

**Verwaltungsvorschrift
des Sächsischen Staatsministeriums der Justiz
zur Gewährleistung der Informationssicherheit
(VwV Informationssicherheit Justiz – VwVISichJus)**

Vom 17. September 2021

I.

Regelungsgegenstand, Begriffsbestimmung

Diese Verwaltungsvorschrift dient der Schaffung eines Informationssicherheitsprozesses zur Gewährleistung der Informationssicherheit. Die allgemeinen Grundsätze und Ziele der Informationssicherheit, die Aufgaben und Verantwortlichkeiten sowie die Informationssicherheitsorganisation sind in der Leitlinie Informationssicherheit (Anlage 1) ausgeführt. Staatliche Stellen im Sinne dieser Verwaltungsvorschrift sind das Staatsministerium der Justiz und sämtliche ihm nachgeordneten Behörden sowie die Gerichte.

II.

Beauftragte für Informationssicherheit

1. Die Beauftragten für Informationssicherheit fördern die Informationssicherheit mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten.
2. Den Beauftragten für Informationssicherheit werden keine Entscheidungsbefugnisse übertragen.
3. Bei der organisatorischen Zuweisung der Aufgaben sollen Interessenkonflikte vermieden werden. Insbesondere soll keine Personenidentität zwischen der oder dem Verantwortlichen für IT und der oder dem Beauftragten für Informationssicherheit der staatlichen Stelle bestehen.
4. Über Ernennungen der Beauftragten für Informationssicherheit ist das Staatsministerium der Justiz durch die Leiterin oder den Leiter der staatlichen Stelle auf dem Dienstweg zu unterrichten.
5. In die Beurteilung, ob Vorgänge im jeweiligen Zuständigkeitsbereich Auswirkungen auf die Informationssicherheit haben, ist die oder der jeweils zuständige Beauftragte für Informationssicherheit der staatlichen Stelle einzubeziehen. Hierbei sind der oder dem Beauftragten für Informationssicherheit wesentliche Informationen zur Beurteilung zu übermitteln. Die oder der Beauftragte für Informationssicherheit hat binnen drei Monaten Stellung zu nehmen, ob die Informationssicherheit berührt ist. Falls dies der Fall ist, ist sie oder er anschließend an allen Vorgängen im jeweiligen Zuständigkeitsbereich zu beteiligen, die Auswirkungen auf die Informationssicherheit haben. Die oder der Beauftragte für Informationssicherheit kann hierzu Informationen und Dokumente anfordern, den für die Vorgänge Verantwortlichen Vorgaben der Informationssicherheit mitteilen und bei der Umsetzung der Vorgaben unterstützend mitwirken. Die Gesamtverantwortung nach Nummer 3.1 der Anlage 1 bleibt hiervon unberührt.

III.

Information und Sensibilisierung der Bediensteten

1. Bedienstete im Sinne dieser Verwaltungsvorschrift sind alle im Geschäftsbereich des Staatsministeriums der Justiz tätigen Richterinnen und Richter, Beamtinnen und Beamten, Referendarinnen und Referendare sowie Tarifbeschäftigten und Auszubildenden. Für Praktika sowie andere Dienst- und Beschäftigtenverhältnisse gilt die Verwaltungsvorschrift entsprechend.
2. Die Bediensteten sind auf diese Verwaltungsvorschrift und die Anlage 1 sowie auf deren Ablageort im Intranet hinzuweisen. Auf Anforderung sind diese Verwaltungsvorschrift und die Anlage 1 in Papierform auszuhändigen.
3. Die Bediensteten sind über ihre Pflichten gemäß Nummer 3.5 der Anlage 1 zu informieren. Die Information erfolgt unverzüglich nach dem Dienstantritt der Bediensteten. Die staatlichen Stellen haben die Durchführung der Information aktenkundig zu machen. Bereits im Dienst befindliche Bedienstete sind binnen sechs Monaten nach Inkrafttreten dieser Verwaltungsvorschrift zu informieren.
4. Die Bediensteten sind mittels geeigneter Maßnahmen fortlaufend zu sensibilisieren. Geeignete Maßnahmen können insbesondere Hinweise zum verantwortungsvollen Umgang mit IT-Technik, Informationen zu aktuellen und für die Justiz relevanten Geschehnissen aus der Informationssicherheit sowie Anweisungen zum informationssicheren Verhalten im Dienst und zum Umgang mit Hard- und Software sein.
5. Zukünftige, im Rahmen der Informationssicherheit erforderliche Belehrungen der Bediensteten haben unverzüglich zu erfolgen und sind jeweils aktenkundig zu machen.
6. Die Bediensteten sind verpflichtet, sich zur Informationssicherheit durch Kenntnisnahme der im Intranet

