Freistaat Thüringen Finanzministerium

Informationssicherheits-leitlinie der Thüringer Landesverwaltung

(ThISL)

Inhalt:

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.

In Fortschreibung der Leitlinie vom 08.03.2013 hat der IT-Planungsrat am 12.03.2019 die „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung 2018“ verabschiedet, die nunmehr auf die Wirkung von Sicherheitsmaßnahmen, insbesondere auf eine lückenlose Umsetzung von Sicherheitskonzepten und deren Messbarkeit, fokussiert und ein einheitliches Sicherheitsniveau zwischen den Bundesländern und dem Bund anstrebt. Der IT-Planungsrat erkennt die Gewährleistung der Informationssicherheit der Verwaltung damit als stetigen und dauerhaften Prozess an, dessen Ziel es ist, den angestrebten Sicherheitsstand zu erreichen und dauerhaft zu festigen.

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 Informationssicherheitsleitlinie 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 im Angesicht des steigenden Digitalisierungsgrades aller Verwaltungsprozesse 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 oder der Verlust von Daten zu erwarten ist.

Es soll eine kontinuierliche Verbesserung des sicheren Umgangs mit Informationen und Informations- und Kommunikationstechnik in den jeweiligen Verantwortungsbereichen erreicht werden. Information, Weiterbildung und 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 die 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 200-1 bis 200-4 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;
- der Dokumentation von vorhandenen IT-Verfahren;
- der Beschaffung und der Beseitigung/Entsorgung von IT-Produkten;
- 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 dem modernisierten IT-Grundschutzkompendium des BSI i. V. m. dessen Umsetzungshinweisen 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. Hierbei sind stets für die individuellen Risiken konkrete Einzelfallabwägungen zu treffen.

2.2 Bereitstellung von Ressourcen

Zur Erreichung der Informationssicherheitsziele sind durch die Thüringer Ministerien und die Staatskanzlei ausreichende finanzielle, personelle sowie zeitliche Ressourcen zur Verfügung zu stellen. Sollten einzelne Informationssicherheitsprozesse nicht wirtschaftlich sein, sind die Informationssicherheitsmaßnahmen sowie die Art und Weise der Informationsverarbeitung 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 Informationssicherheitsmaßnahmen aufgeklärt und Verhaltensempfehlungen vermittelt werden. Die Beschäftigten der gesamten Thüringer Landesverwaltung gewährleisten die notwendige und angemessene Informationssicherheit durch verantwortungsvolles Handeln.

2.4 Sicherheit vor Verfügbarkeit

Wird die IT-Infrastruktur der Thüringer Landesverwaltung angegriffen oder bedroht, können entsprechend den Schutzbedarfen 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 zur zentralen Steuerung der Informationssicherheitsprozesse. In den Thüringer Ministerien und der Staatskanzlei sind für den jeweiligen Geschäftsbereich und dessen Sicherheitsziele angepasste ISMS nach dem BSI-Standard 200-1 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 Behördenleitungen als Teil ihrer allgemeinen Leitungsverantwortung.

3.1 Informationssicherheitsbeauftragter des Freistaats Thüringen:

Für die Thüringer Landesverwaltung ist beim für E-Government und ressortübergreifende IT zuständigen Ministerium ein Informationssicherheitsbeauftragter des Freistaats (ISB 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 ISB Land umfassen:

- Fortschreibung der Informationssicherheitsleitlinie;
- Planung, Koordination, Kontrolle, Steuerung und Dokumentation der ressortübergreifenden und zentralen Informationssicherheitsprozesse;
- Initiierung und Koordinierung der Erstellung von landeseinheitlichen 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 und
- Unterstützung des Beauftragten des Freistaats für E-Government und IT.

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

3.2 Informationssicherheitsbeauftragter des Ressorts

Jedes Ministerium und die Staatskanzlei haben mindestens einen Informationssicherheitsbeauftragten für ihren Geschäftsbereich (ISB Ressort) zu benennen. Der ISB des Ressorts hat direktes Vortragsrecht bei der Leitung seines Geschäftsbereichs.

