Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern zur Gewährleistung der Informationssicherheit im Geschäftsbereich (VwV Informationssicherheit SMI)

Vom 22. August 2014

I. Regelungsgegenstand

Die Verwaltungsvorschrift regelt die Strategien und Organisationsstrukturen, die für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind. Die allgemeinen Grundsätze und Ziele der Informationssicherheit, die Verantwortlichkeiten und Rollen im Informationssicherheitsprozess und die Informationssicherheitsorganisation sind in der Anlage ausgeführt.

II. Geltungsbereich

Die Verwaltungsvorschrift gilt für alle Behörden des Geschäftsbereichs des Staatsministeriums des Innern mit Ausnahme der Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst. Die Vorgaben sind entsprechend der jeweiligen Aufgabenverantwortung umzusetzen und auszugestalten.

III. Inkrafttreten

Diese Verwaltungsvorschrift tritt am Tage nach ihrer Veröffentlichung in Kraft.

Dresden, den 22. August 2014

Der Staatsminister des Innern
Markus Ulbig

Anlage
(zu Ziffer I Satz 2)

Leitlinie
des Sächsischen Staatsministeriums des Innern
zur Gewährleistung der Informationssicherheit im Geschäftsbereich
(Leitlinie Informationssicherheit SMI)

Inhaltsverzeichnis

1 Einleitung

Das Staatsministerium des Innern (SMI) und dessen nachgeordneter Bereich bedienen sich zur effizienten Wahrnehmung der ihnen obliegenden Aufgaben in hohem und ständig wachsendem Maße der Informationstechnik (IT). Somit kommt der IT eine Schlüsselrolle bei der Erfüllung aller wesentlichen strategischen und operativen Aufgaben zu.

Durch die Nutzung der zugrunde liegenden IT-Infrastrukturen, -Produkte und -Verfahren ergeben sich jedoch, neben den Vorteilen für die Gestaltung der Geschäftsprozesse, auch neue Gefährdungspotentiale, denen es zu begegnen gilt, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

Um alle Geschäftsprozesse und Informationen vor Gefährdungen zu schützen und somit die zur Aufgabenerfüllung notwendige Arbeitsfähigkeit und -güte zu gewährleisten, ist ein ganzheitlicher Informationssicherheitsprozess zu initiieren und zu etablieren. Hierfür sind die angestrebten Informationssicherheitsziele zu identifizieren sowie Umsetzungsstrategien zu entwickeln und effiziente Organisationsstrukturen zu schaffen.

Die vorliegende Leitlinie bildet hierfür, konkretisierend und ergänzend zur Verwaltungsvorschrift der Sächsischen Staatsregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung (VwV Informationssicherheit) vom 7. September 2011 (SächsABl. S. 1294), zuletzt enthalten in der Verwaltungsvorschrift vom 13. Dezember 2013 (SächsABl. SDr. S. S 802), die Basis und ist durch Sicherheitsrichtlinien, Konzepte sowie gegebenenfalls weitere Regelungen zu unterlegen. Insbesondere soll sie eine grundlegende Sensibilität der Bediensteten für die Belange und die Notwendigkeit der Informationssicherheit fördern, da eine wirksame Umsetzung nur unter Mitwirkung aller Beteiligten gelingen kann.

Der Staatsminister des Innern bekennt sich mit dieser Leitlinie zu seiner Gesamtverantwortung für den Informationssicherheitsprozess im Ressort und unterstützt den Beauftragten für Informationssicherheit (BfIS) des SMI, die weiteren Beteiligten sowie die entsprechenden Maßnahmen aktiv.

2 Allgemeine Vorschriften und Definitionen

2.1 Geltungsbereich

Die vorliegende Leitlinie gilt dem Schutz aller geschäftsrelevanten Informationen und deren Verarbeitung. Dies umfasst einerseits die klassische elektronische Datenverarbeitung und die Telekommunikation, andererseits aber auch die Informationen, die nicht oder nur teilweise elektronisch abgebildet sind (zum Beispiel Papierdokumente) sowie Geschäftsprozesse. Ausgenommen sind die für Abteilung 3 des SMI, deren nachgeordnete Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst sowie für Referat 16 und das Landesamt für Verfassungsschutz betriebenen fachbezogenen IT-Verfahren, -Vorhaben und Netze.