bereitgestellten Dokumente und der durch die Beauftragten für Informationssicherheit übermittelten Hinweise selbst laufend fortzubilden.

7. Die Bediensteten mit einem Active-Directory-Benutzerkonto (AD-Benutzerkonto) haben binnen zwei Monaten nach Dienstantritt das durch den Beauftragten für Informationssicherheit des Landes angebotene elektronische Lernprogramm zum Thema "Informationssicherheit am Arbeitsplatz" in der jeweils aktuellen Fassung zu absolvieren. Dies gilt nicht, wenn ein Nachweis über die Absolvierung des Lernprogramms bereits erfolgt ist.
8. Bedienstete mit einer beabsichtigten Verweildauer unter zwei Monaten in der Dienststelle oder ohne AD-Benutzerkonto sind unverzüglich nach Dienstantritt unter Nutzung des Musters in Anlage 3 schriftlich zur Informationssicherheit am Arbeitsplatz zu belehren. Stattdessen können die Bediensteten das elektronische Lernprogramm absolvieren. Die Belehrung oder der Nachweis über die Absolvierung des Lernprogramms ist von der Dienststellenleitung aktenkundig zu machen.

IV.

Externe Leistungserbringer

1. Soweit die staatlichen Stellen es für erforderlich halten, haben sie die von ihnen mit der Durchführung von Leistungen beauftragten Personen, Behörden und Unternehmen, die nicht zum Geschäftsbereich gehören (externe Leistungserbringer), gemäß Nummer 3.6 der Anlage 1 zur Gewährleistung der Einhaltung der Informationssicherheitsziele zu informieren. Hierzu sind diese Verwaltungsvorschrift und die Anlage 1 zu verwenden und zur Verfügung zu stellen. Die erfolgte Information ist von der staatlichen Stelle zu dokumentieren.
2. Die Verpflichtung wird schriftlich oder in elektronischer Form unter Nutzung des Musters in der Anlage 2 nach Einbindung der oder des zuständigen Beauftragten für Informationssicherheit vorgenommen. Dabei ist auf die strafrechtlichen Folgen einer Pflichtverletzung hinzuweisen.

V.

Inkrafttreten, Außerkrafttreten

Diese Vorschrift tritt am Tag nach ihrer Veröffentlichung in Kraft. Gleichzeitig tritt die **Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz zur Gewährleistung der Informationssicherheit** vom 6. Januar 2017 (SächsJMBI. S. 4), zuletzt enthalten in der Verwaltungsvorschrift vom 6. Dezember 2019 (SächsABl. SDR. S. S 374), außer Kraft.

Dresden, den 17. September 2021

Die Staatsministerin der Justiz und für Demokratie, Europa und Gleichstellung
Katja Meier

Anlage 1

Leitlinie des Sächsischen Staatsministeriums der Justiz zur Gewährleistung der Informationssicherheit (Leitlinie Informationssicherheit)

Inhaltsübersicht

1. Einleitung
2. Grundsätze und Ziele der Informationssicherheit
 - 2.1 Begriffe
 - 2.2 Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
 - 2.3 Informationssicherheit als Leistungsmerkmal von Geschäftsprozessen und IT-Verfahren
 - 2.4 Regelungskompetenz und Subsidiarität
 - 2.5 Informationssicherheitsmanagement-Team
 - 2.6 Sicherheit vor Verfügbarkeit
3. Aufgaben und Verantwortlichkeiten
 - 3.1 Verantwortung des Staatsministeriums der Justiz
 - 3.2 Verantwortung der Leitungsebene
 - 3.3 Verantwortung der Beauftragten für Informationssicherheit
 - 3.4 Verantwortung der Leitstelle für Informationstechnologie der sächsischen Justiz
 - 3.5 Verantwortung der Bediensteten

