Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus zur Gewährleistung der Informationssicherheit im Geschäftsbereich (VwV Informationssicherheit SMK)

Vom 27. Januar 2016

I. Regelungsgegenstand

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

II. Geltungsbereich

Die Verwaltungsvorschrift gilt nach Maßgabe der Nummer 2.1 der Anlage für die dort genannten Behörden und Einrichtungen. Die Vorgaben der Anlage sind entsprechend der jeweiligen Aufgabenverantwortung umzusetzen und auszugestalten.

III. Inkrafttreten

Diese Verwaltungsvorschrift tritt am Tag nach ihrer Veröffentlichung in Kraft.

Dresden, den 27. Januar 2016

Die Staatsministerin für Kultus
Brunhild Kurth

Anlage
(zu Ziffer I)

Leitlinie des Sächsischen Staatsministeriums für Kultus zur Gewährleistung der Informationssicherheit im Geschäftsbereich (Leitlinie Informationssicherheit SMK)

Inhaltsverzeichnis:

1. Einleitung

Die Möglichkeiten der Informationstechnik (IT) bilden im Geschäftsbereich des Staatsministeriums für Kultus zunehmend die Grundlage für die Bewältigung der zu erfüllenden Fachaufgaben und der behördlichen Abläufe. Ohne den Einsatz der IT ist ein effizienter Verwaltungsbetrieb heute nicht mehr denkbar.

Mit der Nutzung der Informationstechnologie gehen jedoch auch erhebliche Gefährdungen einher. Jede Störung des IT-Betriebes kann Geschäftsprozesse behindern und die Leistungsfähigkeit der Verwaltung negativ beeinflussen. Beeinträchtigungen können zum Beispiel durch vorsätzliche Angriffe von innen und außen, fahrlässiges Handeln, Nachlässigkeiten, Ignoranz und Unkenntnis entstehen.

Vor diesem Hintergrund muss es das Ziel sein, alle IT-unterstützten Geschäftsprozesse sowie alle im Geschäftsbereich des Staatsministeriums für Kultus vorhandenen Informationen vor den genannten Gefährdungen zu schützen. Nur durch die Gewährleistung eines funktionierenden und sicheren IT-Betriebes können die dem Staatsministerium für Kultus, seinen nachgeordneten Behörden und den Schulen in Landesträgerschaft übertragenen Aufgaben in der erforderlichen Qualität erfüllt werden. Hierfür sind die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich. Dieser erstreckt sich nicht nur auf die Rahmenbedingungen elektronischer Datenverarbeitungsprozesse, sondern auch auf organisatorische Maßnahmen und die Ausgestaltung fachlich-inhaltlicher Geschäftsprozesse.

Die vorliegende Leitlinie beschreibt die vom Staatsministerium für Kultus angestrebten Informationssicherheitsziele, die Organisationsstrukturen und die verfolgte Sicherheitsstrategie, die für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind. Sie gilt in allen Behörden und Einrichtungen des Geschäftsbereichs des Staatsministeriums für Kultus.

Die Regelungen dieser Leitlinie folgen den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Sie entsprechen zudem den Festlegungen der VwV Informationssicherheit vom 7. September 2011 (SächsABl. S. 1294), die durch die Verwaltungsvorschrift vom 27. Januar 2015 (SächsABl. S. 214) geändert worden ist, zuletzt enthalten in der Verwaltungsvorschrift vom 16. Dezember 2015 (SächsABl. SDr. S. S 342).

Die Behördenleitung des Staatsministeriums für Kultus bekennt sich hiermit zu ihrer Gesamtverantwortung und unterstützt alle angemessenen und geeigneten Maßnahmen zur Etablierung, Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit.

2. Begriffsbestimmungen

2.1 Geltungsbereich und Begriffe

Die vorliegende Leitlinie gilt dem Schutz aller geschäftsrelevanten Informationen und deren Verarbeitung im Staatsministerium für Kultus und den nachgeordneten Behörden und Einrichtungen für:

- das Staatsministerium für Kultus
- die Sächsische Bildungsagentur
- das Sächsische Bildungsinstitut
- die Sächsische Landeszentrale für politische Bildung
- das Sächsische Landesgymnasium Sankt Afra zu Meißen
- das Sächsische Landesgymnasium für Sport Leipzig
- das Sächsische Landesgymnasium für Musik Carl Maria von Weber
- die Sächsische Landesschule für Gehörlose Samuel Heinicke
- die Sächsische Landesschule für Blinde und Sehbehinderte mit dem Landeszentrum.

