Freistaat Thüringen
Thüringer Landesrechenzentrum

Informationssicherheitsmanagement des TLRZ

Leitlinie Informationssicherheit CNFT

Version / Datum	5.0	28.09.2020
Dateiname	1010.ISMS.RL_Leitlinie Informationssicherheit.docx	
Dokumententyp	Richtlinie	
Vertraulichkeitsstufe	**TLP WHITE**	
Verantwortlicher	Leiter des Informationsverbunds	
Erstellt am	31.01.2014	
Status	**freigegeben**	
Verteiler	Alle Nutzer des Landesdatennetz	
Dokumentenablage	VIS: 25.10-1073-20259/2020	
Ersteller (Name/Rolle)	TLRZ Wittmann, Daniel	

Dokumentenfreigabe:

Stufe	Z.S.	Kategorie	Erlassen von	Erlassen für	Fällig am	erledigt	Aufgabe	Vermerk
1	1.1	Mitzeichnung	Weide, Günter	Sperling, Stefan	28.09.2020	02.10.2020 14:58	bitte mitzeichnen	Anpassung in Kap. 8 zur Abstellung der Abweichung AG-002 (Klarstellung der Weisungsbefugnis) erfordert neue Freigabe durch L
2	1.1	Mitzeichnung	Weide, Günter	Plehn Dr., Claudia	02.10.2020	02.10.2020 15:57	bitte mitzeichnen	
3	1.1	Unterschrift	Weide, Günter	Brückner Dr., Thomas	02.10.2020	05.10.2020 09:54	bitte unterschreiben	

Inhaltsverzeichnis

1 Allgemeines

1.1 Zielsetzung

Ziel dieses Dokumentes ist eine verbindliche Festlegung der Leitlinie zur Informationssicherheit. Alle Beschäftigten im Geltungsbereich gewährleisten die IT-Sicherheit durch ihr verantwortliches Handeln und halten die für die IT-Sicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Für den IT-Einsatz sind die Sicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität, im jeweils erforderlichen Maße zu erreichen.
Neben der Beachtung gesetzlich vorgeschriebener Sicherheitsanforderungen müssen sich daraus ergebende Sicherheitsmaßnahmen zugleich auch immer im Verhältnis zum Schutzzweck einer Angemessenheitsprüfung unterzogen werden (gem. § 54 ThürDSG). Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen ist darauf zu achten, dass der Ablauf von Geschäfts- und Verwaltungsprozessen möglichst wenig durch Maßnahmen, welche die Informationssicherheit betreffen, beeinträchtigt wird.

1.2 Geltungsbereich

Das vorliegende Dokument gilt für den Informationsverbund „Corporate Network Freistaat Thüringen CNFT“ [2].

1.3 Geltungsdauer/ Revision

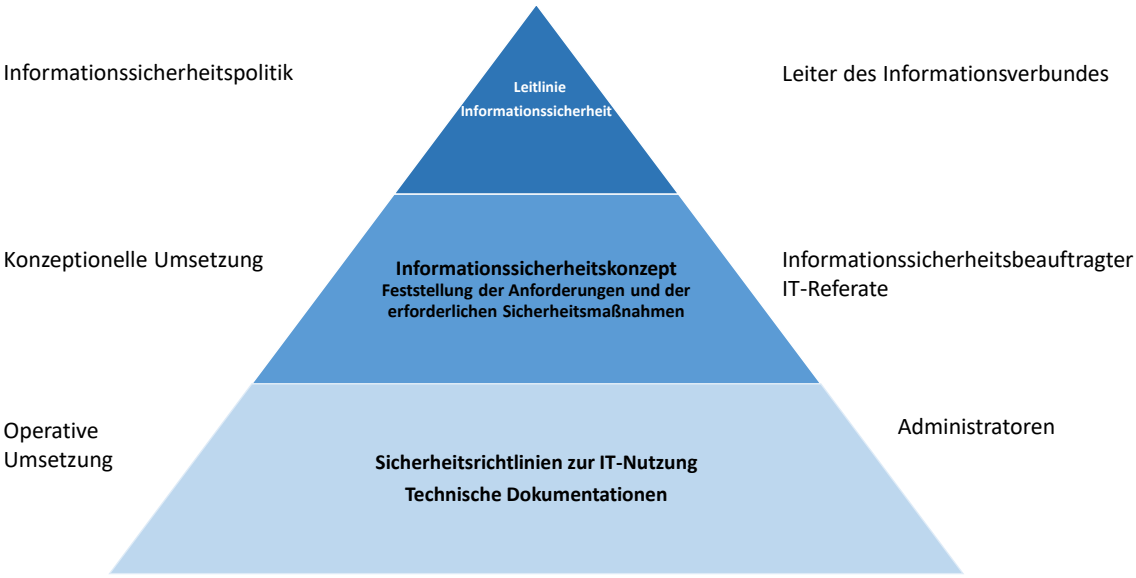
Die Gültigkeitsdauer dieses Dokuments ist nicht befristet.
Das vorliegende Dokument wird entweder anlassbezogen oder mindestens alle 2 Jahre einer überprüfenden Fortschreibung unterzogen. Das Dokument wird dabei, nach dem KVP durch Mitglieder des ISM-Teams des Informationsverbundes inhaltlich überprüft und im Bedarfsfall fortgeschrieben. Dieses Dokument unterliegt der Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen [1].

