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

Vom 17. September 2021

I. Regelungsgegenstand

Diese Verwaltungsvorschrift dient der Schaffung eines Informationssicherheitsprozesses zur Gewährleistung der Informationssicherheit. Die allgemeinen Grundsätze und Ziele der Informationssicherheit, die Verantwortlichkeiten und Rollen sowie die Informationssicherheitsorganisation sind in der Leitlinie Informationssicherheit (Anlage 1) ausgeführt.

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. Über Ernennungen der Beauftragten für Informationssicherheit ist das Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung durch die Leiterin oder den Leiter der staatlichen Stelle auf dem Dienstweg zu unterrichten.
4. 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. 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.
2. Die Bediensteten sind über ihre Pflichten gemäß Nummer 3.3 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.
3. 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.
4. Zukünftige, im Rahmen der Informationssicherheit erforderliche Belehrungen der Bediensteten haben unverzüglich zu erfolgen und sind jeweils aktenkundig zu machen.
5. 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.

6. Die Bediensteten haben binnen sechs 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. Bereits im Dienst befindliche Bedienstete haben das elektronische Lernprogramm binnen eines Jahres nach Inkrafttreten dieser Verwaltungsvorschrift zu absolvieren. Dies gilt nicht, wenn ein Nachweis über die Absolvierung des Lernprogramms bereits erfolgt ist.

IV.
Externe Leistungserbringer

1. Mit der Durchführung von Leistungen beauftragte externe Leistungserbringer sind gemäß Nummer 3.5 der Anlage 1 zur Gewährleistung der Einhaltung der Informationssicherheitsziele durch ihre Mitarbeiterinnen und Mitarbeiter sowie Beauftragten zu informieren. Hierzu sind diese Verwaltungsvorschrift und die Anlage 1 zu verwenden und in Papierform auszuhändigen.
2. Die Verpflichtung wird schriftlich 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 (SächsJMBl. 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 und für Demokratie, Europa und Gleichstellung zur Gewährleistung der Informationssicherheit (Leitlinie Informationssicherheit)

Inhaltsübersicht

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 für Demokratie, Europa und Gleichstellung 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 und für Demokratie, Europa und Gleichstellung 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 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 und für Demokratie, Europa und Gleichstellung 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) Um die Belange der Informationssicherheit bei allen strategischen Entscheidungen und Einzelmaßnahmen mit möglichen Auswirkungen auf die Informationssicherheit sicherzustellen, wird ein Informationssicherheitsmanagement-Team gemäß § 9 Satz 1 des Sächsischen Informationssicherheitsgesetzes gebildet.

b) Das Informationssicherheitsmanagement-Team setzt sich wie folgt zusammen:

aa) die oder der Beauftragte beim Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung;

bb) die oder der Beauftragte der Leitstelle für Informationstechnologie der Justiz;

cc) vier Beauftragte als Vertreterinnen und Vertreter der Ordentlichen Gerichtsbarkeit, darunter zwingend die oder der Beauftragte des Oberlandesgerichts Dresden;

dd) zwei Beauftragte als Vertreterinnen und Vertreter der Fachgerichtsbarkeit;

ee) zwei Beauftrage als Vertreterinnen und Vertreter der Justizvollzugsanstalten;

ff) eine Beauftragte oder ein Beauftragter als Vertreterin 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 und für Demokratie, Europa und Gleichstellung 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. Verantwortlichkeiten und Rollen

3.1 Verantwortung der Leitungsebene

Die Leiterin oder der Leiter hat insbesondere folgende Aufgaben:

a) sie oder er trägt die Verantwortung für die Umsetzung der vereinbarten Sicherheitsmaßnahmen und eine geeignete Dokumentation,

b) sie oder er stellt die bereitgestellten Mittel für die Beschaffung und den Betrieb der vereinbarten Sicherheitsmaßnahmen zur Verfügung,

c) sie oder er veranlasst erforderliche Schulungsmaßnahmen,

d) sie oder er gibt die aktuellen Regelungen den Bediensteten bekannt und sorgt dafür, dass diese sich jederzeit darüber informieren können.

3.2 Verantwortung der Beauftragten für Informationssicherheit

Die Aufgaben der Beauftragten für Informationssicherheit umfassen insbesondere:

a) die in § 7 Absatz 3 des Sächsischen Informationssicherheitsgesetzes normierten Aufgaben,

b) die Sicherstellung der korrekten und verantwortungsbewussten Umsetzung der Standards des BSI in der jeweils aktuellen Fassung,

c) die Steuerung und Koordinierung des Sicherheitsprozesses,

d) die Mitwirkung bei der Erstellung von Sicherheitskonzepten,

e) die Beschreibung von Sicherheitsmaßnahmen sowie die Initiierung und Prüfung ihrer Umsetzung,

f) die Beratung der Leitungsebene,

g) die Berichterstattung an die Leitungsebene und an die Beauftragten für Informationssicherheit übergeordneter Stellen über den Status der Informationssicherheit im Zuständigkeitsbereich,

h) die Mitwirkung bei der Koordinierung sicherheitsrelevanter Projekte,

i) die Koordinierung und Dokumentation der Behandlung sicherheitsrelevanter Vorfälle,

j) die Initiierung und Koordinierung von Sensibilisierungs- und Schulungsmaßnahmen,

k) die Gewährleistung des Zugangs der Bediensteten zu den erforderlichen Informationen.

3.3 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.

3.4 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

c) die Frage, inwieweit die Informationen für die jeweiligen Geschäftsanforderungen zugänglich sein müssen.

3.5 Beschäftigung externer Leistungserbringer

Personen, Behörden und Unternehmen, die nicht zum Geschäftsbereich gehören, für diesen aber in dessen Auftrag Leistungen erbringen, haben die Vorgaben zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie einzuhalten. Der Auftraggeber informiert die Auftragnehmer über diese Regeln und verpflichtet sie in geeigneter Weise zur Einhaltung. Dazu gehört, dass die Auftragnehmer bei erkennbaren Mängeln und Risiken der durch ihn veranlassten Sicherheitsmaßnahmen den Auftraggeber nach Maßgabe des jeweiligen Auftragsverhältnisses zu informieren haben. Davon nicht umfasst sind durch andere staatliche Stellen des Freistaates Sachsen beauftragte externe Leistungserbringer.

4. Umsetzung

Auf der Grundlage dieser Leitlinie und der für die gesamte Landesverwaltung geltenden Richtlinien für Informationssicherheit können im Geschäftsbereich eigene spezifische Informationssicherheitsrichtlinien, Informationssicherheitskonzepte 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. Notfallmanagement

Gleich dem Informationssicherheitsmanagementsystem ist ein Notfallmanagementsystem aufzubauen, um die Kontinuität des Geschäftsbetriebs in Notfällen sicherzustellen. Es gilt, Schäden

durch Notfälle oder Krisen zu minimieren. Hierbei bilden ebenfalls die BSI-Standards in der jeweils gültigen Form die Grundlage.

Anlage 2

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 (SächsJMBl. S. 2)

Enthalten in

Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz und für Demokratie, Europa und Gleichstellung über die geltenden Verwaltungsvorschriften des Staatsministeriums der Justiz und für Demokratie, Europa und Gleichstellung

vom 9. Dezember 2021 (SächsABl. SDr. S. S 199)