Schleswig-Holstein
Der echte Norden

Schleswig-Holstein
Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung

Schleswig-Holsteinischer Landtag
Umdruck 19/4668

Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung | Postfach 71 51 | 24171 Kiel

Der Staatssekretär

An den
Vorsitzenden des Finanzausschusses
des Schleswig-Holsteinischen Landtages
Herrn Stefan Weber, MdL
Landeshaus
24105 Kiel

Nachrichtlich:
Frau Präsidentin
des Landesrechnungshofs
Dr. Gaby Schäfer
Berliner Platz 2
24103 Kiel

über das
Finanzministerium des
Landes Schleswig-Holstein
Düsternbrooker Weg 64
24105 Kiel

Ihr Zeichen:
Ihre Nachricht vom: /
Mein Zeichen: V 31 - 3169/2019
Meine Nachricht vom: 29.04.2019

gesehen
und weitergeleitet
Kiel, den 14.10.2020

2. Oktober 2020

Bemerkungen 2017 des Landesrechnungshofs Schleswig-Holstein mit Bericht zur Landeshaushaltsrechnung 2015; Bericht und Beschlussempfehlung des Finanzausschusses vom 01.12.2017, Drucksache 19/364;
hier: Aktuelle Nachberichterstattung zu unserem Bericht vom 29.04.2019

Sehr geehrter Herr Vorsitzender,

mit Beschluss vom 13. Dezember 2017 hat der Schleswig-Holsteinische Landtag in seiner 7. Tagung der Landesregierung für das Haushaltsjahr 2015 Entlastung erteilt mit der Maßgabe, die vom Finanzausschuss des Schleswig-Holsteinischen Landtages in der Drucksache 19/364 angeregten Maßnahmen einzuleiten und dem Finanzausschuss über die eingeleiteten Maßnahmen zu berichten.

Für meinen Geschäftsbereich hat der Finanzausschuss Voten zu Tz. 12 (Betreuung der IT-Arbeitsplätze) und Tz. 13 (Sicherheitsmanagement in der Landesverwaltung) abgegeben und um Berichte zu diesen Themen gebeten.

Die Antwort wurde im Finanzausschuss am 30.08.2018 (Umdruck 19/1216) behandelt. Beschlossen wurde, dass das Ministerium für Digitalisierung bis Ende des 1. Quartals 2019 erneut berichten soll. Diesem Auftrag bin ich mit Schreiben vom 29.04.2019 nachgekommen.

Zu Teilziffer 13 berichte ich heute ergänzend den aktuellen Sachstand, wie folgt:

Tz. 13: Gemeinsam zu mehr Informationssicherheit

Die zum letzten Berichtszeitpunkt noch im Entwurfsstadium befindliche Neufassung der Informationssicherheitsleitlinie (ISLL) für die Landesverwaltung wurde nunmehr vom Kabinett beschlossen und die neue ISLL am 24. August 2020 in Kraft gesetzt. Zu Ihrer Information füge ich die neue ISLL diesem Schreiben bei.

Wesentliche Inhalte des in meinem letzten Bericht genannten „Informationssicherheitsmanagement-Plans“ wurden in die Leitlinie selbst integriert.

Mit freundlichen Grüßen
gez. Tobias Goldschmidt

SH Schleswig-Holstein
Der echte Norden

Informationssicherheitsleitlinie für die Landesverwaltung Schleswig-Holstein

Inhalt

1 Einleitung und Zielsetzung

Modernes Verwaltungshandeln ist in hohem Maße abhängig von zuverlässig und ordnungsgemäß funktionierender Informationsverarbeitung. Das Ziel der Informationssicherheit ist es, Informationen jeglicher Art und Herkunft zu schützen, insbesondere die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen und ihrer Verarbeitung zu gewährleisten. IT-Sicherheit als Teilmenge der Informationssicherheit konzentriert sich auf den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.

Die Digitalisierung der Verwaltungsarbeit in den Landesbehörden in Schleswig-Holstein nimmt stetig zu. Gleichzeitig ist ein stetiger Anstieg von Bedrohungen der informationsverarbeitenden Systeme festzustellen. Durch die zunehmenden Bedrohungen steigen die Anforderungen an die Gewährleistung der Informationssicherheit, wobei die Gefährdungen der Informationssicherheit sowohl technische als auch nicht-technische, insbesondere organisatorische, Aspekte umfassen. Es besteht die Herausforderung, die Informationssicherheit in allen Bereichen der Landesverwaltung aufrecht zu erhalten und im Lichte der sich ständig ändernden Gefährdungslage kontinuierlich zu verbessern und dabei den Grundsatz der Wirtschaftlichkeit zu beachten.

