Informationssicherheitsleitlinie für den Sächsischen Landtag

Vom 3. Juli 2019

Inhaltsübersicht

Präambel

Staat, Wirtschaft und Gesellschaft werden durch die immer intensivere Nutzung moderner Informationstechnik (IT) geprägt. Informationsinfrastrukturen gehören heute neben Straßen, Wasser- und Stromleitungen zu den nationalen Infrastrukturen, ohne die das berufliche und das private Leben zum Stillstand kämen. Auch für den Sächsischen Landtag wäre eine effektive parlamentarische Arbeit ohne geeignete Informationsinfrastruktur nicht mehr denkbar.

Der Freistaat Sachsen stellt mit dem Sächsischen Verwaltungsnetz eine Informationsinfrastruktur bereit. Diese steht einem Verbund staatlicher und nichtstaatlicher Stellen, dem der Sächsische Landtag einschließlich seiner gewählten Mitglieder und deren Beschäftigten, der Fraktionen und deren Mitarbeitern und seiner Verwaltung angehört, zur Nutzung zur Verfügung. Das Sächsische Verwaltungsnetz gilt es gegen Angriffe auf die Informationssicherheit und auf die IT-Sicherheit zu schützen, um sowohl die Vertraulichkeit und die Integrität der gespeicherten Daten als auch die Verfügbarkeit und die Funktionsfähigkeit der Informations- und Kommunikationssysteme sicherzustellen.

Um die Informationssicherheit im Freistaat Sachsen zu erhöhen und Gefahren für informationstechnische Systeme abzuwehren, hat der Sächsische Landtag ein Gesetz zur Gewährleistung der

Informationssicherheit im Freistaat Sachsen (Sächsisches Informationssicherheitsgesetz) beschlossen. Es trägt der verfassungsmäßigen Stellung des Sächsischen Landtages Rechnung, indem es den Sächsischen Landtag nur teilweise in seinen Geltungsbereich einbezieht und ihm im Übrigen die Verpflichtung auferlegt, sich eine Informationssicherheitsleitlinie zu geben.

Mit der Informationssicherheitsleitlinie hat der Sächsische Landtag nicht nur für sich selbst ein angemessenes Sicherheitsniveau festzulegen, sondern darüber hinaus auch sicherzustellen, dass sich seine Schutzmechanismen wirkungsvoll in das Gesamtsystem, welches sich aus der Einbindung in das Sächsische Verwaltungsnetz zum einen und aus dem vom Sächsischen Informationssicherheitsgesetz vorgegebenen Rahmen zum anderen ergibt, eingliedert. Die vorliegende Informationssicherheitsleitlinie basiert auf der bereits seit dem Jahre 2014 in der Landtagsverwaltung etablierten Leitlinie zur Gewährleistung der IT-/Informationssicherheit für den Sächsischen Landtag.

1 Bedeutung der IT-/Informationssicherheit für den Sächsischen Landtag

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. Auch der Sächsische Landtag ist diesen Risiken ausgesetzt.

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

Die Informationssicherheitsleitlinie beschreibt die allgemeinen Ziele, Strategien und Organisationsstrukturen, welche für die Initiierung und Etablierung eines ganzheitlichen IT-/Informationssicherheitsprozesses erforderlich sind. Sie bildet außerdem den Rahmen für spezifische Sicherheitskonzepte und Organisationsanweisungen des Sächsischen Landtages im Bereich der IT-/Informationssicherheit, insbesondere für das IT-Sicherheitskonzept und das Notfallkonzept.

2 Geltungsbereich

Diese Informationssicherheitsleitlinie gilt

- für jegliche Informations- und Kommunikationstechnik, die über die IT-Infrastruktur des Sächsischen Landtages an das Sächsische Verwaltungsnetz angebunden ist und
- von den Mitgliedern des Sächsischen Landtages (nachfolgend: Abgeordnete) und deren Beschäftigten, den Fraktionen des Sächsischen Landtages (nachfolgend: Fraktionen) und deren Beschäftigten sowie von den Beschäftigten der Landtagsverwaltung genutzt wird.

Externe, die vom Sächsischen Landtag, von Abgeordneten, den Fraktionen beziehungsweise der Landtagsverwaltung mit der Erbringung von Leistungen im Zusammenhang mit Informations- und Kommunikationstechnik beauftragt werden, haben die Vorgaben dieser Informationssicherheitsleitlinie ebenfalls einzuhalten. Sie sind dazu vom jeweiligen Auftraggeber auf die Einhaltung dieser Informationssicherheitsleitlinie vertraglich zu verpflichten.