Die Leitlinie gilt für alle durch das SMI oder dessen nachgeordnete Behörden genutzten Räume und für deren Bedienstete, jeweils mit Ausnahme der der Abteilung 3 – Öffentliche Sicherheit und Ordnung, Landespolizeipräsidium – nachgeordneten Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst. Bedienstete sind hierbei alle Beamten, Beschäftigten, Auszubildenden, Referendare sowie Praktikanten.

Ebenso gilt die Leitlinie auch für externe Leistungserbringer und durch sie genutzte Räumlichkeiten (siehe Nummer 6.2.6).

2.2 Begriffe

a) Informationssicherheit (IS)
Die Informationssicherheit bezeichnet einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten.

b) Daten/Informationen
Die Begriffe „Daten“ und „Informationen“ werden nachfolgend synonym verwendet. Hierunter sind insbesondere analoge und digitale Schriftstücke, Datensätze sowie Karten und Grafiken zu verstehen.

c) Informationstechnik
Als IT wird die Gesamtheit der technischen Mittel zur Erhebung, Erfassung, Aufbereitung, Nutzung, Speicherung, Übermittlung, programmgesteuerten Verarbeitung, internen Darstellung, Ausgabe und Wiedergewinnung von Daten bezeichnet. Hierbei ist ein IT-Produkt eine abgegrenzte, eigenständige Funktionalität beinhaltende Hard- oder Software, während ein IT-Verfahren die informationstechnische Unterstützung eines Prozesses durch Anwendungen und Dienste der IT ist.

d) Informationssicherheits-Vorschriften (IS-Vorschriften)
Die IS-Vorschriften umfassen die VwV Informationssicherheit sowie sonstige ressortübergreifende, ressortweite und behördenbezogene Sicherheitsleitlinien, -richtlinien und -konzepte in den jeweils geltenden Fassungen.

e) Informationssicherheits-Normen (IS-Normen)
Die IS-Normen bilden die Grundlage für die Festlegung, Erarbeitung und Aufrechterhaltung der jeweils angestrebten angemessenen Informationssicherheitsniveaus. Hierzu gehören die einschlägigen Gesetze, Verwaltungsvorschriften (beispielsweise Verschlusssachenanweisung) die Standards und Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie die IS-Vorschriften.

2.3 Regelungshierarchie und Öffnungsklausel

Diese Leitlinie sowie künftige, darauf aufbauende Regelungen bilden in ihrem jeweiligen Geltungsbereich den Rahmen für konkretisierende Regelungen (insbesondere Sicherheitsziele, Rollen, inter- und innerbehördliche Prozessgestaltung). Auch neue Regelungsgegenstände können erschlossen werden, wobei die Widerspruchsfreiheit in Bezug auf bestehende Regelungen sicherzustellen ist.

3 Grundsätze und Prinzipien

3.1 Bedeutung der Informationssicherheit

Für eine effiziente und korrekte Aufgabenerledigung bedarf es der jeweils angemessenen Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit der verarbeiteten Daten. Die Informationssicherheit stellt somit eine wesentliche und schutzbedürftige Arbeitsgrundlage für die Aufrechterhaltung und Durchführung der Geschäftsprozesse dar.

3.2 Informationssicherheit als Leistungsmerkmal

Die Informationssicherheit ist als unerlässliches Leistungsmerkmal von IT-Produkten, IT-Verfahren und Geschäftsprozessen zu verstehen. Sie sind hinsichtlich ihres Schutzbedarfes und des erreichten Erfüllungsgrades

zu bewerten. Sofern der Schutzbedarf nicht gedeckt ist, ist dies durch geeignete Maßnahmen herbeizuführen. Maßnahmen der Informationssicherheit orientieren sich am Grundsatz der Verhältnismäßigkeit. Bleiben im Einzelfall trotz Sicherheitsvorkehrungen Risiken untragbar, ist auf den IT-Einsatz zu verzichten beziehungsweise der Geschäftsprozess anzupassen.

Belange der Informationssicherheit sind in jeder Phase eines IT-Verfahrens (Entwicklung, Einführung, Betrieb/Pflege), beim Umgang mit IT-Produkten (Beschaffung, Betrieb/Pflege, Beseitigung/Entsorgung) sowie bei der Nutzung von Diensten Dritter zu berücksichtigen. Um dies zu gewährleisten, ist die frühzeitige Einbindung des zuständigen BfIS sicherzustellen.

