1081

Diplomatinnen und Diplomaten und andere bevorrechtigte Personen in der Bundesrepublik Deutschland

Im Rundschreiben des Auswärtigen Amtes vom 15. September 2015 (GMBl. S. 1206) sind die Regelungen für die Behandlung von Diplomatinnen und Diplomaten und anderen bevorrechtigten Personen in der Bundesrepublik Deutschland („Rundschreiben“) zusammengefasst. Das Rundschreiben ist auf der Internetseite des Auswärtigen Amtes unter der folgenden Adresse abrufbar: https://www.auswaertiges-amt.de/blob/259366/95fb05e9a6a89de129f15d27f92f00aa/rundschreiben-beh-diplomaten-data.pdf.

Teil 5 des Rundschreibens bezeichnet die Ausweistypen, die für Mitglieder ausländischer Vertretungen und internationaler Organisationen ausgestellt werden, und enthält eine Liste der Abkürzungen des jeweiligen Ausweistyps.

Beruft sich eine Person auf konsularische Vorrechte, Immunität und Befreiungen (siehe Teil 1 C. des Rundschreibens), kann Auskunft bei dem Protokoll der Hessischen Staatskanzlei in Wiesbaden durch Fernruf (0611/32 38 83), per Fax (0611/32 38 79) oder per E-Mail (protokoll.konsulate@stk.hessen.de) eingeholt werden.

Wegen Beschaffung der ein- bis zweimal jährlich erscheinenden Liste diplomatischer Missionen und konsularischer Vertretungen wird auf Teil 1 C. 3. des Rundschreibens verwiesen. Eine aktuelle Liste diplomatischer Missionen und konsularischer Vertretungen ist auf der Homepage des Auswärtigen Amts zu finden.

Die Listen (hier: Anciennitätenlisten) der berufs- und honorarkonsularischen Vertretungen sind nach dem jeweiligen neuesten Stand im Internet unter folgender Adresse abrufbar: https://www.hessen.de/fuer-buerger/europa-internationales/konsulate-hessen. Eine Verlinkung der aktuellen Listen der berufs- und honorarkonsularischen Vertretungen in Hessen ist auch im Informationsportal Hessen unter dem Navigationspunkt „für Bürger“ auf der Seite „Europa und Internationales“ zu finden.

Diese Verwaltungsvorschrift tritt am 1. Januar 2022 in Kraft.

Wiesbaden, den 2. November 2021

Hessisches Ministerium des Innern und für Sport
LPP 2-21a99-01-21/008
– Gült.-Verz. 18 –

StAnz. 47/2021 S. 1517

1082

Informationssicherheitsleitlinie für die hessische Landesverwaltung (2021)

1. Vorbemerkung

1.1 Die Prozesse zur Aufgabenerfüllung in der hessischen Landesverwaltung werden durch Informationstechnologie (IT) unterstützt. Eine wichtige Rolle spielen dabei gemeinsam genutzte Infrastrukturen und Systeme. Damit wird ein Raum gemeinsamer Sicherheit und gemeinsamer Sicherheitsbedrohungen geschaffen.

1.2 Vor diesem Hintergrund ist ressort- und dienststellenübergreifend zur Gewährleistung der Arbeitsfähigkeit der Landesverwaltung und entsprechend den staatlichen Aufgaben eine angemessene Informationssicherheit unabdingbar.

Dazu gehören zumindest

(1) organisatorische Rahmenbedingungen der Informationssicherheit aufrecht zu erhalten und weiter zu entwickeln,

(2) das Informationssicherheitsmanagement kontinuierlich zu verbessern,

(3) abgestimmte Sicherheitsstandards fortzuschreiben,

(4) Komponenten zur Gewährleistung der Informationssicherheit zu standardisieren und

(5) alle Sicherheitsvorkehrungen und -maßnahmen hinreichend zu dokumentieren.

1.3 Für die Staatskanzlei, die Landesministerien und die ihnen nachgeordneten Dienststellen, Einrichtungen und Landesbetriebe wird im Folgenden der Begriff „Landesverwaltung“ verwendet.

1.4 Soweit in dieser Leitlinie von Ressorts gesprochen wird, sind hierunter auch die Staatskanzlei und der jeweilige nachgeordnete Bereich zu verstehen.

