Informationssicherheitsleitlinie für die Hessische Landesverwaltung (2016)

1. Vorbemerkung

Aus Gründen der Lesbarkeit und Übersichtlichkeit sowie in Orientierung an den grundsätzlichen Richtlinien zur deutschen Rechtschreibung werden im vorliegenden Dokument nicht an allen Stellen explizit geschlechtsneutrale Begriffe verwendet.
Soweit Begriffe, wie z.B. „der/die Mitarbeiter“ (Singular/Plural) verwendet werden, wird darunter immer der Einbezug beider Geschlechter verstanden.

Die Prozesse zur Aufgabenerfüllung in der hessischen Landesverwaltung werden durch Informationstechnologie (IT) unterstützt. Eine wichtige Rolle spielen dabei gemeinsam genutzte Infrastrukturen und Systeme. Damit wird ein Raum gemeinsamer Sicherheit und gemeinsamer Sicherheitsbedrohungen geschaffen.

Vor diesem Hintergrund ist ressort- und dienststellenübergreifend eine angemessene Informationssicherheit unabdingbar. Dazu sind

- organisatorische Rahmenbedingungen der Informationssicherheit aufrecht zu erhalten und weiter zu entwickeln,
- das Informationssicherheitsmanagement kontinuierlich zu verbessern,
- abgestimmte Sicherheitsstandards fortzuschreiben,
- Komponenten zur Gewährleistung der Informationssicherheit zu standardisieren und
- alle Sicherheitsvorkehrungen und -maßnahmen hinreichend zu dokumentieren.

Die Regelungen dieser Informationssicherheitsleitlinie werden vom zentralen Informationssicherheitsmanagement der Hessischen Landesverwaltung kontinuierlich weiterentwickelt.[1] Die Ressorts werden über den Arbeitskreis Informationssicherheit in das zentrale Informationssicherheitsmanagement einbezogen.

Die Regelungen der Informationssicherheitsleitlinie orientieren sich sowohl an den Grundschutz-Standards und der Grundschutzkataloge des BSI sowie der Informationssicherheitsleitlinie des Bundes und der Länder[2] als auch an den internationalen Normen DIN ISO/IEC 27001ff.

In dieser Leitlinie werden ressortübergreifend Rahmenvorgaben für Ziele und Grundsätze der Informationssicherheit definiert und die Art der Maßnahmen sowie die Anforderungen an die Organisationstrukturen (Aufbau- und Ablauforganisation) beschrieben.

2. Geltungsbereich und Begriffsbestimmungen

Die Informationssicherheitsleitlinie ist nach Inkraftsetzung durch die Ressorts für die hessische Landesverwaltung verbindlich.[3]

Die Staatskanzlei und die Ressorts können für ihren Zuständigkeitsbereich ergänzende und

---

[1] Beschluss der Hessischen Landesregierung über die Zuständigkeit der einzelnen Ministerinnen und Minister nach Artikel 104 Abs. 2 der Verfassung des Landes Hessen vom 28. März 2014 (Gesetz- und Verordnungsblatt für das Land Hessen, Teil I, S. 82); Stand Juli 2015: Hessisches Ministerium des Innern und für Sport

[2] http://www.it-planungsrat.de/DE/Entscheidungen/2013/10_Sitzung/10_Sitzung_Entscheidungen.html?nn=1852114#doc3348826bodyText1

[3] (vgl. Kapitel 7)

konkretisierende Regelungen treffen.

Informationstechnologie (IT) umfasst die Gesamtheit der genutzten technischen Systeme und Kommunikationstechnik und die auf dieser Basis realisierten fachlichen IT–Anwendungen.

IT-Verfahren: Unter IT-Verfahren wird die Summe aus einer oder mehrerer IT-Anwendungen und der zum Einsatz dieser Anwendung bzw. Anwendungen begleitenden Geschäftsprozesse verstanden. Diese können betrieblich und fachlich sein. Ziel ist es, fachliche Aufgaben zu realisieren.
IT-Verfahren ist ein Begriff, der vor allen Dingen im Umfeld der IT von Verwaltungen verwendet wird und in der Literatur ungebräuchlich ist. Hier wird IT-Verfahren synonym zu Informationssystem eingesetzt.

