Freistaat Thüringen Finanzministerium

Informationssicherheitsleitlinie der Thüringer Landesverwaltung

(ThISL)

Version:	2.2
Stand vom:	19.04.2016
Ablageort:	Intranet
Dokumententyp	LL = Leitlinie
Status:	Freigegeben
Vertraulichkeitsstufe:	Offen

		Firma/Rolle Datum	Name Unterschrift
Review	von: am:	TFM/ IT-SiBe 08.04.2016	H. Hartwig
Freigegeben:	von: am:	CIO des Freistaats Thüringen 23.05.2016	Dr. H. Schubert

Inhalt:

Einleitung und Geltungsbereich 4
1. Ziele und Strategie der Informationssicherheit 4
2. Grundsätze der Informationssicherheit 5
2.1 Angemessenheit der IT-Sicherheitsmaßnahmen 6
2.2 Bereitstellung von Ressourcen 6
2.3 Prinzip des informierten und sensibilisierten Mitarbeiters 6
2.4 Sicherheit vor Verfügbarkeit 6
2.5. Sicherung und Verbesserung 7
3. Informationssicherheitsorganisation 7
3.1 IT-Sicherheitsbeauftragter des Freistaats Thüringen: 7
3.2 IT-Sicherheitsbeauftragter des Ressorts: 8
3.3 Informationssicherheitsmanagement-Team (ISM-Team ThLV): 9
3.4 ThüringenCERT 10
4. Fortschreibung 11
5. Umsetzung der Leitlinie 11
6. Schlussbestimmungen 12

Einleitung und Geltungsbereich

Die Verwaltungsabläufe zur Aufgabenerfüllung in der Thüringer Landesverwaltung werden zunehmend durch den Einsatz von Informations- und Kommunikationstechnik unterstützt und sind von dieser abhängig. Gleichzeitig erhöhen sich die Risiken und Gefährdungen durch die zunehmende technische Vernetzung und Integration sowie durch die Entwicklung von externen Bedrohungslagen. Zur Sicherstellung der Erfüllung der Fachaufgaben ist eine Beeinträchtigung von Informationsinfrastrukturen und deren Komponenten weitestgehend zu vermeiden.

Gemäß § 3 des Vertrages über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG hat der IT-Planungsrat am 08.03.2013 eine Leitlinie Informationssicherheit einschließlich eines Umsetzungsplans beschlossen (Entscheidung 2013/01). Der Umsetzungsplan sieht eine Einführung eines Informationssicherheitsmanagementsystems (ISMS) auf der Grundlage von ISO 27001 oder des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI) vor.

Die Landesregierung erlässt im Bekenntnis zum Stellenwert der Informationssicherheit und im Einklang mit dem abgestimmten Vorgehen von Bund und Ländern für die Landesverwaltung die vorliegende Informationssicherheitsleitlinie als die grundlegende Regelung zur Informationssicherheit. In diesem Dokument werden die Ziele, Vorgehensweisen, Organisationsstrukturen sowie Aufgaben für das Informationssicherheitsmanagement für die Landesverwaltung festgelegt.

Die Informationssicherheitsleitlinie basiert auf den Methoden und Sicherheitsstandards des BSI. Weitergehende Regelungen werden insbesondere in Form von Sicherheitsstandards oder Richtlinien durch das Sicherheitsmanagement der Thüringer Landesverwaltung erarbeitet.

Die Thüringer Staatskanzlei sowie jedes Ministerium achten in ihrem jeweiligen Geschäftsbereich auf die Einhaltung dieser Leitlinie. Soweit diese für ihre Geschäftsbereiche Regelungen zur Informationssicherheit erarbeiten, geschieht dies stets auf Grundlage dieser Leitlinie.

Dem Thüringer Landtag sowie dem Thüringer Rechnungshof wird die Anwendung der IT-Sicherheitsleitlinie empfohlen. Darüber hinaus wird angeregt, dass die Maßgaben dieser Informationssicherheitsleitlinie in den Verwaltungen der kommunalen Gebietskörperschaften entsprechend Anwendung finden.

1. Ziele und Strategie der Informationssicherheit

Der interne Dienstbetrieb und der Informationsaustausch zwischen Behörden und öffentlichen Einrichtungen sowie mit Bürgern und Unternehmen können nur auf einer vertrauenswürdigen Basis erfolgen. Voraussetzung dafür sind geeignete technische und organisatorische Maßnahmen, um die Informationssicherheit zu gewährleisten.

