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

**Vom 11. Dezember 2023**

## I.

Die VwV Informationssicherheit Justiz vom 17. September 2021 (SächsJMBl. S. 84; 2022 S. 2) wird wie folgt geändert:

1. Ziffer I wird wie folgt geändert:
   a) Die Überschrift wird wie folgt gefasst:

      „I.
      Regelungsgegenstand, Begriffsbestimmung“.

   b) Nach Ziffer I Satz 2 wird folgender Satz eingefügt:

      „Staatliche Stellen im Sinne dieser Verwaltungsvorschrift sind das Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung und sämtliche ihm nachgeordneten Behörden sowie die Gerichte.“
2. Ziffer III wird wie folgt geändert:
   a) Vor Nummer 1 wird folgende Nummer 1 eingefügt:

      „1. Bedienstete im Sinne dieser Verwaltungsvorschrift sind alle im Geschäftsbereich des Staatsministeriums der Justiz und für Demokratie, Gleichstellung und Europa 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.“

   b) Die bisherige Nummer 1 wird Nummer 2.
   c) Die bisherige Nummer 2 wird Nummer 3 und die Angabe „3.3“ wird durch die Angabe „3.4“ ersetzt.
   d) Die bisherigen Nummern 3 bis 5 werden die Nummern 4 bis 6.
   e) Die bisherige Nummer 6 wird Nummer 7 und wie folgt geändert:
      aa) In Satz 1 werden die Wörter „Die Bediensteten haben binnen sechs Monaten“ durch die Wörter „Die Bediensteten mit einem Active-Directory-Benutzerkonto (AD-Benutzerkonto) haben binnen zwei Monaten“ ersetzt.
      bb) Satz 2 wird aufgehoben.
   f) Nach Nummer 7 wird folgende Nummer 8 eingefügt:

      „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 Dienstellenleitung aktenkundig zu machen.“
3. Ziffer IV Nummer 1 wird wie folgt geändert:
   a) Satz 1 wird wie folgt gefasst:

      „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.“

   b) Nach Satz 2 wird folgender Satz eingefügt:

      „Die erfolgte Information ist von der staatlichen Stelle zu dokumentieren.“
4. Anlage 1 wird wie folgt geändert:
   a) Nummer 2.5 Buchstabe a wird wie folgt gefasst:

      „Beim Sächsischen Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung 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 und für Demokratie, Europa und Gleichstellung festgesetzt werden.“

b) Nummer 3.2 wird wie folgt geändert:

aa) Nach Nummer 3.2 Buchstabe b wird folgender Buchstabe c eingefügt:

„c) die Beratung der jeweiligen staatlichen Stelle bei der organisatorischen Umsetzung strategischer Entscheidungen,“

bb) Die bisherigen Buchstaben c bis k werden die Buchstaben d bis l.

c) Nach Nummer 3.2 wird folgende Nummer 3.3 eingefügt:

„3.3 Verantwortung der Leitstelle für Informationstechnologie der sächsischen Justiz

a) Die Leitstelle für Informationstechnologie der sächsischen Justiz ist für die Umsetzung der technischen Aufgaben, die sich aus den strategischen Entscheidungen ergeben, verantwortlich.

b) Zwischen den Beauftragten für Informationssicherheit beim Staatsministerium der Justiz und für Demokratie, Europa und Gleichstellung sowie bei der Leitstelle für Informationstechnologie der sächsischen Justiz finden regelmäßige Abstimmungen zur Umsetzung der technischen Aufgaben und zu den damit verbundenen weiterführenden Maßnahmen statt.“

d) Die bisherigen Nummern 3.3 und 3.4 werden die Nummern 3.4 und 3.5.

e) Die bisherige Nummer 3.5 wird Nummer 3.6 und wie folgt gefasst:

„3.6 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 veranlassten Sicherheitsmaßnahmen die staatliche Stelle nach Maßgabe des jeweiligen Auftragsverhältnisses zu informieren.“

f) Die Nummer 6 wird wie folgt gefasst:

„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[1].“

5. Nach Anlage 2 wird Anlage 3 in der aus dem Anhang zu dieser Verwaltungsvorschrift ersichtlichen Fassung eingefügt.

**II.**

Diese Verwaltungsvorschrift tritt am 1. Januar 2024 in Kraft.

Dresden, den 11. Dezember 2023

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

**Anhang zu Ziffer I Nummer 5**

**Anlage 3**
**(zu Ziffer III Nummer 8 Satz 1)**

.....
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 Virenscanner 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 vertrauenswürde 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.sachsden.de zu senden.

..... .....

Ort, Datum Unterschrift Bedienstete/Bediensteter

---

1 Einsehbarkeit im Intranet Justiz unter Informationssicherheit, Grundlagen/Richtlinien