Die **Informationssicherheit im Sinne dieser Leitlinie** bezieht sich auf den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der Daten unter Berücksichtigung der datenschutzrechtlichen und sonstigen gesetzlichen Vorgaben.

Verfahrensverantwortlicher ist jede Person oder Organisationseinheit, der von der Ressortleitung die Verantwortung für die Kontrolle von Produktion, Entwicklung, Pflege, Gebrauch und Sicherheit von Daten und der sie verarbeitenden IT-Komponenten übertragen wurde (vgl. DIN ISO 27002 Nr. 7.1.2).

Zentraler Informationssicherheitsbeauftragter der Landesverwaltung (Chief Information Security Officer, **CISO**). Gemäß der Informationssicherheitsleitlinie des Bundes und der Länder müssen der Bund und alle Länder einen zentralen Informationssicherheitsbeauftragten benennen. Die Aufgaben und Befugnisse des CISO werden mit dieser Richtlinie beschrieben.

IT-Dienstleister im Sinne dieser Leitlinie sind alle Dienststellen **der hessischen Landesverwaltung** die IT zur Nutzung durch andere Dienststellen bereitstellen.

Der **Auftraggeber** eines IT-Projekts oder –Verfahrens schafft die finanziellen und organisatorischen Voraussetzungen, um mit einem **Auftragnehmer** (IT-Dienstleister) einen Vertrag abschließen zu können**.** Somit begleitet der Auftraggeber den kompletten Lebenszyklus von der Projektidee bis hin zur Einstellung eines IT-Verfahrens. Hierbei können zu bestimmten Phasen Aufgaben delegiert werden - z.B. an den Projektleiter oder den Verfahrensmanager – jedoch bleibt die Gesamtverantwortung immer bei dem Auftraggeber.

Sicherheitskonzepte im Sinne dieser Leitlinie beschreiben die zur Erreichung der Schutzziele in einem definierten Ausschnitt der IT notwendigen Maßnahmen. Dabei sind für alle Komponenten des Ausschnitts die spezifischen Gefährdungen aufzulisten und jeweils Maßnahmen zur Risikominderung bzw. Risikovermeidung zu beschreiben (Mindestanforderung IT-Sicherheitskonzept).

Sicherheitskonzepte sollen sich am BSI-Standard orientieren.

Für Ebenen-übergreifende IT-Verfahren im Sinne der Ziffer 3.3 der Informationssicherheitsleitlinie des Bundes und der Länder sind Sicherheitskonzepte nach BSI 100-2 zu erstellen und gemäß Ziffer 3.2 dieser Leitlinie beim direkten Anschluss an das gemeinsame Netz von Bund und Ländern im Sinne des IT-NetzG die BSI-Standards 100-1, 100-2, 100-3 und 100-4 umzusetzen.

Sicherheitsvorfall im Sinne dieser Leitlinie ist jedes Ereignis, das die Informationssicherheit

beeinträchtigt und in der Folge Schäden nach sich ziehen kann.

Der **Jahresbericht** zur Informationssicherheit dient der Information der Behördenleitung und des zentralen Informationssicherheitsmanagements / CISO zum Stand der Informationssicherheit im jeweiligen Zuständigkeitsbereich.

Der Jahresbericht beinhaltet mindestens folgende Punkte:

- Wesentliche organisatorische und personelle Änderungen im Bereich der Informationssicherheit
- Ergebnisse von Audits und der Kontrollen zur Einhaltung der Informationssicherheit nach 6.10
- Berichte über Sicherheitsvorfälle
- Berichte über bisherige Erfolge und Probleme im Informationssicherheitsprozess

CERT steht für Computer Emergency Response Team.[4]

3. Grundsätze der Informationssicherheit

In Abwägung der Werte der zu schützenden Informationen, der Risiken sowie des Aufwands an Personal und Finanzmitteln für Informationssicherheit soll für eingesetzte und geplante IT in der Hessischen Landesverwaltung ein angemessenes Informationssicherheitsniveau erreicht werden. Dabei sind die von der Landesregierung beschlossenen finanzpolitischen Leitlinien zu beachten. Notwendige Maßnahmen der Informationssicherheit sind zu beschreiben und von den jeweils Zuständigen in die Haushaltsplanung einzubringen.

Dabei sind die Mittel für die Wartung, Pflege und zyklische Erneuerung zu berücksichtigen.