Mit dem ressortübergreifenden Vorgehen in der Informationssicherheit soll ein einheitliches Sicherheitsniveau erlangt und datenschutzrechtliche sowie weitere gesetzliche Anforderungen an die Sicherheit der Informationsverarbeitung erfüllt werden.

Durch eine einheitliche Vorgehensweise, die auch mit Bund, Ländern und Kommunen abgestimmt wird, soll eine effiziente und effektive IT-Unterstützung der Verwaltungsabläufe erfolgen. Die hohen Investitionen in IT-Systeme müssen zu einer nachhaltigen Verfügbarkeit und Kontinuität des Verwaltungshandelns führen, ohne dass Manipulation, unberechtigter Zugriff und Verlust von Daten zu erwarten ist.

Es soll eine kontinuierliche Verbesserung des sicheren Umgangs mit Informationen und Informationstechnik in den jeweiligen Verantwortungsbereichen erreicht werden. Information, Weiterbildung, Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit sind hierbei wesentliche Eckpfeiler.

Verantwortlich für die Informationssicherheit einer Behörde ist die Behördenleitung als Teil der allgemeinen Leitungsverantwortung.

Übergeordnete und unabdingbare Bedeutung für die Thüringer Landesverwaltung erlangen dabei die drei Grundschutzziele:

Vertraulichkeit – Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.

Integrität – Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Informationen.

Verfügbarkeit – Eigenschaft, dass Informationen einer berechtigten Einheit auf Verlangen zugänglich und nutzbar sind.

Die Betrachtung weiterer Sicherheitsziele bzw. Grundwerte kann je nach Einsatzfall zu einer differenzierteren und ausgewogeneren Bewertung des Schutzbedarfes der Informationen führen. Insofern besteht grundsätzlich die Möglichkeit, weitere Sicherheitskriterien – unbeschadet etwaiger Schnittmengen oder Konkurrenzen zwischen einzelnen Kriterien – heranzuziehen. Beispielhaft seien hier die Authentizität und die Revisionsfähigkeit sowie Transparenz genannt.

Authentizität - Echtheit, Zuverlässigkeit und Zurechenbarkeit einer Information.

Verbindlichkeit - Jede Verarbeitung von Informationen muss eindeutig nachvollziehbar und beweisbar und somit revisionssicher sein.

2. Grundsätze der Informationssicherheit

Im Geltungsbereich dieser Leitlinie finden die Methoden und Sicherheitsstandards des IT-Grundschutzes 100-1 bis 100-4 in der jeweils gültigen Fassung Anwendung.

Belange der Informationssicherheit sind von Beginn an zu beachten bei

- ✓ der Planung und der Konzeption von IT-Verfahren;
- ✓ der Entwicklung und der Einführung von IT-Verfahren;
- ✓ dem Betrieb und der Pflege von IT-Verfahren;
- ✓ Dokumentation von vorhandenen IT-Verfahren;
- ✓ der Beschaffung und der Beseitigung/ Entsorgung von IT-Produkten sowie
- ✓ der Nutzung von Diensten Dritter;
- ✓ der Aus- und Weiterbildung der Mitarbeiter;
- ✓ der Sensibilisierung der Mitarbeiter sowie
- ✓ der Planung, Übung und Durchführung von Notfallplänen und Krisenmanagement.

Belange der Informationssicherheit von landesweitem Interesse werden in Abstimmung mit dem Informationssicherheitsmanagement-Team der Thüringer Landesverwaltung (ISM-Team ThLV) einheitlich geregelt. Ressortspezifische Sicherheitsfragen regeln betroffene Dienststellen der Landesverwaltung entsprechend den ressortspezifischen Anforderungen im Einklang mit dieser Leitlinie.

2.1 Angemessenheit der IT-Sicherheitsmaßnahmen

Um Gefährdungen vorzubeugen sind organisatorische und technische Maßnahmen entsprechend der IT-Grundschutzkataloge des BSI umzusetzen und bei hohem und sehr hohem Schutzbedarf individuelle Betrachtungen und ggf. weitere Maßnahmen vorzusehen. Die Sicherheitsmaßnahmen sind entsprechend dem Verwaltungsaufbau, der Personalausstattung und dem technischen Umfeld anzupassen. Dabei soll der finanzielle und technische Aufwand in einem ausgewogenen Verhältnis zu den tatsächlichen Risiken stehen.

