Informationssicherheitsleitlinie im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben des Landes Niedersachsen (ISLL DF BOS NI)

Version 1.0

Stand: 12.10.2017

Inhalt

Dokumenteneigenschaften

Dokumentbezeichnung

Bezeichnung	Informationssicherheitsleitlinie im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben des Landes Niedersachsen (ISLL DF BOS NI)
Version	1.0
Datum der letzten Änderung	12.10.2017
Status	Entwurfsfassung

Änderungshistorie

Version	Status	Datum	Bearbeiter	Bemerkungen
0.1	Entwurfs-fassung	09.02.2016	Herr Rösemann, MI	---
0.2	Entwurfs-fassung	10.02.2016	Herr Rösemann, MI	---
0.3	Entwurfs-fassung	11.02.2016	Herr Rösemann, MI	---
0.4	Entwurfs-fassung	17.02.2016	Herr Rösemann, MI	---
0.5	Entwurfs-fassung	19.02.2016	Herr Rösemann, MI	---
0.6	Entwurfs-fassung	25.05.2016	Herr Plenk, ASDN (extern)	Neugliederung in Anlehnung an die ISL Digitalfunk BOS der BDBOS Fachliche Ergänzungen und Präzisierungen, insbesondere bzgl. Des Geltungsbereichs für die BOS in NI
0.7	Entwurfs-fassung	17.01.2017	Herr Lang, ASDN	
0.8	Entwurfs-fassung	01.02.2017	Herr Ihmor ASDN	
09	Entwurfs-fassung	21.02.2017	Herr Plenk, ASDN (extern)	Finaler und mit der Leitung der ASDN abgestimmter Entwurf
091	Entwurfs-fassung	22.02.2017	Herr Köchling, ASDN (extern)	QS
092	Entwurfs-fassung	19.06.2017	Herr Lang, ASDN	Finaler und mit dem MI - Ref. 26 abgestimmter Entwurf
1.0	Endfassung	12.10.2017	Herr Lang, ASDN	

Ansprechpartner

Organisationseinheit
Zentrale Polizeidirektion Niedersachsen Autorisierte Stelle für den Digitalfunk Niedersachsen (ASDN) / Dezernat 44 Tannenbergallee 11 30163 Hannover E-Mail: asdn@zpd.polizei.niedersachsen.de

1 Gegenstand und Geltungsbereich

Die Informationssicherheitsleitlinie für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben Niedersachsen (ISLL DF BOS NI) regelt den Aufbau und den Betrieb eines Informationssicherheitsmanagementsystems (ISMS) für den Digitalfunk BOS Niedersachsen. Sie ist integraler Bestandteil des ISMS der Polizei und folgt einem risikobasierten Vorgehen auf Basis des IT-Grundschutzes.

Alle am Digitalfunk teilnehmenden BOS in Niedersachsen, insbesondere die Autorisierte Stelle Digitalfunk Niedersachsen (ASDN), setzen sie in geeigneter Weise um.

Außerhalb des Digitalfunks BOS geltende Regelungen zur Informationssicherheit bleiben hiervon unberührt.

2 Rahmenbedingungen

Die ISLL DF BOS NI ergänzt die Regelungen der Informationssicherheitsleitlinie für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (ISLL Digitalfunk BOS) der BDBOS zur Etablierung eines ISMS für den Digitalfunk BOS auf Landesebene sowie die ressortübergreifenden Vorgaben der niedersächsischen Leitlinie zur Gewährleistung der Informationssicherheit (ISLL).

Die Initiierung, Begleitung und Weiterentwicklung des ISMS auf Landesebene erfolgt soweit möglich unter synergetischer Nutzung bereits vorhandener Ressourcen und Umsetzung von Beschlussfassungen auf Gremienebene.