Für IT, mit der Daten mit einem normalen Schutzbedarf verarbeitet werden, sind Sicherheitsmaßnahmen - ausgehend von den in dieser Leitlinie definierten Normen - vorzusehen und umzusetzen.

Für IT, mit der Daten mit einem hohen oder sehr hohen Schutzbedarf verarbeitet werden, muss eine ergänzende Sicherheitsanalyse durchgeführt werden. Die sich daraus ergebenen zusätzlichen Sicherheitsmaßnahmen sind zu berücksichtigen.

4. Ziele der Informationssicherheit

4.1 Für IT sind die Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität im jeweils erforderlichen Maße zu schützen. Bei der Anwendung der daraus abgeleiteten Sicherheitsmaßnahmen ist die Verhältnismäßigkeit zu wahren.[5]

4.2 Die Sicherheit der IT ist neben deren Leistungsfähigkeit und Funktionalität zu gewährleisten. Bleiben im Einzelfall nicht übernahmefähige Risiken, ist auf den Einsatz zu verzichten.

4.3 Bei Anbindung an das gemeinsame Netz von Bund und Ländern und das Betreiben von Ebenen-übergreifenden IT-Verfahren im Sinne der Ziffern 3.2 und 3.3 der Informationssicherheitsleitlinie des Bundes und der Länder[1] sind Rahmenbedingungen mit den Vertragspartnern außerhalb des Landes Hessen abzustimmen und weitestgehend zu vereinheitlichen.

---

[4] Die Aufgaben des CERT-Hessen werden unter 6.12 beschrieben.
[5] Ziffer 2 Absatz 1

5. Maßnahmen

5.1 Für alle IT-Systeme und -verfahren sind Sicherheitskonzepte einschließlich einer Schutzbedarfsfeststellung zu erstellen und aktuell zu halten. Dafür hat der Verfahrensverantwortliche zu sorgen.[6]

Die IT-Sicherheitsbeauftragten der Ressorts berichten dem CISO jährlich über die Vollständigkeit, Aktualität und den Umsetzungsstand der Sicherheitskonzepte der in Ihrem Zuständigkeitsbereich genutzten Verfahren.

Die Verfahrensverantwortlichen sind für die Umsetzung der Sicherheitskonzepte verantwortlich.

5.2 Die Beschäftigten aller Entscheidungsebenen gewährleisten die Informationssicherheit durch verantwortliches Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und Regelungen ein.

Für die regelmäßigen Informationen, Weiterbildung und Sensibilisierungsmaßnahmen werden in den Ressorts und im Programm der Zentralen Fortbildung des Landes Hessen entsprechende Angebote unterbreitet.

5.3 Alle Sicherheitsvorfälle[7] sind zu erfassen und der zuständigen Stelle im Ressort zu melden. Sicherheitsvorfälle, die andere Stellen beeinträchtigen können, sind den zuständigen Stellen im Ressort unverzüglich zu melden. Diese Meldungen sind zusätzlich an das CERT-Hessen weiterzuleiten.[8]

5.4 Der Zugriff auf IT ist auf den unbedingt erforderlichen Personenkreis zu beschränken.

Zugriffsberechtigungen werden nur zur Erfüllung von dienstlichen Aufgaben erteilt.

Die Erteilung und der Entzug von Zugriffsrechten werden von den Verfahrensverantwortlichen veranlasst und sind zu dokumentieren. Die Verfahrensverantwortlichen überprüfen die Notwendigkeit der erteilten Zugriffsrechte regelmäßig.

5.5 Durch regelmäßige IT-Krisenmanagement-Übungen wird das ressortübergreifende Zusammenspiel von Organisationen, Prozessen und Technologien der Informationssicherheit überprüft und weiterentwickelt.

6. Verantwortlichkeit, Koordination und Aufgaben

6.1 Die Verantwortung für eine angemessene Informationssicherheit im Geschäftsbereich trägt die Leitung des Ressorts. Sie stellt die erforderlichen personellen und finanziellen Ressourcen zur Verfügung

Die Leitung des Ressorts richtet Prozesse ein, mit denen die Eignung und Umsetzung der Sicherheitsmaßnahmen regelmäßig kontrolliert werden.

Die Dienststellenleitung trägt die Verantwortung für eine angemessene Informationssicherheit in dem ihr zugewiesenen Umfang.