2.2 Bereitstellung von Ressourcen

Zur Erreichung der IT-Sicherheitsziele sind durch die Thüringer Ministerien und die Staatskanzlei ausreichende finanzielle, personelle sowie zeitliche Ressourcen zur Verfügung zu stellen. Sollten einzelne IT-Sicherheitsprozesse nicht finanzierbar sein, sind die IT-Sicherheitsmaßnahmen sowie die Art und Weise des IT-Betriebs zu überdenken und gegebenenfalls anzupassen.

2.3 Prinzip des informierten und sensibilisierten Mitarbeiters

Ein wesentliches Sicherheitsrisiko stellen bewusste sowie unbewusste sicherheitsgefährdende Handlungen der Anwender dar. Gezielte Sensibilisierung sowie Qualifizierung von Mitarbeitern sind Grundvoraussetzungen für die Informationssicherheit. Anwender müssen ggf. über notwendige einschränkende IT-Sicherheitsmaßnahmen aufgeklärt und Verhaltensempfehlungen vermittelt werden. Die Beschäftigten der gesamten Thüringer Landesverwaltung gewährleisten die notwendige und angemessene IT-Sicherheit durch verantwortungsvolles Handeln.

2.4 Sicherheit vor Verfügbarkeit

Wird die IT-Infrastruktur der Thüringer Landesverwaltung angegriffen oder bedroht, können entsprechend der Schutzbedarfe vorübergehende Verfügbarkeitsbeschränkungen der betroffenen IT-Systeme vorgenommen werden. Dabei können in Abwägung der

widerstreitenden Schutzgüter Einschränkungen beim Betrieb sowie im Komfort der Bedienung von IT-Systemen, insbesondere bei Netzübergängen in das Internet oder dem Anschluss an das Landesdatennetz vertretbar sein.

2.5. Sicherung und Verbesserung

Die Festlegung des Mindestsicherheitsniveaus in Anwendung des IT-Grundschutzes ermöglicht die Vergleichbarkeit des erreichten Sicherheitsniveaus. Ein kontinuierlicher Qualitätsverbesserungsprozess ist erforderlich, der neben der internen Optimierung auch eine ressortübergreifende Vergleichbarkeit des erreichten Sicherheitsniveaus ermöglicht. Die regelmäßige Aktualisierung, Vervollständigung, Verbesserung und Wirksamkeitsprüfung der eingesetzten Sicherheitsmaßnahmen stellen einen permanenten Prozess dar.

3. Informationssicherheitsorganisation

Die Planungs-, Lenkungs- und Kontrollaufgaben, die erforderlich sind, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und diesen kontinuierlich umzusetzen, werden als Managementsystem für Informationssicherheit (Informationssicherheitsmanagementsystem - ISMS) bezeichnet.

Diese Leitlinie beschreibt das ressortübergreifende ISMS für die Thüringer Landesverwaltung für die zentrale Steuerung der Informationssicherheitsprozesse. In den Thüringer Ministerien und der Staatskanzlei sind für den jeweiligen Geschäftsbereich und dessen Sicherheitsziele angepasste ISMS nach dem BSI-Standard 100-1 zu etablieren und zu betreiben. Dabei sind die behördenspezifischen Sicherheitsanforderungen und die Strukturierung bzw. Organisation des jeweiligen Geschäftsbereichs sowie deren Behörden in ausreichendem Maße zu berücksichtigen. Verantwortlich für die Umsetzung im Geschäftsbereich sind die jeweiligen Ministerien und die Staatskanzlei als Teil der allgemeinen Leitungsverantwortung.

3.1 IT-Sicherheitsbeauftragter des Freistaats Thüringen:

Für die Thüringer Landesverwaltung ist beim für E-Government und ressortübergreifende IT zuständigen Ministerium ein IT-Sicherheitsbeauftragter des Freistaats (IT-SiBe Land) einzusetzen, der dem Beauftragten des Freistaats Thüringen für E-Government und IT (Chief Information Officer - CIO) des Freistaats direkt unterstellt ist. Die Aufgaben des IT-SiBe Land umfassen:

- Fortschreibung der Informationssicherheitsleitlinie;
- Planung, Koordination, Kontrolle, Steuerung und Dokumentation der ressortübergreifenden und zentralen Informationssicherheitsprozesse;
- Initiierung und Koordinierung der Erstellung von Informationssicherheitsstandards;
- Initiierung der Erstellung landeseinheitlicher Richtlinien und Regelungen zur Informationssicherheit in der Thüringer Landesverwaltung;
- Mitwirkung bei der Erstellung von Sicherheits- und Notfallvorsorgekonzepten von IT-Verbünden mit zentraler Steuerung;
- Mitwirkung an der IT-Strategie und IT-Architektur der Thüringer Landesverwaltung;

- Mitwirkung an strategischen IT-Projekten;
- Kontrolle und Mitwirkung bei der Umsetzung gesetzlicher Vorgaben zur Informationssicherheit;
- Leitung der Sitzungen des ISM-Teams der ThLV;
- Erstellung von Berichten an die Landesregierung und an das ISM-Team ThLV über den Status der Informationssicherheit;
- Untersuchung und Eskalation sicherheitsrelevanter Vorfälle von erheblicher Bedeutung und Initiierung und Steuerung von Angeboten für Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit;
- Begleitung von Audits des BSI nach ISO 27001 auf Basis des IT-Grundschutzes;
- Unterstützung des Beauftragten des Freistaats für E-Government und IT.

Dem IT-SiBe Land sowie dessen Stellvertretung sind ausreichende Möglichkeiten einer qualifizierten Aus- und Fortbildung in Themen der Informationssicherheit zu gewähren.

3.2 IT-Sicherheitsbeauftragter des Ressorts:

Jedes Ministerium und die Staatskanzlei haben einen IT-Sicherheitsbeauftragten für ihren Geschäftsbereich (IT-SiBe Ressort) zu benennen. Der IT-SiBe Ressort hat direktes Vortragsrecht bei der Leitung seines Geschäftsbereichs.

Die Aufgaben eines IT-SiBe Ressorts umfassen insbesondere:

- Beratung der Leitung des Geschäftsbereichs in Belangen der Informationssicherheit;
- Umsetzung des sich aus dieser Leitlinie und den daraus abgeleiteten Standards zur Informationssicherheit notwendigen Handlungsbedarfs im Geschäftsbereich;
- Planung, Aufbau, Koordination, Kontrolle, Steuerung sowie Dokumentation des ressortspezifischen Informationssicherheitsmanagementsystems und ressortspezifischer Informationssicherheitsprozesse auf Grundlage dieser Leitlinie;
- Unterstützung bei der Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten;
- Sicherstellung der Anwendung zentraler Regelungen, Hinweise und Empfehlungen;
- Untersuchung von sicherheitsrelevanten Vorfällen im Geschäftsbereich und Auswertung sowie Meldung an das ThüringenCERT;
- Mitwirkung bei der Auswahl und bei der Durchsetzung von notwendigen IT-Sicherheitsmaßnahmen im Geschäftsbereich;
- Kontrolle und Mitwirkung bei der Umsetzung gesetzlicher Vorgaben zur Informationssicherheit;
- Unterstützung der Behörden im Geschäftsbereich bei der Erstellung von IT-Sicherheitsrichtlinien und IT-Sicherheitskonzepten;
- Mitwirkung an der IT-Strategie und IT-Architektur des Geschäftsbereichs;
- Mitwirkung an strategischen IT-Projekten des Geschäftsbereichs;
- Unterstützung bei der Initiierung und Durchführung sicherheitsrelevanter Projekte des Geschäftsbereichs;
- Mitwirkung im ISM-Team des Landes;

- Berichterstattung über den Status der Informationssicherheit im Geschäftsbereich an die jeweilige Leitung und den IT-SiBe-Land;
- Begleitung und Mitwirkung an internen Audits und Informationssicherheitsrevisionen;
- Mitwirkung bei landesweiten Maßnahmen zur Sensibilisierung und Schulung im Bereich der Informationssicherheit in Abstimmung mit dem für die ressortübergreifende Fortbildung zuständigen Ressort;

Dem IT-SiBe Ressort sowie dessen Stellvertretung sind zur Aufgabenwahrnehmung und fachlichen Qualifikation entsprechend den Anforderungen an die Informationssicherheit im Geschäftsbereich ausreichend Zeit und Ressourcen zu gewähren.