2 Einleitung

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 die zunehmende technische Vernetzung, Integration sowie Entwicklung der externen Bedrohungslage. Zur Sicherstellung der Erfüllung der Fachaufgaben ist eine Beeinträchtigung von Informationsinfrastrukturen und deren Komponenten weitestgehend zu vermeiden.
Kraft Erlass (O 1009 – 25.30/2017/2018 – 18.1; Dok.:13741/2018 vom 1.3.2018) zum Übergang der Betriebsverantwortung für den Informationsverbund gemäß Geltungsbereich, erlässt der Leiter des TLRZ, im Bewusstsein des Stellenwerts der Informationssicherheit für die Landesverwaltung und der Bedeutung des Landesdatennetzes sowie der Telefonie für die Aufgabenerfüllung, die vorliegende Informationssicherheitsleitlinie als die grundlegende Regelung zur Informationssicherheit. In diesem Dokument werden die Ziele, Vorgehensweisen, Organisationsstrukturen sowie Aufgaben für das Informationssicherheitsmanagement des Informationsverbundes „"Corporate Network Freistaat Thüringen (CNFT)"“ 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 und des Informationsverbundes erarbeitet.
Die Thüringer Staatskanzlei, jedes Ministerium sowie der Thüringer Rechnungshof und der Thüringer Landtag achten in ihrem jeweiligen Geschäftsbereich auf die Einhaltung dieser Leitlinie. Soweit diese für ihre Geschäftsbereiche Regelungen zur Informationssicherheit erarbeiten, geschieht dies stets im Einklang mit dieser Leitlinie.

3 Stellenwert der Informationsverarbeitung

Informationsverarbeitung spielt eine Schlüsselrolle für die Aufgabenerfüllung in der Thüringer Landesverwaltung. Sie ist ein integraler Bestandteil der Prozesse, insbesondere der Geschäftsprozesse. Damit ist sie wesentlich für die Aufrechterhaltung des geforderten, hohen Sicherheitsniveaus, für das Wirken der Verwaltung und zum Schutz der Daten und Informationen der Dienstleister, der Lieferanten sowie der Bürger und Mitarbeiter verantwortlich. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Für die Thüringer Landesverwaltung ist die Gewährleistung der Informationssicherheit nicht nur Verpflichtung zur Erfüllung gesetzlicher und regulatorischer Auflagen, sondern auch ein Gütezeichen für die bürgerorientierten Dienstleistungen.
Informationssicherheit hat damit einen bedeutenden Stellenwert für die Thüringer Landesverwaltung. Auch in Teilbereichen darf der Betrieb nicht zusammenbrechen oder komplett ausfallen. In Abwägung der Werte der zu schützenden Informationen, der Risiken und des Aufwands an Personal und Finanzmitteln für Informationssicherheit ist für eingesetzte und geplante IT-Systeme im Thüringer Landesverbund ein angemessenes Informationssicherheitsniveau anzustreben und zu verwirklichen. Für IT-Systeme mit normalem Schutzbedarf sind Sicherheitsmaßnahmen auf der Grundlage der IT Grundschutzkataloge des BSI als Standard vorzusehen und umzusetzen. Für Bereiche, in denen ein höherer Schutzbedarf festgestellt wird, müssen ergänzende Sicherheitsmaßnahmen eingeführt werden.



3.1 Grundsätze der Informationssicherheit

Im Geltungsbereich dieser Leitlinie finden die Methoden und Sicherheitsstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 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 sowie Sensibilisierung der Mitarbeiter.