Die Landesregierung stellt sich dieser Herausforderung und bekennt sich mit dieser Leitlinie deutlich sichtbar zu ihrer Verantwortung für die Gewährleistung von Informationssicherheit in der Landesverwaltung.

Mit dieser Leitlinie legt die Landesregierung den übergreifenden Rahmen der Informationssicherheit verbindlich fest. Grundlage ist ein umfassendes Informations-sicherheitsmanagement auf Basis des IT-Grundschutzes und der entsprechenden Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie der entsprechenden ISO-Normenreihe zur Informationssicherheit.

Mit der vorliegenden Informationssicherheitsleitlinie wird die bisherigen Leitlinie zur IT-Sicherheit[1] in Schleswig-Holstein fortgeschrieben und damit zugleich den geänderten rechtlichen Rahmenbedingungen Rechnung getragen.

2 Geltungsbereich

Diese Leitlinie gilt in der unmittelbaren Landesverwaltung Schleswig-Holstein.

Im Landesrechnungshof und beim Präsidenten des Landtages Schleswig-Holstein findet diese Leitlinie keine Anwendung. Diese Behörden können die Regelungen in ihrem Zuständigkeitsbereich jedoch für anwendbar erklären.

Diese Leitlinie findet im Bereich der Justiz keine Anwendung, sofern die Regelungen des IT-Gesetzes für die Justiz des Landes Schleswig-Holstein (ITJG) und die auf dieser Grundlage getroffenen Bestimmungen und Regelungen dem entgegenstehen.

[1] IT-Sicherheitsleitlinie für die IT-Basisinfrastruktur der Schleswig-Holsteinischen Landesverwaltung vom 20.07.2010.

Anderen Trägern der öffentlichen Verwaltung steht die Anwendung dieser Leitlinie offen.

Diese Leitlinie gilt als übergreifender Mindeststandard. Sie kann seitens einzelner Einrichtungen durch Regelungen hinsichtlich höherer Anforderungen oder weiterer Maßnahmen ergänzt werden. Sofern sich aus bestehenden Regelungen zusätzliche oder weitergehende Anforderungen an die Informationssicherheit ergeben, bleiben diese unberührt.

3 Rechtliche Grundlagen

Die vom IT-Planungsrat auf Grundlage des IT-Staatsvertrags verabschiedete Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung[2] verpflichtet die Länder zur Erstellung einer Informationssicherheitsleitlinie und zum Aufbau eines Informationssicherheitsmanagementsystems auf Basis des BSI-IT-Grundschutzes. Durch die gemeinsame Leitlinie für Informationssicherheit von Bund und Ländern soll sichergestellt werden, dass dem jeweiligen Schutzziel angemessene und dem Stand der Technik sowie dem Grundsatz der Wirtschaftlichkeit entsprechende Sicherheitsmaßnahmen ergriffen werden, um das Eintreten von Sicherheitsvorfällen weitestgehend zu verhindern und mögliche Schäden zu minimieren. Es wird ein Sicherheitsniveau angestrebt, das festgelegten Mindestanforderungen genügt und keine hohen Risiken akzeptiert.

Für die Verarbeitung personenbezogener Daten stellen insbesondere die Vorschriften der Europäischen Datenschutzgrundverordnung (DSGVO) seit dem Inkrafttreten am 25.05.2018, das Bundes- sowie das Landesdatenschutzgesetz SH (LDSG) ergänzende Anforderungen.

Gemäß Organisationserlass ITSH (OrgErl ITSH)[3], Ziffer 4.5, koordiniert die oder der Chief Information Officer (CIO) das integrierte Sicherheitsmanagement des Landes Schleswig-Holstein. Zudem ist gemäß Ziffer 5.8 des OrgErl ITSH das Zentrale IT-Management (ZIT SH) in unmittelbarer Abstimmung mit der oder dem CIO zuständig für das integrierte Sicherheitsmanagement des Landes Schleswig-Holstein. Diese Zuständigkeit schließt Konzeption und Planung des Sicherheitsprozesses, die Erstellung, Fortschreibung und Umsetzung der IT-Sicherheitsleitlinie sowie die Leitung und Koordination des Informationssicherheitsmanagements ein. Das ZIT SH kann in Fragen der IT-Sicherheit abschließende Maßgaben erteilen und deren Umsetzung kontrollieren.