3.3 Informationssicherheitsmanagement-Team (ISM-Team ThLV):

Zur einheitlichen Umsetzung der Informationssicherheitsorganisation und Abstimmung von Maßnahmen wird ein ISM-Team ThLV gebildet. Um die verschiedenen Aspekte der Informationssicherheit in der Thüringer Landesverwaltung berücksichtigen zu können, arbeiten im ISM-Team ThLV folgende Vertreter als ständige, nichtständige sowie als beratende Mitglieder zusammen. Das ISM-Team ThLV gibt sich in Abstimmung mit dem für ressortübergreifende IT und E-Government zuständigen Ministerium eine Geschäftsordnung.

Ständige Mitglieder sind:

- der IT-Sicherheitsbeauftragter Land (IT-SiBe Land);
- der IT-Sicherheitsbeauftragte des Ressorts (IT-SiBe Ressort) und
- der IT-Sicherheitsmanager der Thüringer Polizei;
- der IT-Sicherheitsbeauftragte des IT-Landesdienstleisters TLRZ

sowie

- der IT-Sicherheitsbeauftragte des Thüringer Rechnungshofs und
- der IT-Sicherheitsbeauftragte des Thüringer Landtags

sofern sie diese Leitlinie anwenden.

Nichtständige Mitglieder mit beratender Funktion sind:

- Vertreter des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit;
- Vertreter des Gemeinsamen Ausschusses der Hauptpersonalräte (GHPR) und

- Vertreter des Thüringer Rechnungshofs und
- Vertreter des Thüringer Landtags

sofern sie diese Leitlinie nicht anwenden.

Nichtständige Mitglieder können jederzeit an Sitzungen des ISM-Teams ThLV teilnehmen. Andere Stellen der Landesverwaltung sollen in beratender Funktion bei Entscheidungen des ISM-Teams ThLV beteiligt werden, sofern deren Belange betroffen sind. Dies können insbesondere der:

- IT-Verantwortliche des jeweiligen IT-Verfahrens oder
- Vertreter der betroffenen IT-Anwender sein.

Die Aufgaben des ISM-Teams ThLV umfassen insbesondere:

- die Fortschreibung der Informationssicherheitsziele und der Leitlinie für Informationssicherheit der Thüringer Landesverwaltung;
- die Erstellung von IT-Sicherheitsstandards für den Geltungsbereich der Thüringer Landesverwaltung;
- die Erstellung und Fortschreibung des Sicherheitskonzepts, des Notfallvorsorgekonzepts sowie weiterer Richtlinien und Regelungen zur Informationssicherheit in der Thüringer Landesverwaltung;
- die landesweite Überwachung der Umsetzung der Vorgaben aus der Informationssicherheitsleitlinie, den Sicherheitsstandards und den IT-Sicherheitskonzepten;
- die Fortschreibung eines landesweiten Realisierungsplans für die Informationssicherheitsmaßnahmen;
- die Entwicklung und Überwachung von Kennzahlen zur Bewertung der Informationssicherheit;
- die Mitwirkung und Beratung bei der Erstellung von IT-Sicherheitskonzepten für ressortübergreifende Verfahren und Projekte;
- Abstimmung des Jahresplans für interne Audits und IS-Revisionen;
- die Erarbeitung landesweiter Schulungs- und Sensibilisierungsprogramme für die Informationssicherheit;
- die Beratung der auf Landesebene bestehenden Gremien sowie der Landesregierung in Fragen der Informationssicherheit;
- die Erstellung und Fortschreibung von landesweiten Vorgaben zur Informationssicherheit bei Inanspruchnahme von IT-Dienstleistern;
- die Weiterleitung von kritischen Sicherheitsvorfällen an das **C**omputer **E**mergency **R**esponse **T**eam (ThüringenCERT) zur Überprüfung.

3.4 ThüringenCERT

Das „CERT“ (Computer Emergency Response Team) ist eine geeignete strukturelle und personell ausgestattete Einheit, die zur Prävention und Bearbeitung von Informationssicherheitsvorfällen sowie zur allgemeinen Erhöhung der Qualität der Informationssicherheit dient.