3 Grundsätze und Ziele der IT-/Informationssicherheit

3.1 Grundsätze

3.1.1 Begriffseinführung

IT-/Informationssicherheit: IT-/Informationssicherheit bezeichnet einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. Die IT-/Informationssicherheit umfasst die Sicherheit der IT-Systeme und der darin gespeicherten Daten.

Vertraulichkeit: Vertrauliche Informationen, Daten 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 et cetera) sowie die Daten über den Sende- und Empfangsvorgang.

Integrität: Integrität heißt Vollständigkeit und Korrektheit. Der Begriff der Integrität bezieht sich auf

Informationen, Daten und gesamte IT-Systeme. Die Integrität der Daten kann nur bei ordnungsgemäßer Verarbeitung und Übertragung sichergestellt werden.

Vollständigkeit: Vollständigkeit setzt voraus, dass alle Teile der Information verfügbar sind.

Korrektheit: Korrekt sind Daten, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben.

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

3.1.2 IT-/Informationssicherheitsstandards

Für das IT-Sicherheitskonzept, das Notfallkonzept, die Risikoanalysen und die weiteren Maßnahmen zur Erreichung und Aufrechterhaltung eines angemessenen und ausreichenden IT-/Informationssicherheitsniveaus gelten grundsätzlich die Standards und Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der jeweils aktuellen Fassung.

3.1.3 IT-/Informationssicherheit als Leistungsmerkmal von IT-Verfahren

Die IT-/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 IT-/Informationssicherheit sind zu berücksichtigen bei:

- der Entwicklung und Einführung von IT-Verfahren
- dem Betrieb und der Pflege von IT-Verfahren
- der Beschaffung und Beseitigung/Entsorgung von IT-Produkten
- der Nutzung von Diensten Dritter

3.1.4 IT-/Informationssicherheit als Leistungsmerkmal der Organisation

Bei der Gestaltung von technischen und organisatorischen Sicherheitsmaßnahmen ist darauf zu achten, dass diese stets integraler Bestandteil der Prozesse sind. Belange der IT-/Informationssicherheit sind zu berücksichtigen bei:

- der Gestaltung der Organisation
- der Schaffung und Besetzung von Rollen
- der Führung von Mitarbeitern
- dem Bereich Aus- und Weiterbildung
- der Gestaltung von Arbeitsabläufen
- der Zusammenarbeit mit anderen Behörden und Externen
- der Auswahl und dem Einsatz von Arbeits- und Hilfsmitteln

3.1.5 Ressourcenbereitstellung und Ausstattung

Für die Umsetzung der in dieser Leitlinie beschriebenen erforderlichen und angemessenen Sicherheitsmaßnahmen sind die notwendigen Ressourcen und Investitionsmittel und die erforderlichen Haushaltsmittel bereitzustellen. Zu bewerten sind besonders die Auswirkungen auf die physische und psychische Unversehrtheit von Menschen, bestimmbare finanzielle Schäden und die Beeinträchtigung des Ansehens des Sächsischen Landtages.

3.1.6 Sicherheit vor Verfügbarkeit

Bei Bedrohung der IT-/Informationssicherheit des Sächsischen Landtages kann die Verfügbarkeit von Informations- und Kommunikationstechnik, IT-Anwendungen, Daten und Netzwerken entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit des gesamten Hauses ist der Schutz vor Schäden vorrangig. Vertretbare Einschränkungen in Bedienung und Komfort sind hinzunehmen. Dies gilt insbesondere für alle Übergänge zu anderen Netzwerken.

3.1.7 Prinzip des informierten Nutzers

Die Nutzer sind bezüglich der IT-/Informationssicherheit wiederkehrend zu sensibilisieren und fortwährend zu qualifizieren. Die aktuellen Regelungen sind den Nutzern bekannt zu machen und regelmäßig in Erinnerung zu rufen.

3.2 IT-/Informationssicherheitsziele

Alle Einrichtungen, die der Erstellung, Speicherung, Aufbewahrung und Übertragung von Daten dienen, sind so auszuwählen, zu integrieren und zu konfigurieren, dass für die auf ihnen verarbeiteten Daten zu jeder Zeit und unter allen Umständen das angemessene Maß an Verfügbarkeit, Vertraulichkeit und Integrität sichergestellt ist. Die Einhaltung dieser Anforderungen ist unabdingbarer Bestandteil jedes Einsatzes von Informations- und Kommunikationstechnik.

