Informationssicherheitsordnung

Vom 06.03.2025

1. Informationssicherheit 2

1.1 Grundlage 2
1.2. Besondere programmliche Anforderungen 2
1.3 Sicherheitsziele 3
1.4 Geltungsbereich 3

2. Organisation der Informationssicherheit 4

2.1 Informationssicherheitsgremium 4
2.2 Informationssicherheitbeauftragte:r 5
2.3 Bereichs-Informationssicherheitsbeauftragte 6
2.4 IT-Sicherheitsbetrieb 6
2.5 Informationsverantwortliche 7
2.6 Informationstreuhänder:innen 7
2.7 IT-Administratoren:innen 9
2.8 IT-Anwender:innen 9

3. Sicherheitsstandards und Sicherheitskonzepte 9

3.1 Sicherheitsstandards 9
3.2 Sicherheitskonzepte 10

4. Maßnahmen 10

4.1 Nutzung 10
4.2 Sicherheitsdokumentation 10
4.3 Systemzugangskontrolle 10
4.4 Protokollierung und Auswertung 11

5. Inkrafttreten 12

Anlage 1 Glossar 13

Anlage 2 Vorgaben und Standards zur Informationssicherheit 14

1. Informationssicherheit

Informationssicherheit im Sinne dieser Ordnung ist der Schutz von digitalen Informationen sowie von IT-Systemen, Anwendungen und Dienste vor Verlust der Vertraulichkeit, Integrität und Verfügbarkeit durch Einhaltung bestimmter Vorgaben und Standards.

Der Begriff IT steht für Informationstechnik. IT-Systeme sind demnach sämtliche technischen Mittel, die der Verarbeitung (zum Beispiel Computer), der Speicherung (zum Beispiel Serverlaufwerke) oder der Übertragung (zum Beispiel Netzwerk) von digitalen Informationen dienen.

1.1 Grundlage

Die Digitalisierung in Hörfunk und Fernsehen sowie die Präsenz im Internet führen im Westdeutschen Rundfunk (WDR) zu IT-gestützten Arbeitsabläufen, in denen dezentrale Systeme über die IT-Infrastruktur verbunden sind. Der Einsatz von Informationstechnologie in den sendekritischen Bereichen hat zur Folge, dass die Funktionen der IT-Systeme essenziell für die Erfüllung des Programmauftrags sind.

Maßnahmen zur Informationssicherheit sind jedoch nicht nur gesetzlich vorgeschrieben, sondern auch eine Verpflichtung gegenüber den Aufsichtsgremien, den Beschäftigten des WDR und seinem Publikum. Daher müssen sich alle, die im WDR mit IT befasst sind, der Notwendigkeit von Informationssicherheit bewusst sein und entsprechend handeln.

Diese Informationssicherheitsordnung ist die Grundlage für Informationssicherheit im WDR. Sie unterstützt die Erstellung von Risikoanalysen und Sicherheitskonzepten. Sie dient nicht der automatisierten Verhaltens- und Leistungskontrolle von Beschäftigten. Eine angemessene Informationssicherheitsstrategie muss eine ordnungsgemäß funktionierende IT sowie den Datenschutz bei der Verarbeitung personenbezogener Daten sicherstellen und die besonderen Bedürfnisse der programmlichen Arbeit berücksichtigen.

1.2. Besondere programmliche Anforderungen

Konzepte und Maßnahmen zur Gewährleistung des Schutzes von digitalen Informationen, Datenträgern und Netzen vor nicht autorisiertem Zugriff sind auch aus Programmsicht von großer Bedeutung. Sie müssen somit auch die Redaktions- und Produktionsabläufe berücksichtigen und unterstützen. Das ist umso notwendiger, da Produktions-, Redaktions-, Sende- und Archivierungssysteme weitgehend digital basiert sind und daher ein Teil der IT-Infrastruktur des WDR sind.