Insbesondere folgende Normen in der jeweils aktuell gültigen Fassung haben einen Bezug zur Errichtung und zum Betrieb des Digitalfunknetzes BOS und darüber hinaus zur Informationssicherheit:

- Telekommunikationsgesetz
- Gesetz über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS-Gesetz)
- Verwaltungsabkommen über die Zusammenarbeit von Bund und Ländern beim Aufbau und Betrieb eines bundesweit einheitlichen digitalen Sprech- und Datenfunksystems für alle Behörden und Organisationen mit Sicherheitsaufgaben in der Bundesrepublik Deutschland
- Bestimmungen für Frequenzzuteilungen zur Nutzung für das Betreiben von Funkanlagen der Behörden und Organisationen mit Sicherheitsaufgaben (BOS-Funkrichtlinie)
- Niedersächsisches Datenschutzgesetz
- Niedersächsisches Sicherheitsüberprüfungsgesetz
- Verschlusssachenanweisung für das Land Niedersachsen
- Richtlinien zum Geheimschutz von Verschlusssachen beim Einsatz von Informationstechnik

3 Begriffsbestimmungen

Die im Glossar dieses Dokuments unter Ziffer 11 definierten Begriffe gelten für das gesamte ISMS DF BOS NI und somit auch für diese ISLL.

4 Bedeutung der Informationssicherheit

Die ISLL DF BOS NI dient der Gewährleistung der Informationssicherheit im Digitalfunk BOS des Landes Niedersachsen und trägt damit ihren Teil zur Sicherstellung eines übergreifenden, angemessenen und einheitlichen Informationssicherheitsniveaus des Digitalfunks für die BOS von Bund und Ländern bei.

Der Digitalfunk BOS ist ein Kernelement der Deutschen Sicherheitsarchitektur und zählt damit zu den „Kritischen Infrastrukturen“ der Bundesrepublik Deutschland. In dieser Leitlinie wird daher die besondere Bedeutung der Grundwerte der Informationssicherheit Verfügbarkeit, Integrität und Vertraulichkeit berücksichtigt.

Ziel ist es die Verfügbarkeit des Digitalfunks BOS NI zu gewährleisten und ihn vor weitreichenden Schäden zu schützen. Insbesondere muss die Funktionsfähigkeit auch und gerade in Not- und Krisenfällen sichergestellt sein.

5 Sicherheitsziele

Durch die ISLL DF BOS NI soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um dem Eintreten von sicherheitsrelevanten Ereignissen (z.B. Verlust von Digitalfunkendgeräten oder Kompromittierung der Systeminfrastruktur des DF BOS NI und dem damit einhergehenden Risiko des Informationsdiebstahls durch nicht-berechtigte Dritte) vorzubeugen. Sie dient insbesondere

- der Sicherstellung eines angemessenen und einheitlichen Informationssicherheitsniveaus innerhalb aller BOS in NI für alle Personen und Komponenten, die den Digitalfunk BOS nutzen oder an dessen Bereitstellung mitwirken,
- der Sicherstellung der Kontinuität der Arbeitsabläufe durch die zuverlässige Unterstützung der Geschäftsprozesse des DF BOS NI durch die IT,
- der Wahrung von Amts- und Dienstgeheimnissen,
- der Gewährleistung der aus den gesetzlichen Vorgaben resultierenden Anforderungen (Compliance),
- der Gewährleistung des informationellen Selbstbestimmungsrechts der oder des Betroffenen bei der Verarbeitung personenbezogener Daten,
- der Reduzierung der bei einem Schadensvorfall im Digitalfunk BOS entstehenden materiellen und immateriellen Schäden,
- der Sensibilisierung von Mitarbeiterinnen und Mitarbeitern zum sorgfältigen Umgang mit Informationen sowie
- dem Schutz von Informationen im Digitalfunk BOS gegen unbeabsichtigte und vorsätzliche Verfälschung.

6 Verantwortlichkeiten

6.1 Ministerium für Inneres und Sport / KSDN

Die Koordinierende Stelle für den Digitalfunk Niedersachsen (KSDN) im Niedersächsischen Ministerium für Inneres und Sport legt die Rahmenbedingungen für die Ausgestaltung des ISMS DF BOS NI fest und gibt strategische Informationssicherheitsziele und –strategien in Form dieser ISLL vor.