3.2.1 Verfügbarkeit

Für jedes IT-Verfahren sind die Zeiten, in denen es verfügbar sein soll, festzulegen.

Die Beschreibung der notwendigen Verfügbarkeit umfasst:

- die regelmäßigen Betriebszeiten
- die Zeiten mit erhöhter Verfügbarkeitsanforderung
- die maximal tolerierbare Dauer einzelner Ausfälle

Ebenfalls festzulegen sind Konditionen planbarer Ausfallzeiten.

3.2.2 Vertraulichkeit

Die in allen IT-Verfahren erhobenen, gespeicherten, verarbeiteten und weitergegebenen Daten sind zu klassifizieren. Dementsprechend ist der zugriffsberechtigte Personenkreis zu bestimmen. Der Zugriff auf IT-Systeme, IT-Anwendungen und Daten sowie Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken. In diesem Zusammenhang sind vor allem die mit der parlamentarischen Arbeit verbundenen Besonderheiten zu beachten.

3.2.3 Integrität

Alle IT-Verfahren sollen stets aktuelle und vollständige Informationen liefern, eventuelle verfahrens- oder informationsverarbeitungsbedingte Einschränkungen sind zu dokumentieren. Entsprechend ihrer Klassifizierung sind Daten gegen unbeabsichtigte Veränderung und Verfälschung zu schützen.

3.2.4 Festlegungen

Die Festlungen zur Verfügbarkeit, Vertraulichkeit und Integrität erfolgen im IT-Sicherheitskonzept und im Notfallkonzept.

4 Verantwortlichkeiten

4.1 Verantwortlichkeit der Leitungsebene

Der Präsident des Sächsischen Landtages ist für eine angemessene IT-/Informationssicherheit des Sächsischen Landtages in seiner Gesamtheit und insbesondere als Teilnehmer im Sächsischen Verwaltungsnetz verantwortlich.

Verantwortlich sind des Weiteren

- für die Bereiche der Fraktionen der jeweilige Fraktionsvorsitzende oder ein von ihm benannter Verantwortlicher (Abgeordneter oder leitender Angestellter als akkreditierter Fraktionsmitarbeiter),
- die Abgeordneten für ihre Bereiche,
- für den Bereich der Landtagsverwaltung der Direktor beim Landtag.

4.2 Verantwortung des Nutzers

Im Übrigen ist jeder Nutzer dafür verantwortlich, dass die IT-/Informationssicherheit in dem von ihm beeinflussbaren Bereich durch verantwortungsvolles Handeln gewährleistet wird. Er hat die für die IT-/Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen einzuhalten sowie korrekt und verantwortungsbewusst mit den genutzten Informationen, Daten und IT-Systemen umzugehen.

5 IT-/Informationssicherheitsorganisation

Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung und damit auch für die Informationssicherheit verbleibt beim Präsidenten des Sächsischen Landtages. In gleicher Weise ist der Direktor des Sächsischen Landtages verantwortlich für die Informationssicherheit in der Verwaltung, die Abgeordneten für die Informationssicherheit im Rahmen ihrer Mandatsausübung, die Fraktionsvorsitzenden für die Informationssicherheit in den Fraktionen, soweit von den Fraktionsvorsitzenden hierfür nicht andere Verantwortliche benannt werden. Die Verantwortung erstreckt sich jeweils auch auf die Beschäftigten der jeweiligen Organisationseinheiten sowie gegebenenfalls auf Dritte, die als Auftragnehmer für die unter den Sätzen 1 und 2 Genannten Leistungen erbringen.

5.1 IT-/Informationssicherheitsbeauftragter

Für den Sächsischen Landtag wird durch den Präsidenten im Benehmen mit dem Präsidium ein Mitarbeiter der Landtagsverwaltung als IT- und Informationssicherheitsbeauftragter bestellt. Der IT- und Informationssicherheitsbeauftragte berichtet an den Direktor des Landtages und kann sich unmittelbar an den Präsidenten, das Präsidium und das Informationssicherheitsteam wenden. Der IT- und Informationssicherheitsbeauftragte ist zentrale IT-/Informationssicherheitsinstanz im Sächsischen Landtag. Er untersteht bei der Ausübung seiner Aufgaben nur dem Weisungsrecht des Präsidenten des

Sächsischen Landtages.

