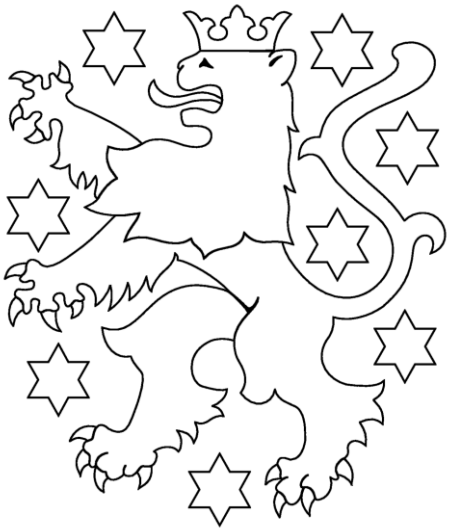
Freistaat Thüringen Finanzministerium

Informationssicherheits-management des Freistaats Thüringen

Passwortrichtlinie

Version **1.1**



Übersicht

Version	1.1	
Dokumentenname	ISMS_TFM_RL_Passwortrichtlinie_1.1.Docx	
Dokumententyp	Richtlinie	
Vertraulichkeitsstufe	**TLP:GREEN**	
Verantwortliche/ Autoren	Dirk Cieslak	
Erstellt am	15.07.2019	
Zuletzt geändert	06.05.2022	
Status	**freigegeben**	
	Name/Rolle/Datum	Unterschrift
Ersteller	Dirk Cieslak/TFM/03.05.2022	gez. D. Cieslak
Review/Prüfung	Holger Hartwig/ ISB-Land/06.05.2022	gez. H. Hartwig
Freigabe	Holger Hartwig/ ISB-Land/06.05.2022	gez. H. Hartwig
Dokumentenablage	1040-53-O 1009/1069-10-55398/2022	

Inhaltsverzeichnis

1 Allgemeines

1.1 Zielsetzung

Ziel dieses Dokumentes ist es, einheitliche verbindliche Mindestregeln für die Bildung und den Gebrauch von Passwörtern zum Systemzugang sicherzustellen, die zur Authentisierung berechtigter Benutzer eingesetzt werden. Im Rahmen zusätzlicher Dokumente können ressort- oder dienstellenspezifische Regelungen zur Ergänzung und Konkretisierung erlassen werden ohne dabei die nachstehenden Anforderungen zu senken.

Die Richtlinie ist im Rahmen der technischen Möglichkeiten auf alle IT-Systeme (Hardware) und Anwendungen anzuwenden und dient der Authentifizierung sowie dem Schutz der Ressourcen und Daten durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung.

1.2 Geltungsbereich

Das vorliegende Dokument gilt für alle Mitarbeiter der Thüringer Landesverwaltung in den Rollen „Nutzer/Service-Anwender“ und „Administrator/IT-Operator“ sowie für alle Anwender von IT-Fachverfahren der Thüringer Landesverwaltung. Gleiches gilt für beauftragte Dritte mit Zugriff auf die in der Landesverwaltung vorhandenen IT-Systeme oder deren Daten. Weiterführende Regelungen können in den Dienststellen in eigener Zuständigkeit festgelegt werden. Dabei darf das Sicherheitsniveau nicht herabgesetzt werden. Nutzungshinweise zur Anwendung der Richtlinie sind in eigener Verantwortung durch die Ressorts zu erstellen.

1.3 Revision

Die vorliegende Richtlinie wird entweder anlassbezogen oder mindestens alle 2 Jahre einer Fortschreibung unterzogen. Die Richtlinie wird gemäß dem Kontinuierlichen Verbesserungsprozess (KVP) durch den ISB-Land in Abstimmung mit den Mitgliedern des Informationssicherheitsmanagement-Teams Thüringen (ISM-Team) inhaltlich überprüft und im Bedarfsfall fortgeschrieben. Diese Richtlinie unterliegt der Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen [2].

2 Einleitung

Werden Daten mit Hilfe von Computern verarbeitet, so ist sicherzustellen, dass nur berechtigte Personen darauf zugreifen können und dies auch nur im dienstlich notwendigen Umfang stattfindet. Notwendig ist daher, dass sich derjenige, der auf diese Daten zugreifen will, zunächst gegenüber dem Computersystem authentisiert und seine Zugriffsberechtigung nachweist.