6.2 Zentrale Polizeidirektion Niedersachsen (ZPD NI)

Die ZPD NI verantwortet den landesweiten Informationssicherheitsprozess im DF BOS NI und initiiert diesen.

6.2.1 Autorisierte Stelle Digitalfunk Niedersachsen (ASDN)

Die Autorisierte Stelle Digitalfunk Niedersachsen unterstützt die strategische und die operative Informationssicherheit der Polizei NI und den oder die Beauftragte für Informationssicherheit im DF BOS sowie die operative Ebene mit fachspezifischem Wissen bei der Erfüllung der ihnen obliegenden Aufgaben.

Sie erstellt auch das Informationssicherheitskonzept des DF BOS NI für alle Komponenten[1] in ihrem Zuständigkeitsbereich.

6.2.2 Beauftragte bzw. Beauftragter für Informationssicherheit im Digitalfunk BOS NI (BfIS DF BOS NI)

Die oder der Beauftragte für Informationssicherheit im Digitalfunk BOS NI ist organisatorisch der ZPD zugeordnet. Sie bzw. er ist verantwortlich für die Koordinierung des ISMS DF BOS NI, in Abstimmung mit den BOS in NI, der BDBOS und den anderen Bundesländern.

Sie bzw. er hat insbesondere folgende Aufgaben:

- Initiierung, Begleitung und Weiterentwicklung des Informationssicherheitsmanagements DF BOS NI
- Weiterentwicklung der ISLL in Abstimmung mit den verantwortlichen Stellen gem. Ziffer 6.1 und 6.2
- Entwicklung bzw. Weiterentwicklung von BOS-übergreifenden Regelungen bezüglich des DF BOS NI
- Erstellung eines halbjährlichen Berichtes zur Informationssicherheit im DF BOS NI zur Unterrichtung der KSDN
- Unterstützung bei der Bearbeitung von Sicherheitsvorfällen bzw. Schwachstellen im Digitalfunk BOS NI,
- Initiierung von IS-Revisionen und Penetrationstests im Bereich des DF BOS NI, sowie deren Begleitung bzw. Durchführung im Einvernehmen mit den betroffenen Einrichtungen[2]
- Beratung der BOS NI in Fragen der Informationssicherheit im Bereich Digitalfunk BOS.

Sie bzw. er hat die nachfolgenden Befugnisse und Kompetenzen:

- Mitsprache- und Vetorecht bei Entscheidungen, die ihren/seinen Verantwortungsbereich betreffen

[1] Mit Komponenten sind die Zielobjekte im Sinne des IT-Grundschutzes gemeint. Also Liegenschaften, Gebäude, Räume, Netze, IT-Systeme und IT-Anwendungen in der Zuständigkeit der ASDN.

[2] Potentiell sind das alle Einrichtungen, in denen Digitalfunkkomponenten gelagert oder betrieben werden.

- Direktes Vorspracherecht gegenüber der Behördenleitung der ZPD NI und der KSDN

6.3 Behördenleitungen und Organisationsleitungen BOS

Die Behördenleitungen bzw. Organisationsleitungen der einzelnen BOS tragen die Verantwortung für die Informationssicherheit im Digitalfunk BOS NI ihrer Behörde bzw. Organisation. Sie haben zu veranlassen, dass

- der Schutzbedarf von Informationen ihrer Behörde im Digitalfunk BOS NI festgestellt und eine Risikoanalyse durchgeführt wird,
- Konzepte für Informationssicherheit im Digitalfunk BOS NI im Bereich Ihrer Behörde erstellt und die sich daraus ergebenen Maßnahmen zum Schutz der Informationen im Digitalfunk BOS umgesetzt werden[3],
- Verantwortlichkeiten im Umgang mit den Digitalfunk BOS-Komponenten explizit definiert und verbindlich gegenüber den Nutzerinnen und Nutzern festgelegt werden und
- der Zugang zu und der Zugriff auf Informationen im Digitalfunk BOS sowie der Umfang und die Art der Autorisierung definiert und verbindlich gegenüber den Nutzerinnen und Nutzern festgelegt werden[4].