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

3.2 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 muss der finanzielle und technische Aufwand im Verhältnis zu den tatsächlichen Risiken stehen.

3.3 Bereitstellung von Ressourcen

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

3.4 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.
Die Bediensteten der gesamten Landesverwaltung gewährleisten die notwendige und angemessene Informationssicherheit durch verantwortungsvolles Handeln.

3.5 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.

3.6 Einhaltung von Gesetzen, Richtlinien und Regeln (Compliance)

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

3.7 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.

3.8 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. Kein Zugriff erfolgt ohne Antrag.

3.9 Sicherung und Verbesserung

Die regelmäßige Aktualisierung, Vervollständigung, Verbesserung und Wirksamkeitsprüfung der eingesetzten Sicherheitsmaßnahmen stellen einen permanenten Prozess dar.

4 Übergreifende Ziele

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.

5 Definierte Sicherheitsziele

Zur Gewährleistung eines Sicherheitsniveaus für die Nutzer und deren Daten/ Informationen, welches den gesetzlichen Anforderungen entspricht, gelten die folgenden Sicherheitsziele für den definierten IT- Informationsverbund:

- Informationen nur für den notwendigen Nutzerkreis „Kenntnis nur, wenn nötig“;
- Nutzung nur nach Schulung;
- Zugang wird nur auf Antrag erteilt;
- Einsatz von zulässigen und zwingend notwendigen informationstechnischen Sicherheitsinstrumenten;
- Einsatz von unbedingt notwendigen informationstechnischen Sicherheitsinstrumenten und Darstellung der Konsequenzen bei Nichteinsatz und
- Darstellung des Verhältnisses von Schutzmaßnahmen und Schutzzweck.

5.1 Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Nachrichten, Daten und Informationen gegenüber anderen Nutzern, unautorisierten Mitarbeitern oder Dritten. Vertrauliche Daten und Informationen werden ausschließlich Befugten in der zulässigen Weise zugänglich gemacht.
Dies beinhaltet für den IT- Informationsverbund insbesondere:

- Vermeidung unbefugten Zutritts;
- Verhinderung des unbefugten Zugangs;
- Verhinderung des unbefugten Zugriffs auf sensible Daten sowie
- verschlüsselter Transport der Daten.

5.2 Integrität

Integrität beinhaltet den Schutz vor unerlaubter Veränderung oder Verfälschung / Manipulierung von Informationen. Dies betrifft die Daten, die im IT- Informationsverbund gespeichert sind und die Daten, die zwischen verschiedenen Netzanbietern übertragen werden. Sofern unautorisierte Veränderungen erfolgen, sind diese feststellbar. Auch die Konfiguration von Diensten und Systemen darf nicht unautorisiert verändert werden.

5.3 Verfügbarkeit

Verfügbarkeit ist die Zur-Verfügung-Stellung von Diensten und Dienstleistungen, die es den Benutzern jederzeit (mit Ausnahme zumutbarer Ausfallzeiten) ermöglichen, diese im zugesicherten Rahmen zu nutzen. Im Einzelnen wird sichergestellt, dass eine Verfügbarkeit der Dienste des Landesdatennetzes von 99,5 % pro Jahr gewährleistet ist. Ein Ausfall bis zu 24 Stunden, im Falle eines schwerwiegenden Ereignisses bis zu 48 Stunden ist hinnehmbar.

