Verwaltungsvorschrift des Sächsischen Staatsministeriums für Wirtschaft, Arbeit und Verkehr zur Herstellung der Bindungswirkung der Leitlinie Informationssicherheit im Geschäftsbereich (VwV Leitlinie Informationssicherheit SMWA)

Vom 14. Mai 2012

I. Regelungsgegenstand

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

II. Geltungsbereich

Die Verwaltungsvorschrift gilt für alle Behörden des Geschäftsbereichs des Staatsministeriums für Wirtschaft, Arbeit und Verkehr. Die Vorgaben der Anlage sind entsprechend der jeweiligen Aufgabenverantwortung umzusetzen und auszugestalten.

III. Inkrafttreten

Diese Verwaltungsvorschrift tritt am Tage nach ihrer Veröffentlichung in Kraft.

Dresden, den 14. Mai 2012

Sächsisches Staatsministerium
für Wirtschaft, Arbeit und Verkehr
Roland Werner
Amtschef

Anlage
zu Ziffer I Satz 2

Leitlinie des Staatsministeriums für Wirtschaft, Arbeit und Verkehr zur Gewährleistung der Informationssicherheit im Geschäftsbereich (Leitlinie Informationssicherheit SMWA)

1. Einleitung

Die Möglichkeiten der Informationstechnik (IT) bilden im Geschäftsbereich des Sächsischen Staatsministeriums für Wirtschaft, Arbeit und Verkehr (SMWA) zunehmend die Grundlage für die Bewältigung der zu erfüllenden Fachaufgaben und der behördlichen Abläufe. Ohne den Einsatz der IT-Technik ist ein effizienter Verwaltungsbetrieb heute nicht mehr denkbar.

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

Vor diesem Hintergrund muss es das Ziel sein, alle IT-unterstützten Geschäftsprozesse sowie alle im Geschäftsbereich SMWA vorhandenen Informationen vor den genannten Gefährdungen zu schützen. Nur durch die Gewährleistung eines funktionierenden und sicheren IT-Betriebes können die dem SMWA und seinen Behörden aufgetragenen 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 SMWA angestrebten Informationssicherheitsziele, die Organisationsstrukturen und die verfolgte Sicherheitsstrategie, die für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind. Sie gilt in allen Behörden des Geschäftsbereichs SMWA.

Die Regelungen dieser Leitlinie folgen den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Sie entsprechen zudem den Vorgaben der Verwaltungsvorschrift der Sächsischen Staatsregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung (VwV Informationssicherheit) vom 7. September 2011 (SächsABl. S. 1294).

Die Hausleitung des SMWA hat diese Leitlinie beschlossen. Sie bekennt sich zu ihrer Gesamtverantwortung und unterstützt die Maßnahmen zur Informationssicherheit.

2. Begriffsbestimmungen

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.

Dabei bedeuten:

Verfügbarkeit: Die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen stehen dem Anwender zum geforderten Zeitpunkt zur Verfügung.

Vertraulichkeit: Vertrauliche Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Nachrichteninhalte, die näheren Informationen über den Kommunikationsvorgang sowie die Daten über den Sende- und Empfangsvorgang.

Integrität: Der Begriff der Integrität bezieht sich sowohl auf Informationen und Daten als auch auf das gesamte IT-System. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. Das gilt entsprechend für die Integrität von Daten. Zum anderen bezieht sich der Begriff Integrität auch auf IT-Systeme, da die Integrität der Informationen und Daten nur bei ordnungsgemäßer Verarbeitung und Übertragung sichergestellt werden kann.

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

3. Grundsätze

3.1 Bedeutung der Informationssicherheit

Im Geschäftsbereich SMWA ist es das Ziel, dass alle 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 SMWA und ist durch geeignete Maßnahmen sicherzustellen.

3.2 Standards des Bundesamtes für Sicherheit in der Informationstechnik

Zur Erreichung und Aufrechterhaltung eines angemessenen und ausreichenden Informationssicherheitsniveaus sind für die Behörden des Geschäftsbereichs SMWA die Handlungsanweisungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) maßgeblich. 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 zu ermitteln und mit geeigneten Sicherheitsmaßnahmen zu gewährleisten.

3.3 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 harmonisch in diese einfügen.

3.4 Wirtschaftlichkeit

Die Sicherheitsmaßnahmen müssen 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, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden innerhalb und außerhalb der Verwaltung, Beeinträchtigungen des Ansehens der Behörden des Geschäftsbereichs SMWA und die Folgen von Gesetzesverstößen.

Das Kriterium der wirtschaftlichen Angemessenheit ist nicht anwendbar, soweit Sicherheitsmaßnahmen erforderlich sind, um rechtliche Anforderungen oder Vorgaben erfüllen zu können.

3.5 Subsidiarität

Vorgaben des SMWA zu Sicherheitszielen können von den nachgeordneten Behörden im Geschäftsbereich SMWA entsprechend den individuellen Anforderungen präzisiert und ergänzt werden. Sie dürfen aber nicht im Widerspruch zu den Vorgaben des SMWA stehen.

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

3.6 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 Beschäftigten des Geschäftsbereichs SMWA bekannt gemacht.