Das National Institute of Standards and Technologie (NIST) hat im Sommer 2017 seine 14 Jahre alten Empfehlungen und Regelungen zur Passwortsicherheit komplett überarbeitet und als Standard SP 800-63 Digital Identity Guidelines neu veröffentlicht. Grundlegende, früher ausgesprochene Empfehlungen wurden auf der Basis gewonnener Erkenntnisse in Frage gestellt und die Risiken von digitalen Identitäten neu betrachtet. Änderungen und Neuerungen sind u. a. bei der Entwicklung von Bedrohungsszenarien, von biometrischen Verfahren und nach modifizierten Anforderungen an die Speicherung von Langzeitgeheimnissen eingeflossen.

Auch die Datenschutz-Grundverordnung (DSGVO) stellt im Artikel 5 (Grundsätze für die Verarbeitung personenbezogener Daten), Artikel 32 (Sicherheit der Verarbeitung) sowie Artikel 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) Anforderungen in Bezug auf organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung bei der Erhebung, Verarbeitung und Speicherung personenbezogener Daten. Die Anforderungen der Informationssicherheit und des Datenschutzes werden in dieser Richtlinie berücksichtigt und angewendet.

3 Anforderungen an den Passwortaufbau

Aufgrund neuer Erkenntnisse des NIST und geänderter Bedrohungslage werden folgende Anforderungen an die Passwortbildung gestellt:

Ein sicheres Passwort hat beim Nutzer mindestens 12, beim Administrator 16 Zeichen lang zu sein (siehe Kapitel 8). Dafür ist die Komplexität einfach zu begrenzen, um eine leichte Handhabung zu ermöglichen. Bei der Passworterstellung gilt, dass **mindestens zwei von vier Merkmalen** der Passwortzeichenvergabe erfüllt sein müssen. Merkmale von Passörtern sind:

- Großbuchstaben (A bis Z)
- Kleinbuchstaben (a bis z)
- Ziffern/Zahlen (0 bis 9)
- Sonderzeichen (! * # , ; ? + - _ . = ~ ^ % ( ) { } [ ] | : ")

Hinweis: Bei der Verwendung von Umlauten, Satzzeichen, diakritischen Zeichen kann es auf Grund abweichender Tastaturbelegungen zu fehlerhaften Interpretationen bei der Passwortauswertung kommen. Daher sollte auf Sonderzeichen wie z. B. der Umlaute ä, ö, ü, Ä, Ö, Ü und ß zu Gunsten der Ersetzung ae, oe, ue usw. verzichtet werden.

Jedes weitere Zeichen erhöht die Passwortsicherheit.

Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden. Wortkombinationen oder logische Zahlen- oder Buchstabenreihen sind zu vermeiden. Bekannte Zitate, Redewendungen oder leicht zu erratende Zeichenketten sind nicht zu verwenden.
Zu vermeiden sind:

a. Häufige Zeichenwiederholungen (z. B. Tastaturmuster „AAAAA“ oder „BBB666“)
b. Zahlen und Daten aus dem Lebensbereich des Benutzers (z. B. Geburtstage, Telefonnummern, Namen der Kinder und Kombinationen daraus)
c. Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen (z. B. alt: „Sommer2018“ – neu: „Sommer2019“
d. Zeichen, die durch nebeneinanderliegende Tasten eingegeben werden (z. B. Tastaturmuster „qwertz“ oder „123456“)
e. Zeichenkombinationen, die Suchbegriffen in Wörterbüchern und Lexika entsprechen (Trivialpasswörter, wie z. B. Namen von Prominenten, Wörter „Passwort“ oder „Geheim“)

f. Es wird empfohlen, Umlaute zu vermeiden. Dies ist bei einer Nutzung im Ausland sowie bei Recovery-Szenarien sinnvoll, da die in diesen Fällen verwendete Tastatur ggf. Umlaute vermissen lassen, wodurch die Passworteingabe erheblich erschwert wird.

Ein gutes Passwort ist zum Beispiel „Dig:NmT_26.!“ – es besteht aus zwölf Zeichen, aus Groß- und Kleinbuchstaben und mischt Zahlen und Sonderzeichen. Je länger und komplizierter ein Passwort ist, desto länger dauert es, bis es gebrochen werden kann.