Programmarbeit geht heute deutlich über die reine Erstellung eines Radio- oder Fernsehprogramms hinaus. Sendungen und Programmbeiträge sind nicht mehr auf einen einzigen Verbreitungsweg beschränkt, sondern werden zum Teil – auch in Form von Derivaten – auf unterschiedlichen Verbreitungswegen verteilt. Eine dem

jeweiligen Produktionsprozess oder Verbreitungsweg entsprechende inhaltliche und technische Aufbereitung ist dafür Voraussetzung.

Ein erheblicher Teil der Beiträge und Derivate wird in freier Mitarbeit produziert. Daher sollte der betreffende Personenkreis sicher authentifiziert und in die Lage versetzt werden, auf diejenigen Teile der IT-Infrastrukturzuzugreifen, die er für die Erledigung des von ihm für den WDR übernommenen Auftrags benötigt.

Aus Programmsicht ist eine dem Programmentstehungsprozess angepasste Sicherheitsphilosophie mit klaren Zugangsregeln und Verantwortlichkeiten bei gleichzeitig größtmöglicher Flexibilität unumgänglich.

1.3 Sicherheitsziele

Diese Informationssicherheitsordnung unterstützt die Sicherheitsziele des WDR. Diese lauten:

- Erhaltung der in Wissen, Informationen, Arbeitsprozesse und Technik investierten Werte,
- Sicherstellung der Kontinuität der Arbeitsabläufe im WDR,
- Sicherung einer hohen Qualität von Informationen in puncto Rechtzeitigkeit, Richtigkeit und Vertraulichkeit,
- Minimierung der im Schadensfall entstehenden Kosten,
- Schutz vor Datenmissbrauch, Datenverlust sowie Integritätsverlust,
- Beachtung von Gesetzen und Vorschriften, insbesondere der Einhaltung datenschutzrechtlicher Anforderungen.

1.4 Geltungsbereich

Diese Informationssicherheitsordnung gilt für alle digitalen Informationen sowie für IT-Systeme, Anwendungen und Dienste des WDR inklusive der Produktions- und Sendesysteme. Die Informationssicherheitsordnung ist für alle verpflichtend, die beim WDR beschäftigt sind oder mit ihm auf vertraglicher Basis zusammenarbeiten und mit den IT-Einrichtungen des WDR befasst sind. Die zugehörigen Sicherheitsanforderungen gelten auch für dem WDR verbundene Unternehmen sowie andere Unternehmen, welche die IT-Infrastruktur des WDR nutzen oder Informationen für ihn verarbeiten. Die anfordernden Stellen müssen veranlassen, dass die Unternehmen vom WDR vertraglich zur Einhaltung der Sicherheitsanforderungen sowie im Falle von Verstößen zu Vertragsstrafen verpflichtet werden.

2. Organisation der Informationssicherheit

Die Gesamtverantwortung für die Informationssicherheit im WDR liegt bei der Leitung des WDR (Intendant:in). Sie sorgt für die notwendige Unterstützung im Informationssicherheitsprozess, indem sie die Sensibilisierung für Informationssicherheit im Unternehmen fördert und als Qualitätsaspekt in Produkte und Prozesse einbezieht.

Der unternehmensübergreifende Charakter des Informationssicherheitsprozesses bedingt eine klare Definition der Rollen und Verantwortlichkeiten. Nur so kann gewährleistet werden, dass alle wichtigen Aspekte berücksichtigt und sämtliche anfallenden Aufgaben effizient erledigt werden.

Die Verantwortung für eine sichere und ordnungsgemäße IT-gestützte Aufgabenerfüllung wird gleichermaßen in die Linie delegiert, wie die Verantwortung für die originären Aufgaben.

Daher werden die folgenden Funktionen und Verantwortlichkeiten für Informationssicherheit im WDR definiert:

- Informationssicherheitsgremium,
- Informationssicherheitsbeauftragte:r,
- Bereichs-Informationssicherheitsbeauftragte,
- IT-Sicherheitsbetrieb
- Informationsverantwortliche,
- Informationstreuhänder:innen,
- IT-Administrator:innen,
- IT-Anwender:innen .