Sofern einzelne Beschäftigte im Rahmen von Telearbeit tätig sind und zu Hause oder auf Dienstreisen Daten verarbeiten oder Datenträger mit sich führen, gelten die Festlegungen dieser Leitlinie ebenfalls.

Über die Regelungen der VwV Informationssicherheit hinausgehend sind in den öffentlichen Schulen die Arbeitsplätze betroffen, die in das Sächsische Verwaltungsnetz eingebunden sind. Die Schulleiter

öffentlicher Schulen haben daher dafür Sorge zu tragen, dass die Bestimmungen dieser Leitlinie auch von solchen Bediensteten an den öffentlichen Schulen beachtet werden, die beauftragt sind, Aufgaben im Zusammenhang mit SaxSVS zu erfüllen.

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 und Informationen, zum Beispiel Papierdokumente.

Dabei bedeuten die drei Grundwerte der Informationssicherheit (Definition nach BSI):

- Verfügbarkeit: Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern stets wie gewünscht zur Verfügung stehen. Verfügbarkeit ist ein Grundwert der IT-Sicherheit.
- Vertraulichkeit: Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Vertraulichkeit ist ein Grundwert der IT-Sicherheit.
- Integrität: Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten“ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen“ angewendet. Der Begriff „Information“ wird dabei für „Daten“ verwendet, denen je nach Zusammenhang bestimmte Attribute wie zum Beispiel Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. Integrität ist ein Grundwert der IT-Sicherheit.

Beschäftigte im Sinne dieser Leitlinie sind alle im Geschäftsbereich des Staatsministeriums für Kultus tätigen Beamtinnen/Beamten, Tarifbeschäftigten (m/w), Auszubildenden (m/w) und Praktikantinnen/Praktikanten.

2.2 Informationssicherheitsmanagementsystem (ISMS)

Unter einem ISMS wird der Teil des gesamten Managementsystems verstanden, der auf Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung der Informationssicherheit abdeckt. Das Managementsystem umfasst dabei Strukturen, Richtlinien, Planungsaktivitäten, Verantwortlichkeiten, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation.

2.3 Informationseigentümer

Zu jedem IT-unterstützten Geschäftsprozess und jeder Fachanwendung muss ein Ansprechpartner benannt werden, der als so genannter Informationseigentümer für alle Fragen der Informationsverarbeitung und der Informationssicherheit im Rahmen dieses Geschäftsprozesses verantwortlich ist.

Der Verantwortliche für einen Geschäftsprozess muss als Informationseigentümer sicherstellen, dass die für seinen Geschäftsprozess relevanten Sicherheitsmaßnahmen dem Sicherheits- und Kontrollumfang der Schutzbedarfsfeststellung entsprechen.

Wird kein entsprechender Verantwortlicher für IT-unterstützte Geschäftsprozesse bestimmt, ist automatisch die Behörden- beziehungsweise Einrichtungsleitung der Informationseigentümer.

2.4. Sicherheitsdomänen

Informations-Sicherheitsrichtlinien beziehungsweise Sicherheitskonzepte beziehen sich immer auf eine bestimmte Sicherheitsdomäne. Als Sicherheitsdomäne wird dabei ein logisch, organisatorisch oder räumlich zusammengehöriger Bereich mit einheitlichen Sicherheitsanforderungen und/oder einheitlicher Sicherheitsadministration bezeichnet. Insbesondere bilden das Staatsministerium für Kultus, die nachgeordneten Behörden und Einrichtungen (Schulen in Landesträgerschaft) jeweils eigene Sicherheitsdomänen.

3. Ziele der Informationssicherheit

Allgemeingültige Sicherheitsziele innerhalb des Staatsministeriums für Kultus und der nachgeordneten Behörden und Einrichtungen sind:

- Zuverlässige Unterstützung der Geschäftsprozesse durch die IT und Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Sicherheitsdomäne,

- Realisierung sicherer und vertrauenswürdiger E-Government-Verfahren,
- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Erhalt beziehungsweise Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen,
- Gewährleistung des informationellen Selbstbestimmungsrechts des Betroffenen bei der Verarbeitung personenbezogener Daten,
- Reduzierung der im Schadensfall entstehenden Kosten sowie
- Wahrung besonderer Dienst- oder Amtsgeheimnisse.

