Freistaat Thüringen
Thüringer Landesrechenzentrum

Informationssicherheitsmanagement des TLRZ

Richtlinie zur Internetnutzung

Version / Datum	5.1	07.12.2020
Dateiname	2103.ISMS.RL_Internetnutzung.Docx	
Dokumententyp	Richtlinie	
Vertraulichkeitsstufe	**TLP GREEN**	
Verantwortlicher	ISB TLRZ	
Erstellt am	19.02.2020	
Status	**freigegeben**	
Verteiler	TLRZ A1-A3, CNFT	
Dokumentenablage	VIS: 25.10-1073-14533/2020	
Ersteller (Name/Rolle)	TLRZ Wittmann, Daniel	

Dokumentenfreigabe:

Stufe	Z.S.	Kategorie	Erlassen von	Erlassen für	Fällig am	erledigt	Aufgabe	Vermerk
1	1.1	Unter-schrift	Weide, Günter	Sperling, Stefan	20.07.2020	05.10.2020 15:49		

Inhaltsverzeichnis

1 Allgemeines

1.1 Zielsetzung

Dieses Dokument regelt die Anforderungen aus Sicht der Informationssicherheit, für die Nutzung des dienstlich bereitgestellten Internetzugangs.

Umzusetzende Anforderungen sind dabei mit dem Schlüsselwort Festlegung gekennzeichnet, im gesamten Dokument fortlaufend nummeriert und eingerahmt. Texte außerhalb der eingerahmten Festlegungen gelten als Erklärungen und Erläuterungen.

1.2 Geltungsbereich

Das vorliegende Dokument gilt für alle, mit dem Internet verbundene, IT-Systeme die vom TLRZ verwaltet, bereitgestellt und/ oder betrieben werden. Darüber hinaus gilt es explizit für den Informationsverbund „Corporate Network Freistaat Thüringen" (CNFT)“

Den Behörden und Einrichtungen der Thüringer Landesverwaltung wird die sinngemäße Anwendung empfohlen, wenn keine eigenen Regelungen getroffen wurden.

1.3 Geltungsdauer/ Revision

Die Geltungsdauer 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 [2].

2 Goldene Regeln

Die folgenden Regeln gelten als die elementaren Anforderungen und sollen einen schnellen ersten Überblick bieten.

- In Browser und E-Mail-Clients dürfen nur notwendige Funktionalitäten aktiviert werden.
- Medieninhalte Inhalte aus E-Mail oder Webseiten dürfen nicht automatisiert ohne interaktive Bestätigung durch den Nutzer heruntergeladen werden.
- Cookies sollten unterdrückt und mindestens regelmäßig gelöscht werden.
- Der Browserverlauf muss regelmäßig gelöscht werden.
- Passwörter und Daten zur Autovervollständigung dürfen nicht im Browser gespeichert werden.
- Die Verbreitung von Spam-Mails sollte vermieden werden.
- Jeder Nutzer muss sich im Internet so verhalten und nur den Informationsgehalt veröffentlichen, dass kein Schaden für die Institution und den Freistaat Thüringen entsteht.

3 Einleitung

Das Internet als Medium zur Informationsbeschaffung und Kommunikation ist in der heutigen Zeit zur Selbstverständlichkeit geworden. Die Mitarbeiter im Informationsverbund sind auf dessen Nutzung im beruflichen Alltag angewiesen, sei es durch die Nutzung von E-Mail als bevorzugtes Kommunikationsmedium, oder das Internet selbst als Quelle zur Kommunikationsbeschaffung. Mit Hilfe von E-Mails können z.B. kleinere Dateien effizient transportiert und das Mailsystem als Groupware-Lösung genutzt werden.

Jedoch können durch unsachgemäße Nutzung des Internets diverse Bedrohungen für den Freistaat Thüringen entstehen, welche z.B. der Verlust der Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener, vertraulicher und weiterer sensibler Informationen beinhalteten kann. Weiter kann auch bei falschen Verhalten im Internet der Mitarbeiter selbst seiner persönlichen informellen Selbstbestimmung schaden.

Für die Aspekte zu sicheren Internetnutzung existieren im IT-Grundschutzkompendium noch keine Bausteine mit Anforderungen. Deshalb wird in dieser Richtlinie noch auf Maßnahmen aus den IT-Grundschutzkatalogen verwiesen.

4 Administrative Regelungen

Die administrativen Regelungen verfolgen das Ziel, dass E-Mail- und Internet-Programme sowie die jeweiligen Hardwarekomponenten, durch das entsprechende Referat soweit konfiguriert werden, dass ohne das Zutun des Nutzers, die optimale Sicherheit erreicht wird.