3.6 Fachverantwortliche

3.7 Beschäftigung externer Leistungserbringer

4. Umsetzung
5. Sicherung und Verbesserung der Informationssicherheit
6. IT-Notfallmanagement

1. Einleitung

- a) Die umfassende Sicherheit der von der Justiz und der Justizverwaltung verarbeiteten Informationen muss auch bei fortschreitender Digitalisierung sowohl der internen Geschäftsgänge als auch der Kommunikation mit Externen gewährleistet sein, weil dies eine der zwingenden Voraussetzungen ist, um das Vertrauen der Menschen in die Justiz als dritte Gewalt in unserer demokratischen Staatsordnung zu erhalten und zu vertiefen.
- b) Diese Leitlinie konkretisiert die Vorgaben des **Sächsischen Informationssicherheitsgesetzes** vom 2. August 2019 (SächsGVBl. S. 630) für den Geschäftsbereich des Staatsministeriums der Justiz und trifft darüber hinausgehende Regelungen. Die Gewährleistung der Informationssicherheit erfordert einen umfassenden Ansatz, der technische und organisatorische Umsetzungsmaßnahmen sowie rechtliche Regelungen gleichermaßen in den Blick nimmt. Hierfür bedarf es der Initiierung und Etablierung eines umfassenden Informationssicherheitsprozesses, der den gesamten Geschäftsbetrieb umfasst. Diese Leitlinie beschreibt die vom Staatsministerium der Justiz formulierten Informationssicherheitsziele, die verfolgte Informationssicherheitsstrategie und die Organisationsstrukturen, die für die Initiierung und Etablierung des Informationssicherheitsprozesses erforderlich sind. Sie orientiert sich an den aktuellen gültigen Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

2. Grundsätze und Ziele der Informationssicherheit**2.1 Begriffe**

- a) Informationssicherheit: Dies bezeichnet einen Zustand, in dem die Risiken für die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und der sie verarbeitenden Systeme durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. Die Informationssicherheit umfasst neben der Sicherheit von IT-Systemen und den darin gespeicherten Informationen auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.
- b) Vertraulichkeit: Dies bedeutet Schutz vor unbefugter Preisgabe von Informationen.
- c) Integrität: Damit wird die Sicherstellung der Korrektheit und Unversehrtheit von Daten und der korrekten Funktionsweise von Systemen bezeichnet. Der Verlust der Integrität von Informationen kann insbesondere bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.
- d) Verfügbarkeit: Die Verfügbarkeit ist das Vorhandensein von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen gemäß der jeweils für sie geltenden Anforderungen.
- e) Notfallmanagement: Es dient der Erhöhung der Ausfallsicherheit und der adäquaten Vorbereitung der Gerichte und Behörden auf Notfälle und Krisen, damit die wichtigsten Geschäftsprozesse bei einem etwaigen Ausfall schnellstmöglich wieder aufgenommen werden können.

2.2 Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Zur Erreichung und Aufrechterhaltung eines angemessenen und ausreichenden Informationssicherheitsniveaus sind die Standards des BSI in der jeweils aktuell gültigen Fassung ¹ maßgeblich.

2.3 Informationssicherheit als Leistungsmerkmal von Geschäftsprozessen und IT-Verfahren

Informationssicherheit ist ein zu bewertendes und herbeizuführendes Leistungsmerkmal von Geschäftsprozessen und IT-Verfahren. Bei der Gestaltung von Geschäftsprozessen sind technische und organisatorische Sicherheitsmaßnahmen zu berücksichtigen. Bleiben im Einzelfall trotz Sicherheitsvorkehrungen untragbare Risiken, ist auf den Einsatz des IT-Verfahrens zu verzichten oder der Geschäftsprozess anzupassen. Bei der Abwägung zwischen den Belangen der Informationssicherheit und der Gewährleistung einer effektiven Aufgabenerfüllung ist eine Risikobetrachtung erforderlich.