Für alle IT-Verfahren sind die Zeiten, in denen sie verfügbar sein sollen, zu bestimmen. Für regelmäßige Betriebsunterbrechungen, die aus technischen, organisatorischen oder sicherheitsrelevanten Gründen notwendig sind, sind Zeiten festzulegen. Sämtliche Daten, die erhoben, gespeichert oder verarbeitet werden, sind vertraulich zu behandeln und jederzeit vor unbefugtem Zugriff zu schützen. Informationen dürfen nur den Berechtigten zur Verfügung stehen. Berechtigt ist jeder Beschäftigte, soweit er den Zugriff auf die Informationen zur Erfüllung seiner dienstlichen Aufgaben benötigt. Informationen sind gegen unbeabsichtigte Veränderung und vorsätzliche Verfälschung zu schützen. Alle IT-Verfahren sollen stets aktuelle und vollständige Informationen liefern, eventuelle verfahrens- oder informationsverarbeitungsbedingte Einschränkungen sind zu dokumentieren.

Jede Behörde beziehungsweise Einrichtung kann für ihren Bereich weitere angepasste Informationssicherheitsziele aufstellen.

4. Grundsätze

4.1 Bedeutung der Informationssicherheit

Im Geschäftsbereich des Staatsministeriums für Kultus ist es das Ziel, dass alle technischen Einrichtungen, die der Erstellung, Speicherung und Übertragung von Daten dienen, so ausgewählt, integriert und konfiguriert sind, dass für die auf ihnen verarbeiteten Daten zu jeder Zeit und unter allen Umständen das angemessene Maß an Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt ist. Dies gilt auch für die Orte zur Aufbewahrung der Medien zur Datensicherung. Die Einhaltung dieser Anforderungen ist unabdingbarer Bestandteil jedes Einsatzes von Informations- und Kommunikationstechnik im Geschäftsbereich des Staatsministeriums für Kultus und ist durch geeignete Maßnahmen sicherzustellen.

4.2 Standards des Bundesamtes für Sicherheit in der Informationstechnik

Zur Erreichung und Aufrechterhaltung eines angemessenen und ausreichenden Informationssicherheitsniveaus sind für die Behörden und Einrichtungen des Geschäftsbereichs des Staatsministeriums für Kultus die Handlungsanweisungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in ihrer jeweils geltenden Fassung maßgeblich (www.bsi.bund.de). Diese umfassen insbesondere die Anwendung der aktuellen BSI-Standards sowie der IT-Grundschutz-Kataloge.

Die Sicherheitskonzepte sind entsprechend der IT-Grundschutz-Vorgehensweise (BSI Standard 100-2) zu erstellen. Zeichnet sich im Rahmen der Prüfung ein über den Grundschutz hinausgehender Schutzbedarf ab, ist dieser anschließend mit einer Risikoanalyse auf der Basis von IT-Grundschutz gemäß BSI Standard 100-3 in der jeweils aktuellen Fassung zu ermitteln und mit geeigneten Sicherheitsmaßnahmen zu gewährleisten.

4.3 Informationssicherheit als Leistungsmerkmal

Bei sämtlichen IT-Verfahren ist sicherzustellen, dass Belange der Informationssicherheit in jedem Stand des Verfahrens (zum Beispiel Entwicklung, Einführung, Betrieb) hinreichend Berücksichtigung finden. Gleiches gilt für den Umgang (zum Beispiel Beschaffung, Aufbewahrung, Beseitigung, Entsorgung) mit IT-Produkten. Belange der Informationssicherheit sind ferner zu berücksichtigen insbesondere bei:

a) der Gestaltung der Organisation,
b) der Zuweisung von Verantwortlichkeiten,
c) der Führung von Beschäftigten,
d) dem Bereich Aus- und Weiterbildung,
e) der Gestaltung von Arbeitsabläufen,
f) der Zusammenarbeit mit anderen Behörden und Externen und
g) der Auswahl und dem Einsatz von Hilfsmitteln.

Geschäftsprozesse sind so zu gestalten, dass sich Sicherheitsmaßnahmen in diese einfügen und in einem wirtschaftlich vertretbaren Verhältnis zu dem Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann.

4.4 Subsidiarität

Vorgaben des Staatsministeriums für Kultus zur Informationssicherheit können von den nachgeordneten Behörden und Einrichtungen im Geschäftsbereich des Staatsministeriums für Kultus entsprechend den individuellen Anforderungen präzisiert und ergänzt werden. Präzisierungen und Ergänzungen dürfen aber nicht im Widerspruch zu den Vorgaben des Staatsministeriums für Kultus stehen.

Die Behörden und Einrichtungen sind grundsätzlich frei in der Auswahl der Mittel, mit denen sie ihre Sicherheitsziele erreichen wollen. Angemessene Sicherheitsmaßnahmen können eigenständig geplant und umgesetzt werden.