Der IT- und Informationssicherheitsbeauftragte hat insbesondere folgende Aufgaben:

- Unterstützung und Beratung der Verantwortlichen gemäß Nummer 4.1 in allen Fragen der Informationssicherheit,
- Ansprechpartner für die Nutzer zu den Fragen der IT-/Informationssicherheit,
- Aufbau, Betrieb und Weiterentwicklung der IT-/Informationssicherheitsorganisation und des dazugehörigen Managementprozesses,
- Steuerung des IT-/Informationssicherheitsprozesses,
- Überprüfung der Umsetzung der Vorgaben zur IT-/Informationssicherheit,
- Erstellung, Fortschreibung und Umsetzung des IT-Sicherheitskonzeptes und des Notfallkonzeptes,
- Vorschlag von neuen Sicherheitsmaßnahmen und -strategien,
- Analyse und Nachbearbeitung von IT-/Informationssicherheitsvorfällen,
- Unterstützung und Beratung der Beauftragten für Organisation bei allen Prozessen, Regelungen, Maßnahmen und so weiter, die Aspekte der IT-/Informationssicherheit berühren,
- Mitwirkung bei Beschaffungsmaßnahmen, die Auswirkungen auf die Sicherheit der Informationstechnik haben,
- Koordination von Sensibilisierungs- und Schulungsmaßnahmen,
- Maßnahmen nach § 13 Absatz 6, 7 des Sächsischen Informationssicherheitsgesetzes; diese sind im Einvernehmen zu treffen mit:
  1. dem Präsidenten des Sächsischen Landtages und dem jeweiligen Fraktionsvorsitzenden oder dessen benannten anderen Verantwortlichen im Rahmen der Betroffenheit der Fraktion,
  2. dem Präsidenten des Sächsischen Landtages und dem jeweiligen betroffenen Abgeordneten im Rahmen der Betroffenheit der Mandatsausübung,
  3. dem Direktor des Sächsischen Landtages gemeinsam mit einem weiteren Bediensteten mit Befähigung zum Richteramt im Rahmen der Betroffenheit der Verwaltung,
- Meldung von besonders sicherheitsrelevanten Zwischenfällen, insbesondere gemäß § 15 des Sächsischen Informationssicherheitsgesetzes; diese sind im Einvernehmen zu treffen mit:
  1. dem Präsidenten des Sächsischen Landtages und dem jeweiligen Fraktionsvorsitzenden oder dessen benannten anderen Verantwortlichen im Rahmen der Betroffenheit der Fraktion,
  2. dem Präsidenten des Sächsischen Landtages und dem jeweiligen betroffenen Abgeordneten im Rahmen der Betroffenheit der Mandatsausübung,
  3. dem Direktor des Sächsischen Landtages gemeinsam mit einem weiteren Bediensteten mit Befähigung zum Richteramt für die Fälle der Betroffenheit der Verwaltung.

5.2 IT-/Informationssicherheitsteam

Dem IT- und Informationssicherheitsbeauftragten steht ein IT-/Informationssicherheitsteam beratend zur Seite. Ihm gehören neben den vom Direktor entsandten Beschäftigten der Landtagsverwaltung je ein von jeder Fraktion benannter Abgeordneter und ein Abgeordneter als Stellvertreter an. Es darf je Fraktion ein als Mitarbeiter der Fraktion akkreditierter Berater gemeinsam mit dem jeweiligen Abgeordneten an den Sitzungen und Beratungen teilnehmen.

Die Mitglieder des IT-/Informationssicherheitsteams unterstützen den IT- und Informationssicherheitsbeauftragten auf dessen Verlangen hin.

Der IT-/Informationssicherheitsbeauftragte informiert das IT-/Informationssicherheitsteam regelmäßig über seine Arbeit, insbesondere über die Arbeit der Arbeitsgruppe Informationssicherheit.

6 Maßnahmen zur Sicherung und Verbesserung der IT-/Informationssicherheit

6.1 Allgemeine Maßnahmen

Die Verantwortlichen gemäß Nummer 4.1 gewährleisten für ihre Verantwortungsbereiche die Umsetzung dieser Richtlinie, stellen im Rahmen der verfügbaren Haushaltsmittel die Ressourcen für die Beschaffung und den Betrieb der vereinbarten und angeordneten Sicherheitsmaßnahmen zur Verfügung, veranlassen erforderliche Schulungsmaßnahmen und unterstützen einen auf die Verbesserung der IT-/Informationssicherheit gerichteten kontinuierlichen Prozess.