2.1 Informationssicherheitsgremium

Das Informationssicherheitsgremium regelt unternehmensweit die Informationssicherheitsbelange und ist Betreiber des Informationssicherheitsprozesses im WDR. Es stellt die Entwicklung der Informationssicherheitsordnung inklusive der damit verbundenen Standards sowie deren ständige Fortschreibung und Veröffentlichung sicher.

Das Informationssicherheitsgremium wird von der Leitung des WDR bestellt. Es steht in ständigem Austausch mit der beauftragten Person für betrieblichen Datenschutz im WDR (Datenschutzbeauftragte:r), dem Personalrat und dem Justiziariat. Sofern

Beteiligungsrechte der Personalvertretung nach den Vorschriften des Landespersonalvertretungsgesetzes NRW betroffen sind, wird der WDR den Personalrat in der rechtlich gebotenen Weise beteiligen.

Das Informationssicherheitsgremium entscheidet in Fragen der Informationssicherheit einvernehmlich. Im Falle eines Dissenses liegt das Letztentscheidungsrecht bei der Leitung des WDR.

Aufgaben des Informationssicherheitsgremiums sind:

- Weiterentwicklung der Informationssicherheitsordnung des WDR,
- Steuerung und Kontrolle des Informationssicherheitsprozesses,
- Initiierung, Beauftragung und Verabschiedung von Sicherheitsstandards und Vorgaben zur Informationssicherheit sowie beratende Unterstützung bei deren Erstellung,
- Überprüfung der fertigen Konzepte und Standards hinsichtlich des Erreichens der Sicherheitsziele,
- Beratung der Geschäftsleitung bei der Festlegung der für den Informationssicherheitsprozess zur Verfügung stehenden Ressourcen.

2.2 Informationssicherheitbeauftragte:r

Die beauftragte Person für Informationssicherheit im WDR (Informationssicherheitsbeauftragte:r) ist in ihrer Funktion fachlich unabhängig und kann nur von der Leitung des WDR angewiesen werden. Ihre Aufgaben sind:

- Zentrale Ansprechstelle für digitale Informationssicherheit im WDR, Koordination des Informationssicherheitsprozesses und Mitwirkung an allen damit zusammenhängenden Aufgaben,
- Planung und Koordination von Sensibilisierungsmaßnahmen zur Informationssicherheit,
- Verantwortlichkeit für die Erstellung von Standards und Vorgaben zur Informationssicherheit,
- Überwachung der Implementierung von Maßnahmen zur Informationssicherheit,
- Berichten über den Informationssicherheitsprozess an die Geschäftsleitung und an das Informationssicherheitsgremium,
- Beratung der Geschäftsleitung in Fragen der Informationssicherheit,
- Kontrolle der Effektivität von Sicherheitsmaßnahmen im laufenden Betrieb,

- Leitung von Untersuchungen bei sicherheitsrelevanten Ereignissen.

2.3 Bereichs-Informationssicherheitsbeauftragte

Die Bereichs-Informationssicherheitsbeauftragten sind für die Überwachung der betrieblichen Umsetzung der Sicherheitskonzepte und Sicherheitsstandards in einem vom Informationssicherheitsgremium definierten Bereich zuständig. Fachlich sind sie der beauftragten Person für Informationssicherheit im WDR zugeordnet und stellen das Bindeglied zwischen dieser und dem eigenen Bereich dar.

Aufgaben der Bereichs-Informationssicherheitsbeauftragten sind:

- Überwachung der Umsetzung der Vorgaben zur Informationssicherheit,
- Überprüfung der Sicherheitskonzepte auf Erfüllung der Standards und Vorgaben zur Informationssicherheit,
- zentrale Ablage der Sicherheitskonzepte sowie deren turnusmäßige Prüfung auf Aktualität,
- Ansprechstelle für Beschäftigte bei Fragen zur Informationssicherheit,
- Überwachung der Realisierung von Informationssicherheitsmaßnahmen im eigenen Bereich,
- Mitwirkung bei der Erstellung von Sicherheitskonzepten,
- Überwachung der Durchführung geeigneter Schulungsmaßnahmen zur Informationssicherheit im eigenen Bereich,
- Austausch und Abstimmung mit der beauftragten Person für Informationssicherheit im WDR .