4 Pflichten der Bediensteten

Jeder Benutzer muss sich gegenüber dem IT-System oder Anwendung authentisieren, an denen gearbeitet werden soll. Dies erfolgt grundsätzlich unter Verwendung von Passwörtern. Das Erzeugen, Nutzen und Verändern von Passwörtern muss auf der Grundlage folgender Regeln umgesetzt werden:

1. Jeder Benutzer muss unter Berücksichtigung der Anforderungen aus Kapitel 3 ein sicheres Passwort bilden.

2. Für jedes einzelne Nutzerkonto muss ein anderes Passwort verwendet werden. Ausgenommen hiervon sind vollständig automatisierte Anmeldeverfahren, wie z. B. Single Sign-on.

3. Wenn Passwörter gespeichert werden, sind diese nur verschlüsselt und zugleich an einem sicheren Ort zu speichern (Passwortsafe/Kennworttresor möglich).

4. Passwörter sind personenbezogen. Die Weitergabe und das Teilen mi anderen sind nicht gestattet. Die Ausnahme hiervon stellen Serviceaccounts dar, die als nicht personalisierte Dienstkonten zulässig sind.

5. Während der Passworteingabe ist darauf zu achten, dass andere Personen dieses nicht wahrnehmen können.

6. Niedergeschriebene Passwörter sind verschlossen aufzubewahren.

7. Sobald ein Nutzer den Verdacht hat, dass sein Passwort bekannt geworden ist, ist dies **unverzüglich** zu ändern und Mitteilung an den Vorgesetzten sowie zuständigen ISB zu erstatten, um die notwendigen Änderungen und ggf. Schutzmaßnahmen vornehmen zu können.

8. Bei Endgeräten, die über einen Bildschirmschoner bzw. Sperrbildschirm verfügen, ist dieser passwortgeschützt zu aktivieren. Die Entsperrung muss mittels Passwortes, entsprechend den Regeln dieser Richtlinie oder anderen gleichwertigen, nicht zeichengebundenen Entsperrverfahren erfolgen.

9. Das Passwort darf nicht den Namen des Anwender-Accounts oder Teile des vollen Namens mit mehr als zwei aufeinanderfolgenden Zeichen enthalten.

5 Alternativen zur Passworteingabe

An Geräten, welche technisch üblicher Weise mit einer PIN oder biometrischer Verfahren gesichert werden, können diese alternativ zur Passworteingabe genutzt werden.

Auch für PIN-Nummern gelten die Regelungen der Anforderungen an den Passwortaufbau (siehe Kapitel 3) und sind entsprechend anzuwenden. So dürfen z. B. keine logischen Zahlenreihen oder leicht zu erratende Zeichenketten, wie z. B. Geburtstag des Nutzers verwendet werden. Spezielle Regelungen zu PIN-Vergabe und -Nutzung sind durch die Ressorts in eigener Verantwortlichkeit zu erstellen. Die Länge der PIN ist möglichst auf 6 Stellen oder mehr festzulegen.

Auch biometrische Verfahren der Authentisierung können angewendet werden, wenn die gespeicherten Merkmale nur lokal auf dem Endgerät gespeichert werden. Biometrische Daten unterliegen nicht der Pflicht des regelmäßigen Wechsels.

6 Definition der Geräte und Zugänge

Der Zugriff auf IT-Geräte, Daten und IT-Anwendungen ist nach dem aktuellen Stand der Technik und auf der Grundlage der vorliegenden Passwortrichtlinie zu gestalten.

Die Passwortrichtlinie gilt nicht für geschützte WLAN-Zugänge, die durch die Landesverwaltung betrieben werden sowie für Verfahren außerhalb des Geltungsbereichs der Passwortrichtlinie.

7 Systemadministration und Dienstkonten

Die in diesem Dokument getroffenen Regelungen gelten auch grundsätzlich für privilegierte Nutzer und System-Accounts. Auf Grund der exponierten Stellung (z. B. Active Directory Administratoren) handelt es sich um besonders gefährdete Angriffsziele und es müssen hierfür spezielle ergänzende Maßnahmen getroffen werden. So gelten für Tier0-Admin, Dienstkonten und Fehlersucheaccounts im AD spezielle Festlegungen, welche nicht Bestandteil der Richtlinie sind. Abweichende Regelungen hiervon sind in den gesondert erstellten Dokumenten des TLRZ aufgeführt.