Im Anwendungsbereich der CIO-Rahmenvorgabe Standardrollen ITSH[4] haben die jeweiligen IT-Verantwortlichen die Aufgabe, in allen Phasen der IT-Leistungs-

[2] Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung vom 19.02.2013 sowie deren Fortschreibung vom 06.12.2018, IT-Planungsrat-Beschlüsse 2013/01 vom 08.03.2013 und 2019/04 vom 12.03.2019.

[3] OrgErl ITSH NEU (Stand 01.05.2018).

[4] Landeseinheitliche Rahmenvorgabe des CIO des Landes Schleswig-Holstein von Standardrollen für Planung und Umsetzung von IT-Vorhaben/-Verfahren in der Landesverwaltung Schleswig-Holstein.

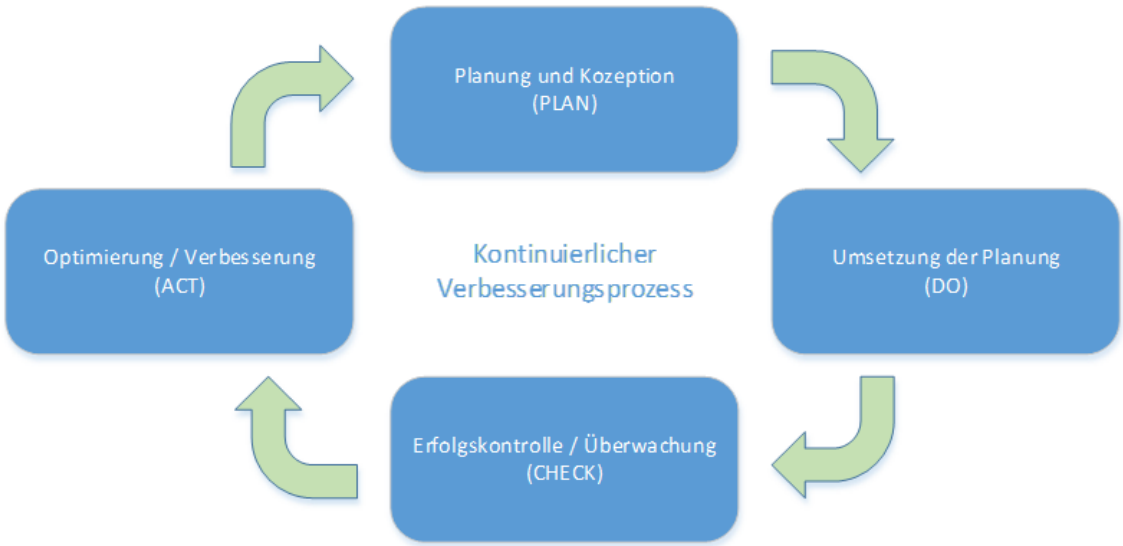
erbringung in Bezug auf das von ihnen verantwortete IT-Verfahren die Belange der IT-Sicherheit zu berücksichtigen und zu gewährleisten.

4 Grundsätze der Informationssicherheit

Zur Sicherung und Weiterentwicklung des Informationssicherheitsniveaus wird ein Informationssicherheitsmanagementsystem (ISMS) mit entsprechender Dokumentation sowie relevanten Prozessen eingeführt. Das ISMS wird im Rahmen der nachfolgend beschriebenen Organisation der Informationssicherheit von der oder dem zentralen Informationssicherheitsbeauftragten für die Landesverwaltung mit Unterstützung der dezentralen Informationssicherheitsbeauftragten umgesetzt. Alle im Geltungsbereich dieser Leitlinie beteiligten Behörden haben dafür Sorge zu tragen, dass die abgestimmten ressortübergreifenden Vorgaben und Standards eingehalten werden. Diese können durch eigene Vorgaben und Standards erweitert werden, wobei die vorgegebenen Mindeststandards nicht unterschritten werden dürfen.

Die Festlegungen der Mindestsicherheitsstandards leiten sich ab aus den Bestimmungen des BSI-IT-Grundschutzes in der jeweils aktuellen Fassung, aus der entsprechenden ISO 2700x-Normenreihe und deren Umsetzungsempfehlungen sowie aus den datenschutzrechtlichen Anforderungen. Die entsprechenden Anforderungen der Rechnungshöfe[5] sowie vorgegebene Mindeststandards im Rahmen der Bund-/Länder-Zusammenarbeit sind zu berücksichtigen.