Für die Thüringer Landesverwaltung betreibt der IT-Landesdienstleister ein ThüringenCERT als zentrale Anlaufstelle für präventive und reaktive Maßnahmen. Das ThüringenCERT ist Teilnehmer im Verwaltungs-CERT-Verbund (VCV), der die vom IT-Planungsrat beschlossene Zusammenarbeit bei der Abwehr von IT-Angriffen zum Ziel hat. Der Informations- und Erfahrungsaustausch im VCV dient der Verbesserung der Informationssicherheit in der öffentlichen Verwaltung in Deutschland. Darüber hinaus soll sich die gegenseitige Zusammenarbeit im Rahmen der rechtlichen Möglichkeiten auf den aktiven Austausch von Fähigkeiten und Kapazitäten in allen CERT-spezifischen Belangen erstrecken.

Die verantwortlichen Betreiber von IT-Infrastrukturen in der Landesverwaltung geben informationssicherheitsrelevante Informationen über geeignete IT-Systeme an das ThüringenCERT weiter. Meldewürdig sind dabei vor allem Ereignisse, bei denen Auswirkungen auf andere nicht ausgeschlossen werden können, oder die auch für andere als relevant eingeschätzt werden, z.B. besondere Auffälligkeiten und klare Abweichungen vom Normalverhalten im Regelbetrieb.

Das ThüringenCERT nimmt dabei in Abstimmung mit dem ISM-Team der Thüringer Landesverwaltung insbesondere folgende Aufgaben wahr:

- das Betreiben eines Warn- und Informationsdienstes für die Thüringer Landesverwaltung in Zusammenarbeit mit den Informationsdiensten des CERT Bund;
- Koordinierende Bearbeitung von landesweit bedeutsamen oder länderübergreifenden Sicherheitsvorfällen;
- Analyse eingehender Vorfallsmeldungen;
- Erstellung von Handlungsempfehlungen für die betroffenen Dienststellen;
- die aktive Alarmierung des ISM-Teams der Thüringer Landesverwaltung bei Gefährdungen der IT-Sicherheit;
- Etablierung von abgestimmten Kommunikationswegen mit den Dienststellen des Landes;
- die Mitarbeit bei der Erstellung von IT-Richtlinien und IT-Sicherheitskonzeptionen;
- Mitwirkung bei der Konzeption zentraler technischer IT-Sicherheitssysteme;
- das Betreiben einer Datenbank über gemeldete IT-Sicherheitsvorfälle;
- Unterstützung der Aufgabenerfüllung des IT-Sicherheitsbeauftragten des Freistaats sowie der IT-Sicherheitsbeauftragten der Ressorts;
- Bereitstellung von Kennzahlen zur Steuerung der Informationssicherheitsmaßnahmen;
- Erstellung von Lagebildern über den Stand der Informationssicherheit sowie
- die Unterstützung bei Schulungsmaßnahmen zum Thema Informationssicherheit in der Thüringer Landesverwaltung.

4. Fortschreibung

Die vorliegende Informationssicherheitsleitlinie wird entweder anlassbezogen oder mindestens alle 3 Jahre einer überprüfenden Revision unterzogen. Die Informationssicherheitsleitlinie wird dabei durch Mitglieder des ISM-Teams der Thüringer Landesverwaltung inhaltlich überprüft und im Bedarfsfall aktualisiert und danach zur Abstimmung gebracht.

5. Umsetzung der Leitlinie

Das für die jeweiligen Geschäftsbereich und dessen Sicherheitsziele angepasste ISMS ist innerhalb von drei Jahren nach Inkrafttreten dieser Leitlinie einzurichten.
Alle IT-Infrastrukturen, IT-Systeme und Anwendungen, welche nach dem Inkrafttreten dieser Leitlinie implementiert werden, sind unter anderem nach dem Sicherheitsstandard des IT-Grundschutzes umzusetzen. Bestehende IT-Infrastrukturen, IT-Systeme

und Anwendungen sind innerhalb von fünf Jahren nach Inkrafttreten dieser Leitlinie auf die Sicherheitsstandards des IT-Grundschutzes umzustellen.

Zur Einhaltung dieser Sicherheitsleitlinie sind alle Mitarbeiter in der Thüringer Landesverwaltung verpflichtet. Art und Umfang von Sanktionen wegen Verletzung der Bestimmungen zum Schutz der Informationssicherheit sowie die Zuständigkeit für die Verfolgung ergeben sich aus den einschlägigen Straf- und Disziplinargesetzen sowie den dazu erlassenen Richtlinien und Verordnungen.

6. Schlussbestimmungen

Diese Sicherheitsleitlinie tritt am 01.07.2016 in Kraft.