Neuen Beschäftigten wird diese Leitlinie bekannt gemacht, bevor sie Zugang zu geschäftsrelevanten Informationen erhalten.

4. Informationssicherheitsziele

4.1 Verfügbarkeit

Für alle IT-Verfahren sind die Zeiten, in denen sie verfügbar sein sollen, zu bestimmen. Für regelmäßige Betriebsunterbrechungen, die aus technischen, organisatorischen oder sicherheits- relevanten Gründen notwendig sind, sind Zeiten festzulegen.

4.2 Vertraulichkeit

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.

4.3 Integrität

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.

4.4 Weitere Informationssicherheitsziele

Die einzelnen Behörden können über Verfügbarkeit, Vertraulichkeit und Integrität hinaus weitere Sicherheitsziele formulieren.

5. Verantwortlichkeiten

5.1 Behördenleitung

Die Behördenleitung trägt für ihren Bereich die Gesamtverantwortung hinsichtlich der Gewährleistung eines angemessenen Informationssicherheitsniveaus. Sie stellt sicher, dass diese Leitlinie in allen Punkten zielführend umgesetzt wird. Sie erlässt hierfür verbindliche Regeln zur Informationssicherheit, deren Geltungsbereich sich auch auf die nachgeordneten Behörden erstrecken kann, und gibt sie allen Beschäftigten bekannt.

5.2 Führungskräfte

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.

5.3 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 vertraglichen Verpflichtungen.

5.4 Beschäftigung externer Leistungserbringer

Personen, Behörden und Unternehmen, die nicht dem Geschäftsbereich SMWA angehören, für diesen aber Leistungen erbringen, haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie einzuhalten. 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.

6. Informationssicherheitsorganisation

Zur Erreichung der Informationssicherheitsziele wird eine Sicherheitsorganisation nach Maßgabe der folgenden Festlegungen eingerichtet.

6.1 Beauftragter für Informationssicherheit

Die Hausleitung des SMWA delegiert im Rahmen ihrer Gesamtverantwortung die Wahrnehmung der Aufgaben der Informationssicherheit auf den Beauftragten für Informationssicherheit (BfIS). Der BfIS berät und unterstützt die Hausleitung in allen Angelegenheiten der Informationssicherheit.

In den nachgeordneten Behörden soll von der Behördenleitung jeweils ein BfIS benannt werden. Solange keine Bestellung erfolgte, wird die Aufgabe vom Behördenleiter wahrgenommen.

Zu den Aufgaben des BfIS gehören:

- Steuerung des Informationssicherheitsprozesses und Mitwirkung bei allen damit zusammenhängenden Aufgaben,
- Überprüfung der Umsetzung der Vorgaben zur Informationssicherheit,
- Erstellung, Fortschreibung und Umsetzung des 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 sicherzustellen.

6.2 IS-Management-Team

Im SMWA wird ein Management-Team für Informationssicherheit (IS-Management-Team) gebildet.

Das IS-Management-Team setzt sich zusammen aus:

- dem BfIS, der den Vorsitz hat, und
- den für den IT-Service zuständigen Beschäftigten des Referates 14

als ständige Mitglieder sowie – soweit eine Fachanwendung betroffen ist –

- mindestens einem vom BfIS zugezogenen Vertreter der betroffenen Fachreferate

als nichtständiges Mitglied.

Das IS-Management-Team unterstützt den BfIS 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.

In den nachgeordneten Behörden können ebenfalls IS-Management-Teams gebildet werden.

7. Sicherheitskonzeption

Jede Behörde entwickelt ein Sicherheitskonzept. Es wird auf Grundlage der BSI-Standards und der BSI-Grundschutz-Kataloge sowie der Festlegungen dieser Leitlinie erstellt.

Das Sicherheitskonzept ist stets auf dem aktuellen Stand zu halten und den sich verändernden

Rahmenbedingungen anzupassen.

Das Sicherheitskonzept umfasst mindestens folgende Aspekte:

- IT-Strukturanalyse,
- Feststellung und Dokumentation des Schutzbedarfs,
- IT-Grundschutzanalyse,
- Ergänzende Sicherheitsanalyse ab einem hohen Schutzbedarf,
- Festlegung zweckdienlicher Maßnahmen,
- Regelmäßige Überprüfung des Sicherheitskonzepts.

8. Verstöße gegen die Informationssicherheitsleitlinie

Verhalten, das die Sicherheit von Daten, Informationen, IT-Systemen oder der Netze gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden. Bei Vorliegen der jeweiligen Voraussetzungen kann das Verhalten zudem als Ordnungswidrigkeit oder Straftat verfolgt werden.

Beschäftigte, die die Sicherheit von Daten, Informationen, IT-Systemen oder des Netzes gefährden und einen Schaden für den Freistaat oder einen Dritten verursachen, können darüber hinaus nach den gesetzlichen Regelungen zum Schadenersatz herangezogen werden oder einem Rückgriffanspruch ausgesetzt sein.

9. Revision

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 Wirtschaft, Arbeit und Verkehr über die geltenden Verwaltungsvorschriften des Staatsministeriums für Wirtschaft, Arbeit und Verkehr

vom 1. Dezember 2017 (SächsABl.SDr. S. S 402)