Der IT-/Informationssicherheitsprozess wird von den Verantwortlichen gemäß Nummer 4.1 regelmäßig auf seine Aktualität, Wirksamkeit und Einhaltung überprüft. Abweichungen vom angestrebten Sicherheits- und Datenschutzniveau werden mit dem Ziel analysiert, die IT-/Informationssicherheit zu verbessern und

ständig auf dem aktuellen Stand zu halten. Insbesondere werden die Maßnahmen daraufhin evaluiert, ob sie bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

Die Nutzer sind verpflichtet, dem IT- und Informationssicherheitsbeauftragten Unregelmäßigkeiten oder Schwachstellen im System zu melden und darüber hinaus angehalten mögliche Verbesserungen vorzuschlagen.

6.2 IT-Sicherheitskonzept, Notfallkonzept

Das Präsidium beschließt ein für den gesamten Geltungsbereich der Informationssicherheitsleitlinie verbindliches IT-Sicherheitskonzept und Notfallkonzept. Es soll entsprechend § 14 SächsISichG ausgestaltet werden.

Das IT-Sicherheitskonzept enthält eine Strukturanalyse aller im Sächsischen Landtag betriebenen IT-Systeme, Anwendungen, Infrastruktur-Komponenten und Räume sowie im Rahmen einer Schutzbedarfsfeststellung eine Bewertung hinsichtlich Verfügbarkeit, Vertraulichkeit sowie Integrität. Anhand eines Gefährdungskataloges enthält es aufbauend einen Basissicherheitscheck sowie eine erweiterte Sicherheitsanalyse in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität ab Schutzbedarf „hoch“.

Das Notfallkonzept analysiert und bewertet Unterbrechungen von Geschäftsprozessen, die Auswirkung auf den gesamten Landtag haben, sowie deren Schadensentwicklung. Es definiert Verfügbarkeitsanforderungen und legt den Übergang von der Störung zum Notfall fest. Es definiert Rollen und Verantwortlichkeiten sowie eine prioritäre Einstufung von Maßnahmen im Notbetrieb und beim Wiederanlauf.

6.3 Maßnahmen der Gefahrenabwehr

Der IT- und Informationssicherheitsbeauftragte ist berechtigt, die in § 12 Absatz 1 des Sächsischen Informationssicherheitsgesetzes vorgesehenen Maßnahmen im gesamten Geltungsbereich der Richtlinie zu ergreifen. Für die Verantwortlichen gemäß Nummer 4.1 gilt dies eingeschränkt auf den jeweiligen Verantwortungsbereich entsprechend.

Zur Abwehr von Gefahren für die IT-/Informationssicherheit ist der IT- und Informationssicherheitsbeauftragte nach Information der Betroffenen und im Einvernehmen mit den jeweiligen Verantwortlichen gemäß Nummer 4.1 berechtigt, alle erforderlichen Maßnahmen, bis hin zur Sperrung von Anwendungen oder Netzzugängen, zu ergreifen und anzuordnen.

Bei Gefahr in Verzug kann der IT- und Informationssicherheitsbeauftragte die Maßnahmen auch ohne vorherige Information der Betroffenen und Verantwortlichen gemäß Nummer 4.1 durchführen. Dabei hat er den Präsidenten des Landtages, den Direktor beim Landtag sowie den für den betroffenen Bereich Verantwortlichen gemäß Nummer 4.1 unverzüglich nachträglich von der Maßnahme zu unterrichten.

6.4 Weitere Maßnahmen bei Nichtbeachtung der Informationssicherheitsleitlinie

Bei schwerwiegenden oder wiederholten Verstößen gegen die Vorgaben der Informationssicherheitsleitlinie informiert der Präsident das Präsidium. Dieses entscheidet über weitergehende Maßnahmen.

Ein Verhalten, das die Ziele dieser Informationssicherheitsleitlinie gefährdet, kann von den Abgeordneten, den Fraktionen und der Landtagsverwaltung gegenüber den jeweiligen Beschäftigten disziplinar- oder arbeitsrechtlich geahndet werden.

Das Recht zur Geltendmachung von Schadensersatzansprüchen bleibt unberührt.

7 Inkrafttreten, Bekanntmachung

Die Informationssicherheitsleitlinie tritt am Tag nach ihrer Verkündung in Kraft.