4.1 Allgemeine Regelungen

Festlegung 1	Änderungen an den festgelegten Sicherheitseinstellungen durch die Benutzer sind verboten. Die Änderung der Einstellungen durch den Benutzer sollte technisch verhindert werden.

Festlegung 2	Der Schutz vor Schadprogrammen (bspw. Antiviren-Programme) muss bei der Internet Nutzung aktiviert und aktuell sein.

Dazu gelten die getroffenen Festlegungen der Richtlinie zum Schutz vor Schadprogrammen[5].

Festlegung 3	Es sollten bei Browsern und E-Mail-Clients nur die Programme und Funktionalitäten aktiviert werden, die zwingend benötigt werden.

Festlegung 4	Laptops müssen mit einer aktiven Personal Firewall ausgestattet sein, insbesondere vor Anbindung an das Internet über fremde Netze.

Festlegung 5	Für den Datenverkehr und den beteiligten Systemen, sowie bei sicherheitsrelevanten Ereignissen, gelten die Festlegungen der Richtlinie zur Protokollierung[3].

4.2 Regelungen zu E-Mail Clients und deren Administration

Festlegung 6	Im Falle einer automatischen Weiterleitung von E-Mails, muss die Vertraulichkeit gewahrt bleiben, indem sichergestellt wird, das alle Empfänger die E-Mails auch lesen dürfen.

Festlegung 7	Aktive Inhalte dürfen bei der Anzeige in E-Mail-Clients nicht automatisch ausgeführt werden.

Festlegung 8	Die Aktivierung einer automatischen Lesebestätigung sollte (zwecks Spamvermeidung) vermieden werden.

Festlegung 9	E-Mail-Clients sind so zu konfigurieren, dass Anhänge nicht automatisch gespeichert werden.

Festlegung 10	Spam-Filter müssen stetig aktualisiert werden.

4.3 Regelungen zu Browsern und der Administration

Festlegung 11	Es dürfen nur Browser verwendet werden, die TLS unterstützen. Es müssen die Mindeststandards des BSI zur Verwendung von TLS[1] eingehalten werden.

Festlegung 12	Cookies sollten aus datenschutzrechtlichen Gründen unterdrückt und regelmäßig gelöscht werden.

Festlegung 13	Cookies von Drittanbietern dürfen nicht akzeptiert werden.

Festlegung 14	Browserverlauf und die Liste zur Autovervollständigung muss regelmäßig gelöscht werden.

Zur Umsetzung von Festlegung 12 und Festlegung 14 wird empfohlen, die Browser so zu konfigurieren, dass dieser Cookies, Browserverlauf, Autovervollständigungsliste und weitere aufgezeichnete Daten nach Beenden der Internetsitzung automatisch löscht.

Festlegung 15	Die Funktion zur Autovervollständigung muss deaktiviert werden

Festlegung 16	Verfügt der Browser über Adress- und inhaltsbasierte Schutzmechanismen implementiert sind, die mit externen Diensten kommunizieren, müssen diese deaktiviert werden.

Festlegung 17	Die Funktion einiger Browser, heruntergeladene Inhalte automatisch zu öffnen muss deaktiviert sein.

[1] Mindeststandards des BSI zur Verwendung von Transport Layer Security.

Festlegung 18	Die Browser sollten auf den aktuellen Patch- und Update-Stand gehalten werden.

Festlegung 19	Die Same-Origin-Policy[2] muss aktiviert werden.

Festlegung 20	Adobe Flash Funktionen müssen blockiert bzw. an der Ausführung gehindert werden.

Festlegung 21	Der Browser muss so konfiguriert werden, dass eine Erweiterung zur Medienfreigabe nur nach interaktive Bestätigung durch Benutzer ausgeführt wird.

Festlegung 22	Der Browser muss nach seiner Initialisierung mit minimalen Rechten im Betriebssystem ablaufen. Ist es notwendig, dass der Browser für die Initialisierung mit erhöhten Rechten laufen muss, dann muss der Browser diese nach der Initialisierung wieder abgeben.

5 Allgemeine Rechte und Pflichten der Nutzer

Im Allgemeinen sind alle Mitarbeiter dazu angehalten sich stets selbstständig über das Thema „sicherer Umgang mit dem Internet“ zu informieren und auf dem aktuellsten Stand zu halten.

Festlegung 23	Informationen, welche nicht der vertraulichkeitsstufe „offen“ unterliegen oder als „TLP-White“[3] klassifiziert wurden dürfen nicht über ungeschützte Internet-Dienste weitergegeben werden.

Festlegung 24	Die berechtigte Weitergabe von Informationen mit der Vertraulichkeitseinstufung „Für den Dienstgebrauch“ oder einer Klassifizierung als „TLP-Green“[3] muss immer mittels einer Transportverschlüsselung geschützt werden.