Das Vorgehen im ISMS folgt einem ganzheitlichen PDCA-Modell (Plan-Do-Check-Act, Planung-Durchführung-Überprüfung-Aktualisierung):



[5] Etwa https://www.bundesrechnungshof.de/de/veroeffentlichungen/broschueren/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informations-und-kommunikationstechnik

Die ISMS-Dokumente und -Prozesse sind anlassbezogen sowie im Sinne eines kontinuierlichen Verbesserungsprozesses regelmäßig einer Überprüfung (Review) zu unterziehen. Bei identifiziertem Änderungsbedarf müssen die Dokumente und/oder Prozesse angepasst werden.

Um die Informationssicherheit aufrechtzuerhalten und kontinuierlich zu verbessern, bedarf es aufbau- und ablauforganisatorischer, rechtlicher, finanzieller und technischer Maßnahmen. Für die Aufstellung und Planung dieser Maßnahmen werden im Rahmen der festgelegten Organisationsstruktur Informationssicherheits-risiken betrachtet, beurteilt und entsprechend der Kritikalität priorisiert. Die Umsetzung der Maßnahmen zur Erlangung und Aufrechterhaltung des erforderlichen Sicherheitsniveaus wird in entsprechenden Richtlinien, Prozessen, Dokumentationen und Arbeitsanweisungen verankert und erfolgt unter Berücksichtigung der Wirtschaftlichkeit – bezogen auf den jeweiligen Schutzzweck – der zu ergreifenden Maßnahmen.

Soweit Dritte als Auftragnehmer für die öffentliche Verwaltung Leistungen erbringen, sind diese bei der Auftragserteilung auf die Vorgaben der Leitlinie zur Informationssicherheit im notwendigen Umfang zu verpflichten.

5 Ziele der Informationssicherheit

Um eine ordnungsgemäße und sichere Informationsverarbeitung für die hoheitlichen und sonstigen Aufgaben sicherzustellen, basiert die Informationssicherheit des Landes Schleswig-Holstein auf den drei folgenden Zielen zum Schutz von Informationen und Daten sowie den zur Verarbeitung erforderlichen Systemen, Netzen und deren Lokationen. Bei Verarbeitung personenbezogener Daten handelt es sich dabei gleichzeitig um Datenschutzziele.

Gewährleistung der Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Gewährleistung der Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.

Gewährleistung der Verfügbarkeit

Die Verfügbarkeit von Informationen, Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen ist vorhanden, wenn diese stets wie vorgesehen verarbeitet und genutzt werden können.

Zur Erfüllung dieser Ziele müssen Schutzbedarfe bezüglich der Vertraulichkeit, Integrität und Verfügbarkeit für Informationen sowie deren Verarbeitung ermittelt werden. Anhand der ermittelten Schutzbedarfe müssen risikoorientiert Maßnahmen

geplant und umgesetzt werden. Bei IT-Vorhaben und -Verfahren sind Schutzbedarfsfeststellung und Maßnahmenplanung Aufgaben der jeweiligen IT-Verantwortlichen gemäß Standardrollenmodell ITSH. Dabei werden sie von dem jeweils zuständigen Informationssicherheitsmanagement unterstützt.

Auf der Basis dieser Maßnahmen ist das erforderliche Sicherheitsniveau aufrecht zu erhalten. Bei IT-Vorhaben und -Verfahren trifft diese Verpflichtung sowohl die IT-Verantwortlichen als auch diejenigen, die das IT-Verfahren nutzen.

Weiterhin bestehen als zentrale Ziele für die Informationssicherheit:

- die Wirkung von Sicherheitsmaßnahmen zu stärken,
- eine lückenlose Umsetzung der Informationssicherheitskonzepte,
- die Umsetzung der speziellen datenschutzrechtlichen Anforderungen,
- die Unterstützung des Notfallmanagements im Zusammenhang mit der Verfügbarkeit von Systemen durch proaktive und reaktive Sicherheits-maßnahmen.

Für die Aufrechterhaltung der Informationssicherheit und die Erreichung der Ziele gilt der Grundsatz der Wirtschaftlichkeit. Alle Maßnahmen der Informationssicherheit müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen stehen. Die Bereitstellung von ausreichenden zeitlichen und finanziellen Ressourcen obliegt dem jeweiligen Verantwortungs-bereich.