2.4 IT-Sicherheitsbetrieb

Der IT-Sicherheitsbetrieb ist verantwortlich für die operative IT-Sicherheit im WDR und den Schutz des WDR vor Angriffen aus dem Cyberraum.

Zu den Aufgabe des IT-Sicherheitsbetriebs gehören:

- Betrieb der zentralen Sicherheitsinfrastruktur (z. B. Firewall, Endpointschutz, SIEM),
- Bereitstellung des zentralen Log-Managements (inklusive Sammeln, zentrales Aggregieren, Speichern, Aufbewahren und Analysieren von Logs),
- Auswertung des zentralen IT-Sicherheitsmonitoring,

- Detektion und Verfolgung von IT-Schwachstellen,
- Behandlung von IT-Sicherheitsvorfällen,
- Beratung der Informationstreuhänder und IT-Fachbereiche bei der Umsetzung von technischen Sicherheitsmaßnahmen.
- Bereitstellung von technischen Richtlinien zur Umsetzung der Vorgaben und Standards zur Informationssicherheit,
- Unterstützung bei Sensibilisierungsmaßnahmen zur Informationssicherheit.

2.5 Informationsverantwortliche

Der WDR ist Eigentümer aller von ihm beziehungsweise von seinen Beschäftigten im Rahmen ihrer dienstlichen Tätigkeiten erzeugten Informationen. Für all diese Informationen und den damit verbundenen Arbeitsabläufen müssen jeweils Verantwortliche (Informationsverantwortliche) benannt sein. Unabhängig davon bleiben die Rechte des Personalrates nach den Vorschriften des Landespersonalvertretungsgesetzes NRW sowie die Rechte der beauftragten Person für betrieblichen Datenschutz im WDR nach den Vorschriften des WDR-Gesetzes, des Datenschutzgesetztes NRW sowie etwaiger weiterer nationaler und europäischer Datenschutzregelungen unberührt.

Die Informationsverantwortung liegt bei der Leitung der Organisationseinheit (zum Beispiel PBL, AL, HAL), in der die Information erzeugt wurde oder die die Information von Dritten außerhalb des WDR erhalten hat. Die Informationsverantwortlichen entscheiden, wer in welchem Umfang auf die Informationen zugreifen darf und welche Anforderungen an deren Zugang zu erfüllen sind. Sie legen die für die betreffenden Informationen erforderlichen Sicherheitsanforderungen fest und überwachen deren Einhaltung. Die Sicherheitsanforderungen beinhalten unter anderem die Wahrung der Vertraulichkeit, der Integrität und der Verfügbarkeit der Informationen. Sie bestimmen den Kontrollumfang und achten auf die Einhaltung der geltenden Aufbewahrungsvorschriften.

Im Zuge der Bearbeitung oder Übertragung von Informationen in verschiedenen Bereichen kann die Verantwortung für die neu entstandenen Informationen wechseln.

2.6 Informationstreuhänder:innen

Personen mit Informationstreuhänderschaft (Informationstreuhänder:innen) sind für den sicheren Betrieb der ihnen zugeordneten IT-Systeme, Anwendungen und Dienste verantwortlich. Sie sorgen für die Erstellung und die betriebliche Umsetzung der Sicherheitskonzepte sowie die Einhaltung der Vorgaben zur Informationssicherheit.

Sofern ihnen die betreffenden IT-Systeme, Anwendungen und Dienste durch externe Dritte (bspw. in einem externen Rechenzentrum oder in der Cloud) bereitgestellt

werden, haben sie vertragliche Regelungen zu veranlassen, mit denen externen Betreiber dazu verpflichtet werden, die betrieblichen Aufgaben der Informationstreuhänderschaft gemäß der Informationssicherheitsvorgaben des WDR wahrzunehmen und den sicheren Betrieb der jeweiligen IT Systeme, Anwendungen und Dienste zu verantworten.