1.5 Die Regelungen dieser Informationssicherheitsleitlinie werden vom Chief Information Security Officer (CISO)[1] in Abstimmung mit den Ressorts fortgeschrieben.[2]

1.6 Die Regelungen der Informationssicherheitsleitlinie orientieren sich am BSI-Grundschutz und dienen der Umsetzung der Vorgaben der Informationssicherheitsleitlinie des Bundes und der Länder.[3]

1.7 In dieser Leitlinie werden für die hessische Landesverwaltung Rahmenvorgaben für Ziele und Grundsätze der Informationssicherheit und die Rollen in der Informationssicherheit definiert. Darüber hinaus werden die Art der Maßnahmen sowie die Anforderungen an die Organisationsstrukturen (Aufbau- und Ablauforganisation) beschrieben.

2. Geltungsbereich

2.1 Die Informationssicherheitsleitlinie ist für die hessische Landesverwaltung verbindlich.

2.2 Die Ressorts können für ihren Zuständigkeitsbereich ergänzende und konkretisierende Regelungen treffen.

2.3 Dem Hessischen Landtag, dem Hessischen Rechnungshof sowie dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit wird der Erlass einer gleichartigen oder die Anwendung dieser Informationssicherheitsleitlinie empfohlen, um ein gleichartiges Sicherheitsniveau für die gemeinsame Infrastruktur und Verfahren der Landesverwaltung gewährleisten zu können.

3. Ziele der Informationssicherheit

3.1 Informationssicherheit dient der Erhaltung der Arbeits- und Handlungsfähigkeit der Landesverwaltung sowie der Vermeidung von Schäden und der Einhaltung von Rechtsvorschriften.

3.2 Für IT sind die Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität im jeweils erforderlichen Maße zu schützen.

3.3 Die Sicherheit der IT ist neben deren Leistungsfähigkeit und Funktionalität zu gewährleisten. Bleiben im Einzelfall nicht übernahmefähige Risiken (gemäß Ziffer 4.1 und 4.3), ist auf den Einsatz der IT zu verzichten.

3.4 Bei Anbindung an das gemeinsame Netz von Bund und Ländern und das Betreiben von Ebenen-übergreifenden Verfahren im Sinne der Ziffern 3.2 und 3.3 der Informationssicherheitsleitlinie des Bundes und der Länder sind Rahmenbedingungen mit den Vertragspartnern außerhalb des Landes Hessen abzustimmen und weitestgehend zu vereinheitlichen.

4. Grundsätze der Informationssicherheit

4.1 Unter Berücksichtigung der zu schützenden Informationen, der Risiken sowie des Aufwands an Personal und Finanzmitteln für Informationssicherheit, ist für eingesetzte und geplante IT in der hessischen Landesverwaltung ein angemessenes Informationssicherheitsniveau zu erreichen und aufrecht zu erhalten. Dabei sind die Kosten und Wirksamkeitsaspekte zu beachten. Notwendige Maßnahmen der Informationssicherheit sind mit Hilfe von Informationssicherheitskonzepten festzulegen und von den jeweils Zuständigen in die Haushaltsplanung einzubringen und umzusetzen.

4.2 Informationssicherheitskonzepte haben dem **BSI-Standard** zu entsprechen. Es wird eine Umsetzung nach modernisiertem Grundschutz empfohlen. Bei Anwendung des modernisierten Grundschutzes ist die Standardabsicherung umzusetzen. Für den Bereich der Hochschulen des Landes können Sicherheitskonzepte auch nach den Normen DIN ISO/IEC 27001ff erstellt werden, sofern diese nicht gemeinsame Infrastrukturen oder Systeme des Landes nutzen.

4.3 Werden Informationen mit einem hohen oder sehr hohen Schutzbedarf verarbeitet, muss eine Risikoanalyse durchgeführt werden. Die sich daraus ergebenden zusätzlichen Sicherheitsmaßnahmen sind zu berücksichtigen.