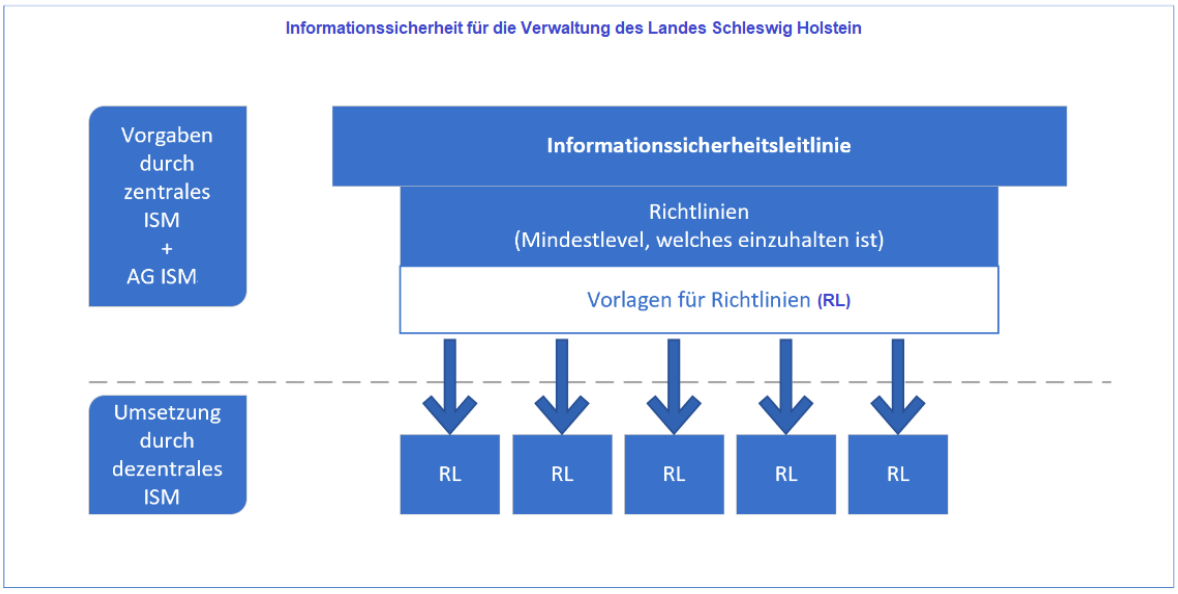
Die Behörden können unter Einhaltung der landesweiten Vorgaben weitere, beispielsweise aus der DSGVO resultierende Sicherheitsziele für ihre Organisation definieren.

6 Dokumentation der Informationssicherheit

Die Informationssicherheitsleitlinie für die Landesverwaltung Schleswig-Holstein ist die Basis für die weiterführende Dokumentation im ISMS. Auf Basis der Vorgaben und Ziele der Leitlinie werden zentrale Richtlinien formuliert, die ein Mindestniveau vorgeben. Mit Hilfe darauf aufbauender Vorlagen können die Behörden und Einrichtungen im Geltungsbereich dieser Leitlinie die eigenen Richtlinien erstellen bzw. aktualisieren.

Das vorgegebene Mindestniveau ist auch in den nachgeordneten Dokumenten einzuhalten und wird in regelmäßigen Dokumentenreviews überprüft. Weitere Konzepte basieren auf der gleichen Hierarchiesystematik und sind dement-sprechend einzuordnen.

Hinsichtlich der Informationssicherheit nehmen die IT-Verantwortlichen und datenverarbeitenden Stellen ihre dokumentarischen Aufgaben und Zuständigkeiten im Rahmen des ISMS wahr.



7 Organisation der Informationssicherheit

Die Organisation des landesweiten ISMS im Geltungsbereich dieser Leitlinie gliedert sich in einen zentralen ressortübergreifenden Bereich, angesiedelt im ZIT SH, und in die dezentralen Bereiche, angesiedelt in der Staatskanzlei und den Ressorts. Es wird eine gemeinsame Strategie zur Informationssicherheit verfolgt und gemeinsam das hierin festgelegte Mindestniveau der Informationssicherheit gewährleistet.

7.1 Informationssicherheitsbeauftragte/r für die Landesverwaltung (Chief Information Security Officer, CISO)

Im ZIT SH wird eine Informationssicherheitsbeauftragte oder ein Informationssicherheitsbeauftragter für die Landesverwaltung (Chief Information Security Officer, CISO) bestellt. Es gibt eine Stellvertretung. Die Bestellung erfolgt durch die für das ZIT SH zuständige Staatssekretärin oder den für das ZIT SH zuständigen Staatssekretär.

Die oder der CISO ist in die Linienorganisation im ZIT SH eingeordnet. Um die erforderliche Eigenständigkeit zu gewährleisten, ist die oder der CISO in Ausübung ihrer oder seiner Tätigkeit fachlich weisungsfrei und hat ein direktes Vortragsrecht bei der für das ZIT SH zuständigen Staatssekretärin oder dem für das ZIT SH zuständigen Staatssekretär.