6.4 Nutzerinnen und Nutzer im DF BOS NI

Alle Nutzerinnen und Nutzer im DF BOS NI haben im Rahmen ihrer jeweiligen Zuständigkeiten und Verantwortungsbereiche für die Erhaltung der Informationssicherheitsgrundwerte Vertraulichkeit, Integrität und Verfügbarkeit in Bezug auf die ihnen anvertrauten Komponenten, Informationen und Prozesse Sorge zu tragen und sicherheitsrelevante Ereignisse im Kontext DF BOS zu melden.

7 Grundsätze der Sicherheitsstrategie

7.1 Informationsklassifizierung

Alle Informationen mit Relevanz für die Geschäftsprozesse im DF BOS NI sind in die Schutzkategorien normal, hoch und sehr hoch zu klassifizieren.[5]

[3] Für die Digitalfunkgeräte erstellt die ASDN in Form von Richtlinien und Vorgaben für die BOS bindende Rahmenbedingungen, hier müssen für Leitstellengeräte mit Anbindung an den Digitalfunk BOS die die Leitstellen betreibenden Behörden und Organisationen selbst Informationssicherheitskonzepte erstellen.

[4] Auch hierfür erstellt die ASDN in Form von Richtlinien und Vorgaben für die BOS bindende Rahmenbedingungen, die Behörden und Organisationen müssen diese für ihren Bereich durchsetzen.

[5] Siehe hierzu auch unter Schutzbedarf / Schutzbedarfskategorien im Glossar

7.2 Risikobasiertes Vorgehen

Im Rahmen einer Risikoanalyse sind mögliche Schadensereignisse, deren Ursachen und Auswirkungen sowie deren Eintrittswahrscheinlichkeit zu analysieren sowie Maßnahmen zur Risikobehandlung zu entwickeln. Verbleibende Risiken (Restrisiken) sind zu beschreiben und durch die jeweilige Behördenleitung zu verantworten.

7.3 Angemessenheit von Sicherheitsmaßnahmen

Finanzieller und organisatorischer Aufwand von Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zum verfolgten Ziel stehen. Dem Gebot der Wirtschaftlichkeit und Sparsamkeit ist Rechnung zu tragen.

7.4 Controlling und Qualitätssicherung

Zum Erreichen der in Ziffer 5 definierten Ziele setzen die ASDN sowie die BOS in NI geeignete Maßnahmen um, deren Vollständigkeit, Wirksamkeit und Angemessenheit eigenverantwortlich regelmäßig zu überprüfen sind.

Durch eine kontinuierliche Überprüfung der Regelungen und deren Einhaltung wird das aktuelle Sicherheitsniveau dargestellt. Abweichungen werden mit dem Ziel, die Informationssicherheit zu erreichen, ggf. zu verbessern bzw. auf dem neuesten Stand zu halten, analysiert.

Diese Maßnahmen zur Qualitätssicherung (z.B. IS-Audits, IS-Revisionen) werden in den Gremien des DF BOS einvernehmlich mit dem Bund, der BDBOS und den anderen Bundesländern geplant, veranlasst und ausgewertet.

Sofern die BOS in NI davon betroffen sind, werden diese durch den BfIS DF BOS NI eingebunden.

8 Ebenen des ISMS im Digitalfunk BOS NI

Das ISMS besteht aus mehreren Ebenen, welche hierarchisch aufeinander aufbauen. Die Hierarchie der erforderlichen Dokumente orientiert sich an den Empfehlungen des BSI. Diese werden sach- und zielgruppenorientiert erstellt und bedarfsgerecht fortgeschrieben.

8.1 Informationssicherheitsleitlinie

Die ISLL DF BOS NI ist das übergeordnete strategische Basisdokument zur Gewährleistung der Informationssicherheit im DF BOS. Die ISLL DF BOS NI berücksichtigt dabei die Vorgaben der Informationssicherheitsleitlinie der BDBOS für den Digitalfunk.