Wenn möglich, sind für an Dienste gebundene Konten „Managed Service Accounts“ zu verwenden.[1]

Für den Fall der unbeabsichtigten Fehlkonfiguration oder Fehlfunktionen wird empfohlen, für derartige Fälle einen speziellen Notfallzugriff einzurichten (Break Glass Account). Dieser ist ausdrücklich nur auf Notfallsituationen oder Szenarien beschränkt, in denen normale Administratorkonten nicht verwendet werden können.

[1] https://blogs.technet.microsoft.com/askds/2009/09/10/managed-service-accounts-understanding-implementing-best-practices-and-troubleshooting/

8 Allgemeine administrative Sicherheitsanforderungen

Für alle anderen Systemadministratoren sowie allgemeinen Computer- und Anwendungskonten gelten folgende Vorgaben:

Anforderung	Nutzer	Administrator
1. Die Passwortgüte ist im Rahmen des technischen Standes so zu gestalten, dass folgendes überprüft und sichergestellt werden kann:		
a. Keine Zeichenwiederholungen	X	X
b. Die Passwörter sind aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und ggf. Sonderzeichen zusammengesetzt (siehe Kap. 3).	X	X
c. Die Passwörter sind aus einer Mindestlänge von n-Stellen zusammengesetzt.[2]	mind. 12 Stellen	mind. 16 Stellen
d. Passwörter, die leicht zu erraten sind oder in einem Sinnzusammenhang stehen, sind nicht zu vergeben.[3]	X	X
e. Die Passwörter sind während der Eingabe nicht lesbar am Bildschirm zu erkennen.	X	X
f. Maximales Kennwortalter: Spätestens nach 12 Monaten ist ein Wechsel der Passwörter zu betreiben, um einem unentdeckten Bekanntwerden entgegenzutreten.	12 Monate	12 Monate
g. Minimales Kennwortalter:	1 Tag	1 Tag

[2] Es gelten für Tier0-Admin, Dienstkonten und Fehlersucheaccounts im AD weiterführende Regeln, welche nicht Bestandteil der Richtlinie sind (siehe Punkt 5 der Passwortrichtlinie).

[3] Überprüfung der Forderung nur, soweit technisch möglich

h. Die Passwörter sind dem Stand der Technik entsprechend nur einweg-verschlüsselt zu speichern (Hash-werte).	X	X
i. Die Passwörter sind im Netzwerk nur verschlüsselt zu übertragen.	X	X
j. Verbot der Benutzung des User-Namens innerhalb des Passworts.	X	X
k. Anzahl der in der Kennworthistorie zu speichernden Passwörtern (Prüfung gegen zuvor gespeicherte Passwörter)	24	24
l. Maximale Anzahl der Anmeldever-suche bis Kontosperrung	10	5
m. Eine automatische Entsperrung nach erfolgter Falscheingabe (siehe 1. l) von Konten erfolgt nach	60 Minuten	180 Minuten
n. Automatische Rückstellung des Lo-gin-Fehlbedienungszählers (siehe 1 l.) nach	60 Minuten	180 Minuten
o. Komplexe Passwörter	Ja	Ja
2. Die Passwortdateien sind vor unbefugten Zugriffen zu schützen.	X	X
3. Endgeräte und Administratorkonsolen sind mit passwortgeschützten Bildschirmscho-nern/Bildschirmabschaltungen bzw. Dis-playsperre zu versehen, die nach maximal 15 Minuten den Zugriff auf das angemel-dete Endgerät verhindern. Für die Reakti-vierung mittels Passwortes gelten die Re-geln dieser Richtlinie.	X	X
4. Alle Falscheingaben der Passwörter sind datenschutzkonform zu protokollieren und zu löschen. Die entstandenen Protokolle sind für eine Auswertung vorzuhalten. Die	X	X

