Verwaltungsvorschrift der Sächsischen Staatsregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung (VwV Informationssicherheit)

Vom 7. September 2011

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 und die Informationssicherheitsorganisation sind in der Anlage ausgeführt.

II. Geltungsbereich

Die Verwaltungsvorschrift gilt für die Behörden und Einrichtungen des Freistaates Sachsen, nicht jedoch für die Gerichte, die Hochschulen, die Schulen in kommunaler Trägerschaft, die Forschungseinrichtungen, den Verfassungsgerichtshof des Freistaates Sachsen, den Rechnungshof, die Verwaltung des Landtags und den Sächsischen Datenschutzbeauftragten. Die Vorgaben sind entsprechend der jeweiligen Aufgabenverantwortung umzusetzen und auszugestalten.

III. Inkrafttreten

Diese Verwaltungsvorschrift tritt am Tage nach ihrer Veröffentlichung in Kraft.

Dresden, den 7. September 2011

Der Ministerpräsident
Stanislaw Tillich

Der Staatsminister der Justiz und für Europa
Dr. Jürgen Martens

Anlage
(zu Ziffer I Satz 2)

Leitlinie der Sächsischen Staatsregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung (Leitlinie Informationssicherheit)

Inhaltsübersicht

1 Einleitung

Auf dem Weg in das Informationszeitalter werden Staat, Wirtschaft und Gesellschaft zunehmend durch die immer intensiver werdende Nutzung moderner Informationstechnik (IT) geprägt. Informationsinfrastrukturen gehören heute neben Straßen, Wasser- und Stromleitungen zu den nationalen Infrastrukturen, ohne die das private wie das berufliche Leben zum Stillstand käme.

Durch die verstärkte Abhängigkeit von moderner Kommunikationstechnik hat sich das Risiko der Beeinträchtigung von Informationsinfrastrukturen und deren Komponenten durch vorsätzliche Angriffe von innen und außen, fahrlässiges Handeln, Nachlässigkeiten, Ignoranz, Unkenntnis und potenzielles Versagen der Technik sowohl qualitativ als auch quantitativ deutlich erhöht.

Unter Beachtung der rechtlichen und wirtschaftlichen Rahmenbedingungen sowie der Anforderungen aus ihren Geschäftsprozessen hat die Landesverwaltung effizient, wirtschaftlich, nachvollziehbar und dienstleistungsorientiert zu handeln. Jede Beeinträchtigung der Informationssicherheit kann zu einer Störung dieser Arbeitsweise führen, die Leistungsfähigkeit der Landesverwaltung mindern und im Extremfall die Geschäftsprozesse zum Erliegen bringen.

Vor diesem Hintergrund ist eine angemessene Informationssicherheit in den Geschäftsprozessen der Landesverwaltung zu organisieren. Danach sind organisatorische Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit zu schaffen, ein Informationssicherheitsmanagement einzurichten, Standards zur Informationssicherheit einschließlich der Definition von Verantwortlichkeiten und Befugnissen zu erarbeiten, Komponenten zur Steigerung der Informationssicherheit zu standardisieren und alle Sicherheitsvorkehrungen und Sicherheitsmaßnahmen hinreichend zu dokumentieren.

Die vorliegende Leitlinie beschreibt die allgemeinen Ziele, Strategien und Organisationsstrukturen, welche für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind.

2 Grundsätze und Ziele der Informationssicherheit

2.1 Grundsätze

2.1.1 Begriffseinführung

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 bedeutet:
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 (wer, wann, wie lange und dergleichen) 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. Verfügbarkeit: Die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen stehen dem Anwender zum geforderten Zeitpunkt zur Verfügung.

2.1.2 Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Zur Erreichung und Aufrechterhaltung eines angemessenen und ausreichenden Informationssicherheitsniveaus sind für die Landesverwaltung die Standards und Kataloge des BSI in der jeweils aktuellen Fassung maßgeblich.

2.1.3 Bedeutung der Informationssicherheit beim Einsatz von IT

In der Landesverwaltung 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 Bereich der Landesverwaltung und ist mit technischen und organisatorischen Maßnahmen verbindlich sicherzustellen.

2.1.4 Informationssicherheit als Leistungsmerkmal von IT-Verfahren

Die Informationssicherheit ist ein zu bewertendes und herbeizuführendes Leistungsmerkmal von IT-Verfahren. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist auf den IT-Einsatz zu verzichten. Belange der Informationssicherheit sind zu berücksichtigen bei:

a) der Entwicklung und Einführung von IT-Verfahren,

b) der Beschaffung und Beseitigung oder Entsorgung von IT-Produkten,

c) dem Betrieb und der Pflege von IT-Verfahren und

d) der Nutzung von Diensten Dritter.