4.5 Beteiligung und Information der Beschäftigten

Die Beschäftigten sind bezüglich der Informationssicherheit im erforderlichen Umfang zu sensibilisieren und zu qualifizieren. Hierfür werden sämtliche Dokumente, die im Zuge des Informationssicherheitsprozesses beschlossen wurden, allen betroffenen Beschäftigten des Geschäftsbereichs des Staatsministeriums für Kultus bekannt gemacht. Neuen Beschäftigten wird diese Leitlinie bekannt gemacht, bevor sie Zugang zu geschäftsrelevanten Informationen erhalten.

5. Rollen und Verantwortlichkeiten

5.1 Behördenleitung und Führungskräfte

Die Behördenleitung oder Einrichtungsleitung trägt für ihren Zuständigkeitsbereich die Gesamtverantwortung für die Gewährleistung eines Informationssicherheitsniveaus im Sinne der Nummer 4.1. Sie stellt sicher, dass diese Leitlinie in allen Punkten umgesetzt wird. Sie erlässt hierfür verbindliche Regeln zur Informationssicherheit und gibt sie allen Beschäftigten bekannt. In der Sächsischen Bildungsagentur ist die Verantwortung zwischen dem Direktor und den Regionalstellenleitern so eindeutig zu regeln und abzugrenzen, dass die Informationssicherheit in der gesamten Sächsischen Bildungsagentur auf dem erforderlichen Niveau gewährleistet ist.

Führungskräfte haben im Rahmen ihrer Leitungsaufgabe darauf zu achten, dass sich die Beschäftigten ihres Zuständigkeitsbereichs sicherheitskonform verhalten. Durch Sensibilisierung fördern sie das Sicherheitsbewusstsein der Beschäftigten.

5.2 Beschäftigte

Alle Beschäftigten tragen die Verantwortung, bestimmungsgemäß und sachgerecht mit den von ihnen genutzten Informationen umzugehen. Sie befolgen die für die Informationssicherheit relevanten Vorschriften und Regelungen.

Folgende Sachverhalte können Straftaten darstellen:

a) das unbefugte Verschaffen von Daten anderer, die nicht für den Handelnden bestimmt und die gegen den unberechtigten Zugang besonders gesichert sind,

b) das Schädigen fremden Vermögens durch unrichtiges Gestalten eines Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugtes Verwenden von Daten oder durch unbefugtes Einwirken auf den Ablauf eines Programms,

c) das rechtswidrige Löschen, Verändern, Unterdrücken und Unbrauchbarmachen von Daten,

d) das unbefugte Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers oder

e) strafbewehrte Verstöße gegen das Sächsische Datenschutzgesetz gemäß § 39 in Verbindung mit § 38 Absatz 1 Nummer 1 bis 8 des Sächsischen Datenschutzgesetzes vom 25. August 2003 (SächsGVBl. S. 330), das zuletzt durch Artikel 17 des Gesetzes vom 29. April 2015 (SächsGVBl. S. 349) geändert worden ist.

5.3 Externe Dienstleister

Personen, Behörden, Einrichtungen und Unternehmen, die nicht dem Geschäftsbereich des Staatsministeriums für Kultus angehören, für diesen aber Leistungen erbringen, haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie zu beachten. Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung. Dazu gehört, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren hat.

5.4 Beauftragter für Informationssicherheit (BfIS)

Der Beauftragte für Informationssicherheit ist für die Steuerung und den Vollzug des Informationssicherheitsprozesses in der jeweiligen Behörde oder Einrichtung verantwortlich. Der BfIS berät und unterstützt die Behördenleitung oder Einrichtungsleitung in allen Angelegenheiten der Informationssicherheit. In den nachgeordneten Behörden und Einrichtungen soll von der Behördenleitung oder Einrichtungsleitung jeweils ein BfIS benannt werden. Solange keine Benennung erfolgt, wird die

Aufgabe vom Behördenleiter oder Einrichtungsleiter wahrgenommen.

Zu den Aufgaben des BfIS gehören insbesondere:

- Steuerung des Informationssicherheitsprozesses und Mitwirkung bei allen damit zusammenhängenden Aufgaben,
- Überprüfung der Umsetzung der Vorgaben zur Informationssicherheit,
- Erstellung, Fortschreibung und Umsetzung des IT-Sicherheitskonzeptes,
- Vorschlag von neuen Sicherheitsmaßnahmen und -strategien,
- Vertretung der Behörde oder Einrichtung in den Angelegenheiten der Informationssicherheit,
- Ansprechpartner für die Beschäftigten in den Fragen der Informationssicherheit,
- Koordination von Sensibilisierungs- und Schulungsmaßnahmen,
- Zusammenfassung von bereichs-, projekt- oder systemspezifischen Informationen,
- Meldung von besonders sicherheitsrelevanten Zwischenfällen.