---

1 Siehe Ziffer 7.1

2 Beschluss über die Zuständigkeit der einzelnen Ministerinnen und Minister nach Art. 104 Abs. 2 der Verfassung des Landes Hessen vom 26. März 2019 (GVBl. S. 56 f.): Hessisches Ministerium des Innern und für Sport

3 https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/28_Sitzung/TOP12_Anlage_Leitlinie.pdf

4.4 Für Ebenen-übergreifende Verfahren im Sinne der Ziffer 3.3 der Informationssicherheitsleitlinie des Bundes und der Länder sind Informationssicherheitskonzepte nach BSI 200-2 zu erstellen und gemäß Ziffer 3.2 der Informationssicherheitsleitlinie des Bundes beim direkten Anschluss an das gemeinsame Netz von Bund und Ländern im Sinne des IT-NetzG die BSI-Standards 200-1, 200-2, 200-3 und 100-4 umzusetzen.

5. Begriffsbestimmungen

5.1 Informationstechnologie (IT) umfasst die Gesamtheit der genutzten informationstechnischen Systeme und Kommunikationstechnik und die auf dieser Basis realisierten fachlichen IT-Anwendungen zur Datenverarbeitung.

5.2 Unter Verfahren wird die Summe aus einer oder mehrerer IT-Anwendungen und der zum Einsatz dieser Anwendung bzw. Anwendungen begleitenden Geschäftsprozesse verstanden. Diese können betrieblich und fachlich sein. Ziel ist es, fachliche Aufgaben zu realisieren.

5.3 Querschnittsverfahren sind alle Verfahren, die ressortübergreifende Aufgaben unterstützen und von IT-Dienstleistern des Landes angeboten werden, insbesondere die Produkte der Hessischen Zentrale für Datenverarbeitung (HZD) und Standardleistungen zum Betrieb von Verfahren im Rechenzentrum der HZD, die über das Portfolio der HZD allen Ressorts zur Verfügung stehen.

5.4 Die Informationssicherheit bezieht sich auf den Schutz der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit von Daten unter Berücksichtigung der datenschutzrechtlichen und sonstigen gesetzlichen Vorgaben.

5.5 Informationssicherheitskonzepte identifizieren und dokumentieren die organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen, die zur Erreichung der Sicherheitsziele im Geltungsbereich notwendig sind. Dabei sind alle zugrundeliegenden Gefährdungen und Risiken zu betrachten und jeweils Maßnahmen zur Risikominderung bzw. Risikovermeidung zu beschreiben.

5.6 Als sicherheitsrelevantes Ereignis wird ein Ereignis bezeichnet, das die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit beeinträchtigen kann.

5.7 Ein Sicherheitsvorfall ist jedes Ereignis, das die Informationssicherheit in mindestens einem ihrer Grundwerte Vertraulichkeit, Verfügbarkeit oder Integrität nicht nur unerheblich beeinträchtigt.

5.8 Ein Verdachtsfall liegt dann vor, wenn in der fachlichen Bewertung eines sicherheitsrelevanten Ereignisses festgestellt wird, dass die Möglichkeit eines Sicherheitsvorfalls besteht oder dieses Ereignis sich zu einem Sicherheitsvorfall entwickeln kann.

6. Maßnahmen und Prozesse

6.1 Für alle IT-Systeme und Verfahren sind Informationssicherheitskonzepte einschließlich einer Schutzbedarfsfeststellung zu erstellen und aktuell zu halten. Gemäß den Grundsätzen des IT-Grundschutzes sind sowohl die allgemeine IT, IT-Infrastrukturen und übergreifende Aspekte, als auch alle Verfahren von Informationssicherheitskonzepten zu erfassen. Diese Vorgehensweise ist grundsätzlich vor der Inbetriebnahme der IT-Systeme und Verfahren anzuwenden.

6.2 Es werden Jahresberichte zum Stand der Informationssicherheit in den Dienststellen und in den Ressorts erstellt.

Der **Jahresbericht** zur Informationssicherheit dient der Information der Dienststellenleitungen und des zentralen Informationssicherheitsmanagements/CISO zum Stand der Informationssicherheit im jeweiligen Zuständigkeitsbereich.

Der Jahresbericht beinhaltet mindestens folgende Punkte:

(1) Wesentliche organisatorische und personelle Änderungen im Bereich der Informationssicherheit

(2) Ergebnisse von Audits und der Kontrolle zur Einhaltung der Informationssicherheit gemäß 6.8

(3) Berichte über Sicherheitsvorfälle und Verdachtsfälle

(4) Berichte über bisherige Erfolge und Probleme im Informationssicherheitsprozess

(5) Sachstand zur Erstellung, Vollständigkeit, Aktualität von Informationssicherheitskonzepten gemäß 6.1

(6) Sachstand der Umsetzung von Informationssicherheitsmaßnahmen gemäß Ziffer 4.