[2] Die Same-Origin-Policy ist ein Protokoll, welche es clientseitigen Script-Sprachen untersagt auf Inhalte (bspw. Grafiken) zuzugreifen, die auf eine andere Webseite verweisen, bzw. weiterleiten. Dies verringert die Gefahr, dass der Browser sowie der Client-PC Ziel eines Angriffes werden.

[3] Die einzelnen Definitionen der Stufen für eine Klassifizierung nach dem TLP-Protokoll und weitere Pflichten, die im Umgang mit TLP klassifizierten Informationen bestehen, können der Richtlinie zur Dokumentenlenkung[2] entnommen werden.

Festlegung 25	Informationen, die den Freistaat Thüringen mit seinen angebundenen Behörden und Einrichtungen in einem falschen Licht erscheinen lassen könnten, dürfen nicht über ungeschützte Internet-Dienste weitergegeben werden

Festlegung 26	Anwendungen, welche für den Zugriff auf Internet-Dienste genutzt werden, müssen durch das TLRZ freigegeben worden sein. Die Nutzung und Installation von nicht freigegebener Software ist verboten.

Diese Festlegung gilt ebenfalls für Browser-Erweiterungen (Plug-Ins) und portable Software.

Festlegung 27	Im Browser dürfen keine Passwörter und Zahlungsinformationen gespeichert werden.

Festlegung 28	Vor einer Weitergabe von Texten, Fotos, etc. müssen das Urheberrecht, das allgemeine Persönlichkeitsrecht (Recht am eigenen Bild) bzw. weitere Gesetze zum Schutz von persönlichen und geschäftlichen Daten berücksichtigt werden.

Die Regelung gilt auch bei der Wiederverwendung oder Zweitverwertung von fremden Informationen.

Festlegung 29	Die geltenden rechtlichen Vorschriften bezgl. Inhalte aus dem Internet, welche als illegal, verfassungsfeindlich, extremistisch oder pornografisch angesehen werden können, müssen eingehalten werden.

Festlegung 30	Jeder Nutzer sollte die Verbreitung von Spam vermeiden.

Dazu werden folgende Maßnahmen empfohlen:

- E-Mail-Adresse sparsam weitergeben
- E-Mail-Adresse nicht im Internet in Klarschrift veröffentlichen
- bei allen verdächtigen wirkenden (Junk)E-Mails und Newslettern nicht auf den enthaltenen Link klicken

Festlegung 31	Bei auftretenden Sicherheitsproblemen oder Verdacht auf solche, muss der zuständige ISB bzw. das Thüringen CERT involviert werden.

Dies schließt auch den Verdacht auf Schadcode-behaftete E-Mails bzw. E-Mail-Anhängen mit ein.

Festlegung 32	E-Mails an mehrere externe Empfänger sollten so versandt werden, dass Verteilerlisten oder die „BCC-Option“ benutzt werden.

Festlegung 33	Dateien und Programme dürfen nur durch Berechtigte von vertrauenswürdigen Quellen heruntergeladen werden.

Festlegung 34	E-Mail Anhänge aus unbekannten Quellen, oder die – mit Hinblick auf die Informationssichert – auffällig erscheinen dürfen nicht geöffnet werden.

6 Korrektes Auftreten im Internet

Auf ein korrektes Verhalten im Internet ist stets von allen Mitarbeiter zu achten, da im Internet getroffene Aussage, in der Öffentlichkeit, häufig nicht als Aussage der Person, sondern der Institution aufgefasst werden.

Festlegung 35	Jeder Benutzer sollte sich im Internet angemessen verhalten, also die Netiquette beachten.

Als Netiquette (die Netz-Etikette) werden Höflichkeitsregeln und Verhaltensvorschläge bezeichnet, die sich mit der Zeit bei der Nutzung des Internet eingebürgert haben und deren Einhaltung gewährleisten soll, dass jeder das Internet effizient und zu aller Zufriedenheit benutzen kann.

Grundsätzlich sind getätigte Aussage oder bereitgestellte Informationen im Internet, einer öffentlichen Bekanntmachung gleichzusetzten (in der analogen Welt vergleichbar mit einer Plakatwand), dies sollte sich jeder Mitarbeiter vor einer Veröffentlichung von Aussagen oder Informationen bewusstmachen.

Festlegung 36	Jegliche Informationen sollten im Internet nur nach genauer Überlegung, wie z.B. können diese Informationen auf ihre Person oder den Freistaat Thüringen zurückfallen, veröffentlicht werden. (Grundsatz der Datensparsamkeit)

Festlegung 37	Informationen dürfen nur denen zugänglich gemacht werden, die sie wirklich kennen sollten. (Need-to-Know Prinzip)

Festlegung 38	Blogs, Foren, Mailinglisten und ähnliche Anwendungen sollten so genutzt werden, dass private Aussagen nicht mit dienstlichen vermischt oder missverstanden werden können.