2.1.5 Informationssicherheit als Leistungsmerkmal der Organisation

Bei der Gestaltung von technischen und organisatorischen Sicherheitsmaßnahmen ist darauf zu achten, dass diese stets integraler Bestandteil der Vorgänge sind und nicht Erweiterungen, die über das vermeintlich Notwendige hinausgehen. Belange der Informationssicherheit sind zu berücksichtigen bei:

a) der Gestaltung der Organisation,

b) der Schaffung und Besetzung von Rollen,

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.

2.1.6 Wirtschaftlichkeit

Die für die Umsetzung der erforderlichen und angemessenen Sicherheitsmaßnahmen notwendigen Ressourcen und Investitionsmittel sind im Rahmen der Einzelpläne der zuständigen Ressorts bereit zu stellen. 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, Beeinträchtigungen des Ansehens der Landesverwaltung und die Folgen von Gesetzesverstößen.

2.1.7 Regelungskompetenz und Subsidiarität

Die einzelnen 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. Durch Richtlinien des Beauftragten für Informationssicherheit des Landes (BfIS Land), die vom Lenkungsausschuss IT und E-Government (LA ITEG) zu bestätigen sind, werden grundsätzlich Belange von

übergeordnetem Interesse geregelt und Mindeststandards zur Informationssicherheit definiert. Die Vorgaben des BfIS Land können entsprechend den individuellen Anforderungen präzisiert und ergänzt sowie den besonderen Bedürfnissen der einzelnen Behörden und Einrichtungen angepasst werden.

2.1.8 Sicherheit vor Verfügbarkeit

Wenn Angriffe auf die Sicherheit der IT- Infrastruktur des Freistaates Sachsen drohen oder bekannt werden oder sonstige Sicherheitsrisiken auftreten, kann die Verfügbarkeit von Informations- und Kommunikationstechnik, IT-Anwendungen, Daten und Netzwerken entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit der gesamten Verwaltung ist der Schutz vor Schäden vorrangig. Vertretbare Einschränkungen in Bedienung und Komfort sind hinzunehmen. Dies gilt in besonderem Maße für die Übergänge zu anderen Netzwerken, insbesondere zum Internet.

2.1.9 Prinzip des informierten Beschäftigten

Die Beschäftigten sind im erforderlichen Umfang bezüglich der Informationssicherheit zu sensibilisieren und zu qualifizieren.

2.2 Informationssicherheitsziele

2.2.1 Verfügbarkeit

Für alle IT-Verfahren sind die Zeiten, in denen sie verfügbar sein sollen, festzulegen. Störungsbedingte Ausfälle sind in diesen Zeiten weitgehend zu vermeiden, das heißt nach Zahl und Dauer zu begrenzen. Die Beschreibung der notwendigen Verfügbarkeit umfasst:

a) die regelmäßigen Betriebszeiten,

b) die Zeiten mit erhöhter Verfügbarkeitsanforderung und

c) die maximal tolerierbare Dauer einzelner Ausfälle.

Ebenfalls festzulegen sind regelmäßig geplante Betriebsunterbrechungen, insbesondere zu Wartungszwecken.

2.2.2 Vertraulichkeit

Die in allen IT-Verfahren erhobenen, gespeicherten, verarbeiteten und weitergegebenen Daten sind vertraulich zu behandeln und jederzeit vor unbefugtem Zugriff zu schützen. Zu diesem Zweck ist für alle Daten der Personenkreis, dem der Zugriff gestattet werden soll, zu bestimmen. Der Zugriff auf IT-Systeme, IT-Anwendungen und Daten sowie Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken. Jeder Beschäftigte erhält eine Zugriffsberechtigung nur auf die Daten, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt.

2.2.3 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.

2.2.4 Weitere Informationssicherheitsziele

Die einzelnen Behörden und Einrichtungen können über Verfügbarkeit, Vertraulichkeit und Integrität hinaus weitere Sicherheitsziele formulieren, zum Beispiel Nachvollziehbarkeit und Authentizität.

3 Verantwortlichkeiten und Rollen

3.1 Verantwortung der Leitungsebene

Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für die Informationssicherheit hat die Leitung der Behörde oder Einrichtung (Behördenleitung). Sie oder die vorgesetzte Dienstbehörde erlässt die erforderlichen Regelungen zur Informationssicherheit für den Bereich der Behörde. Die aktuellen Regelungen sind den Beschäftigten bekannt zu geben. Eine Möglichkeit zur Kenntnisnahme der aktuellen Regelungen ist jederzeit sicherzustellen. Die Behördenleitung trägt die Verantwortung für die Umsetzung der vereinbarten Sicherheitsmaßnahmen und eine geeignete Dokumentation. Sie stellt die Mittel für die Beschaffung und den Betrieb der vereinbarten Sicherheitsmaßnahmen zur Verfügung und veranlasst erforderliche Schulungsmaßnahmen. Die Behörden und Einrichtungen sind für eine dem jeweiligen Aufgabengebiet angemessene Informationssicherheit selbst verantwortlich.