Die Beteiligung des BfIS an sicherheitsrelevanten Vorgängen ist in den Behörden und Einrichtungen sicherzustellen.

5.5 Informationssicherheits-Management-Team (ISM-Team)

Im Staatsministerium für Kultus wird ein Informationssicherheits-Management-Team (ISM-Team) gebildet.

Das Team setzt sich zusammen aus:

- dem BfIS des Staatsministeriums für Kultus, der den Vorsitz hat,
- den BfIS der nachgeordneten Behörden und Einrichtungen und
- dem für den IT-Service zuständigen Beschäftigten des Referates 12 im Staatsministerium für Kultus

als ständige Mitglieder sowie – soweit eine Fachanwendung betroffen ist – mindestens einem vom BfIS des Staatsministeriums für Kultus zugezogenen Vertreter der betroffenen Fachreferate als nichtständiges Mitglied. Weiterhin sind zur Beratung des ISM-Teams bei Bedarf Mitarbeiter des IT-Dienstleisters des Staatsministeriums für Kultus sowie Mitglieder der zuständigen Personalvertretungen einzuladen.

Das ISM-Team unterstützt den BfIS des Staatsministerium für Kultus bei der Wahrnehmung seiner Aufgaben. Durch die Hinzuziehung von Fachanwendern wird gewährleistet, dass sich die Sicherheitsmaßnahmen als integraler Bestandteil der Geschäftsprozesse und nicht als deren Effizienz senkender Annex darstellen.

Das Team erarbeitet und verabschiedet regelmäßig ressortspezifische Regelungen, Konzepte und Richtlinien zur Verbesserung der Informationssicherheit als dieser Leitlinie nachgeordnete Dokumente.

In den nachgeordneten Behörden und Einrichtungen können ebenfalls ISM-Teams gebildet werden.

6. IT-Sicherheitskonzeptionen

Jede Behörde und Einrichtung entwickelt ein IT-Sicherheitskonzept. Es wird auf der Grundlage der BSI-Standards und der BSI-Grundschutz-Kataloge sowie der Festlegungen dieser Leitlinie erstellt. Das IT-Sicherheitskonzept ist stets auf dem aktuellen Stand zu halten und den sich verändernden Rahmenbedingungen anzupassen.

Die Inhalte des IT-Sicherheitskonzepts richten sich nach dem Standard 100-2 und enthalten mindestens:

- Ergebnislisten der IT-Strukturanalyse und den Korrespondierenden Netzplan,
- Ergebnisse der Schutzbedarfsfeststellung der IT-Fachanwendungen, IT-Systeme, Netzverbindungen und Räume,
- Ergebnisse der IT-Grundschutzanalyse (Grundschutzmodell, Basis-Sicherheitscheck),
- Ergebnisse einer ergänzenden Sicherheitsanalyse bei höherem Schutzbedarf sowie
- Maßnahmenliste offener Sicherheitsmaßnahmen als Realisierungsplan mit Verantwortlichkeiten und angemessenen Umsetzungszeiträumen.

Das IT-Sicherheitskonzept wird durch das ISM-Team einer regelmäßigen Überprüfung auf deren Aktualität unterzogen, um den Managementprozess-Gedanken aufrechtzuerhalten.

7. Durchsetzung der Leitlinie Informationssicherheit Staatsministerium für Kultus

Verhalten, das die Sicherheit von Daten, Informationen, IT-Systemen oder der Netze (inklusive Sächsisches Verwaltungsnetz) gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden.

Sicherheitsgefährdendes Verhalten kann 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 Beschäftigten führen.

8. Änderungsmanagement

Das Gesamtkonzept der Informationssicherheit wird regelmäßig auf seine Aktualität, Angemessenheit und Wirksamkeit geprüft. Durch eine kontinuierliche Revision der zum Zwecke der Informationssicherheit erlassenen Regelungen und getroffenen Maßnahmen sowie deren Einhaltung wird das angestrebte Sicherheitsniveau gewährleistet.

Zuletzt enthalten in

Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus über die geltenden Verwaltungsvorschriften des Staatsministeriums für Kultus

vom 9. Dezember 2019 (SächsABl. SDr. S. S 385)