8.2 Informationssicherheitsrichtlinien

Informationssicherheitsrichtlinien legen für einzelne organisatorische oder technische Bereiche im DF BOS NI Standards fest.

In der Regel gelten dabei die Informationssicherheitsrichtlinien der Polizei NI für den DF BOS NI mit. Wo erforderlich, werden sie um Digitalfunk BOS-Spezifika ergänzt.

8.3 Konzepte für Informationssicherheit

Die Konzepte für Informationssicherheit bestimmen auf Basis der Informationssicherheitsrichtlinien mögliche Risiken für organisatorische oder technische Bereiche im DF BOS NI und legen Maßnahmen zur Risikobehandlung fest.

Sie enthalten

- eine Bestimmung des zu schützenden Objektes und des Schutzbedarfs der Informationen,
- eine Analyse der Angriffs- und Schadensszenarien,
- eine Bewertung der Eintrittswahrscheinlichkeit und der potentiellen Schadenshöhe,
- Maßnahmen zur Reduzierung der Eintrittswahrscheinlichkeit bzw. Schadenhöhe und
- eine Analyse der eigenen Risikotragbarkeit sowie
- ggf. die Erklärung der Übernahme des Restrisikos durch die Behördenleitung.

Das Konzept für Informationssicherheit enthält zudem Aussagen zur Datensicherung und Archivierung, zur Notfallvorsorge und dem Schutz vor Schadsoftware.

8.4 Informationssicherheitskonzept (SiKo) des DF BOS NI

Voraussetzung für die Umsetzung der Informationssicherheit auf Basis von IT-Grundschutz ist die systematische risikobasierte Analyse jeder einzelnen, in den Kerngeschäftsprozessen im DF BOS NI genutzten Komponenten hinsichtlich ihrer Eigenschaften, Gefährdungen und Sicherheitsmaßnahmen (Soll / Ist).

Das SiKo auf Basis des risikoorientierten Vorgehens beinhaltet das Ergebnis folgende sieben Arbeitsschritte:

1. die Festlegung des Betrachtungsgegenstandes,
2. die Ermittlung der Ressourcen,
3. die Gefahrenanalyse,
4. die Risikoanalyse,
5. die Erstellung des Katalogs an Sicherheitsmaßnahmen,
6. die Erstellung der Umsetzungsplanung und
7. die Akzeptanz des Risikos nach der Maßnahmenumsetzung.

8.5 Verwaltung der Dokumente

Die im Rahmen der Umsetzung der Informationssicherheitsleitlinie erstellten Dokumente werden in Abhängigkeit ihres Inhaltes dem jeweils berechtigten Personenkreis im erforderlichen Umfang und in geeigneter Weise zugänglich gemacht.

9 Informationssicherheitsprozess

Zur Gewährleistung eines angemessenen Sicherheitsniveaus muss das Informationssicherheitsmanagement im DF BOS NI auf allen Ebenen, also der KSDN, der ASDN und den, den Digitalfunk nutzenden Behörden und Organisationen, einem kontinuierlichen Verbesserungsprozess folgen. Dies soll auf allen Ebenen mittels der nachfolgend beschriebenen, sich ständig fortlaufend wiederholenden Prozessschritte (sog. PDCA-Zyklus[6]) geschehen:

Plan	Den Sicherheitsprozess auf strategischer Ebene anstoßen, steuern und kontrollieren. Hierzu gehört initial das Erstellen von Leitlinien und die Veranlassung der Erstellung von Sicherheitskonzepten und Richtlinien. Danach sind in diesem Prozessschritt die im Prozessschritt Act identifizierten Verbesserungsmaßnahmen und regelmäßige, mindestens jährliche Audits einzuplanen. Die Audits für den DF BOS NI werden dabei zentral von der ZPD geplant.

