

Leitlinie für die Informationssicherheit

(IS-Leitlinie)

Version 1.0
Stand: 1. Oktober 2019

Datum	Version	Änderung durch	Freigabe durch	Kommentar
21.06.2019	1.00	Marc Bauer	Frank Felde	finale Version, fachliche Freigabe
01.10.2019	1.00	Marc Erichsen Anne Rethmann	Frank Felde	finale Qualitätssicherung sowie fachliche Freigabe
(siehe Unterschrift)	1.00		GF	finale Version, Inkraftsetzung

Dokumentenverantwortlicher / Dokumenteneigentümer:	zentraler Informationssicherheitsbeauftragter der Autobahn des Bundes GmbH
---	---

Inhaltsverzeichnis

1. Zeichnung	4
2. Stellenwert der Informationsverarbeitung	5
3. Geltungsbereich	6
4. Etablierung des Informationssicherheitsmanagementsystems (ISMS).....	6
5. Ziele der Informationssicherheit	7
5.1 Grundsatz: Informationssicherheit als integraler Bestandteil der Geschäftspolitik.....	7
5.2 Grundsatz: Orientierung an Standards	8
5.3 Grundsatz: Einhaltung gesetzlicher Regelungen und Normen.....	8
5.4 Grundsatz: Schutz von Informationen und Ressourcen	8
5.5 Grundsatz: Schutz von personenbezogenen Daten	8
5.6 Grundsatz: Nachvollziehbarkeit	8
5.7 Grundsatz: Schutz vor Angriffen und Notfällen	9
5.8 Grundsatz: Gewährleistung des Betriebs	9
5.9 Grundsatz: Wirtschaftlichkeit	9
5.10 Grundsatz: Prozessbasierte Sicherheit.....	9
6. Weitere Regelungsdokumente.....	9
7. Sensibilisierung	10
8. Durchsetzung	10
9. Evaluation und Revision	10
10. Bekanntgabe.....	11

1. Zeichnung

Mit der Unterzeichnung aller Zeichnungspflichtigen gilt das vorliegende Dokument als genehmigt und in Kraft gesetzt. Vorangegangene Versionen werden durch das Dokument vollständig ersetzt.

Die vorliegende Leitlinie für die Informationssicherheit (IS-Leitlinie) und daraus abgeleitete Richtlinien, Konzepte und Hinweise gelten für folgende Einheiten und Geschäftsbereiche:

- Die Autobahn GmbH des Bundes

Die Genehmigung der IS-Leitlinie erfolgt durch die Geschäftsführung der Autobahn GmbH des Bundes. Die IS-Leitlinie ist min. jährlich hinsichtlich der Erfüllung der in der Geschäftsstrategie definierten Geschäftsziele zu prüfen und ggf. anzupassen. Die Geschäftsführung der Autobahn GmbH des Bundes sichert zur Umsetzung der IS-Leitlinie die Verfügbarkeit und Allokation angemessener Ressourcen für das Informationssicherheits-Management zu.

Berlin, den 28/11/2019


Stephan Krenz
Gunther Adler
Anne Rethmann

2. Stellenwert der Informationsverarbeitung

Informationsverarbeitung stellt eine Schlüsselrolle für die Geschäftstätigkeit der Autobahn GmbH des Bundes dar. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnologie maßgeblich unterstützt.

Mit der zukünftig weiterwachsenden Durchdringung der Geschäftsprozesse von querschnittlichen Informationen und der hierdurch notwendigen Unterstützung durch die Informationstechnik (IT) erhöht sich auch die Abhängigkeit von IT-Systemen sowie der durch die IT-Systeme verarbeiteten Daten. Diese sind daher vor unzulässiger und unsachgemäßer Nutzung sowie Missbrauch, Verlust, Preisgabe, Zerstörung und Manipulation zu schützen.

Für die Autobahn GmbH des Bundes stellt die Informationssicherheit daher einen integralen Bestandteil der Geschäftspolitik dar. Die Verlässlichkeit der eingesetzten Produkte und Verfahren sowie eine hohe Verfügbarkeit der Daten und Informationen sichern die Leistungsfähigkeit der Autobahn GmbH des Bundes, das Vertrauen bei Kunden und Geschäftspartnern sowie das Ansehen in der Öffentlichkeit.