Die Aufgaben eines ISB Ressorts umfassen insbesondere:

- Beratung der Leitung des Geschäftsbereichs in Belangen der Informationssicherheit bei der Wahrnehmung der Dienst- bzw. Fachaufsicht;
- Initiierung des ressortspezifischen Informationssicherheitsmanagementsystems und ressortspezifischer Informationssicherheitsprozesse auf Grundlage dieser Leitlinie;
- Unterstützung bei der Bewertung von technischen und organisatorischen Maßnahmen behördenübergreifender automatisierter Verfahren;
- Dienstaufsichtliche Durchsetzung der Anwendung zentraler Regelungen, Hinweise und Empfehlungen unter Einhaltung des Dienstwegs;
- Dienst- oder fachaufsichtliche Mitwirkung bei der Untersuchung von sicherheitsrelevanten Vorfällen im Geschäftsbereich und deren Auswertung sowie interne Koordinierung und Weiterleitung an das ThüringenCERT;
- Mitwirkung bei der dienst- oder fachaufsichtlichen Durchsetzung von IT-Sicherheitsmaßnahmen im Geschäftsbereich und ggf. dienst- oder fachaufsichtliche Anweisung bedeutender IT-Sicherheitsmaßnahmen nach Zustimmung der Ressortleitung;
- Dienst- und fachaufsichtliche 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 IT-Strategie, IT-Architektur und wesentlichen informationssicherheitstechnischen Projekten des Geschäftsbereichs;

- Mitwirkung im ISM-Team des Landes;
- Berichterstattung über den Status der Informationssicherheit im Geschäftsbereich an die jeweilige Leitung und den ISB-Land;
- Dienst- und fachaufsichtliche Begleitung von internen Audits und Informationssicherheitsrevisionen und
- Mitwirkung bei landesweiten Maßnahmen zur Sensibilisierung und Schulung im Bereich der Informationssicherheit in Abstimmung mit dem für die ressortübergreifende Fortbildung zuständigen Ressort.

Den Informationssicherheitsbeauftragten des Ressort sowie dessen Stellvertretungen sind zur Aufgabenwahrnehmung und fachlichen Qualifikation entsprechend den Umsetzungshinweisen zum IT-Grundschutzkompendium 2019 ausreichend Zeit und Ressourcen zu gewähren. Gemäß den Umsetzungshinweisen zum IT-Grundschutzkompendium des Bundesamts für Sicherheit in der Informationstechnik 2019 soll in Behörden ab 250 Mitarbeitern die Funktion eines Informationssicherheitsbeauftragten hauptamtlich wahrgenommen werden.

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 Informationssicherheitsbeauftragte Land (ISB Land);
- der oder die Informationssicherheitsbeauftragte/-n des Ressorts (ISB Ressort) und
- der Informationssicherheitsbeauftragte des IT-Landesdienstleisters TLRZ sowie

- der Informationssicherheitsbeauftragte des Thüringer Rechnungshofs und
- der Informationssicherheitsbeauftragte 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 Arbeitsgemeinschaft der Hauptpersonalräte (ARGE HPR) sowie BAfIS TLKA sowie
- Vertreter des Thüringer Rechnungshofs und
- Vertreter des Thüringer Landtags

sofern sie diese Leitlinie nicht anwenden.

Nichtständige Mitglieder können auf Einladung des ISB des Landes 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 Informationssicherheitsstandards für den Geltungsbereich der Thüringer Landesverwaltung;
- die Erstellung und Fortschreibung von zentralen 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 Entwicklung und Überwachung von Kennzahlen zur Bewertung der Informationssicherheit;
- die Mitwirkung und Beratung bei der Erstellung von IT-Sicherheitskonzepten für ressortübergreifende Verfahren und Projekte;
- die 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 und
- die Erstellung und Fortschreibung von landesweiten Vorgaben zur Informationssicherheit bei Inanspruchnahme von IT-Dienstleistern.

3.4 Informationssicherheitsbeauftragte der Behörde oder Einrichtung

Die Behörden oder Einrichtungen (BoE) eines Ressorts sowie wesentliche, für Recht- und Zweckmäßigkeit der Aufgabenerfüllung eigenverantwortliche Behördenbereiche können einen Informationssicherheitsbeauftragten (ISB) benennen. Der ISB hat direktes Vortragsrecht bei der Behörden-, Einrichtungs- oder Bereichsleitung und unterstützt diese bei der Wahrnehmung ihrer originären Verantwortung für Informationssicherheit im Rahmen ihrer Verantwortung für Recht- und Zweckmäßigkeit der Aufgabenerfüllung.