Festlegung 39	Aus Meta-Daten von Dateien sollten alle unnötigen Zusatzinformationen entfernt werden.

Festlegung 40	Es sollten Informationen immer so weitergegeben werden, dass sie sich im gewählten Medium möglichst einfach lesen und bearbeiten lassen.

7 Sichere Anmeldung bei Internet-Diensten

Die folgenden Festlegungen gelten für Webseiten und Internet-Dienste, die eine Anmeldung des Nutzers fordern.

Festlegung 41	Bei der Anmeldung an Internet-Diensten sollten deren Datenschutz-Hinweise gelesen und überprüft werden, ob diese mit den Regelungen des Freistaats Thüringen konformgehen.

Festlegung 42	Für die Anmeldung an Internet-Diensten, welche nicht ausschließlich für dienstliche Zwecke genutzt werden, dürfen keine dienstliche Anmeldedaten verwendet werden.

Festlegung 43	Bei der Anmeldung an Internet-Diensten muss der Grundsatz der Datensparsamkeit beachtet werden.

Festlegung 44	Für die Anmeldung an Internet-Diensten dürfen nicht die gleichen Passwörter, wie für die Anmeldung an internen Systemen verwendet werden.

Die gewählten Passwörter müssen den Anforderungen der Passwortrichtlinie entsprechen.

Festlegung 45	Anmeldungen sollten nur über SSL gesicherte Verbindungen vorgenommen werden.

Festlegung 46	Um Social Engineering oder Phishing Angriffen vorzubeugen sollten bei Sicherheitsabfragen keine korrekten Antworten hinterlegt werden.

Sicherheitsabfragen zielen meistens auf Informationen aus den persönlichen Lebensbereich. Dieser kann jedoch durch Social Engineering Maßnahmen durch einen Angreifer analysiert werden und somit die richtige Antwort der Sicherheitsabfragen erraten werden. Der ist es sinnvoll eine Antwort auf Sicherheitsabfragen zu wählen, die kein Angreifer erraten, aber die man sich selbst merken kann.

8 Ausnahmeregelung

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

9 Freigaberegelung

Das vorliegende Dokument tritt am Tag nach der Bekanntgabe/Veröffentlichung in Kraft und muss vor der Veröffentlichung, entsprechend den Vorgaben der Richtlinie zur Dokumentenlenkung[2], freigegeben werden.

10 Mitgeltende Unterlagen

[1] Leitlinie zur Informationssicherheit
Dokument: 1010.ISMS.RL_Leitlinie_Informationssicherheit

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

[3] Richtlinie Protokollierung
Dokument: 2456.ISMS.RL Protokollierung

[4] Passwortrichtlinie
Dokument: 2250.ISMS.RL_Passwort

[5] Richtlinie zum Schutz vor Schadprogrammen
Dokument: 2311.ISMS:RL Schutz vor Schadprogramme

[6] Hilfsdokument zum „Mindeststandard des BSI zur Verwendung von Transport Layer Security“
URL:
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards_Bund/TLS-Protokoll/TLS-Protokoll_node.html

11 Änderungsverzeichnis

Datum (aktuelle oben)	Version	Geänderte Kapitel	Beschreibung der Änderung	Autor
07.12.2020	5.1	5	Festlegung 30 formale Korrektur; keine erneute Freigabe notwendig	D. Wittmann
05.10.2020	5		Freigabe	St. Sperling
04.09.2020	4.3	Review		St. Sperling
19.08.2020	V 4.2	Alle	Erweiterung des Geltungsbereiches; Anpassung an neue Dokumentenvorlage; Präzisierung und Aktualisierung der Inhalte;	D. Wittmann
23.10.2019	V 4.1	Alle	Anpassung der Anforderungen an den erhöhten Schutzbedarf	T. Röder
30.01.2019	V 4.0		Freigabe	S. Sperling
21.01.2019	V3.2		Dokumentenvorlage geändert	K. Mühlstein
	V3.1	1.2, 2, 9	Änderungen im Kap. 1.2, 2 und 9	D. Tribess
27.11.2017	V 3.0		Freigabe	H. Hartwig
21.10.2017	V2.9	Alle	Review mit redaktionellen Änderungen	H. Seifert
01.09.2017	V 2.0	3, 4, 5	Präzisierung Festlegung 13, 16, 26, 27, 31, 39	G. Weide
10.08.2017	V 1.0		Dokument erstellt	M. Gischel