Geschäftsprozesse sind so zu gestalten, dass sich Informationssicherheitsmaßnahmen harmonisch in diese einfügen. Belange der Informationssicherheit sind zu berücksichtigen bei:

a) der Gestaltung der Organisation,

b) der Schaffung und Besetzung von Rollen/Regelung von Verantwortlichkeiten,

c) der Führung von Beschäftigten,

d) der Zusammenarbeit mit anderen Behörden und Externen,

e) der Gestaltung von Arbeitsabläufen,

f) dem Bereich Aus- und Weiterbildung und

g) der Auswahl und dem Einsatz von Hilfsmitteln.

3.3 Wirtschaftlichkeit

Die Sicherheitsmaßnahmen sollten in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Dieser wird durch den Wert der zu schützenden Informationen und der IT-Systeme definiert. Zu bewerten sind dabei in der Regel die Auswirkungen auf die körperliche und seelische Unversehrtheit von Menschen, Beeinträchtigungen des Grundrechts auf informationelle Selbstbestimmung, finanzielle Schäden, negative Innen- oder Außenwirkungen (insbesondere Beeinträchtigungen des Ansehens des SMI, der Landesverwaltung, des Freistaates Sachsen oder des Bundes) und die Folgen von Gesetzesverstößen.

Ist die Wirtschaftlichkeit von Sicherheitsmaßnahmen oder gegebenenfalls zu prüfenden Alternativmaßnahmen nicht gegeben, ist auch ein Verzicht auf den IT-Einsatz oder einzelne Bestandteile in Betracht zu ziehen – über die Umsetzung entscheidet die Leitung der Behörde. Das Kriterium der wirtschaftlichen Angemessenheit ist nachrangig, soweit die Sicherheitsmaßnahmen zur Erfüllung rechtlicher Anforderungen oder Vorgaben erforderlich sind.

Die für die Umsetzung der erforderlichen und angemessenen Sicherheitsmaßnahmen notwendigen Ressourcen und Finanzmittel sind im Rahmen der behördeneigenen Haushaltsplanung zu berücksichtigen und bereit zu stellen.

3.4 Information der Bediensteten

Die Bediensteten sind in jeweils erforderlichem Umfang für die Belange der Informationssicherheit zu sensibilisieren und entsprechend zu qualifizieren. Die im Rahmen des Informationssicherheitsprozesses beschlossenen IS-Vorschriften werden den betreffenden Bediensteten im erforderlichen Umfang bekannt gemacht.

Bevor ein Bediensteter Zugang zu IT-Systemen erhält, ist er nachweisbar über die Geltung der jeweils maßgeblichen IS-Normen zu belehren.

4 Informationssicherheitsziele

4.1 Allgemeine Informationssicherheitsziele

Es werden folgende allgemeine Ziele der Informationssicherheit verfolgt:

a) Erfüllung der aus rechtlichen Vorgaben resultierenden Anforderungen (zum Beispiel Datenschutz, Wahrung von Dienst- und Amtsgeheimnissen),

b) Sicherstellung der Kontinuität der Geschäftsprozesse,

c) Sicherung der Informationsinhalte und der in ihre Verarbeitung investierten Werte sowie Reduzierung der im Schadensfall entstehenden Kosten.

4.2 System-, wissens- und verhaltensbezogene Ziele

Für alle Daten ist zu jeder Zeit und unter allen Umständen das jeweils angemessene Maß an Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen.

Die Einhaltung dieser Anforderungen ist unabdingbarer Bestandteil jedes Handelns, insbesondere jedes Einsatzes von Informations- und Kommunikationstechnik, und ist mit technischen, organisatorischen und personellen Maßnahmen verbindlich sicherzustellen.

4.2.1 Systembezogene Ziele

Die Auswahl, Integration und Konfiguration aller der Verarbeitung von Daten dienenden Systeme soll so erfolgen, dass zu jeder Zeit und unter allen Umständen das angemessene Maß an Vertraulichkeit, Integrität und Verfügbarkeit für die auf ihnen verarbeiteten Daten sichergestellt ist. Dies gilt auch für die zur Datenverarbeitung sowie zur Aufbewahrung von Datensicherungsmedien genutzten Räumlichkeiten.