3.2 Verantwortung der Beschäftigten

Alle Beschäftigte gewährleisten die Informationssicherheit durch ihr verantwortungsvolles Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Sie gehen korrekt und verantwortungsbewusst mit den von ihnen genutzten IT-Systemen, Daten und Informationen um.
Verhalten, das die Sicherheit von Daten, Informationen, IT-Systemen oder der Netze gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden. Unter Umständen kann das Verhalten als Ordnungswidrigkeit oder Straftat verfolgt werden. Beschäftigte, die die Sicherheit von Daten, Informationen, IT-Systemen oder des Netzes gefährden und einen Schaden für das Land oder einen Dritten verursachen, können darüber hinaus nach den gesetzlichen Regelungen zum Schadenersatz herangezogen werden oder einem Rückgriffsanspruch ausgesetzt sein.
Folgende Sachverhalte können Straftaten darstellen:

a) das unbefugte Verschaffen von Daten anderer, die nicht für sie 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.

Verstöße gegen die Informationssicherheit sind von den Beschäftigten unverzüglich dem zuständigen BfIS im Ressort zu melden.
Als Verstöße gelten insbesondere Handlungen, die aufgrund einer Abweichung von der Leitlinie oder den Richtlinien für Informationssicherheit:

a) Behörden oder Einrichtungen des Freistaates Sachsen materielle oder immaterielle Schäden zufügen,

b) den unberechtigten Zugriff auf Informationen, deren Preisgabe oder Änderung zulassen,

c) die Nutzung von Behördeninformationen für illegale Zwecke beinhalten oder

d) eine Kompromittierung des Ansehens des Freistaates Sachsen zur Folge haben.

Bei Gefahr im Verzug wegen ressortübergreifender Sicherheitsvorfälle ordnet der BfIS Land die erforderlichen Sicherheitsmaßnahmen kurzfristig an. Dies kann bis zur vorübergehenden Sperrung von Anwendungen oder Netzzugängen führen. Die betroffene Behördenleitung sowie der zuständige BfIS sind hiervon unverzüglich zu unterrichten. Entstehende Kosten für die Abschaltung und die Wiederanschaltung hat die verursachende Behörde oder Einrichtung zu tragen.

3.3 Fachverantwortlicher

Der Fachverantwortliche für einen Geschäftsprozess oder ein IT-Fachverfahren ist zuständig für:

a) die Festlegung der geschäftlichen Relevanz seiner Informationen und deren Schutzbedarf und

b) die Sicherstellung, dass Verantwortlichkeiten explizit definiert und Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz seiner Informationen umgesetzt werden.

Der Fachverantwortliche muss den Zugang auf Informationen sowie den Umfang und die Art der Autorisierung definieren, die im jeweiligen Verfahren erforderlich ist. Bei diesen Entscheidungen ist Folgendes zu berücksichtigen:

a) die Notwendigkeit, die Informationen entsprechend ihrer geschäftlichen Relevanz zu schützen,

b) die Aufbewahrungsvorschriften und die mit den Informationen verbundenen rechtlichen Anforderungen und

c) inwieweit die für die jeweiligen Geschäftsanforderungen erforderlichen Informationen zugänglich sein müssen.

3.4 Beschäftigung externer Leistungserbringer

Personen, Behörden und Unternehmen, die nicht zur Landesverwaltung gehören, für diese 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.

4 Informationssicherheitsorganisation

4.1 Beauftragte für Informationssicherheit (BfIS)

Die zentrale Sicherheitsinstanz ist der BfIS Land. Er ist im Staatsministerium der Justiz und für Europa angesiedelt und für alle ihm vom LA ITEG übertragenen operativen und koordinierenden Belange der Informationssicherheit zuständig. Die Gesamtverantwortung der Ressorts für die Informationssicherheit im Rahmen ihrer Ressortverantwortung bleibt davon unberührt.
In jeder obersten Landesbehörde ist ein BfIS zu ernennen. Dieser ist für alle operativen und koordinierenden Belange und Fragen der Informationssicherheit in seinem Verantwortungsbereich zuständig. Es ist sicherzustellen, dass diesem Beschäftigten dauerhaft ein angemessener Anteil seiner Arbeitszeit für die Erledigung seiner Aufgaben als BfIS zur Verfügung steht.