In Umsetzung und Konkretisierung des Organisationserlasses ITSH, insbesondere Ziffer 5.8, steuert die oder der CISO federführend das ressortübergreifende Informationssicherheitsmanagement und leitet den ressortübergreifenden Informationssicherheitsbereich im ZIT SH.

Die Aufgaben der oder des CISO im Geltungsbereich dieser Leitlinie umfassen insbesondere:

- Planung und Steuerung des landesweiten Informationssicherheits-managements im Sinne des OrgErl ITSH,
- Initiierung und Koordinierung der Erstellung und Fortschreibung des ressortübergreifenden Informationssicherheitskonzepts,
- Mitarbeit bei der Erstellung des IT-Notfallvorsorgekonzepts als Teil des ganzheitlichen Notfallvorsorgekonzepts,

- Erarbeitung von landeseinheitlichen Richtlinien und Regelungen zur Informationssicherheit in Angelegenheiten übergreifender Bedeutung in Abstimmung mit dem Arbeitsgremium Informationssicherheitsmanagement und unter Einbeziehung der IT-Beauftragtenkonferenz (ITBK) bzw. der IT-Beauftragten der betreffenden Ressorts,
- Mitwirkung an der IT-Strategie und IT-Architektur der Landesverwaltung,
- Mitwirkung an strategischen Projekten,
- Erstellung von Berichten an die Landesregierung und an das Gremium zur Informationssicherheit über den Status der Informationssicherheit,
- Betrachtung der Bedrohungen und Risiken für die Informationssicherheit und Steuerung der daraus abgeleiteten übergreifenden Maßnahmen,
- Untersuchung sicherheitsrelevanter Ereignisse und Sachverhalte übergreifender Bedeutung, Analyse entsprechender Schwachstellen und Veranlassung entsprechender Schutzmaßnahmen,
- Überprüfung der Wirksamkeit und Umsetzung übergreifender Informationssicherheitsregelungen und -maßnahmen sowie entsprechende Beratung von IT-Verantwortlichen für deren Zuständigkeitsbereich,
- Initiierung und Steuerung oder Durchführung übergreifender Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit,
- in Zweifelsfällen die Auslegung der Dokumente im ISMS im Sinne der Ziele dieser Leitlinie,
- regelmäßige Prüfung auf Anpassungsbedarf und gegebenenfalls Fortschreibung dieser Informationssicherheitsleitlinie gemäß Ziffer 5.8 OrgErl ITSH in Abstimmung mit dem Arbeitsgremium Informationssicherheitsmanagement,
- Ausübung des Vorsitzes des Arbeitsgremiums Informationssicherheit,
- aktive Mitarbeit in der AG InfoSic des IT-Planungsrates als Vertreterin oder Vertreter des Landes Schleswig-Holstein,
- Funktion als Ansprechperson des Landes in übergreifenden Fragen der Informationssicherheit, soweit nicht im Einzelfall anders geregelt,
- Planung und Verwaltung des Budgets für die zentralen Maßnahmen der Informationssicherheit.

Der oder dem CISO sowie deren oder dessen Stellvertretung sind ausreichende Mittel und Möglichkeiten zur Ausübung ihrer oder seiner Tätigkeit zu gewähren. Das beinhaltet auch eine qualifizierte Aus- und Fortbildung in Themen der Informationssicherheit oder mit anderweitiger Relevanz für die Tätigkeit.

7.2 Informationssicherheitsbeauftragte (ISB)

Die Staatskanzlei und die Ministerien bestimmen jeweils eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten (ISB). Es gibt eine Stellvertretung. Entsprechendes gilt für jene obersten Landesbehörden im Geltungsbereich gemäß Ziffer 2 dieser Leitlinie, die diese Leitlinie für anwendbar erklären. Bei Bedarf können für weitere Organisationsbereiche zuständige Mitarbeiterinnen und Mitarbeiter für die Informationssicherheit benannt werden, beispielsweise bei Ämtern, die nach § 5 Abs. 2 LVwG einer obersten Landesbehörde zugeordnet sind, bei den Landesoberbehörden oder innerhalb eines organisatorisch selbstständigen Teils einer obersten Landesbehörde. Die oder der ISB stellt sicher, dass das Niveau der Informationssicherheit und das Informationssicherheitsmanagement in ihrem oder seinem Zuständigkeitsbereich aufrechterhalten und kontinuierlich verbessert wird. Dazu arbeitet er oder sie eng mit den IT-Verantwortlichen in seinem oder ihrem Bereich zusammen und berät diese bei ihrer Aufgabenwahrnehmung.