Mit der vorliegenden IS-Leitlinie werden die grundlegenden Positionen der Geschäftsführung zur Informationssicherheit festgelegt. Mit Hilfe der IS-Leitlinie definiert die Unternehmensführung die Rahmenbedingungen für die Informationssicherheit der Autobahn GmbH des Bundes. Die IS-Leitlinie steht im Einklang mit der Unternehmensstrategie bzw. der daraus abgeleiteten IT-Strategie (s. Abbildung 1).

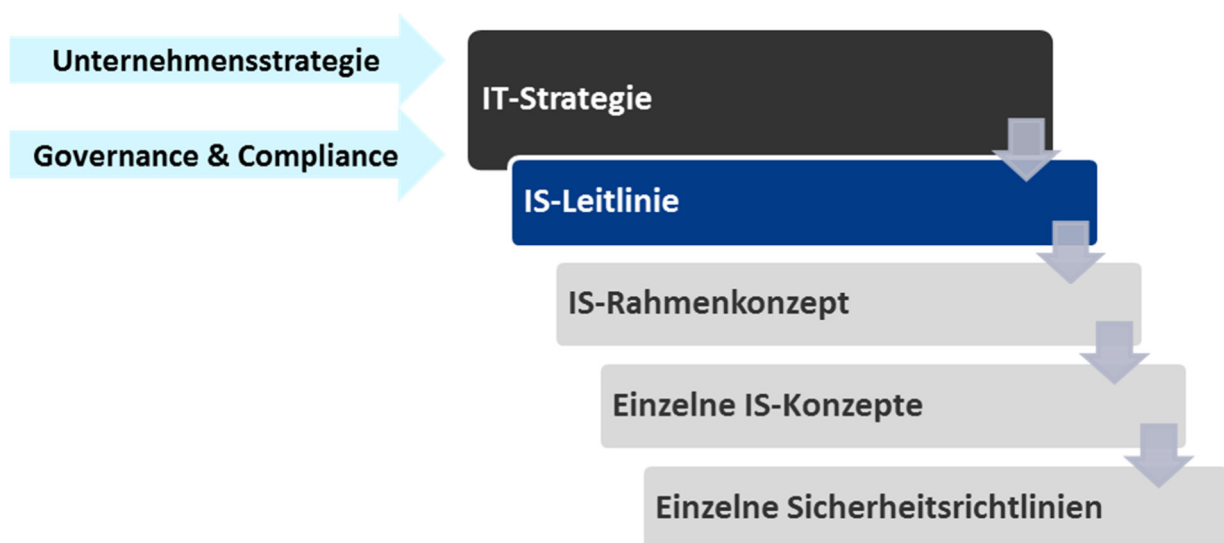


Abbildung 1: Darstellung der Dokumenten-Abhängigkeiten im Rahmen der Informationssicherheit

Die IS-Leitlinie ist für alle Mitarbeiter verbindlich und stellt die Basis für das Erarbeiten eines Ordnungs- und Handlungsrahmens der Informationssicherheit dar.

Die Sicherstellung der Einhaltung und die Umsetzung der IS-Leitlinie werden durch die Bereichs-, Abteilungs- und Teamleiter gewährleistet. Hilfestellung dazu leistet der Informationssicherheitsbeauftragte.

3. Geltungsbereich

Die Leitlinie für die Informationssicherheit gilt uneingeschränkt für die Autobahn GmbH des Bundes. Darüber hinaus gilt sie für alle im Rahmen von Geschäftsbesorgungsverträgen ausgelagerten Bereiche und Gesellschaften und externen Dienstleistern, auch im Fall einer treuhänderischen Verwaltung.

4. Etablierung des Informationssicherheitsmanagementsystems (ISMS)

Das Informationssicherheits-Managementsystem der Autobahn GmbH des Bundes gliedert sich in eine Informationssicherheits-Organisation und zugehörige Prozesse. Die Ziele des ISMS sind:

- die angestrebte Informationssicherheit zu erreichen,
- diese kontinuierlich zu gewährleisten und zu verbessern, sowie
- laufend auskunftsfähig über deren Status zu sein.

Hierzu initiiert die Autobahn GmbH des Bundes den Prozess zum ISMS, legt Verantwortliche und deren Aufgaben fest und stellt die notwendigen Mittel und Ressourcen bereit.

Die Verantwortung für Informationssicherheit verbleibt dabei bei der Unternehmensführung. Die Unternehmensführung wird vom Informationssicherheitsbeauftragten unterstützt.