Auf der Grundlage der Umsetzungshinweise zum IT-Grundschutzkompendium 2019 des Bundesamts für Sicherheit in der Informationstechnik sollen in der Thüringer Landesverwaltung bestellte Informationssicherheitsbeauftragte in obersten und oberen Behörden oder Einrichtungen der Landesverwaltung ab 250 Mitarbeiter im Hauptamt eingesetzt werden.
Seine Aufgaben umfassen innerhalb des behörden-, einrichtungs- bzw. bereichsinternen Zuständigkeitsbereichs unter anderem:

- Steuerung des Aufbaus eines Informationssicherheitsmanagements und Informationssicherheitsprozesses auf Grundlage dieser Leitlinie und Mitwirkung an allen damit zusammenhängenden Aufgaben;
- Beratung der Leitung bei der Wahrnehmung ihrer originären Verantwortung in Belangen der Informationssicherheit insbesondere bei der Erstellung einer internen Leitlinie zur Informationssicherheit;
- Koordination der Erstellung von Sicherheitskonzepten, Notfallvorsorgekonzepten und anderer Teilkonzepte und System-Sicherheitsrichtlinien sowie Sicherstellung des Erlasses weiterer Richtlinien und Regelungen zur Informationssicherheit durch die Leitung;
- Unterstützung bei der Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten;
- Sicherstellung der Anwendung zentraler Regelungen, Hinweise und Empfehlungen;
- Sicherstellung der Untersuchung von sicherheitsrelevanten Vorfällen und Auswertung sowie Meldung an den dienst- oder fachaufsichtlich zuständigen ISB Ressort gem. der Richtlinie zur Behandlung von Informationssicherheitsvorfällen (Agieren als örtlicher Ansprechpartner);
- Mitwirkung an IT-Strategie, IT-Architektur und informationssicherheitsrelevanten Projekten;
- Initiierung der Realisierung und Überprüfung von IT-Sicherheitsmaßnahmen;
- Berichterstattung über den Status der Informationssicherheit an die Leitung;
- Begleitung von und Mitwirkung an internen Audits und Informationssicherheitsrevisionen und
- Mitwirkung bei internen Maßnahmen zur Sensibilisierung und Schulung im Bereich der Informationssicherheit, bei ressortübergreifender Bedeutung ggf. in Abstimmung mit dem für die ressortübergreifende Fortbildung zuständigen Ressort über den Ressort-ISB.

3.5 ThüringenCERT

Für die Thüringer Landesverwaltung betreibt der IT-Landesdienstleister das ThüringenCERT als zentrale Anlaufstelle für präventive und reaktive Maßnahmen im Bereich der Informationssicherheit.

Die verantwortlichen Betreiber von IT-Infrastrukturen in der Landesverwaltung sind verpflichtet, informationssicherheitsrelevante Informationen an das ThüringenCERT weiterzugeben. 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:

- Funktion der zentralen Anlaufstelle für sicherheitsrelevante Ereignisse nach innen und außen;

- Koordinierende Bearbeitung von landesweit bedeutsamen oder länderübergreifenden Sicherheitsvorfällen;
- Analyse eingehender Vorfallsmeldungen;
- Erstellung von Handlungsempfehlungen für die betroffenen Dienststellen;
- Unterstützung bei der Behebung von Sicherheitsvorfällen;
- die aktive Alarmierung des ISM-Teams der Thüringer Landesverwaltung bei Gefährdungen der IT-Sicherheit;
- das Betreiben eines Warn- und Informationsdienstes für die Thüringer Landesverwaltung;
- Allgemeine Informationssicherheitsberatung;
- Unterstützung bei der Erstellung von IT-Richtlinien, IT-Sicherheitskonzeptionen und Mitwirkung bei der Konzeption zentraler technischer IT-Sicherheitssysteme;
- Unterstützung der Aufgabenerfüllung der Informationssicherheitsbeauftragten im Freistaat;
- Bereitstellung von Kennzahlen und Lagebildern über den Stand der Informationssicherheit;
- die Unterstützung bei Schulungsmaßnahmen zum Thema Informationssicherheit in der Thüringer Landesverwaltung sowie
- Bund- und länderübergreifende operative taktische Zusammenarbeit im Verwaltungs-CERT-Verbund (VCV).

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 Geschäftsbereiche und dessen Sicherheitsziele angepasste ISMS ist innerhalb von zwei 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 geschäftskritische IT-Infrastrukturen, IT-Systeme und Anwendungen sind innerhalb von zwei 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

Die Informationssicherheitsleitlinie tritt am 12.01.2022 in Kraft und mit Ablauf des 11.01.2027 außer Kraft.

Dr. Hartmut Schubert
(Staatssekretär im Thüringer Finanzministerium und Beauftragter des Freistaats Thüringen für E-Government und IT)