

Informationssicherheitsrichtlinie zur Lenkung von Dokumenten und Aufzeichnungen

Land Schleswig-Holstein

Version 2026

Dokumenteigenschaften

Dokumententitel	Informationssicherheitsrichtlinie zur Lenkung von Dokumenten und Aufzeichnungen
Dateiname	ISMS_LandSH_ISRL_Dokumentenlenkung_2026.odt
Version	2026
Dokumententyp	Taktisch - Informationssicherheitsrichtlinie (ISRL)
Vertraulichkeitsstufe / TLP-Klassifizierung	Öffentlich / TLP:CLEAR
Konformität	BSI IT-Grundschutz-Kompendium Stand Februar 2023
Zuständige Instanz	██████████ / CISO, StK 37
Letzte Änderung	24.02.2026
Revisionszyklus / nächste Überprüfung	Jährlich / Februar 2027
Berechtigte Rollen (Verteilerkreis)	Landesverwaltung SH
Verantwortliche Instanz (Name / Funktion)	AG ISM, vertreten durch den Vorsitz (██████████ / CISO)
Ablageort (VIS-Akte / Vorgang)	VIS-Akte
Ablageort (Veröffentlichung)	SHIP-Seite wird nach Umzug auf das neue SHIP ergänzt
BCM-Relevanz	nein

Änderungshistorie

Datum	Version	Geänderte Kapitel	Beschreibung der Änderungen	Autorin bzw. Autor
20.02.2026	2026	alle	Initiale Erstellung; Inkrafttreten durch Beschluss des AG ISM	UAG Richtlinien

Inhaltsverzeichnis

1. Einleitung.....	5
1.1. Zielsetzung.....	5
1.2. Rechtsgrundlage.....	5
1.3. Geltungsbereich.....	5
2. Strukturelle und inhaltliche Vorgaben.....	6
2.1. Dokumentenstruktur.....	6
2.2. Beschlussvorlage.....	6
2.3. Abkürzungsverzeichnis / Glossar.....	7
2.4. Verwendung von Modalverben in Dokumenten.....	7
2.5. Dokumententypen.....	8
2.6. Dokumenteninformationen für vollumfängliche Lenkung.....	10
2.7. Dokumenteninformationen für minimale Lenkung.....	11
2.8. Aufbau des Dateinamens.....	12
2.9. Einstufung der Vertraulichkeit.....	14
2.10. Austausch mit Externen / TLP-Klassifizierung.....	15
3. Prozessbeschreibung.....	16
3.1. Überblick.....	16
3.2. Rollen.....	16
3.3. Lebenszyklus.....	17
3.4. Ablageort, Bekanntgabe und Inkrafttreten.....	17
3.5. Änderungsmanagement.....	18
3.6. Fortschreibung und Revision.....	18
3.7. Dokumentenübersicht.....	18
3.8. Aufbewahrungsfristen.....	18
3.9. Aussonderung und Löschen.....	19
4. Quellenverzeichnis.....	19
5. Anhänge.....	19

Tabellenverzeichnis

Tabelle 1: Beschreibung der Dokumentenarten.....	8
Tabelle 2: Abkürzungen der Dokumentarten.....	13
Tabelle 3: Zuordnung TLP-Klassen zu Vertraulichkeitsstufen.....	15

1. Einleitung

1.1. Zielsetzung

Die Landesverwaltung Schleswig-Holstein etabliert ein Managementsystem für Informationssicherheit (ISMS), das dem IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) genügt. Im IT-Grundschutz nimmt die Dokumentation eine zentrale Rolle ein. Für alle Dokumente sind Eigenschaften für deren Lenkung festzulegen. Diese umfassen u.a. Zuständigkeiten, Bekanntgabe und Revisionszyklen des Dokuments. Lenkung bedeutet Steuerung der Dokumente z.B. im Prüfungs- und Freigabeprozess sowie deren Kennzeichnung.