Vertraulichkeit
Sämtliche verarbeitete Daten sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Nachrichteninhalte, die Meta-Informationen über den Kommunikationsvorgang sowie die Daten über den Sende- und Empfangsvorgang. Sie dürfen nur den Berechtigten zur Verfügung stehen. Berechtigt ist eine Person, soweit diese den Zugriff auf die Informationen zur Erfüllung ihrer dienstlichen Aufgaben beziehungsweise ihrer vertraglichen Pflichten benötigt sowie gegebenenfalls entsprechend überprüft und ermächtigt wurde.

Integrität
Daten sind gegen unbeabsichtigte Veränderung und vorsätzliche Verfälschung zu schützen. Alle IT-Verfahren sollen stets aktuelle, unversehrte und vollständige Daten liefern. Bei IT-Systemen ist eine ordnungsgemäße Verarbeitung und Übertragung der Daten sicherzustellen. Eventuelle verfahrens- oder informationsverarbeitungsbedingte Einschränkungen sind zu dokumentieren.

Verfügbarkeit
Dienstleistungen, Funktionen eines IT-Systems sowie Informationen stehen zum geforderten Zeitpunkt ordnungsgemäß zur Verfügung. Hierfür sind Soll-Verfügbarkeiten zu bestimmen. Für regelmäßige

Betriebsunterbrechungen, die aus technischen, organisatorischen oder sicherheitsrelevanten Gründen notwendig sind, sind ebenfalls Zeiten festzulegen.

Zudem sollen die Authentizität (Zuordenbarkeit von Daten zu ihrem Ursprung), Revisionsfähigkeit (Nachvollziehbarkeit der Datenverarbeitung bezüglich Inhalt, Zeitpunkt und Art) und Transparenz (vollständige, aktuelle und nachvollziehbare Dokumentation der Datenverarbeitungsverfahren) gewährleistet werden.

Die Verwendung sicherer Standards ist anzustreben beziehungsweise, soweit es sich aus IS-Normen ergibt, zwingend erforderlich.

Die Ziele sind auch bei Regelungen zur Aufbau- und Ablauforganisation sowie zur Personalauswahl zu berücksichtigen.

4.2.2 Wissens- und verhaltensbezogene Ziele

Alle Bediensteten kennen die für ihren Tätigkeitsbereich relevanten IS-Normen sowie sonstige IS-relevante Vorgaben und halten diese ein. Sie sind sich ihrer Verantwortung bewusst und unterstützen aktiv den Informationssicherheitsprozess.

5 Vorgehen

Jede Behörde entwickelt unter Anwendung oder Berücksichtigung der IS-Normen ein Sicherheitskonzept für ihren Verantwortungsbereich und passt dieses an sich ändernde Rahmenbedingungen an.

Hierbei ist sie unter Beachtung des Subsidiaritätsgrundsatzes grundsätzlich frei in der Auswahl, Planung und Umsetzung von Sicherheitsmaßnahmen, mit denen die jeweils angemessenen Sicherheitsziele erreicht werden können, sofern sie nicht im Widerspruch zu höherrangigen Vorgaben stehen.

Sofern ein über den BSI-Grundschutz hinausgehender Schutzbedarf besteht, ist eine Risikoanalyse durchzuführen, deren Ergebnisse im Rahmen der wirtschaftlichen Vertretbarkeit zu berücksichtigen sind. Der BSI-Grundschutz ergibt sich dabei aus der vom BSI entwickelten Vorgehensweise zum Identifizieren und Umsetzen von institutionsspezifischen IT-Sicherheitsmaßnahmen, welche dazu beitragen, ein mittleres, angemessenes und ausreichendes Schutzniveau für IT-Systeme und Informationen zu erreichen.

Um die Informationssicherheitsziele zu erreichen, sind Sicherheitsmaßnahmen zu ergreifen. Dies sind insbesondere

a) die Definition von Verantwortlichkeiten für Informationen, Verfahren, Anwendungen und Systemen,

b) die Feststellung von Schutzbedarfen für IT-Verfahren und Informationen,

c) die Erstellung konkretisierender Richtlinien und Handlungsempfehlungen sowie die Ergreifung von Maßnahmen zur Abdeckung des jeweiligen Schutzbedarfs,

d) die zyklische Kontrolle der Maßnahmen auf Wirksamkeit, Vollständigkeit und Effizienz und gegebenenfalls Anpassung.

Die frühzeitige Beteiligung des zuständigen BfIS an sicherheitsrelevanten Vorgängen ist sicherzustellen.