Ursache von nicht nachvollziehbaren Kontosperrungen ist auszuwerten.		
5. Eine Längenbeschränkung von Passwörtern ist aufzuheben (maximal 127 Zeichen in Windows-Systemen im Logondialog möglich[4]).	X	X
6. Soweit es sich um einen hohen Schutzbedarf der Daten bzw. sicherheitskritische Anwendungsbereiche handelt, wird die Anwendung einer starken Authentisierung (Zwei-Faktor-Authentisierung bzw. Multi-Faktor-Authentisierung, z. B. mittels SmardCard) empfohlen. Siehe dazu auch Hinweise im jeweils aktuellen BSI-Grundschutzkompendium[5].	X	X
7. Umsetzung weiterer Schutzmechanismen um Keylogger- und Phishingangriffe zu verhindern. Die Umsetzung weiterer Schutzmaßnahmen sind in Eigenverantwortung der Ressorts umzusetzen (z. B. keine Verwendung fremder USB-Speichermedien, Sensibilisierung im Umgang mit E-Mails).	X	X
8. Durchführung regelmäßiger Betriebssystem- und Schutzprogrammupdates.	X	X
9. Es sind keine Sicherheitsfragen zur Freischaltung zulässig. Durch soziale Medien oder Kenntnisse zum Nutzer können Fragen wie z. B. “Wie heißt Ihr Haustier?” leicht beantwortet werden.	X	X
10. Passwörter dürfen in der Regel höchstens einmal am Tag gewechselt werden. Sie sind jedoch unverzüglich zu wechseln, wenn der Verdacht besteht, dass diese Dritten bekannt geworden sein könnten. Ist	X	X

[4] https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc512606(v=technet.10)?redirected-from=MSDN

[5] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

hierbei das Mindestalter unterschritten, muss der Wechsel ggf. durch einen Administrator erfolgen.		
11. Einstiegs- und Übergangspasswörter für Nutzer- und Administratorenkonten sind nach dem initialen Login sofort durch nutzereigene Passwörter zu ersetzen.	X	X

Passwortfehleingaben sind zu loggen (Aktivierung des Auditlog). Für die Administratorenaccounts wird empfohlen, wenn technisch möglich, eine automatisierte Auswertung der Falscheingaben mit Benachrichtigungsfunktion, z. B. per Email an den Vorgesetzen und zuständigen ISB, bei Fehleingaben zu realisieren (speziell im Kontext mit dem Punkt 1l).

Hinweise für die Umsetzung verschiedener Funktionen bei Windowssystemen können der Anlage zum Dokument entnommen werden.

9 In-Kraft-Treten, Übergangsregelung, Befristung

Diese Regelung tritt am Tag nach ihrer Bekanntgabe in Kraft.

Die Mindestsicherheitsanforderungen dieser Verwaltungsanweisung sind innerhalb von sechs Monaten nach In-Kraft-Treten umzusetzen. Sofern aufgrund besonderer technischer Anforderungen die Umsetzung nicht oder nur mit unverhältnismäßigem Aufwand möglich sein sollte, können im Rahmen einer Risikobetrachtung nach BSI-Grundschutz-Standard 200-3 vorübergehend vergleichbar wirksame Maßnahmen getroffen werden, bis die Umsetzung vollständig erfolgt.

Die Richtlinie ist ab dem Tag ihrer Bekanntgabe in Ihrer Gültigkeitsdauer auf 5 Jahre befristet.

10 Geschlechtergerechte Formulierung

Im Text dieser Richtlinie wurde zur besseren Lesbarkeit auf die Verwendung der weiblichen und diversen Form verzichtet, die jeweils unter der männlichen Form subsummiert wurden. Dies soll keinesfalls eine Geschlechterdiskriminierung oder eine Verletzung des Gleichheitsgrundsatzes zum Ausdruck bringen.

11 Verwandte Themen und Hinweise

[1] Informationssicherheitsleitlinie der Thüringer Landesverwaltung (ThISL) der jeweils gültigen Fassung