6 Detailziele

Verspätete oder fehlerhafte Entscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für die Leitungsebene bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungsdaten wichtig.
Die Datenschutzgesetze verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten sowie der Daten der Bürger und Unternehmen. Die Daten und die IT-Anwendungen der Behörden und Einrichtungen der Thüringer Landesverwaltung werden daher als besonders schützenswert betrachtet.
Die Abwicklung von Verwaltungsprozessen darf nicht verzögert oder gar gefährdet werden. Wenn festgelegte Fristen nicht eingehalten werden können, kann dies weitreichende negative Folgen haben.
Insbesondere eine mangelhafte Verfügbarkeit der IT-Systeme und Daten, aber auch Fehlfunktionen können zu Einschränkungen der Verwaltung des Landes und der Dienste für Bürger und Unternehmen führen. Die Aufrechterhaltung der Kommunikation und der ständige Zugriff auf korrekte Daten für die Mitarbeiter haben einen wichtigen Stellenwert.
Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch entsprechende Maßnahmen ist sicherzustellen, dass die Risiken der Internet- und E-Mailnutzung möglichst gering bleiben.
Für bereits betriebene und für geplante Informationstechnik wird ein Informationssicherheitskonzept erstellt und fortgeschrieben. Um den möglichen Risiken und Schäden vorzubeugen, müssen organisatorische und technische Maßnahmen zur Informationssicherheit umgesetzt werden.
Die Verantwortlichen haben bei Verstößen und Beeinträchtigungen die zur Aufrechterhaltung des IT-Betriebes und der Informationssicherheit geeignete und angemessene Maßnahmen zu ergreifen.
Der Zugriff auf IT-Systeme, Anwendungen und Daten und Informationen muss auf den unbedingt erforderlichen Personenkreis beschränkt werden. Jeder Bedienstete erhält nur auf diejenigen Daten und Informationen die Zugriffsberechtigungen, die er zur Erfüllung seiner dienstlichen Aufgaben benötigt. Abweichungen hiervon bedürfen einer besonderen Begründung und Regelung. Anträge sind schriftlich zu stellen.

Die Informationssicherheit soll besonders durch Anwendung von Verfahren und Tools nach dem jeweiligen Stand der Technik maximiert werden.
Alle Beschäftigten werden im Zuge von Schulungs- und Sensibilisierungsprogrammen für Informationssicherheit in die Lage versetzt, Sicherheitsmaßnahmen in ihrem Bereich umzusetzen und zu unterstützen.
Die für die Umsetzung der Maßnahmen zur Informationssicherheit erforderlichen Ressourcen und Investitionsmittel werden bereitgestellt.
Die Wirksamkeit der Maßnahmen zur Informationssicherheit muss regelmäßig kontrolliert werden. Bei Bedarf sind diese anzupassen.

7 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 (ISM) bezeichnet.

7.1 Referatsleiter Informationssicherheit

Alle Aufgabenbereiche der Informationssicherheit sind im TLRZ im Referat 25 gebündelt. Der Referatsleiter dieses Referats gibt deshalb alle operativen Dokumente dazu frei und leitet das ISM Team des Informationsverbundes

7.2 Informationssicherheitsbeauftragter des Informationsverbundes

Für das zentrale ressortübergreifende Verbindungsnetz und den Dienst der zentralen Telefonanlage ist für den Informationsverbund gemäß Geltungsbereich ein Informationssicherheitsbeauftragter (ISB-Verbund) einzusetzen.
Der ISB-Verbund nimmt folgende Aufgaben für diesen ressortübergreifenden Verbund wahr:

- Planung, Koordination, Steuerung und Dokumentation des landesweiten Informationssicherheitsprozesses für den Informationsverbund;
- Initiierung und Koordinierung der Erstellung und Fortschreibung des ressortübergreifenden Sicherheitskonzepts für den Informationsverbund,
  - des Notfallvorsorgekonzepts sowie
  - weiterer landeseinheitlicher Richtlinien und Regelungen zur Informationssicherheit in der Landesverwaltung bezogen auf den Informationsverbund;
- Initiierung und Koordinierung eines landesweiten Realisierungsplans für Sicherheitsmaßnahmen und Kontrolle der Umsetzung des landesweiten Realisierungsplans bezogen auf den Informationsverbund;
- Untersuchung sicherheitsrelevanter Vorfälle von erheblicher Bedeutung und

- Initiierung und Steuerung von Angeboten für Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit.

- Regelmäßiges Reporting an den Leiter des Informationsverbundes

7.3 Informationssicherheitsmanagement-Team (ISM-Team CNFT)

Zur Umsetzung der Informationssicherheitsorganisation wurde ein ISM-Team für den Informationsverbund gebildet (ISM-Team CNFT). Um die verschiedenen Aspekte der Informationssicherheit dieses Informationsverbundes berücksichtigen zu können, arbeitet dieses ISM-Team eng mit dem ISB-Land zusammen. Dem ISM-Team CNFT gehört mindestens ein Vertreter des TFM, ein Vertreter des CERT-Thüringen, der ISB-IVB sowie der verantwortliche Betriebsleiter des TLRZ an.