Bei der organisatorischen Zuweisung der Aufgaben sollen Interessenkonflikte vermieden werden. Der oder dem ISB sind ausreichende Zeitanteile zur Wahrnehmung ihrer oder seiner Aufgaben einzuräumen und die Möglichkeit zu angemessener Aus- und Fortbildung zu gewähren.

Die Aufgaben der ISB im jeweiligen Zuständigkeitsbereich umfassen insbesondere:

- Umsetzung der auf Basis der Informationssicherheitsleitlinie für die Landesverwaltung Schleswig-Holstein getroffenen Regelungen,
- Steuerung der Informationssicherheit sowie Initiierung von und Mitwirkung bei damit zusammenhängenden Maßnahmen und Aufgaben,
- Meldung von sicherheitsrelevanten Vorfällen; Näheres regelt eine Richtlinie zum Sicherheitsvorfallmanagement,
- Überprüfung der Wirksamkeit und Umsetzung der Informationssicherheitsregelungen und -maßnahmen sowie entsprechende Beratung von IT-Verantwortlichen für deren Zuständigkeitsbereich,
- Erstellung, Fortschreibung und Umsetzung des Sicherheitskonzeptes des Ressorts oder Bereichs,
- aktive Mitarbeit im Arbeitsgremium Informationssicherheitsmanagement als stimmberechtigtes Mitglied,
- Ansprechperson der Behörde in Angelegenheiten der Informationssicherheit,
- Koordination und gegebenenfalls Durchführung von Sensibilisierungs- und Schulungsmaßnahmen,
- Zusammenfassung einschlägiger bereichs-, projekt- oder systemspezifischer Informationen und Weiterleitung an die oder den CISO, gegebenenfalls Beratung im Arbeitsgremium Informationssicherheitsmanagement,
- Berichtet an die oder den CISO und im Arbeitsgremium Informationssicherheitsmanagement über Themen der Informationssicherheit aus dem

jeweiligen Zuständigkeitsbereich und ist diesbezüglich Ansprechperson für die oder den CISO.

Die Ressorts können die Aufgabe der oder des ISB unter Verlagerung entsprechender Stellenanteile an das ZIT SH übertragen.

7.3 Arbeitsgremium Informationssicherheitsmanagement (AG ISM)

Die Schnittstelle zwischen dem zentralen und den dezentralen Bereichen bildet das ressortübergreifende Arbeitsgremium Informationssicherheitsmanagement (AG ISM). Das AG ISM setzt sich mindestens aus der oder dem CISO (Vorsitz) und den benannten ISB der obersten Landesbehörden gemäß Ziffer 7.2 dieser Leitlinie zusammen. Das Gremium gibt sich eine Geschäftsordnung, in der auch Näheres zur Aufnahme weiterer Mitglieder und deren Stimmberechtigung geregelt werden kann.

Das AG ISM koordiniert landesweit die Maßnahmen der Informationssicherheit und sorgt für eine geeignete Informationssicherheitsorganisation sowie ein angemessenes Berichtswesen. Es kann Mindeststandards beschließen, die im betreffenden Geltungsbereich bindend sind und im Einklang mit dem OrgErl ITSH in Kraft gesetzt werden; Näheres regelt eine Richtlinie auf Basis dieser Leitlinie.

Die ISB und der oder die CISO tauschen sich im AG ISM regelmäßig über den Status der Informationssicherheit in ihren Zuständigkeitsbereichen aus.

7.4 Behördenleitung

Bei der Behördenleitung liegt die Gesamtverantwortung für die IT-Verfahren und die Informationssicherheit im jeweiligen Zuständigkeitsbereich. Bei Zentralen IT-Verfahren liegt die Verfahrensverantwortung bei der jeweiligen zentralen Stelle; hier ist eine dezentrale Behördenleitung im Sinne einer geteilten Verantwortung verantwortlich für die jeweilige dezentrale Umsetzung der zentralen Vorgaben und entsprechende Maßnahmen. Die Behördenleitung trägt dafür Sorge, dass die Mitarbeiterinnen und Mitarbeiter die entsprechenden Vorgaben und Anforderungen berücksichtigen. Im Sinne der Vorbildfunktion kommt dem eigenen Sicherheitsverhalten der Behördenleitung besondere Bedeutung zu.