[2] Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen

12 Änderungsverzeichnis

Datum (aktuelle oben)	Version	Geänderte Kapitel	Beschreibung der Änderung	Autor
06.05.2022	1.1 Dok.: 55398/2022		Finales Review/Freigabe Hinweis: Freigabe durch ISB-Land – Überarbeitungsinhalte nur organisatorisch/technisch – Keine erneute CIO-Freigabe erforderlich	H. Hartwig
03.05.2022	1.08 Dok.: 55395/2022	alle	Prüfung der Aktualität des Dokuments mit TLRZ (keine Änderungen); Formatierung	D. Cieslak; D. Martin
30.11.2021	1.07 Dok.: 164253/2021		Review	H. Hartwig
11.11.2021	1.06 Dok.: 145810/2021	alle; 3; 4; 6; 7; 8; 11	redaktionelle Änderungen; Änderung auf ISB; Hinweis zu Tastaturbelegung eingefügt; Änderung zu Single Sign-on; Zusatz zur LV eingefügt; Notfallzugriff eingefügt; Punkt 1 Reinfolge neu angepasst und teilweise. aufgeteilt; Punkt 5 Fußnote überarbeitet; Punkt 7 Hinweis ergänzt; Punkt 10 und 11 ergänzt; Hinweis auf Passwortfehleingaben eingefügt; umbenannt und Inhaltlich überarbeitet	D. Cieslak; M. Lasch

Datum (aktuelle oben)	Version	Geänderte Kapitel	Beschreibung der Änderung	Autor
18.10.2021	1.05 Dok.: 62598/2021	Dokument; 3; 7; 8; alle	Umstellung auf TLP; redaktionelle Änderungen; Notfallzugriff hinzugefügt; 1 k: Kennworthistorie auf 24 gesetzt; 1 m und n: Zeitraum auf 60 und 180 Minuten geändert; Hinweis auf Logging von Passwortfehleingaben eingefügt; Notfallaccount entfernt; Hinweis auf Sonderzeichen usw. eingefügt; Formatierung; Anlage eingefügt	D. Cieslak; D. Martin
20.10.2020	1.0 Dok.: 110760/2020		Freigabe CIO	Dr. H. Schubert
06.10.2020	0.991	9	Befristung aufgenommen	D. Cieslak
30.09.2020	0.99		Review/finale Überarbeitung	H. Hartwig
22.09.2020	0.94	1.2; 8; 10	Einarbeitung der Hinweise ARGE-HPR; Kap. 10 hinzugefügt; Formatierung	D. Cieslak
12.06.2020	0.93	alle	Einarbeitung Änderungen des IT-SiBe-Land; Punkt 5 eingefügt; Formatierung	D. Cieslak
03.06.2020	0.92	alle	Review	H. Hartwig
12.05.2020	0.91	alle	Einarbeitung der Rückmeldungen der Ressortabstimmung	D. Cieslak; H. Seifert
19.02.2020	0.90		Abstimmung mit den Ressorts	D. Cieslak
05.02.2020	0.86		Review IT-SiBe-Land; Freigabe des Dokuments zur Ressortabstimmung	H. Hartwig
30.01.2020	0.85	3; 4; 6; 7	Bearbeitung der Hinweise des IT-SiBe-Land	D. Cieslak; H. Seifert
20.01.2020	0.80		Review IT-SiBe-Land; Einarbeitung von Hinweisen	H. Hartwig

Datum (aktuelle oben)	Version	Geänderte Kapitel	Beschreibung der Änderung	Autor
17.01.2020	0.72	1.2; 5; 7	Geändert; Eingefügt; Überarbeitet (Streichungen)	H. Hartwig; H. Seifert; D. Cieslak
16.01.2020	0.71		Kommentierung IT-SiBe Land	H. Hartwig
16.01.2020	0.70	4; 6	Punkt 11 hinzugefügt; Punkt 6 geändert	D. Cieslak
15.01.2020	0.65	5; 6	Hinweis auf TLRZ-Regelungen eingefügt; Umstellung/Änderung Tabelle	H. Seifert; D. Cieslak
16.12.2019	0.60	1; 4	Hinweise ISM-Team eingeflossen	D. Cieslak
28.11.2019	0.59	3; 4; 5	Hinweise TLRZ eingeflossen	D. Martin; D. Cieslak
28.11.2019	0.58	3; 4; 5	Hinweise TLRZ, TMUEN eingeflossen	D. Martin; Dr. J. Haupt; D. Cieslak
08.11.2019	0.57	alle	redaktionelle Änderungen	D. Cieslak: H. Seifert
29.10.2019	0.56	6; alle	Umformatierung; redaktionelle Anmerkungen	D. Cieslak; J. Grell
25.09.2019	0.55	6	Umstrukturierung	D. Cieslak; H. Seifert
24.09.2019	0.50	alle	Inhaltliche Überarbeitung; Kapitel 6 neu gegliedert	D. Cieslak; H. Seifert
20.09.2019	0.30	alle	Inhaltliche Überarbeitung	D. Cieslak; H. Seifert
07.08.2019	0.25	alle	Dopplungen und Hinweise angefügt	H. Hartwig
29.07.2019	0.20	alle	Kapitel bearbeitet	D. Cieslak
15.07.2019	0.10	Erstellt	Dokument erstellt	H. Seifert