Die Aufgaben des ISM-Teams CNFT Konvergentes Sprach- und Datennetz der Thüringer Landesverwaltung – Corporate Network umfassen:

- die Erarbeitung der Informationssicherheitsziele und der Informationssicherheitsleitlinie sowie deren Fortschreibung;

- die Erstellung von IT-Sicherheitsstandards;

- die Erstellung und Fortschreibung des Sicherheitskonzepts, des Notfallvorsorgekonzepts sowie weiterer Richtlinien und Regelungen zur Informationssicherheit;

- die landesweite Überwachung der Umsetzung der Vorgaben der Regelungen zur Informationssicherheit bezogen auf den Informationsverbund;

- 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 mit Bezug zum Informationsverbund;

- die Erarbeitung von Schulungs- und Sensibilisierungsprogrammen für die Informationssicherheit sowie

- die Weiterleitung von kritischen Sicherheitsvorfällen an das Computer Emergency Response Team (ThüringenCERT) zur Überprüfung.

8 Durchsetzung der Leitlinie

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.

Verstöße der angeschlossenen Behörden und Einrichtungen gegen die CNFT-Anschlussbedingungen werden nicht toleriert. Wenn Abweichungen festgestellt werden und nicht in angemessener Zeit abgestellt werden, kann der ISB-Land die Trennung der jeweiligen Behörde oder Einrichtung vom Landesdatennetz veranlassen.

9 Sicherheitsmaßnahmen

Für alle verantwortlichen Funktionen sind Vertretungen eingerichtet. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können.
Gebäude und Räumlichkeiten sind durch ausreichende Zutrittskontrollen zu schützen. Der Zugang zu IT-Systemen ist durch angemessene Zugangskontrollen und der Zugriff auf die Daten ist durch ein restriktives Berechtigungskonzept zu schützen.
Schadsoftware-Schutzprogramme sind auf allen IT-Systemen einzusetzen. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.
Details hierfür werden in den CNFT-Anschlussbedingungen festgelegt [4].
Ein Notfallvorsorgekonzept ist zu erstellen, um bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.
Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.
Sofern IT-Dienstleistungen an externe Stellen ausgelagert sind, werden konkrete Sicherheitsanforderungen in den Service Level Agreements (SLA) vorgegeben und in entsprechenden Verträgen dokumentiert.

10 Verbesserung der Sicherheit

Das Managementsystem der Informationssicherheit und die Umsetzung von Anschlussbedingungen werden regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.
Die Leitung der Behörden und Einrichtungen unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.
Der ISB des Informationsverbundes führt mit dem Referatsleiter Informationssicherheit mindestens einmal jährlich ein Reviewmeeting zum Status und der Entwicklung der Informationssicherheit im Verbund durch.
Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und die IT-Sicherheit ständig auf dem aktuellen Stand der Technik zu halten.

11 Ausnahmeregelung

Eine Abweichung von den vorgenannten Festlegungen ist in der Dokumentation des entsprechenden Veränderungsvorgangs (Change) zu begründen, vom zuständigen ISB zu befürworten und vom zuständigen Vorgesetzten gemäß CAB zu genehmigen.

12 Freigaberegelung

Das vorliegende Dokument tritt am Tag nach der Bekanntgabe/Veröffentlichung in Kraft.

13 Mitgeltende Unterlagen

[1] Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen
Dokument: 1030.ISMS.RL_Dokumentenlenkung

[2] Definition Untersuchungsgegenstand
Dokument: 0002.ISMS_Index_Definition_Untersuchungsgegenstand

[3] Organigramm
Dokument: 0040.ISMS.Index_Aufbauorganisation_(Organigramm)

[4] CNFT-Anschlussbedingungen
Dokument: 0070_RL_Anschlussbedingungen_Dienststelle

14 Änderungsverzeichnis

Datum (aktuelle oben)	Version	Geänderte Kapitel	Beschreibung der Änderung	Autor
05.10.2020	5.0		Freigabe	Dr. T. Brückner
28.09.2020	4.2	Alle	Änderung Formatvorlage und Redaktion	D. Wittmann
31.08.2020	4.1	8	Anpassung AG-002 Audit	G. Weide
24.06.2019	4.0		Freigabe	T. Gräbe
13.06.2019	3.1	1.2	Prüfung auf AS-001 Auditbericht. Geltungsbereich angepasst.	G. Weide
13.11.2018	3.0		Freigabe (Leiter TLRZ)	Dr. T. Brückner
15.10.2018	2.0		Freigabe (Leiter TLRZ)	Dr. T. Brückner
15.09.2015	1.2		Endredaktion und Freigabe	H. Hartwig