6 Organisation/Verantwortlichkeiten/Rollen

6.1 Ressortübergreifende Instanzen

Grundlage hierfür ist die VwV Informationssicherheit in der jeweils geltenden Fassung.

Der Beauftragte für Informationssicherheit des Landes (BfIS Land) ist als die zentrale Sicherheitsinstanz für alle ihm vom Lenkungsausschuss IT und E-Government (LA ITEG) übertragenen operativen und koordinierenden Belange der Informationssicherheit zuständig.

Koordinierendes Gremium für alle ressortübergreifenden Aspekte der Informationssicherheit ist die Arbeitsgemeinschaft Informationssicherheit (AG IS).

6.2 Ressortspezifische Regelungen

6.2.1 Leitungsebene

Die Gesamtverantwortung für die Informationssicherheit obliegt im Rahmen ihres jeweiligen Verantwortungsbereichs der Behördenleitung. Diese erlässt notwendige Regelungen, deren Geltung sich auch auf nachgeordnete Behörden erstrecken kann und stellt eine zielgerichtete Umsetzung sowie die Dokumentation aller getroffenen Regelungen und die Information der Bediensteten sicher.

6.2.2 Beauftragter für Informationssicherheit

Ein Beauftragter für Informationssicherheit ist für die Steuerung und den Vollzug des Informationssicherheitsprozesses verantwortlich und nimmt hierbei insbesondere folgende Aufgaben wahr:

a) Erstellung, Fortschreibung und Umsetzung des Sicherheitskonzeptes,

b) Überprüfung der Umsetzung der Vorgaben zur Informationssicherheit,

c) Vorschlag von neuen Sicherheitsmaßnahmen und -strategien,

d) Koordination von Sensibilisierungs- und Schulungsmaßnahmen,

e) Mitwirkung bei allen Behördenaktivitäten mit IS-Bezug (zum Beispiel IT-Projekte, Infrastruktur-Projekte, Regelungen der Zutrittskontrolle),

f) Zuarbeit und Aufbereitung von Informationen sowie Bewertung von Sachverhalten, insbesondere für die Leitung, Organisationseinheiten der Behörde sowie als Vertreter der Behörde im Kontakt mit anderen Institutionen,

g) Meldung relevanter Schwachstellen und Sicherheitsvorfälle entsprechend definierter beziehungsweise zu definierender Meldewege,

h) Durchführung beziehungsweise Mitwirkung an behörden- beziehungsweise ressortbezogenem Berichtswesen,

i) Vertretung der Behörde in den Angelegenheiten der Informationssicherheit,

j) Ansprechpartner für die Bediensteten in den Fragen der Informationssicherheit.

Die Wahrnehmung der Aufgaben des Informationssicherheitsprozesses im SMI erfolgt durch einen hauptamtlichen BfIS des SMI (BfIS SMI), welcher die Hausleitung in allen diesbezüglichen Angelegenheiten berät und unterstützt. Ihm obliegen zudem die Information der Beauftragten für Informationssicherheit des nachgeordneten Bereichs über Belange der Informationssicherheit von behördenübergreifender Bedeutung sowie die Abstimmung von behördenübergreifenden Fragen der Informationssicherheit im Geschäftsbereich des SMI (außer

Polizeidienststellen und Einrichtungen für den Polizeivollzugsdienst).

Für den Bereich der Polizei ist gemäß Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern zur Gewährleistung der Informationssicherheit im Polizeivollzugsdienst des Freistaates Sachsen (VwV Informationssicherheit Polizei – VwV IS-Pol) vom 2. Januar 2013 (nicht veröffentlicht) sowie der VwV Informationssicherheit ein separater Beauftragter für Informationssicherheit (BfIS [PVD]) benannt.

BfIS SMI und BfIS (PVD) stimmen ihre Zuständigkeiten und Tätigkeiten an den Schnittstellen der Aufgabenbereiche ab.

In jeder Behörde des Geschäftsbereiches soll von der Behördenleitung ein BfIS ernannt werden. Bis zu einer Ernennung wird die Aufgabe vom Behördenleiter selbst wahrgenommen.

Die Beauftragten für Informationssicherheit sind in alle Projekte und Vorhaben, die die Informationssicherheit ihres Zuständigkeitsbereichs betreffen könnten, frühzeitig einzubinden. Bei der Erfüllung ihrer Aufgaben sind sie, unabhängig von ihrer organisatorischen Zuordnung, weisungsfrei und der jeweiligen Behördenleitung unmittelbar unterstellt.