6.3 Die Beschäftigten einer Dienststelle sind in der Informationssicherheit und zur Umsetzung der Informationssicherheit in der hessischen Landesverwaltung in Bezug auf geltende Regelungen, Maßnahmen und Meldewege bei sicherheitsrelevanten Ereignissen zu sensibilisieren und zu schulen. Hierfür werden in den Ressorts und vom HMdIS Sensibilisierungsmaßnahmen und Schulungen angeboten, für deren Teilnahme die Beschäftigten freizustellen sind.

6.4 Alle Verdachtsfälle und Sicherheitsvorfälle sind zu erfassen.

6.5 Sicherheitsrelevante Ereignisse, Verdachtsfälle und Sicherheitsvorfälle werden den in den Dienststellen definierten zuständigen Stellen unverzüglich gemeldet.

Alle Verdachts- und Sicherheitsvorfälle sind summarisch monatlich an das Hessen CyberCompetenceCenter (Hessen3C)[4] zu berichten.

Verdachtsfälle und Sicherheitsvorfälle, die andere Stellen beeinträchtigen können, die öffentlichkeitswirksam sind oder die politische Bedeutung haben, sind dem Hessen3C unverzüglich zu melden (Sofortmeldung).

Das Verfahren der Vorfallsmeldung (Vorfallserkennung, Verhaltensregeln, Handlungsschritte und Meldewege) wird der CISO in Abstimmung mit den Ressorts in einem gesonderten Umsetzungskonzept festlegen.

6.6 Der Zugang zu IT ist auf den erforderlichen Personenkreis zu beschränken. Zugriffsberechtigungen werden nur zur Erfüllung von dienstlichen Aufgaben erteilt.

6.7 Durch regelmäßige IT-Krisenmanagement-Übungen wird das ressortübergreifende Zusammenspiel von Organisationen, Prozessen und Technologien der Informationssicherheit überprüft und weiterentwickelt.

6.8 In jedem Ressort werden Prozesse eingerichtet, mit denen die Eignung und Umsetzung der Sicherheitsmaßnahmen regelmäßig kontrolliert werden.

Die Einhaltung der Informationssicherheit ist auf der Grundlage der jeweiligen Informationssicherheitskonzepte regelmäßig und anlassbezogen zu überprüfen. Über die Ergebnisse der Prüfung ist im Rahmen des Jahresberichts zum Stand der Informationssicherheit zu berichten.

Die Überprüfung kann durch unabhängige Dritte erfolgen. In diesem Fall ist zu gewährleisten, dass diese Dritten zur Verschwiegenheit verpflichtet sind und mit der Überprüfung keine unzulässige Kenntnisnahme von Daten und Informationen verbunden ist.

6.9 Für die vom IT-Dienstleister angebotenen Querschnittsverfahren werden die notwendigen Maßnahmen für mindestens normalen Schutzbedarf von ihm in eigener Verantwortung umgesetzt. Er bestätigt die Umsetzung der Maßnahmen den betroffenen Dienststellen auf Nachfrage und gewährt neben den gesetzlich berechtigten Stellen den Informationssicherheitsbeauftragten der Ressorts Einsicht in die Informationssicherheitskonzepte.

Stellen Anwender der Querschnittsverfahren fest, dass ggf. ein höherer Schutzbedarf erforderlich ist, sind diese Bedarfe über den AK Informationssicherheit in den IT-Standardisierungsprozess einzubringen. Die IT-Dienstleister bewerten im Rahmen dieses Prozesses die organisatorischen und finanziellen Auswirkungen. Über die Umsetzung entscheiden die entsprechenden Gremien. Das Verfahren der Integration von Querschnittsverfahren in Informationssicherheitskonzepte der Landesverwaltung (Berichterstattung des Dienstleisters, Festlegung der Schutzbedarfe, Integration in Sicherheitskonzepte) wird der CISO in Abstimmung mit den Ressorts in einem gesonderten Umsetzungskonzept festlegen.