Personen mit Informationstreuhänderschaft sorgen insbesondere für die Wahrung der

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit,
- Authentizität,
- Verbindlichkeit,
- Revisionsfähigkeit und
- Transparenz

Der Informationen in dem mit den jeweiligen Informationsverantwortlichen vereinbarten Umfang. Sie sind verpflichtet, die Informationsverantwortlichen über akute oder mögliche Risiken zu informieren. Darüber hinaus übernehmen sie für das IT-System, den Dienst oder die Anwendung die Produktverantwortung aus sicherheitstechnischer Sicht (Prüfung und zeitnahe Installation von sicherheitsrelevanten Updates, Planung von Änderungen im Produktlebenszyklus und Verwaltung der Lizenzen sowie die Erfassung in den relevanten Dokumentationssystemen).

Bei der Beschaffung von IT-Systemen, Anwendungen und Diensten ist das zentrale Software-Lizenzmanagements einzubeziehen. Dabei werden die Erfüllung der für die Softwarebeschaffung erforderlichen Voraussetzungen geprüft und durch das zentrale Software-Lizenzmanagement erfasst.

Für die von den IT-Betrieben bereitgestellten und betriebenen IT-Systeme, Anwendungen und Dienste liegt die Informationstreuhänderschaft bei der Leitung des jeweils zuständigen IT-Bereichs.

Für alle anderen IT-Systeme, Anwendungen und Dienste liegt die Informationstreuhänderschaft, soweit dies nicht anders vereinbart wurde, bei den Leitungen der Organisationseinheiten, für die diese IT-Systeme, Anwendungen und Dienste beschafft wurden (bedarfsanmeldenden Organisationseinheiten). Bei der Beschaffung und dem Betrieb der IT-Systeme, Anwendungen und Dienste ist in diesen Fällen verpflichtend die Unterstützung des zuständigen IT-Bereichs einzuholen.

Stellen Personen mit Informationstreuhänderschaft einen IT-Dienst mehreren Informationsverantwortlichen zur Verfügung (zum Beispiel E-Mail), müssen sie den Schutzbedarf für die Anwendung vorab festlegen oder gemeinsam mit den Informationsverantwortlichen abstimmen.

2.7 IT-Administratoren:innen

IT administrierende Personen (IT-Administrator:innen) sind für den geordneten Betrieb und die Sicherheitsbelange der von ihnen betreuten IT-Systeme verantwortlich. Sie werden von den betreffenden Personen mit Informationstreuhänderschaft benannt. IT administrierende Personen sind für die Sicherheitsbelange aller von ihnen betreuten IT-Systeme zuständig. Sie müssen die dafür erforderlichen Fachkenntnisse stets auf dem aktuellen Stand der Technik halten (bspw. mittels Schulungen, Weiterbildungen). Für alle IT-Systeme im WDR müssen IT administrierende Personen benannt sein.

Näheres hierzu regelt die DA IT-Administration.

2.8 IT-Anwender:innen

IT anwendende Personen (IT-Anwender:innen) nutzen Informationen oder geben sie ein. Sie sind bei der Erstellung, Nutzung und Verwaltung von Informationen verpflichtet, die Informationssicherheitsordnung sowie die daraus resultierenden Standards und Vorgaben zur Informationssicherheit einzuhalten. Hierzu sind sie durch geeignete Schulungsmaßnahmen in die Lage zu versetzen.

Näheres hierzu regelt die DA IT-Anwendung.

3. Sicherheitsstandards und Sicherheitskonzepte

Jede im oder für den WDR betriebene Hard- und Software muss den Sicherheitsanforderungen des WDR entsprechen.

Detaillierte Zielsetzungen und Anforderungen zur Gewährleistung der Sicherheit von digitalen Informationen sowie der zugehörigen IT-Systeme, Anwendungen und Dienste werden in den betreffenden Sicherheitsstandards und Sicherheitskonzepten festgelegt.