Die Behördenleitung veranlasst in ihrem Zuständigkeitsbereich ergänzend zur Umsetzung der Regelungen des OrgErl ITSH, dass

- bei obersten Landesbehörden gemäß Ziffer 7.2 dieser Leitlinie eine oder ein ISB samt Stellvertretung für diese oberste Landesbehörde benannt werden,
- bei Bedarf weitere Mitarbeitende für die Informationssicherheit samt deren jeweiliger Zuständigkeit benannt werden,
- die erforderlichen personellen und finanziellen Ressourcen für eine angemessene Informationssicherheit zur Verfügung gestellt werden,
- die übergreifenden Regelungen zur Informationssicherheit sowie gegebenenfalls die ergänzenden Regelungen im Ressort umgesetzt werden,

- die Wirksamkeit und Umsetzung der Informationssicherheitsregelungen sowie -maßnahmen regelmäßig überprüft werden
- bedarfsgerechte Risikoanalysen zu den Aufgaben der Informationsverarbeitung des jeweiligen Zuständigkeitsbereichs durchgeführt werden,
- die Verantwortlichkeiten im Umgang mit Informationen definiert und gegenüber den Mitarbeiterinnen und Mitarbeitern kommuniziert werden.

Die Behördenleitung lässt sich regelmäßig über den Stand der Informationssicherheit in ihrem Zuständigkeitsbereich berichten. Sie entscheidet im Rahmen der zentralen Vorgaben über die Umsetzung angemessener Sicherheitsmaßnahmen und übernimmt für verbleibende Restrisiken die Verantwortung.

7.5 Mitarbeiterinnen und Mitarbeiter

Informationssicherheit muss durchgehend über alle organisatorischen Ebenen gewährleistet sein. Mitarbeiterinnen und Mitarbeiter sind im Rahmen ihrer allgemeinen Dienstpflichten dafür verantwortlich, Vorgaben zur Informationssicherheit in ihrem Arbeitsbereich zu beachten und einzuhalten. Hierzu müssen die Informationssicherheitsleitlinie und die – gegebenenfalls mitbestimmungspflichtigen – mitgeltenden Richtlinien, Arbeitsanweisungen und sonstige Vorgaben allen Mitarbeiterinnen und Mitarbeitern in jeweils geeigneter Weise bekannt gemacht werden.

Sicherheitsrelevante Ereignisse sind umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können; Näheres regelt eine Richtlinie zum Sicherheitsvorfallmanagement.

Den Mitarbeiterinnen und Mitarbeitern sind ausreichende Mittel und Möglichkeiten zur qualifizierten Aus- und Fortbildung in Themen der Informationssicherheit zu gewähren. Dies gilt auch für die spezifische Aus- und Fortbildung der IT-Verantwortlichen im Rahmen ihrer Zuständigkeit bei IT-Vorhaben und -Verfahren.

7.6 Computer Emergency Response Team (CERT Nord)

Bei dem Landes-IT-Dienstleister ist ein Computer Emergency Response Team (CERT Nord) zur Unterstützung bei Maßnahmen zur Informationssicherheit, insbesondere dem Sicherheitsvorfallmanagement, eingerichtet. Relevante Sicherheitsvorfälle müssen dem CERT Nord gemeldet werden; Näheres regelt eine Richtlinie zum Sicherheitsvorfallmanagement. Das CERT Nord berichtet anlassbezogen und regelmäßig über Themen der Informationssicherheit in seinem Bereich an das zentrale Informationssicherheitsmanagement der Landesverwaltung.

7.7 Landes-IT-Dienstleister

Der Landes-IT-Dienstleister als Betreiber wesentlicher Infrastrukturen und Dienste spielt eine zentrale Rolle bei der Gewährleistung der Informationssicherheit im

Auftrag des Landes. Der Landes-IT-Dienstleister berichtet anlassbezogen und regelmäßig über Themen der Informationssicherheit in seinem Bereich an das zentrale Informationssicherheitsmanagement der Landesverwaltung.

8 Schlussbestimmungen

8.1 Bekanntgabe

Diese Informationssicherheitsleitlinie ist allen Mitarbeiterinnen und Mitarbeitern in geeigneter Weise bekannt zu gegeben.

8.2 Überprüfung

Diese Informationssicherheitsleitlinie soll entsprechend den Vorgaben der BSI-Standards in regelmäßigen Abständen, möglichst alle zwei Jahre, auf ihre Aktualität und Wirksamkeit überprüft werden. Die erste derartige Überprüfung ist binnen zwei Jahren nach Inkrafttreten vorzunehmen.

8.3 Inkrafttreten

Diese Informationssicherheitsleitlinie tritt mit ihrer Unterzeichnung in Kraft und löst die bisher bestehende Leitlinie „IT-Sicherheitsleitlinie für die IT-Basisinfrastruktur der Schleswig-Holsteinischen Landesverwaltung“ ab

Kiel, den

Jan Philipp Albrecht