2.4 Regelungskompetenz und Subsidiarität

Das Staatsministerium der Justiz regelt Belange von übergeordnetem Interesse für den Geschäftsbereich, definiert Mindeststandards zur Informationssicherheit und formuliert Vorgaben zur Erreichung von Sicherheitszielen. Bei der Umsetzung der Aufgaben sind die staatlichen Stellen an diese aufgestellten Regelungen, Mindeststandards und Vorgaben gebunden. Sie können für den jeweiligen Zuständigkeitsbereich entsprechend den individuellen Anforderungen präzisiert und ergänzt sowie an die besonderen Bedürfnisse der einzelnen staatlichen Stellen angepasst werden. Die staatlichen Stellen sind im Übrigen, unbeschadet fachaufsichtlicher Vorgaben, in der Auswahl der Mittel frei, mit denen sie die Ziele der Informationssicherheit erreichen wollen.

2.5 Informationssicherheitsmanagement-Team

- a) Beim Sächsischen Staatsministerium der Justiz wird ein Informationssicherheitsmanagement-Team im Sinne

von § 9 Satz 1 des **Sächsischen Informationssicherheitsgesetzes** gebildet. Zur Sicherstellung der Informationssicherheit wirkt das Informationssicherheitsmanagement-Team beratend an der Festlegung von strategischen Entscheidungen und Einzelmaßnahmen mit möglichen Auswirkungen auf die Informationssicherheit mit, die vom Staatsministerium der Justiz festgesetzt werden.

- b) Das Informationssicherheitsmanagement-Team setzt sich wie folgt zusammen:
 - aa) die oder der Beauftragte beim Staatsministerium der Justiz;
 - bb) die oder der Beauftragte der Leitstelle für Informationstechnologie der sächsischen Justiz;
 - cc) vier Beauftragte als Vertreterinnen oder Vertreter der Ordentlichen Gerichtsbarkeit, darunter zwingend die oder der Beauftragte des Oberlandesgerichts Dresden;
 - dd) eine Beauftragte oder ein Beauftragter als Vertreterin oder Vertreter der jeweiligen Fachgerichtsbarkeit;
 - ee) zwei Beauftragte als Vertreterinnen oder Vertreter der Justizvollzugsanstalten;
 - ff) zwei Beauftragte als Vertreterinnen oder Vertreter der Staatsanwaltschaften;
 - gg) eine Beauftragte oder ein Beauftragter als Vertreterin oder Vertreter des Ausbildungszentrums Bobritzsch.
- c) Das Informationssicherheitsmanagement-Team führt den Informationssicherheitsprozess ein und gestaltet ihn, formuliert Rahmenrichtlinien zur Gewährleistung der Informationssicherheit des Geschäftsbereiches und beachtet dabei die aktuell gültigen Standards des BSI. Es tritt auf Anforderung und Einladung der oder des Beauftragten beim Staatsministerium der Justiz zusammen.

2.6 Sicherheit vor Verfügbarkeit

Im Falle einer Bedrohungs- oder sonstigen Risikolage kann die Verfügbarkeit von Informations- und Kommunikationstechnik, IT-Anwendungen sowie Daten und Netzwerken entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit der Justiz und der Verwaltung ist der Schutz vor Schäden vorrangig. Vertretbare Einschränkungen in Bedienung und Komfort sind hinzunehmen. Dies gilt in besonderem Maße für die Übergänge zu anderen Netzwerken, vor allem zum Internet.

3. Aufgaben und Verantwortlichkeiten

Die Aufgaben und Verantwortlichkeiten betreffen strategische, taktische und operative Aufgaben.

3.1 Verantwortung des Staatsministeriums der Justiz

Die Aufgaben des Staatsministeriums der Justiz umfassen insbesondere:

- a) strategische Aufgaben, wie
 - aa) den Aufbau eines Informationssicherheitsmanagementsystems als Anliegen der Justiz zu konzipieren; die Durchführung obliegt der oder dem Beauftragten für Informationssicherheit unter Mitwirkung der oder des Beauftragten für Informationssicherheit der Leitstelle für Informationstechnologie der sächsischen Justiz und des Informationssicherheitsmanagement-Teams,
 - bb) die Erarbeitung von Methodikvorgaben; die Durchführung obliegt der oder dem Beauftragten für Informationssicherheit,
 - cc) die Entwicklung und Herausgabe von Leitlinien, übergeordneten Richtlinien, übergeordneten Konzepten und anderen grundsätzlichen Maßnahmen für das Informationssicherheitsmanagementsystem; die oder der Beauftragte für Informationssicherheit, das Informationssicherheitsmanagement-Team und die oder der Beauftragte für Informationssicherheit der Leitstelle für Informationstechnologie der sächsischen Justiz wirken an der Entwicklung mit,
 - dd) die Bekanntgabe von definierten und abgestimmten Aufgaben der Leitstelle für Informationstechnologie der sächsischen Justiz und deren Abgrenzung im Geschäftsbereich des Staatsministeriums der Justiz,
 - ee) die Mitwirkung in strategischen Arbeitsgruppen,
- b) taktische Aufgaben, wie
 - aa) das Abstimmen und Spezifizieren von Aufgaben, die strategisch im Staatsministerium der Justiz verankert und durch die Leitstelle für Informationstechnologie der sächsischen Justiz umzusetzen sind,
 - bb) die Entwicklung von Richtlinien für Informationssicherheit und anderen Vorgaben zur Informationssicherheit für den Geschäftsbereich des Staatsministeriums der Justiz im Rahmen des Informationssicherheitsmanagementsystems,
 - cc) die Gremienarbeit im Geschäftsbereich des Staatsministeriums der Justiz; die Durchführung obliegt der oder dem Beauftragten für Informationssicherheit,
 - dd) die Mitwirkung in taktischen Arbeitsgruppen im Freistaat Sachsen; die Durchführung obliegt der oder dem Beauftragten für Informationssicherheit.

3.2 Verantwortung der Leitungsebene

Die Leiterinnen und Leiter der staatlichen Stellen haben insbesondere folgende Aufgaben:

- a) sie tragen die Verantwortung für die Umsetzung der vereinbarten Festlegungen im Bereich der Informationssicherheit und eine geeignete Dokumentation,
- b) sie stellen die vom Staatsministerium der Justiz bereitgestellten Mittel für die Beschaffung und den Betrieb der vereinbarten Sicherheitsmaßnahmen zur Verfügung,
- c) sie veranlassen erforderliche Schulungsmaßnahmen,
- d) sie geben die aktuellen Regelungen den Bediensteten bekannt und sorgen dafür, dass diese sich jederzeit darüber informieren können,
- e) sie sichern die Lieferkette zu unmittelbaren Lieferanten oder Dienst Anbietern ab,
- f) sie wirken bei der Bewältigung von Sicherheitsvorfällen mit.

3.3 Verantwortung der Beauftragten für Informationssicherheit

Die Aufgaben der Beauftragten für Informationssicherheit umfassen insbesondere:

- a) taktische Aufgaben, wie
 - aa) die Beratung der Leitungsebene,
 - bb) abhängig vom Inhalt der jeweiligen Arbeitsgruppe, die Berechtigung in taktischen Arbeitsgruppen im Freistaat Sachsen mitzuwirken,
- b) operative Aufgaben, wie
 - aa) die in § 7 Absatz 3 des **Sächsischen Informationssicherheitsgesetzes** normierten Aufgaben,
 - bb) die Sicherstellung der korrekten und verantwortungsbewussten Umsetzung der Standards des BSI in der jeweils aktuellen Fassung,
 - cc) die Beratung der jeweiligen staatlichen Stelle bei der organisatorischen Umsetzung strategischer Entscheidungen,
 - dd) die Steuerung und Koordinierung des Sicherheitsprozesses,
 - ee) die Mitwirkung bei der Erstellung von Sicherheitskonzepten,
 - ff) die Beschreibung von Sicherheitsmaßnahmen sowie die Initiierung und Prüfung ihrer Umsetzung,
 - gg) die Berichterstattung an die Leitungsebene und an die Beauftragten für Informationssicherheit übergeordneter Stellen über den Status der Informationssicherheit im Zuständigkeitsbereich,
 - hh) die Mitwirkung bei der Koordinierung sicherheitsrelevanter Projekte,
 - ii) die Koordinierung und Dokumentation der Behandlung sicherheitsrelevanter Vorfälle,
 - jj) die Initiierung und Koordinierung von Sensibilisierungs- und Schulungsmaßnahmen,
 - kk) die Gewährleistung des Zugangs der Bediensteten zu den erforderlichen Informationen.