7. Rollen, Aufgaben und Zuständigkeiten

Rollen

7.1 **Zentrale Informationssicherheitsbeauftragte oder Zentraler Informationssicherheitsbeauftragter der Landesverwaltung** (Chief Information Security Officer, **CISO**). Gemäß der Informationssicherheitsleitlinie des Bundes und der Länder sind für den Bund und alle Länder zentrale Informationssicherheitsbeauftragte zu benennen.

7.2 **IT-Dienstleister** sind alle Stellen der hessischen Landesverwaltung, die IT zur Nutzung durch andere Dienststellen bereitstellen.

7.3 **Verfahrensverantwortliche** sind Personen oder Organisationseinheiten, die für die Konzeptionierung einer Strategie sowie für die Fortentwicklung eines Verfahrens zuständig und die für die Kontrolle von Gebrauch und Sicherheit von Daten und der sie verarbeitenden IT-Komponenten verantwortlich ist. Die verfahrensverantwortlichen Stellen werden im IT-Produktportfolio des Landes geführt.[5]

---

4 Siehe Ziffer 7.10 und 7.15

5 Die fachliche Zuständigkeit ergibt sich aus dem Beschluss der Landesregierung zur Zuständigkeit der Ministerinnen und Minister.

7.4 Die **auftraggebende Stelle** eines IT-Projekts oder Verfahrens schafft die finanziellen und organisatorischen Voraussetzungen, um mit einer Auftragnehmenden Stelle (IT-Dienstleister) einen Vertrag abschließen zu können. Somit begleitet die auftraggebende Stelle den kompletten Lebenszyklus von der Projektidee bis hin zur Einstellung eines Verfahrens. Hierbei können zu bestimmten Phasen Aufgaben delegiert werden – zum Beispiel an den Projektleitung oder die verfahrensverantwortliche Stelle – jedoch bleibt die Gesamtverantwortung immer bei der auftraggebenden Stelle.

7.5 Für die **Ressorts** werden zentrale **Ressort-Informationssicherheitsbeauftragte** und deren Vertretungen benannt.

7.6 Für **jede Dienststelle** müssen zuständige **Informationssicherheitsbeauftragte** und deren Vertretung benannt werden. Dies können die Ressort-Informationssicherheitsbeauftragten oder andere von der Leitung des Ressorts bzw. Dienststellenleitung bestimmte Personen sein.

7.7 Die **Informationssicherheitsbeauftragten** werden in ihrer Arbeit durch alle Bereiche ihrer Dienststelle unterstützt. Die Informationssicherheitsbeauftragten und die Vertretungen bilden sich regelmäßig weiter. Sie werden darin von der Dienststelle unterstützt.

Bei der organisatorischen Zuweisung der Aufgaben der Informationssicherheitsbeauftragten sollen Interessenkonflikte vermieden werden.

7.8 Bei den Informationssicherheitsbeauftragten wird ein **Informationssicherheitsmanagement-Team** gebildet, das mindestens aus den Informationssicherheitsbeauftragten und deren Vertretern besteht. Je nach Größe der Organisationseinheit wird empfohlen, weitere Personen hinzu zu ziehen.

7.9 Zur Koordination der landesweiten Sicherheitsprozesse und zur Unterstützung und Beratung der Informationssicherheitsbeauftragten in den Ressorts sowie zur Abstimmung und Koordination ressortübergreifender, gemeinsamer Maßnahmen zur Informationssicherheit richtet das HMdIS einen ständigen **Arbeitskreis für die Informationssicherheitsbeauftragten der Ressorts** ein (**AK Informationssicherheit**). Einzelheiten und die organisatorische Einbindung regelt eine Geschäftsordnung, die mit den Ressorts abgestimmt ist.

7.10 Im für die IT- und Cybersicherheit zuständigen Ministerium[6] der Landesverwaltung wird das **Hessen CyberCompetenceCenter (Hessen3C)** betrieben.

7.11 Das **IT-Krisenmanagement** ist zuständig für die Identifikation und Analyse von IT-Krisensituationen, die Entwicklung von Strategien zur Bewältigung der Krise sowie die Einleitung und Verfolgung von Gegenmaßnahmen. Die Rollen und Aufgaben wird der CISO in Abstimmung mit den Ressorts in einem IT-Krisenmanagementkonzept regeln.