---

[6] Die fachliche Zuständigkeit ergibt sich aus dem Beschluss der Landesregierung zur Zuständigkeit der Ministerinnen und Minister.

[7] Siehe Kapitel 2 „Begriffsbestimmungen“

[8] Sofortmeldung

6.2 Für die Landesverwaltung wird ein zentraler Informationssicherheitsbeauftragter der Landesverwaltung (Chief Information Security Officer, CISO) eingesetzt[9].

Für die Staatskanzlei und die Ressorts werden Informationssicherheitsbeauftragte eingesetzt.

Für jede nachgeordnete Dienststelle muss ein zuständiger Informationssicherheitsbeauftragte benannt werden. Dies kann der Informationssicherheitsbeauftragte des Ressorts oder eine andere von der Leitung des Ressorts bestimmte Stelle sein.

Bei der organisatorischen Zuweisung der Aufgaben sollen Interessenkonflikte vermieden werden.

6.3 Der für die Dienststelle zuständige Informationssicherheitsbeauftragte koordiniert die Maßnahmen zur Verbesserung der Informationssicherheit. Er und seine Vertretung werden im Geschäftsverteilungsplan ausgewiesen.[10]

Er kann sich unmittelbar an die Leitung der Dienststelle und den Informationssicherheitsbeauftragten des Ressorts wenden. Er berichtet beiden mindestens jährlich über den Stand der Informationssicherheit.

Der Informationssicherheitsbeauftragte ist für die Einhaltung von Meldepflichten nach 5.2 verantwortlich.

Die Verfahrensverantwortlichen informieren bei Verdacht von Informationssicherheitsvorfällen den zuständigen Informationssicherheitsbeauftragten unverzüglich.

Der Informationssicherheitsbeauftragte wird in seiner Arbeit durch die IT-Organisation seines Zuständigkeitsbereiches unterstützt. Er und die Vertretung bilden sich regelmäßig weiter. Sie werden darin von der Dienststelle unterstützt.

6.4 Der für die Staatskanzlei bzw. für ein Ressort eingesetzte Informationssicherheitsbeauftragte fördert die Belange der Informationssicherheit innerhalb des jeweiligen Ressorts und koordiniert entsprechende Maßnahmen.

Er hat ein unmittelbares Vortragsrecht bei der Leitung des Ressorts.

Er berichtet der Leitung der Ressorts und dem CISO mindestens einmal jährlich zum Stand der Informationssicherheit im Ressort.

Er ist für die Einhaltung der Meldepflichten zu Informationssicherheitsvorfällen im Ressort verantwortlich.

6.5 Der für die Landesverwaltung eingesetzte zentrale Informationssicherheitsbeauftragte (CISO) hat folgende Aufgaben, Verantwortungen und Kompetenzen:

1. Fortschreibung der Informationssicherheitsleitlinie des Landes in Abstimmung mit der Staatskanzlei und den Ressorts und kontinuierliche Verbesserung der Informationssicherheit in der Landesverwaltung,
2. Beratung des CIO, der Staatskanzlei und der Ressorts, Entwicklung von Empfehlungen für die Staatskanzlei und die Ressorts in Fragen der Informationssicherheit;
3. Koordinierung von landesweiten Informationssicherheits-Maßnahmen, Eskalationsinstanz für alle ressortübergreifenden Informationssicherheitsthemen,
4. Außenvertretung der hessischen Landesverwaltung in Belangen der Informationssicherheit, insbesondere in Ergänzung etablierter Strukturen

[9] Entspricht Ziffer 1.6.a des Umsetzungsplans zur Informationssicherheitsleitlinie des Bundes und der Länder
[10] Siehe 5.1 Abs. 1 und Abs. 4

5. Leitung des IT-Krisenmanagements der Landesverwaltung, Fachberater Informationstechnik im Landeskrisenstab.
6. Er hat ein unmittelbares Vortragsrecht bei der für die IT-Sicherheit des Landes zuständigen Ministerin oder dem für die IT-Sicherheit des Landes zuständigen Minister und bei der Beauftragten oder dem Beauftragten der Landesregierung für E-Government (CIO).

6.6 Der Informationssicherheitsbeauftragte arbeitet mit dem behördlichen Datenschutzbeauftragten und den IT-Verantwortlichen zusammen.