3.1 Sicherheitsstandards

Der WDR orientiert sich an der ISO/IEC 27001 sowie dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die jeweils aktuelle Version des BSI-Grundschutz-Kompendiums bildet die Grundlage für die Sicherheitskonzepte im WDR.

Die spezifischen Sicherheitsstandards finden sich in den WDR Vorgaben und Standards zur Informationssicherheit (siehe Anlage 2).

3.2 Sicherheitskonzepte

Die Sicherheitskonzepte basieren auf dieser Informationssicherheitsordnung sowie auf den zuvor vereinbarten Sicherheitsstandards. Sie legen die Sicherheitsanforderungen an die IT-Systeme, Anwendungen und Dienste fest. Die Umsetzung dieser Anforderungen und die Dokumentation der Umsetzung ist durch die Personen mit Informationstreuhänderschaft sicherzustellen.

4. Maßnahmen

Zur Wahrung der Informationssicherheit sind im WDR sowohl für die Nutzung als auch für den Betrieb von IT-Systemen die folgenden Maßnahmen verbindlich:

4.1 Nutzung

Die Nutzung der IT-Systeme im WDR ist grundsätzlich nur mit IT-Geräten des WDR gestattet. Ausnahmefälle (zum Beispiel bei externer Fernwartung, Dienstleistung für Dritte) sind unter Beachtung der WDR-Vorschriften zur Informationssicherheit von den Informationsverantwortlichen beziehungsweise den zuständigen Personen mit Informationstreuhänderschaft zu genehmigen sowie entsprechend zu dokumentieren.

Die Benutzung der IT-Systeme des WDR für private Zwecke ist grundsätzlich nicht zulässig, sofern sie nicht durch andere WDR-Regelungen erlaubt ist (siehe zum Beispiel DV Internet- und E-Mail-Nutzung).

4.2 Sicherheitsdokumentation

Für alle im oder für den WDR betriebenen IT-Systeme, Anwendungen und Dienste sind von den Personen mit Informationstreuhänderschaft Sicherheitskonzepte auf Basis der Sicherheitsstandards zu erstellen. Die Sicherheitskonzepte sind bei jeder Änderung eines IT-Systems sowie bei Veränderungen der Rahmenbedingungen zu überprüfen und gegebenenfalls zu aktualisieren.

4.3 Systemzugangskontrolle

Zum Schutz der Informationen und des ordnungsgemäßen Ablaufs des IT-Betriebs werden grundsätzlich alle IT-Systeme im WDR mit einer Zugangskontrolle gesichert. Diese dient auch dem Schutz von personenbezogenen Daten vor unberechtigtem Zugriff. Daher ist grundsätzlich für jedes IT-System eine eindeutige Identifizierung und sichere Authentifizierung der IT anwendenden und IT administrierenden Personen erforderlich. Ausnahmen (zum Beispiel Funktionskennungen) sind mit der

beauftragten Person für Informationssicherheit im WDR abzustimmen und zu dokumentieren. Die Ausgestaltung der Zugangskontrolle sollte die betrieblichen Arbeitsabläufe berücksichtigen, sofern sich daraus keine zusätzlichen Sicherheitsrisiken ergeben. In jedem Falle ist die Nutzung einer von mehreren Personen verwendeten Kennung revisionssicher (siehe Anlage 1) zu dokumentieren.

4.4 Protokollierung und Auswertung

Protokolldateien im Sinne dieser Ordnung werden zu den nachfolgend genannten innerbetrieblichen Zwecken geführt:

- Sicherstellung und Überprüfung eines ordnungsgemäßen Betriebs (zum Beispiel Aufrechterhaltung der Informationssicherheit, Störungsbehebung),
- Abrechnungszwecke,
- statistische Erhebungen (zum Beispiel Kapazitätsermittlung, regelmäßige Information der Geschäftsleitung),
- Ermittlung bei begründetem Verdacht auf Verstöße gegen Gesetze und Vorschriften (zum Beispiel Strafrecht, Datenschutzgesetze, WDR-Geschäftsordnung, DV Internet- und E-Mail-Nutzung).