Aufgaben und Zuständigkeiten

7.12 Chief Information Security Officer (CISO)

Die/Der für die Landesverwaltung eingesetzte zentrale Informationssicherheitsbeauftragte (CISO) hat folgende Aufgaben, Verantwortungen und Kompetenzen:

(1) Fortschreibung der Informationssicherheitsleitlinie des Landes in Abstimmung mit der Staatskanzlei und den Ressorts

(2) Kontinuierliche Verbesserung der Informationssicherheit in der Landesverwaltung

(3) Beratung des CIO, der Staatskanzlei und der Ressorts

(4) Entwicklung von Empfehlungen für die Ressorts in Fragen der Informationssicherheit

(5) Koordinierung von landesweiten Informationssicherheitsmaßnahmen

(6) Eskalationsinstanz für alle ressortübergreifenden Informationssicherheitsthemen, insbesondere im IT-Krisenmanagement

(7) Außenvertretung der hessischen Landesverwaltung in Belangen der Informationssicherheit, insbesondere in Ergänzung etablierter Strukturen

(8) Leitung des IT-Krisenmanagements der Landesverwaltung

(9) Der CISO hat ein unmittelbares Vortragsrecht bei der für IT- und Cybersicherheit in der Landesverwaltung zuständigen Ministerin oder dem hierfür zuständigen Minister und bei der Beauftragten oder dem Beauftragten der Landesregierung für E-Government (CIO). Bei schwerwiegenden Anlässen hat der CISO ein unmittelbares Vortragsrecht bei der Chefin oder dem Chef der Staatskanzlei oder bei den Staatssekretärinnen oder Staatssekretären der Ressorts und kann die Ressortleitungen um Einsichtnahme in Informationssicherheitskonzepte bitten.

7.13 Hessen CyberCompetenceCenter (Hessen3C)

Das Hessen3C hat folgende Aufgaben, Verantwortungen und Kompetenzen:

(1) Das Hessen3C informiert die Landesverwaltung über akute Bedrohungslagen und Sicherheitsdefizite in Soft- und Hardware-Produkten. Es erstellt ein werktägliches Lagebild zur Informationssicherheit, bewertet Sicherheitsbedrohungen und empfiehlt Maßnahmen zur Risikominderung und Schadensvermeidung.

(2) Das Hessen3C nimmt die Sofortmeldungen aus der Landesverwaltung über übergreifende Sicherheitsvorfälle entgegen und koordiniert deren Beseitigung durch die beteiligten Stellen.

(3) Alle Dienststellen und insbesondere die IT-Dienstleister unterstützen das Hessen3C im Rahmen ihrer technischen, rechtlichen und personellen Möglichkeiten bei seinen Aufgaben, insbesondere bei der Bereitstellung der erforderlichen Daten zur Abwehr von Gefahren für die Informationssicherheit in der Landesverwaltung.

(4) Beratung und Unterstützung der hessischen Landesverwaltung bei der Bewertung und Behebung von sicherheitsrelevanten Ereignissen, Verdachtsfällen und Sicherheitsvorfällen. Bei herausgehobenen Fällen unterstützt das Hessen3C mit einem Mobile Incident Response Team (MIRT) auch vor Ort.

(5) Durchführung von IT-Krisenmanagement-Übungen (gemäß 6.7)

7.14 IT-Dienstleister

Die IT-Dienstleister haben folgende Aufgaben:

(1) Umsetzung der notwendigen Maßnahmen für die von ihnen angebotenen Querschnittsverfahren für ihren Einflussbereich in eigener Verantwortung (gemäß 6.9)

(2) Auf Nachfrage Bestätigung der Umsetzung der Maßnahmen gegenüber den betroffenen Dienststellen (gemäß 6.9)

(3) Gewährt neben den gesetzlich berechtigten Stellen den Ressort-Informationssicherheitsbeauftragten und den Verfahrensverantwortlichkeiten Einsicht in die Informationssicherheitskonzepte (gemäß 6.9)

(4) Bewertung der organisatorischen und finanziellen Auswirkungen im Rahmen des Standardisierungsprozesses bei höherem Schutzbedarf für Anwender von Querschnittsverfahren (gemäß 6.9)

(5) Unterstützung des Hessen3C (gemäß 7.13 (3))

7.15 Ressortleitung

(1) Die Leitung des Ressorts trägt die Verantwortung für eine angemessene Informationssicherheit im Geschäftsbereich. Sie stellt die erforderlichen personellen und finanziellen Ressourcen zur Verfügung.