3.4 Verantwortung der Leitstelle für Informationstechnologie der sächsischen Justiz

Die Aufgaben der Leitstelle für Informationstechnologie der sächsischen Justiz umfassen insbesondere:

- a) strategische Aufgaben, wie die Mitwirkung in strategischen Arbeitsgruppen,
- b) taktische Aufgaben, wie
 - aa) das Abstimmen und Spezifizieren von Aufgaben, die strategisch im Staatsministerium der Justiz verankert und von der Leitstelle für Informationstechnologie der sächsischen Justiz umzusetzen sind,
 - bb) die Entwicklung von Richtlinien für Informationssicherheit und anderen Vorgaben zur Informationssicherheit für den Geschäftsbereich des Staatsministeriums der Justiz im Rahmen des Informationssicherheitsmanagementsystems,
 - cc) die Mitwirkung in taktischen Arbeitsgruppen im Freistaat Sachsen; die Durchführung obliegt der oder dem Beauftragten für Informationssicherheit,
- c) operative Aufgaben, wie
 - aa) die Umsetzung der technischen Aufgaben, die sich aus den strategischen beziehungsweise taktischen Festlegungen im Bereich der Informationssicherheit ergeben,
 - bb) die Herausgabe von technischen Richtlinien für Informationssicherheit und damit verbundener organisatorischer Rahmenbedingungen für den Geschäftsbereich des Staatsministeriums der Justiz im Rahmen des Informationssicherheitsmanagementsystems,
 - cc) die Planung und Umsetzung von Maßnahmen zur Erfüllung der Vorgaben zur Informationssicherheit in der Leitstelle für Informationstechnologie der sächsischen Justiz,
 - dd) die Planung und Umsetzung der IT-Sicherheit in der Leitstelle für Informationstechnologie der sächsischen Justiz, insbesondere die Gewährleistung von Sicherheit bei Erwerb, Entwicklung und Wartung von informationstechnischen Komponenten und Systemen einschließlich Schwachstellenmanagement,
 - ee) regelmäßige Abstimmungen zur Umsetzung der technischen Aufgaben und zu den damit verbundenen

weiterführenden Maßnahmen mit der oder dem Beauftragten für Informationssicherheit beim Staatsministerium der Justiz; die Durchführung obliegt der oder dem Beauftragten für Informationssicherheit.

3.5 Verantwortung der Bediensteten

- a) Alle Bediensteten gewährleisten die Informationssicherheit durch ihr verantwortungsvolles Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Sie gehen korrekt und verantwortungsbewusst mit den von ihnen genutzten IT-Systemen, Daten und Informationen um.
- b) Die Bediensteten haben sich in Belangen der Informationssicherheit fortlaufend und eigenverantwortlich in geeigneter Weise zu informieren und fortzubilden. Hierfür werden ihnen die maßgeblichen Grundlagen zur Verfügung gestellt. Sie sind im erforderlichen Umfang durch die Beauftragten für Informationssicherheit zu sensibilisieren und zu qualifizieren.
- c) Jegliches Verhalten, das die Sicherheit von Daten, Informationen, IT-Systemen oder der Netze gefährdet, kann zu schwerwiegenden Folgen für Geschäftsprozesse und Schäden für den gesamten Geschäftsbereich führen und soll daher unterlassen werden. Bei Auftreten eines Sicherheitsvorfalls sind die jeweiligen Meldewege konsequent zu beachten. Die Bediensteten sind angehalten, auf mögliche Schwachstellen und Verbesserungsmöglichkeiten der Informationssicherheit hinzuweisen.