[6] **P**lan**D**o**C**heck**A**ct-Zyklus

Do	Hierzu gehört initial die Erstellung von Sicherheitskonzepten und Richtlinien für alle Ebenen des DF BOS NI. Danach erfolgt in diesem Prozessschritt die Umsetzung der geplanten Verbesserungsmaßnahmen.
Check	Hierzu gehört die Durchführung der Audits sowie auf allen Ebenen das Entgegennehmen von Berichten zur Informationssicherheit.
Act	Hierzu gehört auf allen Ebenen die Identifizierung von notwendigen Verbesserungsmaßnahmen aus den Berichten und den Audits.

10 Inkrafttreten

Die ISLL DF BOS tritt auf Grundlage des Erlasses MI 26.24-2850-ISMS DF BOS NI vom 05.10.2017 mit der Veröffentlichung durch die Zentrale Polizeidirektion Niedersachsen in Kraft.

.

11 Glossar

Administrator / Administratorin

Eine Administratorin bzw. ein Administrator ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems. Eine Administratorin bzw. ein Administrator verwaltet und betreut Rechner sowie Computernetze. Sie bzw. er installiert Betriebssysteme und Anwendungsprogramme, richtet neuen Benutzerkennungen ein und verteilt die für die Arbeit notwendigen Rechte.

ASDN – Autorisierte Stelle Digitalfunk Niedersachsen

Die Autorisierte Stelle Digitalfunk Niedersachsen überwacht und administriert durch einen 24/7-Dienst (Leitstand) in Niedersachsen das bundesweite Digitalfunknetz der Behörden und Organisationen mit Sicherheitsaufgaben (BOS).

Zu den zentralen Aufgaben der ASDN gehören:

- Zentrales Betriebsmanagement
- Verwaltung des Budgets
- Einsatzmanagement und Berichtswesen
- Landesweite Leitstellenanbindung
- Anforderungs- und Releasemanagement Digitalfunk
- BOS-Sicherheitskarten-Management
- Standort-Management
- Service-Level-Management
- Sicherstellung geplanter Maßnahmen am Wirknetz
- Öffentlichkeitsarbeit
- Informationen zur elektromagnetischen Umweltverträglichkeit (EMVU)

Die wesentlichen Aufgaben des Leitstandes der ASDN sind:

- Gewährleistung eines Gesamtüberblicks über das Digitalfunknetz
- Übernahme der Betriebs- und Sicherheitsverantwortung für Niedersachsen
- Analyse von Alarmmeldungen
- Bestimmung der Störwirkbreite

Sie ist organisatorisch der Abteilung 4, „Informations- und Kommunikationstechnologie“ der Zentralen Polizeidirektion Niedersachsen (ZPD) zugeordnet und bearbeitet die Belange des Digitalfunks aller BOS in Niedersachsen.

Siehe auch: BOS

BDBOS – Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben

Eine Anstalt des öffentlichen Rechts im Geschäftsbereich des Bundesministers des Inneren. Die Aufgaben der BDBOS sind Aufbau, Betrieb und Sicherstellung der Funktionsfähigkeit eines digitalen Sprech- und Datenfunksystems für die Berechtigten gemäß der BOS-Funkrichtlinie.

Betriebsverantwortlicher / Betriebsverantwortliche

Betriebsverantwortliche sind alle Personen, zu deren Aufgaben es gehört, anderen die bestimmungsgemäße Nutzung von IKT-Anlagen im DF BOS NI zu ermöglichen. Sie

überwachen den Zustand und die Betriebssicherheit der Anlagen. Sie werten anfallende Betriebsdaten aus, untersuchen Störungen und gewährleisten die Verfügbarkeit.

BOS – Behörden und Organisationen mit Sicherheitsaufgaben

BOS sind alle Stellen, die mit der Aufrechterhaltung bzw. der Wiederherstellung der öffentlichen Sicherheit und Ordnung betraut sind. Dazu zählen insbesondere die Polizei, der Verfassungsschutz, die Freiwilligen-, Werks- und Berufsfeuerwehren, die Rettungsdienste und der Katastrophenschutz.