Der Informationssicherheits-Prozess umfasst folgende als Kreislauf wiederkehrend zu betrachtende Schritte:

- Planung von Maßnahmen zur Informationssicherheit
- Umsetzung von Maßnahmen zur Informationssicherheit
- Überwachung und Prüfung der umgesetzten Maßnahmen
- Optimierung der Maßnahmen
- Bericht an die Geschäftsführung

Die Autobahn GmbH des Bundes orientiert sich am Umsetzungsplan Bund 2017 (UP Bund 2017) und daraus abgeleitet an den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI). In Bezug auf die Informationssicherheit wird daher die Standardabsicherung nach BSI-Standard 200-2 als Schutzniveau festgelegt. Die zur Umsetzung der Standardabsicherung angegebenen Maßnahmen des BSI IT-Grundschutz-Kompendiums sind daher grundsätzlich umzusetzen. In begründeten Einzelfällen können alternative Maßnahmen

umgesetzt werden, soweit diese zur Erreichung des gleichen Schutzniveaus führen und vom Informationssicherheitsbeauftragten mitgetragen werden.

Das Bundesministerium des Innern hat gemäß §10 BSIg in §8 BSI-KritisV i. V. m. Anhang 7 Teil 3 Spalte B BSI-KritisV bestimmt, dass Verkehrssteuerungs- und Leitsysteme der Bundesfernstraßen zur kritischen Infrastruktur gehören. Für die zugehörigen Bereiche sind die sich daraus und aus abgeleiteten Vorschriften ergebenden Anforderungen ergänzend zum Mindestschutzniveau umzusetzen (siehe §8a BSIg).

Das Business Continuity Management (BCM) dieser Bereiche richtet sich nach dem BSI-Standard 100-4 zum Notfallmanagement aus.

Die Umsetzung des ISMS erfolgt toolgestützt, um jederzeit gegenüber der Geschäftsführung und berechtigten Dritten auskunftsfähig über dem aktuellen Umsetzungsstand des ISMS zu sein. Das Tool unterstützt außerdem die Verfolgung der Umsetzung von Maßnahmen sowie die regelmäßige Aktualisierung und Prüfung bereits umgesetzter Maßnahmen.

5. Ziele der Informationssicherheit

Die Geschäftsführung konkretisiert die Ziele der Informationssicherheit in Form der folgenden Grundsätze. Diese Grundsätze verdeutlichen, dass die Informationssicherheit zur Unterstützung der Geschäftsziele, der Abwicklung der Geschäftsprozesse sowie zur Zufriedenheit der Kunden und Mitarbeiter beiträgt.

Die aus den jeweiligen Grundsätzen abgeleiteten Regelungen und Vorgaben dienen dazu, ein wirksames und angemessenes Sicherheitsniveau für Daten, Systeme, Netze und Standorte zu erreichen und aufrechtzuerhalten. Die Mitarbeiter sind verpflichtet, die Informationssicherheit durch ihr persönliches Verhalten zu erhalten und zu fordern. Als Grundwerte der Informationssicherheit definiert die Geschäftsführung in Übereinstimmung mit dem BSI-Standard 200-1:

- **Verfügbarkeit** zur Gewährleistung des Zugangs zu Informationen für berechtigte Benutzer,
- **Vertraulichkeit** zur Gewährleistung des Zugangs zu Informationen nur für Zugangsberechtigte,
- **Integrität** zur Sicherstellung der Richtigkeit und Vollständigkeit von Informationen.

5.1 Grundsatz: Informationssicherheit als integraler Bestandteil der Geschäftspolitik

Die Geschäftsführung legt fest, Informationssicherheit als strategisches Unternehmensziel zu definieren und bei der Ausrichtung der Geschäftspolitik zu berücksichtigen. Entscheidungen sind im Hinblick auf ihre Auswirkungen auf die Grundwerte Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität zu bewerten. Die Verantwortung für die Einhaltung interner und externer Vorgaben zur Informationssicherheit sowie für die Angemessenheit und Wirksam-

keit der zur Erreichung des Schutzniveaus umgesetzten Maßnahmen verbleibt bei der Geschäftsführung. Der Geschäftsführung ist regelmäßig durch nachgeordnete Stellen und Gremien mit Bezug zur Informationssicherheit zu berichten.

Die Informationssicherheit umfasst dabei insbesondere das Rahmenwerk des ISMS, die Betriebsprozesse, die Regelungen und Vorgaben des Notfallmanagements, die Vorgaben zur logischen und physischen Datensicherheit, das Vertrags- und Kundenmanagement sowie die Funktionen und Prozesse zur Erfüllung der Anforderungen an kritische Infrastruktur und zur Einhaltung der datenschutzrechtlichen Vorgaben.