3.6 Fachverantwortliche

- a) Die oder der Fachverantwortliche ist inhaltlich für einen oder mehrere Geschäftsprozesse oder Fachverfahren zuständig. Sie oder er hat im Rahmen der Informationssicherheit zu gewährleisten:
 - aa) die Festlegung der geschäftlichen Relevanz der Informationen und deren Schutzbedarf sowie
 - bb) die Sicherstellung, dass Verantwortlichkeiten explizit definiert und Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz der Informationen umgesetzt werden.
- b) Die oder der Fachverantwortliche muss den Zugang zu Informationen sowie den Umfang und die Art der Autorisierung definieren, die im jeweiligen Verfahren erforderlich ist. Bei diesen Entscheidungen sind folgende Faktoren zu berücksichtigen:
 - aa) die Notwendigkeit, die Informationen entsprechend ihrer geschäftlichen Relevanz zu schützen,
 - bb) die Aufbewahrungsvorschriften und die mit den Informationen verbundenen rechtlichen Anforderungen und
 - cc) die Frage, inwieweit die Informationen für die jeweiligen Geschäftsanforderungen zugänglich sein müssen.

3.7 Beschäftigung externer Leistungserbringer

Die staatliche Stelle informiert, wenn sie dies nach Ziffer IV Nummer 1 für erforderlich hält, die externen Leistungserbringer über die Vorgaben zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie und verpflichtet sie diese einzuhalten. Die externen Leistungserbringer haben bei erkennbaren Mängeln und Risiken der von ihnen veranlassenen Sicherheitsmaßnahmen die staatliche Stelle nach Maßgabe des jeweiligen Auftragsverhältnisses zu informieren.

4. Umsetzung

Auf der Grundlage dieser Leitlinie und der für die gesamte Landesverwaltung geltenden Richtlinien für Informationssicherheit können im Geschäftsbereich eigene spezifische Richtlinien für Informationssicherheit, Konzepte und weitere Regelungen zur Informationssicherheit im erforderlichen Umfang gestaltet werden. Eine Unterschreitung der in dieser Leitlinie aufgestellten Maßstäbe ist nicht zulässig.

5. Sicherung und Verbesserung der Informationssicherheit

- a) Die Beauftragten für Informationssicherheit überprüfen regelmäßig den Informationssicherheitsprozess auf seine Aktualität und Wirksamkeit. Insbesondere werden die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Bediensteten bekannt, umsetzbar und in den Betriebsablauf integrierbar sind. Das Informationssicherheitsmanagement-Team gibt den Ablauf des Überprüfungsprozesses vor. Die Leiterinnen und Leiter der staatlichen Stellen unterstützen die ständige Verbesserung des Sicherheitsniveaus.
- b) Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheit zu verbessern und ständig auf dem aktuellen Stand zu halten.

6. IT-Notfallmanagement

Es ist ein IT-Notfallmanagementsystem entsprechend dem Informationssicherheitsmanagement auf Grundlage der jeweils geltenden BSI-Standards aufzubauen, um die Kontinuität des Geschäftsbereichs in Notfällen sicherzustellen und Schäden durch Notfälle oder Krisen zu minimieren. Näheres bestimmt die Leitlinie IT-Notfallmanagement Justiz des Sächsischen Staatsministeriums der Justiz und für Demokratie, Europa und Gleichstellung vom 10. Februar 2023

.....
Dienststelle

Belehrung zur Informationssicherheit am Arbeitsplatz

I. Umgang mit Daten, Dokumenten und Informationen

1. Es sind keine personenbezogenen Daten oder dienstlichen Dokumente und Informationen unbefugt an Dritte weiterzugeben (z. B. per E-Mail oder per Telefon), sie dürfen nicht unbefugt Dritten zur Kenntnis gelangen (etwa durch Einsichtnahme am Bildschirm oder Ausdrucke).
2. Es ist untersagt, dienstliche Dokumente unbefugt zu scannen, zu kopieren oder zu anderen als dienstlichen Zwecken zu verwenden.
3. Eventuelle Ausdrucke mit vertraulichen Informationen (z. B. personenbezogenen Daten) müssen sicher vernichtet werden, wenn sie nicht mehr benötigt werden. Insbesondere ist eine Entsorgung mit dem Haus- oder Papiermüll nicht zulässig. Unterlagen sind grundsätzlich in der Dienststelle nach den dort geltenden Vorgaben zu entsorgen.
4. Dienstliche Dokumente und Informationen sind nicht zu veröffentlichen und vor allem nicht auf Social-Media-Plattformen zu verbreiten.
5. Dienstliche Dokumente und Informationen dürfen per E-Mail nicht unverschlüsselt übermittelt werden. Z. B. sind Übermittlungen an Empfänger mit einer Sachsen.de-E-Mail-Adresse verschlüsselt.
6. Mobile Datenträger und analoge Dokumente mit dienstlichen Inhalten dürfen nicht frei zugänglich aufbewahrt werden.
7. Dienstliche Akten und Dokumente sind außerhalb der Dienststelle diebstahlsicher zu transportieren und aufzubewahren.
8. Dienstliche Dokumente und Informationen dürfen nicht in der Öffentlichkeit bearbeitet werden.