Anlage

1. Die Aktivierung des Tools „Ereignisanzeige“ per GPO

Bild 1

Umsetzungshinweis: Die Aktivierung der Funktion ist über *„Aufgabe an dieses Ereignis anfügen …“* zu erreichen.

2. Freigabe von Speicherplatz für das Logging per GPO

Für das Logging muss genügend freier Speicher auf dem System vorgehalten werden. Eine Einstellung zur Speichernutzung ist unter Windows per GPO möglich. Im Bild 2 dargestellt sind exemplarisch: 2TB Securitylog, Loggingmethode: neue Einträge überschreiben die ältesten, wenn die Loggröße erreicht ist.

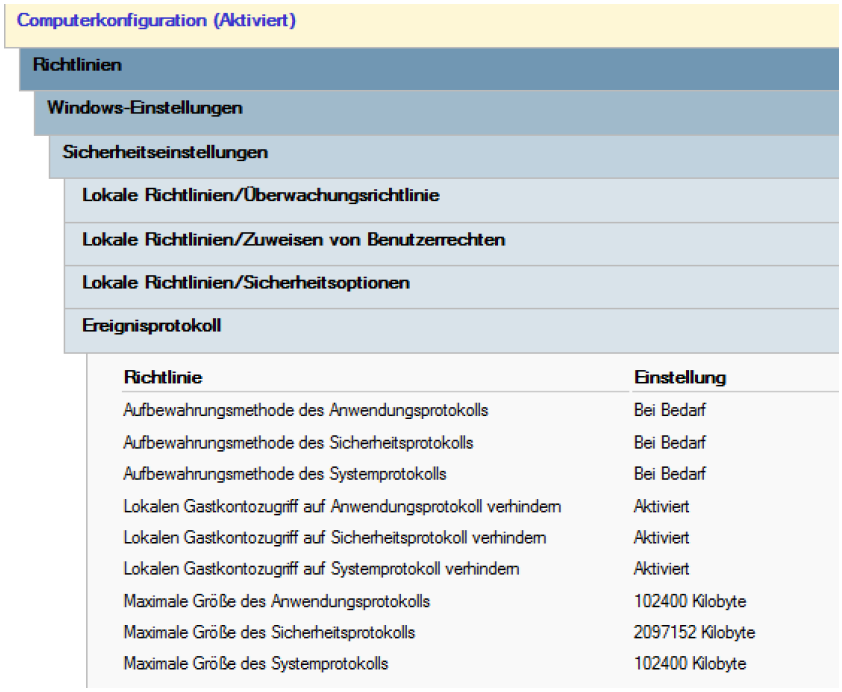


Bild 2

3. PowerShell Befehle zum Setzen der Vorgaben der Passwortrichtlinie auf einem Domaincontroller

Admin-Richtlinie:

Set-ADDefaultDomainPasswordPolicy -Identity thlv.de -MaxPasswordAge 365.00:00:00 -MinPasswordLength 16 -MinPasswordAge 1.00:00:00 -PasswordHistoryCount 24 -ComplexityEnabled $True -LockoutThreshold 5 -LockoutDuration 03:00:00 -LockoutObservationWindow 03:00:00

Benutzer-Richtlinie:

Set-ADDefaultDomainPasswordPolicy -Identity zv.thlv.de -MaxPasswordAge 365.00:00:00 -MinPasswordLength 12 -MinPasswordAge 1.00:00:00 -PasswordHistoryCount 24 -ComplexityEnabled $True -LockoutThreshold 10 -LockoutDuration 01:00:00 -LockoutObservationWindow 01:00:00

Achtung: Es gibt in einer Domäne nur eine Default-Richtlinie! Der zuletzt verwendete Befehl zählt also für alle Domänennutzer.