(2) Die Leitung des Ressorts berichtet jährlich dem HMdIS zum Stand der Informationssicherheit.

(3) Die Leitung des Ressorts richtet Prozesse zur Prüfung der Informationssicherheit gemäß 6.8 ein und legt darin Art und Umfang der Kontrolle fest.

7.16 Dienststellenleitung

(1) Die Dienststellenleitung trägt die Verantwortung für eine angemessene Informationssicherheit in dem ihr zugewiesenen Umfang.

7.17 Beschäftigte

(1) Die Beschäftigten gewährleisten die Informationssicherheit durch verantwortliches Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und Regelungen ein.

(2) Die Beschäftigten melden sicherheitsrelevante Ereignisse unverzüglich den in den Dienststellen definierten zuständigen Stellen.

7.18 Verfahrensverantwortliche

(1) Die Verfahrensverantwortlichen sind für die Erstellung, Fortschreibung und Umsetzung der Informationssicher-

6 Beschluss über die Zuständigkeit der einzelnen Ministerinnen und Minister nach Art. 104 Abs. 2 der Verfassung des Landes Hessen vom 26. März 2019 (GVBl. S. 56 f.): Hessisches Ministerium des Innern und für Sport

heitskonzepte für Verfahren in ihrem Verantwortungsbereich verantwortlich.

(2) Die Verfahrensverantwortlichen stellen sicher, dass die Erteilung und der Entzug von Zugriffsrechten geprüft und dokumentiert wird. Die Notwendigkeit zur Erteilung von Zugriffsrechten ist regelmäßig zu überprüfen.

(3) Die Verfahrensverantwortlichen informieren bei Kenntnis von sicherheitsrelevanten Ereignissen, Verdachtsfällen und Sicherheitsvorfällen die zuständigen Stellen unverzüglich.

7.19 Ressort-Informationssicherheitsbeauftragte

(1) Die Ressort-Informationssicherheitsbeauftragten unterstützen die Leitung eines Ressorts bei der Sicherstellung der Belange der Informationssicherheit innerhalb des jeweiligen Ressorts und koordinieren entsprechende Maßnahmen.

(2) Die Ressort-Informationssicherheitsbeauftragten haben ein unmittelbares Vortragsrecht bei der Leitung des Ressorts.

(3) Die Ressort-Informationssicherheitsbeauftragten berichten der Leitung der Ressorts mindestens einmal jährlich zum Stand der Umsetzung der Informationssicherheitsmaßnahmen im Ressort (Jahresbericht)

(4) Die Ressort-Informationssicherheitsbeauftragten stellen sicher, dass alle Verdachts- und Sicherheitsvorfälle im Ressort gemäß 6.4 erfasst werden.

(5) Die Ressort-Informationssicherheitsbeauftragten sind für die Einhaltung der Meldepflichten zu Verdachts- und Sicherheitsvorfällen im Ressort verantwortlich.

(6) Die Ressort-Informationssicherheitsbeauftragten stellen sicher, dass alle Sofortmeldungen gemäß 6.5 unverzüglich an das Hessen3C gemeldet werden.

7.20 Informationssicherheitsbeauftragte

(1) Die für die Dienststellen zuständigen Informationssicherheitsbeauftragten koordinieren die Maßnahmen zur Verbesserung der Informationssicherheit in ihrem Zuständigkeitsbereich. Sie und ihre Vertretung werden im Geschäftsverteilungsplan ausgewiesen.

(2) Die Informationssicherheitsbeauftragten können sich unmittelbar an die Leitung der Dienststelle und die Ressort-Informationssicherheitsbeauftragten wenden.

(3) Die Informationssicherheitsbeauftragten berichten der Dienststellenleitung und den Ressort-Informationssicherheitsbeauftragten mindestens einmal jährlich über den Stand der Informationssicherheit.

(4) Die Leitung des Informationssicherheitsmanagement-Teams obliegt den Informationssicherheitsbeauftragten.

(5) Die Informationssicherheitsbeauftragten sind für die Einhaltung der Dokumentation nach 6.4 und der Meldepflicht nach 6.5 verantwortlich.