5.2 Grundsatz: Orientierung an Standards

Zur Erfüllung der Anforderungen an die Informationssicherheit sollen erprobte und standardisierte Verfahren zum Einsatz kommen. Wesentliche Standards der Informationssicherheit stellen für die Autobahn GmbH des Bundes dabei die BSI-Standards 200-1 bis 200-3 zum Informationssicherheits- und Risikomanagement sowie der Standard 100-4 zum Notfallmanagement dar. Die Umsetzung von Maßnahmen und Schaffung von Prozessen mit Bezug zur Informationssicherheit hat daher immer unter der Maßgabe der Orientierung an anerkannten nationalen oder internationalen Standards zu erfolgen.

5.3 Grundsatz: Einhaltung gesetzlicher Regelungen und Normen

Alle für die Informationssicherheit relevanten gesetzlichen und regulatorischen Anforderungen sind zu identifizieren und deren Umsetzung bzw. Einhaltung verbindlich zu regeln und kontinuierlich sicherzustellen.

5.4 Grundsatz: Schutz von Informationen und Ressourcen

Unternehmenseigene und anvertraute Daten sowie Ressourcen sind gegen vorsätzlichen oder versehentlichen nicht autorisierten Zugriff und vor Veränderungen zu schützen, die Authentizität, Integrität, Vertraulichkeit oder Verfügbarkeit der Daten gefährden könnten. Dies gilt für alle durch das Unternehmen oder im Auftrag des Unternehmens betriebenen Systeme und Infrastrukturkomponenten.

5.5 Grundsatz: Schutz von personenbezogenen Daten

Personenbezogene Daten von Kunden, Mitarbeitern, Dienstleistern und Partnern sind vor missbräuchlicher Erhebung, Verarbeitung oder Nutzung durch technische und organisatorische Maßnahmen zu schützen. Die Wirksamkeit der Schutzmaßnahmen ist regelmäßig zu prüfen. Die Umsetzung dieses Grundsatzes erfolgt in Zusammenarbeit mit dem Datenschutzbeauftragten.

5.6 Grundsatz: Nachvollziehbarkeit

Sicherheitsrelevante Aktivitäten und Prozesse sind nachvollziehbar zu gestalten und angemessen zu dokumentieren. Die dabei erhobenen Daten sind sicher zu verwahren und angemessen vor unberechtigtem Zugriff zu schützen. Die Erhebung der Daten erfolgt in Abstimmung mit dem Datenschutzbeauftragten.

Die Erhebung der Daten umfasst Daten zur Nachvollziehbarkeit von Datenzugriffen, Transaktionen und geschäftlicher Kommunikation zwischen Mitarbeitern, Partnern und Kunden.

5.7 Grundsatz: Schutz vor Angriffen und Notfällen

Geschäftsprozesse sind angemessen vor Angriffen und Notfällen zu schützen. Hierzu sind geeignete Notfall- und Wiederanlaufpläne zu entwickeln, zu testen und regelmäßig zu aktualisieren.

5.8 Grundsatz: Gewährleistung des Betriebs

Der IT-Betrieb ist grundsätzlich so auszugestalten, dass die Anforderungen des Geschäftsbetriebs vollständig erfüllt werden. Dies betrifft auch ausgelagerte Bereiche des IT-Betriebs. Für die Sicherstellung der Angemessenheit bei der Ausgestaltung des IT-Betriebs sind mindestens folgende Prozesse und Verfahren gem. ITIL V3 (oder höher) zu etablieren: Kapazitätsmanagement, Verfügbarkeitsmanagement, Datensicherungsmanagement, Change- und Releasemanagement, Incident- und Problemmanagement.

Die Gewährleistung des Betriebes ist auch bei der Umsetzung von IT-Projekten jeglicher Art zu berücksichtigen.

5.9 Grundsatz: Wirtschaftlichkeit

Die Maßnahmen zur Informationssicherheit sind unter der Maßgabe der Wirtschaftlichkeit zu betrachten und auszugestalten, soweit sie über das festgelegte Mindestschutzniveau der Standardabsicherung nach BSI Standard 200-2 hinausgehen. Bei der Konzeption entsprechender Maßnahmen sind daher immer die Kosten der Maßnahme dem bestehenden Risiko gegenüberzustellen und Abwägungen vorzunehmen. Dabei sind grundsätzlich auch Risiken zu betrachten, die keinen unmittelbaren Bezug zur jeweiligen Maßnahme haben.