6.2.3 Informationssicherheits-Management-Team

Im SMI besteht zur Unterstützung des BfIS SMI ein Informationssicherheits-Management-Team (ISM-Team). Dieses setzt sich zusammen aus:

a) dem BfIS SMI als Vorsitzendem,

b) einem Bediensteten des IuK-Bereichs des Referates 11 und

c) dem Datenschutzbeauftragten des SMI oder dessen Vertreter sowie

d) dem BfIS (PVD) in beratender Funktion.

Bei Bedarf können weitere Fachkräfte hinzugezogen werden.

Die Bildung von ISM-Teams in nachgeordneten Behörden liegt im Ermessen der jeweiligen Behörde. Die Entscheidung sollte sich insbesondere auch an der Qualität und Quantität der zu bewältigenden Aufgaben orientieren.

6.2.4 Führungskräfte

Führungskräfte haben im Rahmen ihrer Leitungsfunktion die Bediensteten ihres Zuständigkeitsbereichs für Belange der Informationssicherheit zu sensibilisieren und darauf zu achten, dass diese sich den IS-Normen gemäß verhalten.

6.2.5 Bedienstete

Bedienstete sind verantwortlich für den bestimmungsgemäßen und sachgerechten Umgang mit den ihnen zugänglichen Daten und Informationen und verhalten sich gemäß den für sie jeweils relevanten IS-Normen und sonstigen Vorgaben (zum Beispiel vertraglichen Verpflichtungen).

6.2.6 Externe Leistungserbringer

Auf vertraglicher Basis tätige externe Leistungserbringer sind mit Zuschlag auf die Einhaltung der relevanten IS-Vorschriften nachweisbar zu verpflichten. Dessen ungeachtet, verbleibt die Verantwortung für die Gewährleistung der Informationssicherheit bei der Behörde.

Bei der Vergabe von IT-Dienstleistungen an externe Leistungserbringer sind die Anforderungen an die Informationssicherheit sowie explizite Kontrollrechte und -möglichkeiten vertraglich zu fixieren.

Stellt ein externer Leistungserbringer Mängel oder Risiken hinsichtlich praktizierter Sicherheitsmaßnahmen fest, ist die Behörde, für die die Leistung erbracht wird, hierüber unverzüglich zu informieren.

6.2.7 Kostentragung

Durch einen Sicherheitsvorfall entstehende Kosten trägt grundsätzlich die Behörde, der die Entstehung des Sicherheitsvorfalls zuzurechnen ist.

6.2.8 Berichtswesen

Für den Geltungsbereich der Leitlinie wird durch den BfIS SMI zum 30. Juni jedes Jahres ein Bericht zum Stand der Informationssicherheit erstellt. Dem SMI nachgeordnete Behörden arbeiten entsprechende Informationen zum Umsetzungsstand des Informationssicherheitsprozesses sowie zu sicherheitsrelevanten Vorfällen zu.

6.3 Beeinträchtigungen der Informationssicherheit und Haftung

Verstöße gegen IS-Normen sowie Beeinträchtigungen der Informationssicherheit sind dem zuständigen BfIS zu melden. Sofern deren Wirkungen nicht auf die Behörde begrenzt sind, ist auch der BfIS SMI zeitnah zu informieren.

Sicherheitsgefährdendes Verhalten kann disziplinar- oder arbeitsrechtlich, gegebenenfalls auch ordnungswidrigkeits- oder strafrechtlich verfolgt werden (vergleiche Nummer 3.2 der Anlage zur VwV Informationssicherheit) und im Schadensfall zu Schadenersatzforderungen oder Rückgriffsansprüchen gegenüber dem Bediensteten führen.

7 Fortentwicklung

Alle zum Zwecke der Informationssicherheit erlassenen Regelungen (zum Beispiel Leitlinien, Richtlinien, Konzepte) sowie daraus abgeleitete Maßnahmen werden regelmäßig auf Aktualität und Verhältnismäßigkeit geprüft und bei Bedarf fortgeschrieben, um das angestrebte Sicherheitsniveau gewährleisten zu können.

Zuletzt enthalten in

Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern über die geltenden Verwaltungsvorschriften des Staatsministeriums des Innern

vom 4. Dezember 2017 (SächsABl.SDr. S. S 352)