(6) Die Informationssicherheitsbeauftragten arbeiten mit den behördlichen Datenschutzbeauftragten und den IT-Verantwortlichen in ihrem Verantwortungsbereich zusammen.

7.21 Personalverantwortliche

(1) Die verantwortlichen personalbearbeitenden Bereiche stellen die Daten über Zu- und Abgang von Beschäftigten dem jeweiligen IT-Betrieb zur Verfügung, um den Zugang zur IT gemäß 6.6 prüfen zu können.

7.22 Auftraggebende Stelle und Auftragnehmende Stelle

(1) Die auftraggebende Stelle und die auftragnehmende Stelle eines Verfahrens, einer Dienstleistung oder einer IT-Infrastruktur haben die zur Einhaltung der Informationssicherheitsziele erforderlichen Sicherheitsanforderungen zu vereinbaren. Die auftraggebende Stelle hat die auftragnehmende Stelle zu verpflichten, bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen oder bei Sicherheitslücken in eingesetzter Software und IT-Infrastruktur, die auftraggebende Stelle zu informieren.

(2) Die auftraggebende Stelle benennt im Rahmen ihrer Gesamtverantwortung die verfahrensverantwortliche Stelle.

8. Umsetzung

Diese Informationssicherheitsleitlinie ist allen Beschäftigten in geeigneter Weise bekannt zu geben.

9. Inkrafttreten

Diese Informationssicherheitsleitlinie tritt am Tage nach der Verkündung in Kraft.

Wiesbaden, den 1. November 2021

Hessisches Ministerium des Innern und für Sport
VII 3-03y-28-21/003
– Gült.-Verz. 300 –

StAnz. 47/2021 S. 1517

1083

Polizeiliche Bekanntmachung des Polizeipräsidiums Frankfurt am Main nach Nr. 43.4.2.4 VwV-HSOG;

Aufforderung zur Anmeldung von Rechten an polizeilich sichergestellten Sachen

Das Polizeipräsidium Frankfurt am Main hat am 27. Oktober 2020 in Frankfurt am Main mutmaßliches Diebesgut zur Eigentumssicherung (§ 40 Abs. 1 Nr. 2 HSOG) sichergestellt und in polizeiliche Verwahrung genommen.

Es handelt sich dabei um ein Mountainbike des Herstellers„Bulls“; Modell: Sharptail Street; Farbe: schwarz/grün; Rahmennummer: SA6048111.

Die Eigentümer oder sonstigen Berechtigten werden hiermit aufgefordert, bis zum 31. Januar 2022 ihre Rechte beim **Polizeipräsidium Frankfurt am Main, Abteilung Verwaltung – V 12 –, Adickesallee 70, 60322 Frankfurt am Main, Tel.: 069/755-0,** anzumelden und in geeigneter Form glaubhaft zu machen.

Frankfurt am Main, den 9. November 2021

Polizeipräsidium Frankfurt am Main
V 12 – 21a 02 – 537/21

StAnz. 47/2021 S. 1520

1084

Polizeiliche Bekanntmachung des Polizeipräsidiums Frankfurt am Main nach Nr. 43.4.2.4 VwV-HSOG;

Aufforderung zur Anmeldung von Rechten an polizeilich sichergestellten Sachen

Das Polizeipräsidium Frankfurt am Main hat am 6. Februar 2020 in Frankfurt am Main mutmaßliches Diebesgut zur Eigentumssicherung (§ 40 Abs. 1 Nr. 2 HSOG) sichergestellt und in polizeiliche Verwahrung genommen.

Es handelt sich dabei um ein Samsung Galaxy J2 Smartphone; Farbe: blau; IMEI1: 357474103050718; IMEI2: 357475103050715 mit Zubehör (Ladegerät und Kabel).

Die Eigentümer oder sonstigen Berechtigten werden hiermit aufgefordert, bis zum 15. Januar 2022 ihre Rechte beim **Polizeipräsidium Frankfurt am Main, Abteilung Verwaltung – V 12 –, Adickesallee 70, 60322 Frankfurt am Main, Tel.: 069/755-0,** anzumelden und in geeigneter Form glaubhaft zu machen.

Frankfurt am Main, den 9. November 2021

Polizeipräsidium Frankfurt am Main
V 12 – 21a 02 – 401/21

StAnz. 47/2021 S. 1520