BOS auf Bundesebene sind zudem die Bundespolizei, das Bundeskriminalamt, der Bundesnachrichtendienst, die Zollverwaltung und die Bundesanstalt Technisches Hilfswerk.

Change-Manager / Change-Managerin

Die Change-Managerin oder der Change-Manager ist verantwortlich, ein effizientes und effektives Patch- und Änderungsmanagement zu betreiben. Aufgabe ist es, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten.

Entwickler / Entwicklerin

Mit Entwicklerin oder Entwickler wird im Kontext des IT-Grundschutzes eine Person bezeichnet, die Software, Hardware oder ganze Systeme entwirft, die aus mehreren Software- und Hardware-Komponenten bestehen können.

Externer Dienstleister

Ein externer Dienstleister ist eine Wirtschaftseinheit, welche nicht in die Organisationsstruktur im DF BOS NI eingebunden ist und aufgrund vertraglicher Regelungen Dienstleistungen erbringt.

Siehe auch: BOS

Externes Personal

Unter externem Personal werden alle Personen zusammengefasst, die für die im DF BOS NI aufgrund eines Dienstleistungs- oder Werkvertrages tätig sind oder zu Ausbildungszwecken temporär eingesetzt werden.

Siehe auch: BOS

Fachverantwortlicher / Fachverantwortliche

Die oder der Fachverantwortliche ist inhaltlich für ein oder mehrere Geschäftsprozesse oder Fachverfahren verantwortlich.

Informationssicherheit

Informationssicherheit ist die Herstellung und Aufrechterhaltung der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität.

Siehe auch: Vertraulichkeit, Verfügbarkeit, Integrität

Informationssicherheitsmanagementsystem

Ein Informationssicherheitsmanagementsystem ist die Aufstellung von Verfahren oder Regeln, welche dazu dienen die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Siehe auch: Informationssicherheit

Informationssicherheitsprozess

Der Informationssicherheitsprozess im DF BOS NI ist ein sich dauerhaft wiederholender sukzessiver Ablauf von Planungs-, Umsetzungs-, Überprüfungs- und Verbesserungsphasen mit dem Ziel, die Informationssicherheit langfristig zu gewährleisten.

Siehe auch: Informationssicherheit

Informationstechnik

Informationstechnik ist jedes technische Mittel zur Verarbeitung oder Übertragung von Informationen.

Integrität

Die Herstellung und Aufrechterhaltung der Integrität i.S.d. Informationssicherheit bedeutet die Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden.

Siehe auch: Informationssicherheit

Konzepte für Informationssicherheit (KfIS)

Konzepte für Informationssicherheit sind Dokumente, welche den Schutzbedarf von Informationen festlegen, die Angriffs- und Schadensszenarien eines bestimmten organisatorischen oder technischen Bereichs durch vorsätzliche Schädigungen und durch menschliches Versagen analysieren, um Risiken, denen die Informationen ausgesetzt sind, zu bestimmen und Sicherheitsmaßnahmen zu beschreiben, um diese Risiken zu behandeln.

KSDN - Koordinierende Stelle Digitalfunk Niedersachsen

Als zentrale Anlaufstelle für strategische Belange des Digitalfunks BOS sind beim Bund und den Ländern Koordinierende Stellen eingerichtet.

In Niedersachsen wurde hierzu die Koordinierende Stelle Digitalfunk Niedersachsen im Niedersächsischen Ministerium für Inneres und Sport angebunden.

Die KSDN bündelt alle eingehenden Erkenntnisse und Anforderungen der BOS in ihrem Verantwortungsbereich und stimmt diese mit Bund und Ländern ab.