Die technische Gewährleistung für die Protokollierung obliegt den zuständigen Personen mit Informationstreuhänderschaft.

Die Aufbewahrungsdauer für Protokolldaten mit Personenbezug ist mit der beauftragten Person für betrieblichen Datenschutz abzustimmen und entsprechend zu dokumentieren.

Eine personenbezogene Auswertung darf nur unter Einbeziehung der beauftragten Person für betrieblichen Datenschutz und ausschließlich zur Sicherstellung und Überprüfung des ordnungsgemäßen Betriebs, zu Abrechnungszwecken sowie zur Ermittlung bei begründetem Verdacht auf Verstöße gegen Gesetze und Vorschriften erfolgen. Hierbei sind die gesetzlichen Vorschriften, insbesondere die EU-Datenschutzgrundverordnung, das Datenschutzgesetz NRW und das Landespersonalvertretungsgesetz NRW, sowie die einschlägigen Regelungen des WDR (zum Beispiel WDR-Geschäftsordnung, Dienstvereinbarungen und Dienstanweisungen) zu beachten.

5. Inkrafttreten

Diese Ordnung tritt zum 01.03.2025 in Kraft und ersetzt die Informationssicherheitsordnung vom 11.05.2022.

Die Anlagen können durch die beauftragte Person für Informationssicherheit im WDR aktualisiert werden, ohne dass es hierzu einer Änderung dieser Ordnung bedarf.

Köln, 06.03.2025
gez. Katrin Vernau
Intendantin

Anlage 1 Glossar

Authentizität	Grundsatz, dass eine Empfängerin oder ein Empfänger zweifelsfrei sicher sein kann, dass eine empfangene Nachricht tatsächlich von der angegebenen Quelle stammt und nicht gefälscht oder anderweitig durch Dritte verändert worden ist.
Derivat	Abgeleitete Version eines Programmbeitrags.
Informationen	Daten, die gespeichert oder verwaltet werden auf Systemen oder Medien, wie zum Beispiel auf mobilen Datenträgern, CDs, in der Infrastruktur oder im Rahmen von Geschäftsabläufen.
Integrität	Vermeidung unberechtigter Änderungen, Erstellung oder Duplizierung von Informationen.
Revisionssicherheit	Wesentliche Merkmale einer revisionssicheren Dokumentation sind, die Wiederauffindbarkeit und Nachvollziehbarkeit der Daten, sowie die Gewährleistung ihrer Integrität.
Verbindlichkeit	Dieser Grundsatz besagt, dass später nachgewiesen werden kann, dass die an einer Transaktion Beteiligten die Transaktion tatsächlich autorisiert haben und sie über keinerlei Mittel verfügen, ihre Beteiligung zu bestreiten.
Verfügbarkeit	Vermeidung einer nicht annehmbaren Verzögerung bei der Durchführung eines genehmigten Zugriffs auf Informationen.
Vertraulichkeit	Vermeidung der Offenlegung von Informationen ohne Erlaubnis der Eigentümerin oder des Eigentümers.

Anlage 2 Vorgaben und Standards zur Informationssicherheit

(Stand: 05.02.2025)

Vorgaben

- Informationssicherheitsordnung
- DA IT-Anwendung
- DA IT-Administration
- DA IT-Wartung
- DA IT-Sicherheitsvorfallbehandlung
- DA Vertraulichkeit

Standards

- Erstellung von Sicherheitskonzepten
- Festlegung des Schutzbedarfs
- Konzept zum Schutz vor Schadsoftware
- Kryptokonzept
- ARD-Mindeststandard zur Authentisierung
- ARD-Verfahren zur Berücksichtigung der Informationssicherheit bei Kooperationen und gemeinsamen Projekten
- ARD-Verfahren zur Durchführung einer ergänzenden Risikoanalyse bei Kooperationen und gemeinsamen Projekten
- BSI IT-Grundschutz-Kompendium