Die Behörden und Einrichtungen können in ihren Zuständigkeitsbereichen weitere BfIS ernennen oder extern beauftragen. Falls erforderlich, können weitere BfIS für bestimmte Bereiche, Projekte und Systeme ernannt werden. Aufgrund der besonderen Stellung in der Landesverwaltung werden für die Polizei und den Staatsbetrieb Sächsische Informatik Dienste (SID) je ein hauptamtlicher BfIS ernannt.
Im jeweiligen Zuständigkeitsbereich haben die BfIS folgende Aufgaben:

a) Steuerung des Informationssicherheitsprozesses und Mitwirkung bei allen damit zusammenhängenden Aufgaben,

b) Überprüfung der Umsetzung der Vorgaben zur Informationssicherheit,

c) Erstellung, Fortschreibung und Umsetzung des Sicherheitskonzeptes,

d) Vorschlag von neuen Sicherheitsmaßnahmen und -strategien,

e) Vertretung der Behörde oder Einrichtung in den Angelegenheiten der Informationssicherheit,

f) Ansprechpartner für die Beschäftigten in den Fragen der Informationssicherheit,

g) Koordination von Sensibilisierungs- und Schulungsmaßnahmen,

h) Zusammenfassung von bereichs-, projekt- oder systemspezifischen Informationen und Weiterleitung an den zuständigen BfIS der Arbeitsgruppe Informationssicherheit (AG IS) und

i) Meldung von besonders sicherheitsrelevanten Zwischenfällen.

4.2 Arbeitsgruppe Informationssicherheit (AG IS)

Das koordinierende Gremium für alle ressortübergreifenden Aspekte der Informationssicherheit ist die AG IS. Die AG IS besteht aus dem BfIS Land als Vorsitzenden, den BfIS der Staatskanzlei, der Staatsministerien, der Polizei und des SID. Weitere Mitglieder können auf Antrag aufgenommen werden.
Die Mitglieder der AG IS bringen die für ihren Bereich spezifischen Aspekte und Anliegen ein. Ihre Arbeit ist von dem Willen getragen, im Interesse der Informationssicherheit gemeinsame Lösungen zu finden. Sie sorgen für eine geeignete Sicherheitsorganisation und für die Umsetzung der Leitlinie und der Richtlinien für Informationssicherheit innerhalb ihres Zuständigkeitsbereiches. Die AG IS beobachtet laufend die technischen und organisatorischen Fortentwicklungen im Bereich der Informationssicherheit und schlägt notwendige Maßnahmen vor. Die Mitglieder der AG IS müssen dazu über die nötige technische und organisatorische Kompetenz verfügen und in der Lage sein, die erforderlichen Maßnahmen in ihrem Zuständigkeitsbereich umzusetzen.
Die AG IS berät den LA ITEG und den Arbeitskreis für IT und E-Government (AK ITEG) zu Fragen der Informationssicherheit. Die von der AG IS getroffenen Empfehlungen werden dem AK ITEG vorgelegt.

4.3 Sicherheitsnotfallteam

Das Sicherheitsnotfallteam (Computer Emergency Response Team – CERT) ist im SID

angesiedelt und wird vom BfIS des SID geleitet. Besondere Aufgaben des CERT sind:

a) das Aufzeigen von Lösungen bei konkreten Sicherheitsvorfällen,

b) die Mitwirkung als koordinierende Instanz für Informationssicherheit,

c) die Information zu Sicherheitslücken und

d) die Unterstützung zur Beseitigung von Sicherheitsrisiken.

Das Team unterstützt die BfIS als Ansprechpartner in technischen Sicherheitsfragen.

4.4 Informationssicherheitsmanagementteams

Um die Belange der Informationssicherheit bei allen strategischen Entscheidungen und Einzelmaßnahmen mit möglichen Auswirkungen auf die Informationssicherheit sicherzustellen, können in den Behörden und Einrichtungen grundsätzlich Informationssicherheitsmanagementteams eingerichtet werden. Diese unterstützen den BfIS bei der Erfüllung seiner Aufgaben.

5 Umsetzung

Auf der Grundlage dieser Leitlinie und der für die gesamte Landesverwaltung geltenden Richtlinien für Informationssicherheit haben die Ressorts eigene ressortspezifische Informationssicherheitsrichtlinien, Informationssicherheitskonzepte und weitere Regelungen zur Informationssicherheit im erforderlichen Umfang zu gestalten.

6 Sicherung und Verbesserung der Informationssicherheit

Der Informationssicherheitsprozess wird regelmäßig auf seine Aktualität und Wirksamkeit überprüft. Insbesondere werden die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Beschäftigten bekannt, umsetzbar und in den Betriebsablauf integrierbar sind. Die Leitungsebenen unterstützen die ständige Verbesserung des Sicherheitsniveaus. Die Beschäftigten sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheit zu verbessern und ständig auf dem aktuellen Stand zu halten.

Zuletzt enthalten in

Verwaltungsvorschrift der Sächsischen Staatsregierung über die geltenden Verwaltungsvorschriften der Staatsregierung
vom 13. Dezember 2013 (SächsABl.SDr. S. S 802)