Zu den wesentlichen Aufgaben der KSDN gehören:

- Strategische Steuerung des BOS Digitalfunk
- Verantwortlichkeit in allen Grundsatzangelegenheiten
- Planung und Steuerung folgender Bereiche:
    - Betrieb des Funknetzes
    - Leitstellensysteme
    - Teilnehmerzulassung, Dienste und Anwendungsmanagement
    - BOS-Funkrichtlinie (Bund / Länder)
    - Frequenzkoordination
    - Vertragsmanagement
    - Fachbezogene Aufstellung des Haushalts zum Digitalfunk

Notfallmanager / Notfallmanagerin

Die Notfallmanagerin oder der Notfallmanager steuert alle Aktivitäten rund um das Notfallmanagement. Sie bzw. er ist für die Erstellung, Umsetzung, Pflege und Betreuung des institutionsweiten Notfallmanagements und der zugehörigen Dokumente, Regelungen und Maßnahmen zuständig. Sie bzw. er analysiert den Gesamtablauf der Notfallbewältigung nach einem Schadensereignis.

Schutzbedarf

Schutzbedarf von Informationen oder zugehörigen Werten ist das unter Berücksichtigung der Bedeutung einer Information angemessene Maß von Sicherheitsmaßnahmen.

Siehe auch: Sicherheitsmaßnahme

Schutzkategorien

Bei Schutzkategorien handelt es sich um Gruppen annähernd gleichen Schutzbedarfs. Dabei bedeutet

- „normaler Schutzbedarf“, dass die Auswirkungen eines Schadens begrenzt und überschaubar wären,
- „hoher Schutzbedarf“, dass die Auswirkungen eines Schadens beträchtlich sein können,
- „sehr hoher Schutzbedarf“, dass die Auswirkungen eines Schadens ein existenzielles bzw. katastrophales Ausmaß erreichen können.

Siehe auch: Schutzbedarf

Sicherheitsmaßnahme

Eine Sicherheitsmaßnahme ist eine technische oder organisatorische Lösung mit dem Ziel, ein bestehendes Risiko zu minimieren oder zu beherrschen.

Sicherheitsrelevantes Ereignis

Ein sicherheitsrelevantes Ereignis ist ein Ereignis, bei dem die Grundwerte Verfügbarkeit, Vertraulichkeit oder Integrität in unzulässiger Weise verletzt werden (z.B. Verlust von Digitalfunkendgeräten oder Kompromittierung von Infrastrukturen des DF BOS NI und dem damit einhergehenden Risiko des Informationsdiebstahls durch nichtberechtigte Dritte).

Siehe auch: Vertraulichkeit, Verfügbarkeit, Integrität

Verfahrensverantwortlicher / Verfahrensverantwortliche

Verfahrensverantwortliche tragen die Gesamtverantwortung für ein spezielles Verfahren und sind für den korrekten Ablauf verantwortlich. Sie bestimmen den Schutzbedarf der Informationen ihrer Verfahren. Bei aufwendigen IT-Verfahren wird die Verantwortung aufgeteilt in eine fachliche und eine technische Verantwortung:

Die fachliche Sicht betrachtet die Verfahren aus Perspektive der fachlichen Eignung für die Arbeit im DF BOS NI.

Die technische Sicht betrachtet die Verfahren aus Sicht der IKT.

Verfügbarkeit

Die Herstellung und Aufrechterhaltung der Verfügbarkeit i.S.d. Informationssicherheit bedeutet die Gewährleistung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechtigte Benutzerinnen und Benutzer.

Siehe auch: Informationssicherheit

Vertraulichkeit

Die Herstellung und Aufrechterhaltung der Vertraulichkeit i.S.d. Informationssicherheit bedeutet die Gewährleistung des physikalischen bzw. logischen Zugangs zu Informationen nur für Zugriffsberechtigte.

Siehe auch: Informationssicherheit

Virusmanagerin / Virusmanager

Die Tätigkeit der Virusmanagerin oder des Virusmanagers zielt vorrangig darauf ab, dass bei Auftreten eines Schadprogramms nicht noch weitere IT-Systeme infiziert werden. Meldungen der Virenschutzsoftware über erkannte Schadprogramme werden automatisiert per E-Mail an die eingetragene Virusmanagerin oder Virusmanager gemeldet. Diese oder dieser prüft die Meldungen und leitet ggf. weitere Maßnahmen ein.