II. Umgang mit Hardware und Software

9. Der dienstliche und der für dienstliche Zwecke genutzte private Computer ist mit einem komplexen Passwort bestehend aus mindestens 14 Stellen zu sichern.
10. Passwörter sind stets sicher aufzubewahren.
11. Beim Verlassen des Arbeitsplatzes ist der Computer zu sperren und nach Möglichkeiten das Arbeitszimmer zu verschließen.
12. Der dienstliche oder für dienstliche Zwecke verwendete private Computer darf nicht mit freien WLAN-Hotspots (z. B. in Internet-Cafés, Bahn, Hotel, Supermärkten) verbunden werden.
13. Auf dem für dienstliche Zwecke genutzten privaten Computer ist ein aktuelles Betriebssystem mit einem aktuellen Virens Scanner zu verwenden.
14. Software darf nur von der Leitstelle für Informationstechnologie der sächsischen Justiz auf dem dienstlichen Computer installiert werden.

III. Umgang mit mobilen Datenträgern

15. Justizfremde Datenträger (u. a. USB-Sticks, CDs, DVDs, SD-Karten) dürfen nicht an dem dienstlichen Computer angeschlossen und ausgelesen werden.
16. Dienstliche Inhalte auf justizeigenen mobilen Datenträgern sind zwingend zu verschlüsseln.

IV. Umgang mit Internet und E-Mail

17. Die Nutzung von E-Mail und Internet ist nur im Rahmen der dienstlich übertragenen Aufgaben gestattet.
18. Links in E-Mails sind vor dem Öffnen zu prüfen, indem die Maus über dem Link, ohne zu klicken, positioniert wird – sogenanntes Mouse-over. Die daraufhin angezeigte Internetadresse ist zu überprüfen, ob diese mit dem Link-Text in der E-Mail übereinstimmt und auf eine vertrauenswürdige Internetadresse verweist. Beispiele für gefälschte Internetadressen sind <https://www.sprakasse.de>, <https://www.arnazon.de>, <https://paypa1.com>
19. Anhänge und Links in verdächtigen E-Mails dürfen nicht geöffnet werden. Verdächtige E-Mails sind zwingend als Anhang einer neuen E-Mail mit aussagekräftigem, daher warnendem, Betreff an spammeldung@lit.justiz.sachsen.de zu senden.

.....
Ort, Datum

.....
Unterschrift Bedienstete/Bediensteter

-
- 1 Einsehbarkeit unter BSI – Bundesamt für Sicherheit in der Informationstechnik unter der Rubrik
Themen/Grundschatz Informationssicherheit/ IT-Grundschatz/BSI-Standards

Änderungsvorschriften

Berichtigung des Sächsischen Staatsministeriums der Justiz und für Demokratie, Europa und Gleichstellung zur Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz und für Demokratie, Europa und Gleichstellung zur Gewährleistung der Informationssicherheit (VwV Informationssicherheit Justiz)

vom 14. Januar 2022 (SächsJMBI. S. 2)

Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz und für Demokratie, Europa und Gleichstellung zur Änderung der VwV Informationssicherheit Justiz

vom 11. Dezember 2023 (SächsJMBI. S. 254)

Zweite Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz zur Änderung der VwV Informationssicherheit Justiz

vom 19. Dezember 2025 (SächsJMBI. S. 7)

Zuletzt enthalten in

Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz über die geltenden Verwaltungsvorschriften des Staatsministeriums der Justiz

vom 4. Dezember 2025 (SächsABl. SDr. S. S 244)