6.7 Die Beschäftigten melden informationssicherheitsrelevante Ereignisse unverzüglich den zuständigen Informationssicherheitsbeauftragten.

6.8 Der Auftraggeber hat die zur Einhaltung der Informationssicherheitsziele erforderlichen Sicherheitsanforderungen zu vereinbaren. Der Auftraggeber hat den Auftragnehmer zu verpflichten, bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren.

6.9 Wird von einem IT-Dienstleister angebotene IT eingesetzt, übernimmt die Leitung des Anbieters die Verantwortung für den Bereich der Informationssicherheit, den sie beeinflussen kann. Ergänzend liegt die Verantwortung für den Anteil der Informationssicherheit, der im Einflussbereich der nutzenden Dienststelle liegt, bei der Leitung dieser Dienststelle.

Die von einem IT-Dienstleister angebotenen IT-Querschnittsverfahren (z.B. E-Mail, Dokumentenmanagement usw.) erfüllen mindestens den Schutzbedarf normal. Stellen Anwender der Querschnittsverfahren fest, dass ggf. ein höherer Schutzbedarf erforderlich ist, sind diese Bedarfe in den IT-Standardisierungsprozess einzubringen. Die IT-Dienstleister bewerten im Rahmen dieses Prozesses die organisatorischen und finanziellen Auswirkungen. Über die Umsetzung entscheiden die entsprechenden Gremien.

6.10 Die Einhaltung der Informationssicherheit ist auf der Grundlage der jeweiligen Informationssicherheitskonzepte zu überprüfen.

Art und Umfang der Kontrolle sind durch die Leitung des Ressorts festzulegen. Die Informationssicherheitsbeauftragten der Ressorts berichten im Rahmen des Jahresberichts zum Stand der IT-Sicherheit über die Ergebnisse.

Die Überprüfung kann durch unabhängige Dritte erfolgen. In diesem Fall ist zu gewährleisten, dass diese Dritten zur Verschwiegenheit verpflichtet sind und mit der Überprüfung keine unzulässige Kenntnisnahme von Daten und Informationen verbunden ist.

6.11 Zur Koordination der landesweiten Sicherheitsprozesse und zur Unterstützung und Beratung der Informationssicherheitsbeauftragten in den Ressorts sowie zur Abstimmung und Koordination ressortübergreifender, gemeinsamer Maßnahmen zur Informationssicherheit richtet das HMdIS einen ständigen Arbeitskreis für die Informationssicherheitsbeauftragten der Ressorts ein (AK Informationssicherheit). Einzelheiten und die organisatorische Einbindung regelt eine Geschäftsordnung.

6.12 Im für die Grundlagen der Informationssicherheit zuständigen Ministerium[11] wird das CERT-Hessen betrieben.

Das CERT-Hessen informiert die Landesverwaltung über akute Bedrohungslagen und Sicherheitsdefizite in Soft- und Hardware-Produkten. Es erstellt ein werktägliches Lagebild zur Infor-

[11] Beschluss der Hessischen Landesregierung über die Zuständigkeit der einzelnen Ministerinnen und Minister nach Artikel 104 Abs. 2 der Verfassung des Landes Hessen vom 28. März 2014 (Gesetz- und Verordnungsblatt für das Land Hessen, Teil I, S. 82); Stand Juli 2015: hessisches Ministerium des Innern und für Sport

mationssicherheit, bewertet Sicherheitsbedrohungen und empfiehlt Maßnahmen zur Risikominderung und Schadensvermeidung.

Das CERT nimmt die Sofortmeldungen aus der Landesverwaltung über übergreifende Sicherheitsvorfälle entgegen und koordiniert deren Beseitigung durch die beteiligten Stellen.

Bei schwerwiegenden Bedrohungen beruft das CERT das IT-Krisenmanagement (IT-KM) der Landesverwaltung ein.

Alle Dienststellen und insbesondere die IT-Dienstleister unterstützen das CERT im Rahmen ihrer technischen, rechtlichen und personellen Möglichkeiten bei seinen Aufgaben.

7. Umsetzung

Die Regelungen dieser Leitlinie wurden von der Landesregierung gebilligt. Sie sind mit ihrer Veröffentlichung durch die einzelnen Ressorts für die jeweiligen Geschäftsbereiche in Kraft zu setzen und bekannt zu machen.[12]

[12] Ausnahme der öffentlichen Schulen