5.10 Grundsatz: Prozessbasierte Sicherheit

Im Fokus der Informationssicherheit stehen die Geschäftsprozesse der Autobahn GmbH, so dass diese in einer Ende-zu-Ende-Betrachtung gem. den Sicherheitsanforderungen zur Verfügung stehen. Dabei spielt es keine Rolle, ob es sich um Führungs-, Kern-, oder Unterstützungsprozesse handelt. Der jeweilige Prozess-Eigentümer ist dafür verantwortlich, dass ein Sicherheitsniveau ermittelt und angewandt wird.

6. Weitere Regelungsdokumente

Zur Umsetzung der Informationssicherheit werden nach Inkraftsetzung dieser Sicherheitsleitlinie weitere Regelungsdokumente erstellt und dem relevanten Adressaten zur Berücksichtigung zur Verfügung gestellt (siehe auch Abbildung 1). Die Erstellung dieser Dokumente orientiert sich dabei an der Methodik des BSI-Rahmenwerkes.

Die Regelungsdokumente werden dabei in folgende Kategorien eingeteilt:

- Organisatorische Konzepte, z. B. Organisation der Informationssicherheit, Informationssicherheits-Risikomanagement, Schulung und Sensibilisierung.

- Logische / Technische Konzepte, z. B. Netzwerktopologie und Schutz der Netzwerkinfrastruktur, Schutz vor Schadsoftware, Protokollierung, Systemhärtung.
- Materielle Konzepte, z. B. Standort- und Raumplanung, Zutrittsschutz, Überwachung
- Notfallkonzepte, z. B. Geschäftsfortführungspläne, Wiederanlaufpläne
- Betriebskonzepte, z.B. Change- und Releasemanagement, Datensicherungskonzept, Incident- und Problemmanagement
- Schnittstellenkonzepte, z. B. Internes Kontrollsystem, Risikomanagement, Datenschutz, Personalwesen

7. Sensibilisierung

Die Einhaltung und Umsetzung von Sicherheitsmaßnahmen sind durch Sensibilisierung und Schulung aller Mitarbeiter zu gewährleisten. Ein angemessenes Sicherheitsbewusstsein ist daher sowohl bei Führungskräften als auch bei Mitarbeitern zu schaffen und aufrechtzuerhalten. Der Wissensstand aller Mitarbeiter ist regelmäßig durch Schulungsmaßnahmen aufzufrischen und an geänderte Rahmenbedingungen anzupassen.

8. Durchsetzung

Verstöße gegen die Leitlinie für die Informationssicherheit können vorsätzliche oder grob fahrlässige Handlungen darstellen, die:

- gegen bestehende Gesetze, Verordnungen oder arbeitsordnende Regelungen verstoßen,
- der Autobahn GmbH des Bundes oder deren Kunden einen tatsächlichen oder potentiellen Vermögensschaden zufügen,
- den Ruf der Autobahn GmbH des Bundes, von Mitarbeiter oder Kunden schädigen oder
- den unberechtigten Zugriff auf Daten und deren Missbrauch ermöglichen.

Verstöße gegen diese IS-Leitlinie und die abgeleiteten Richtlinien und Vorgaben können zu arbeitsrechtlichen Konsequenzen führen. Bei schweren Verstößen sind zivilrechtliche, verwaltungsrechtliche oder strafrechtliche Folgen möglich.

9. Evaluation und Revision

Der Umsetzungsstand von zur Erreichung des angestrebten Schutzniveaus erforderlichen Maßnahmen ist laufend zu erheben und regelmäßig in der Berichterstattung an die Geschäftsführung darzustellen. Dabei kann die Systematik des einzusetzenden ISMS-Tools genutzt werden, soweit diese alle wesentlichen Anforderungen an die Informationssicherheit einbezieht. Deckt das Tool wesentliche Anforderungen nicht ab, sind alternative Erhebungsmethoden zu entwickeln und deren Angemessenheit regelmäßig zu prüfen.

Nachgelagerte Prüfungen der Angemessenheit von Maßnahmen zur Informationssicherheit erfolgen durch die interne IT-Revision. Prüfungen können außerdem anlassbezogen oder regelmäßig durch das BSI erfolgen. Entsprechende Einsichts- und Prüfungsrechte werden dem BSI zugesichert.

10. Bekanntgabe

Die Leitlinie für die Informationssicherheit wird durch die Geschäftsführung allen Mitarbeitern der Autobahn GmbH des Bundes in der jeweils aktuellen Version zur Einsicht bereitgestellt.