Thüringer Informationssicherheitsleitlinie für die Landesverwaltung

Vermerk Vertraulichkeit:	Offen

Inhalt:

Einleitung und Geltungsbereich

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

Die Landesregierung erlässt im Bekenntnis zum Stellenwert der Informationssicherheit 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 beschrieben.

Die Informationssicherheitsleitlinie basiert auf den Methoden und den Sicherheitsstandards des Bundesamts für Sicherheit in der Informationstechnik (BSI). Weitergehende Regelungen werden insbesondere in Form von Sicherheitsstandards oder Richtlinien durch das Informationssicherheitsmanagement der 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 für die Landesverwaltung empfohlen. Darüber hinaus wird angeregt, dass die Maßgaben dieser Informationssicherheitsleitlinie in den Verwaltungen der kommunalen Gebietskörperschaften entsprechend Anwendung finden.

1. Ziele der Informationssicherheit

Für den Schutz von Informationen sind zunächst Zielzustände zu definieren, welche mit geeigneten Sicherheitsmechanismen erreicht werden sollen. Je nach Aufgabenspektrum können unterschiedliche Schwerpunkte gesetzt bzw. Grundwerte formuliert werden.

Übergeordnete und unabdingbare Bedeutung für die Landesverwaltung erlangen 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 zwischen einzelnen Kriterien – heranzuziehen. Beispielhaft seien hier die Authentizität, die Revisionsfähigkeit sowie die Transparenz genannt.

2. Grundsätze der Informationssicherheit

Im Geltungsbereich dieser Leitlinie finden die Methoden und Sicherheitsstandards des Bundesamtes für Sicherheit in der Informationstechnik Anwendung.

Belange der Informationssicherheit sind von Beginn an zu beachten bei:

- ✓ der Planung und Konzeption von IT-Verfahren;
- ✓ der Entwicklung und der Einführung von IT-Verfahren;
- ✓ dem Betrieb und der Pflege von IT-Verfahren;
- ✓ der Beschaffung und der Beseitigung/ Entsorgung von IT-Produkten;
- ✓ der Nutzung von Diensten Dritter sowie
- ✓ Aus- und Weiterbildung der Mitarbeiter.

Belange der Informationssicherheit von landesweitem Interesse werden in Abstimmung mit dem Informationssicherheitsmanagement-Team (ISM-Team) einheitlich geregelt. Ressortspezifische Sicherheitsfragen regeln betroffene Dienststellen der Landesverwaltung entsprechend ihren individuellen Anforderungen im Einklang mit dieser Informationssicherheitsleitlinie.

2.1 Angemessenheit der IT-Sicherheitsmaßnahmen

Um tatsächlichen Risiken, insbesondere möglichen Schäden vorzubeugen, sind organisatorische und technische Maßnahmen vorzusehen. Die Sicherheitsmaßnahmen sind entsprechend dem Verwaltungsaufbau, der Personalausstattung und dem technischen Umfeld anzupassen. Dabei sollte der finanzielle und technische Aufwand im Verhältnis zu den tatsächlichen Risiken stehen.

2.2 Bereitstellung von Ressourcen

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

2.3 Prinzip des informierten und sensibilisierten Mitarbeiters

Das größte Sicherheitsrisiko stellen bewusste sowie unbewusste sicherheitsgefährdende Handlungen der Anwender dar. Gezielte Sensibilisierung sowie Qualifizierung von Mitarbeitern sind die Grundvoraussetzung für die Informationssicherheit. Anwender müssen ggf. über notwendige einschränkende IT-Sicherheitsmaßnahmen aufgeklärt werden. Die Bediensteten der gesamten Landesverwaltung gewährleisten die notwendige und angemessene IT-Sicherheit durch verantwortungsvolles Handeln.

2.4 Sicherheit vor Verfügbarkeit

Wird die IT-Infrastruktur der Landesverwaltung angegriffen oder bedroht, können entsprechend der Schutzbedarfe vorübergehende Verfügbarkeitsbeschränkungen der betroffenen IT-Systeme vorgenommen werden. Dabei sind Einschränkungen beim Betrieb sowie im Komfort der Bedienung, insbesondere bei Netzübergängen in das Internet vertretbar.

2.5. Einhaltung von Gesetzen, Richtlinien und Regeln (Compliance)

Die Thüringer Staatskanzlei und die Ministerien realisieren in ihrem Geschäftsbereich ein System zur Sicherung der Einhaltung bestehender gesetzlicher, vertraglicher sowie politischer Regelungen mit IT-Bezug.

