klicken oder tippen Sie hier, um Text einzugeben.

**Personengruppe c)**

Klicken oder tippen Sie hier, um Text einzugeben.

Die optionalen Schulungsthemen (*nach Erfordernis*) gemäß Abschnitt 3.3.2 der *Grundsätze* sind den Rollen und Tätigkeitsprofilen wie folgt zugeordnet:

Klicken oder tippen Sie hier, um Text einzugeben.

Die Dokumentation für alle Personen, welche an einer oder mehreren Fortbildungsmaßnahmen / Schulungen im Bereich Cybersicherheit teilnehmen, wird auf dem neuesten Stand gehalten. Auf Verlangen wird Einsicht in die Dokumentation gewährt.

1. <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/Zip_Datei_Edition_2023.html> [↑](#footnote-ref-1)
2. <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/krt2023_Excel.html> [↑](#footnote-ref-2)
3. <https://www.allianz-fuer-cybersicherheit.de> [↑](#footnote-ref-3)
4. <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/lageberichte_node.html> und <https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html> [↑](#footnote-ref-4)
5. Weitere Informationen zum Risikomanagement sind insbesondere den *Grundsätzen* Kapitel 2, sowie dem BSI-Standard 200-3 zu entnehmen. [↑](#footnote-ref-5)
6. Das grundsätzliche Vorgehen zur Durchführung der erforderlichen Strukturanalyse ist im BSI-Standard 200-2 Kapitel 8.1) hinterlegt. Ein spezifischeres Beispiel im Anhang B.2.2 der *Grundsätze*. [↑](#footnote-ref-6)
7. Eine beispielhafte und nicht abschließende Aufzählung von KIKS bei Unternehmen nach § 9 und §9a LuftSiG ist in den *Grundsätzen* Anhang B.2.2 dargestellt. [↑](#footnote-ref-7)
8. Eine Musterdatei zur Darstellung der Ergebnisse des Risikomanagements auf Basis einzelner KIKS wird bereitgestellt. Es steht frei dieses Muster oder bereits bestehende Dokumente zu nutzen, sofern die Mindestvorgaben erfüllt werden. [↑](#footnote-ref-8)
9. Die Gefährdungsübersicht kann nach BSI-Standard 200-3 Kapitel 4.1 & 4.2, sowie dem „IT-Grundschutz-Kompendium des BSI - Elementare Gefährdungen“ erstellt werden. [↑](#footnote-ref-9)
10. Die Risikoeinschätzung ist nach Kapitel 2.3 der *Grundsätze* durchzuführen. Dabei kann der BSI-Standard 200-3, Kapitel 5.1 berücksichtigt werden. [↑](#footnote-ref-10)
11. Die Risikobewertung ist nach den Maßgaben der *Grundsätze,* Kapitel 2.3 durchzuführen. Dabei kann der BSI-Standard 200-3, Kapitel 5.2 berücksichtigt werden. [↑](#footnote-ref-11)
12. Beispiele für eine anforderungsgerechte Risikomatrix sind den *Grundsätzen* Anhang B.2.3, sowie dem BSI-Standard 200-3 Kapitel 5.2 zu entnehmen. [↑](#footnote-ref-12)
13. Die Anforderungen hinsichtlich der Risikobehandlung sind den *Grundsätzen*, Kapitel 2.4 zu entnehmen. Weitere grundsätzliche Informationen zur Risikobehandlung sind dem BSI-Standard 200-3, Kapitel 6 zu entnehmen, wobei die Einschränkungen der *Grundsätze*, insbesondere zur Unzulässigkeit von Risikotransfer und Risikoübernahme zu beachten sind. [↑](#footnote-ref-13)
14. Ein Risiko-Level ab 60% auf der Risikoskala ist gemäß Kapitel 2.3 der *Grundsätze* als inakzeptabel zu bewerten. [↑](#footnote-ref-14)
15. Weitere Informationen zur Überwachung – Monitoring von Cybersicherheitsmaßnahmen sind im BSI-Standard 200-2 Kapitel 9 und 10 aufgeführt. [↑](#footnote-ref-15)
16. Die „Bausteine aus dem IT-Grundschutz-Kompendium“ enthalten Informationen, zur Erkennung von Cyberangriffen, sowie der Reaktion und Bewältigung dieser. [↑](#footnote-ref-16)