2.6 Maximalprinzip beim Schutzbedarf

Alle Informationen, die in Prozessen der Landesverwaltung verarbeitet werden, sind hinsichtlich ihres jeweiligen Schutzbedarfs nach den BSI-Standards zu klassifizieren. Der Schutzbedarf für IT-Systeme bemisst sich grundsätzlich nach dem höchsten Einzelwert der betrachteten Grundwerte.

2.7 Minimalprinzip bei Zugriffs- und Nutzungsrechten

Der Zugriff auf IT-Systeme ist auf den erforderlichen Personenkreis einzuschränken. Die Zugriffsrechte werden auf das erforderliche Maß zur Aufgabenerfüllung beschränkt.

2.8. Sicherung und Verbesserung

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 bezeichnet.

3.1 IT-Sicherheitsbeauftragter der Thüringer Landesverwaltung

Für die Landesverwaltung ist beim für E-Government und ressortübergreifende IT zuständigen Ministerium ein IT-Sicherheitsbeauftragter des Landes (IT-SiBe Land) einzusetzen. Die Aufgaben des IT-SiBe Land umfassen:

- Planung, Koordination, Steuerung und Dokumentation des landesweiten Informationssicherheitsprozesses;
- Koordinierung der Erstellung und Fortschreibung der Informationssicherheitsleitlinie;
- Initiierung und Koordinierung der Erstellung von IT-Sicherheitsstandards;
- Initiierung und Koordinierung der Erstellung und Fortschreibung des ressortübergreifenden Sicherheitskonzepts, des Notfallvorsorgekonzepts sowie weiterer landeseinheitlicher Richtlinien und Regelungen zur Informationssicherheit in der Landesverwaltung;
- Initiierung und Koordinierung eines landesweiten Realisierungsplans für Sicherheitsmaßnahmen und Kontrolle der Umsetzung des landesweiten Realisierungsplans;
- Mitwirkung an der IT-Strategie und IT-Architektur der Landesverwaltung;
- Mitwirkung an strategischen Projekten mit IT-Bezug;
- Leitung des ISM-Teams**;**
- Erstellung von Berichten an die Landesregierung und an das ISM-Team über den Status der Informationssicherheit;
- Untersuchung sicherheitsrelevanter Vorfälle von erheblicher Bedeutung und Initiierung und Steuerung von Angeboten für Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit.

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 der Ressorts

Die Thüringer Staatskanzlei und jedes Ministerium hat einen IT-Sicherheitsbeauftragten für ihren Geschäftsbereich (IT-SiBe Ressort) zu benennen. Der IT-SiBe Ressort hat direktes Vortragsrecht bei der Leitung des Ressorts.

Die Aufgaben eines IT-SiBe Ressort umfassen:

- Planung, Koordination, Steuerung sowie Dokumentation des ressortspezifischen Informationssicherheitsprozesses;

- Sicherstellung des sich aus der Leitlinie und den daraus abgeleiteten Standards zur Informationssicherheit ergebenden Handlungsbedarfs im Ressort;
- Sicherstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts sowie weiterer Richtlinien und Regelungen zur Informationssicherheit im Ressort;
- Initiierung, Koordination, Fortschreibung sowie Kontrolle der Umsetzung eines sich aus dem landesweiten Realisierungsplan für Sicherheitsmaßnahmen ergebenden Realisierungsplans für das Ressort;
- Mitwirkung an der IT-Strategie und IT-Architektur des Ressorts;
- Mitwirkung an strategischen Projekten mit IT-Bezug im Ressort;
- Unterstützung des Datenschutzbeauftragten bei der Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten;
- Initiierung und Koordination sicherheitsrelevanter Projekte im Ressort;
- Mitarbeit im ISM-Team der Landesverwaltung;
- Berichterstattung über den Status der Informationssicherheit im Ressort;
- Untersuchung sicherheitsrelevanter Vorfälle von erheblicher Bedeutung im Ressort;
- Umsetzung von landesweiten Maßnahmen zur Sensibilisierung und Schulung im Bereich der Informationssicherheit;
- Initiierung und Steuerung des Angebots von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit im Ressort;
- Planung, Koordination, Auswertung sowie Nachbereitung von Informationssicherheitsrevisionen bzw. -audits im Ressort;
- die Umsetzung der Vorgaben des IT-SiBe Land zur Informationssicherheit im Ressort;
- die Mitwirkung bei der Auswahl und bei der Durchsetzung von notwendigen IT-Sicherheitsmaßnahmen im Ressort;
- die Tätigkeit als Ansprechpartner für Informationssicherheitsfragen vor Ort;
- die Ermittlung des Schulungsbedarfs von Mitarbeitern im Ressort;
- Festlegung von Art, Weise und Umfang der Erstellung und Vorhaltung von Log- und Protokolldateien;
- Initiierung einer möglichen Auswertung von Log- und Protokolldateien im Bedarfsfall;
- sowie weitere noch festzulegende Aufgaben im Rahmen der Informationssicherheit der Landesverwaltung.

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

3.3 Informationssicherheitsmanagement-Team (ISM-Team)

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

Ständige Mitglieder:

Ständige Mitglieder wirken bei allen relevanten Aufgaben des ISM-Teams in der Landesverwaltung mit.

- IT-Sicherheitsbeauftragter Land (IT-SiBe Land);
- IT-Sicherheitsbeauftragte der Ressorts (IT-SiBe Ressort);

Nichtständige Mitglieder:

Nichtständige Mitglieder können jederzeit an Sitzungen des ISM-Teams teilnehmen und haben Mitwirkungsrechte, sofern deren Belange betroffen sind. Nichtständige Mitglieder sind:

- der Thüringer Landesbeauftragte für den Datenschutz;
- der Thüringer Rechnungshof;
- der Gemeinsame Ausschuss der Hauptpersonalräte (GHPR) und
- das Thüringer Landesamt für Verfassungsschutz.

Sonstige Mitglieder mit beratender Funktion:

Andere Stellen der Landesverwaltung sollen bei Entscheidungen des ISM-Teams 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 umfassen:

- die Erarbeitung der Informationssicherheitsziele und der Thüringer Informationssicherheitsleitlinie der Landesverwaltung sowie deren Fortschreibung;
- die Erstellung von IT-Sicherheitsstandards für den Geltungsbereich der Landesverwaltung;
- die Erstellung und Fortschreibung des Sicherheitskonzepts, des Notfallvorsorgekonzepts sowie weiterer Richtlinien und Regelungen zur Informationssicherheit in der Landesverwaltung;
- die landesweite Überwachung der Umsetzung der Vorgaben aus der Informationssicherheitsleitlinie, den IT-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;
- 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 (CERT Thüringen) zur Überprüfung.

3.4 Computer Emergency Response Team (CERT Thüringen)

Für die Landesverwaltung ist beim IT-Landesdienstleister ein CERT-Thüringen als zentrale Anlaufstelle für präventive sowie reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle aufzubauen.

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

- Unterstützung der Arbeit des IT-Sicherheitsbeauftragten des Landes sowie der Ressorts;
- die Mitarbeit bei der Erstellung von IT-Richtlinien und IT-Sicherheitskonzeptionen;
- Unterstützung bei der Auswertung von kritischen IT-Sicherheitsvorfällen in der Landesverwaltung;
- Erstellung von technischen Empfehlungen zur effektiven Vorbeugung von IT-Sicherheitsvorfällen;
- sowie die aktive Öffentlichkeitsarbeit sowie Unterstützung bei Schulungsmaßnahmen zum Thema Informationssicherheit in der Landesverwaltung.

4. Fortschreibung

Die vorliegende Informationssicherheitsleitlinie wird entweder anlassbezogen oder mindestens alle 2 Jahre einer überprüfenden Revision unterzogen. Die Informationssicherheitsleitlinie wird dabei durch Mitglieder des ISM-Teams inhaltlich überprüft und im Bedarfsfall aktualisiert und danach zur Abstimmung gebracht.

5. Umsetzung der Leitlinie

Zur Einhaltung dieser Informationssicherheitsleitlinie sind alle Mitarbeiter in der 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 Tag nach ihrer Veröffentlichung in Kraft und mit Ablauf des 30.06.2016 außer Kraft. Die Zuweisungen der Rollen gemäß der Gliederungspunkte 3.1 / 3.2 sowie die Einrichtung des ISM-Teams gemäß Gliederungspunkt 3.3 sind innerhalb einer Frist von 12 Monaten nach Inkrafttreten dieser Informationssicherheitsleitlinie umzusetzen. Der Aufbau CERT Thüringen gemäß Gliederungspunkt 3.4 soll innerhalb einer Frist von 24 Monaten nach Inkrafttreten dieser Informationssicherheitsleitlinie erfolgen.