Die vorliegende Richtlinie beschreibt die Lenkung von Dokumenten und Aufzeichnungen. Dazu gehört die Definition der Regelungen der Verantwortlichkeiten und Tätigkeiten über den Lebenszyklus eines Dokumentes. Darüber hinaus beschreibt die Richtlinie grundlegende inhaltliche Anforderungen an ISMS-Dokumente. Nicht betrachtet werden formale Kriterien, wie beispielsweise formale Kriterien der Landesdachmarke oder sprachliche Vorgaben wie geschlechtergerechte Sprache. Diese Kriterien werden in den entsprechenden Fachanweisungen definiert. Die hiesige Richtlinie lässt die Vorschriften des Datenschutzrechts (insb. aus der Verordnung EU 2016/679 und dem LDSG-SH) unberührt.

1.2. Rechtsgrundlage

Die vorliegende Richtlinie beschreibt die **Mindeststandards** gemäß §4 Absatz 4 Satz 2 EGovG SH zur Lenkung von Dokumenten und Aufzeichnungen.

1.3. Geltungsbereich

Der Geltungsbereich der vorliegenden Richtlinie gilt analog zur Informationssicherheitsleitlinie für die Landesverwaltung Schleswig-Holstein (ISLL SH) gemäß Ziffer 2 „Anwendungsbereich“ insbesondere Absatz 1. Die in der ISLL SH nicht im Geltungsbereich erfassten Institutionen gemäß Ziffer 2 „Anwendungsbereich“ Absätze 2 und 3 können ihren Beitritt zu dieser Richtlinie erklären. Wurde von einer Institution bereits der Beitritt zur ISLL SH erklärt, so gilt diese Richtlinie gemäß Satz 1.

Dokumente mit Verschlussacheneinstufung (VS) werden aus dem Geltungsbereich ausgeschlossen. Sie unterliegen der Verschlussachenanweisung Schleswig-Holstein (VSA SH) und sind entsprechend der jeweils gültigen VSA SH zu behandeln.

2. Strukturelle und inhaltliche Vorgaben

2.1. Dokumentenstruktur

Grundsätzlich besteht ein strategisches, taktisches oder gestaltendes ISMS-Dokument aus einer Einleitung, die die Zielsetzung, die Rechtsgrundlage und den Geltungsbereich definiert. Bei der Rechtsgrundlage ist es wichtig, eine Einordnung in den Rechtskanon zu ermöglichen. Dazu kann die in diesem Dokument genutzte Formulierung (bis zu einer Überarbeitung des EGovG) verwendet werden. Ebenfalls kann der hier verwendete Geltungsbereich als Vorlage für weitere Dokumente dienen.

Nach der Einleitung wird der eigentliche Inhalt des Dokuments behandelt. Auf eigene Kapitel zu Fortschreibung, Aufbewahrungsfristen, Ablageort, Bekanntgabe und Inkrafttreten kann verzichtet werden, wenn die in dieser Richtlinie definierten Standards gelten.

2.2. Beschlussvorlage

Für die Anmeldung in der Tagesordnung des AG ISM ist folgende standardisierte angepasste Beschlussvorlage zu verwenden. Die in der Beschlussvorlage genannte Anlage 1 ist das jeweilige Dokument. Das Veröffentlichen im Transparenzportal ist je nach Vertraulichkeitsstufe zu entfernen.

Beschlussvorlage gemäß §10 der Geschäftsordnung des AG ISM:

- a) Sachverhalt: Die UAG Richtlinien des AG ISM hat beiliegenden Vorschlag (Anlage 1) für eine Richtlinie zu [...] erarbeitet und Ressort-übergreifend innerhalb der UAG abgestimmt. Diese Richtlinie basiert auf §4 Absatz 4 Satz 2 EGovG SH und definiert Mindeststandards zu [...] innerhalb des ISMS im Geltungsbereich der ISLL SH. Es wird empfohlen, diese Richtlinie gemäß §4 Absatz 4 Satz 2 EGovG SH wie folgt zu beschließen.
- b) Beschlussvorschlag: „Die AG ISM beschließt,
 - die in Anlage 1 beiliegende Version 2026 gemäß §4 Absatz 4 Satz 2 EGovG SH
 - und dass diese Richtlinie durch die Geschäftsstelle der AG ISM
 - nicht nur im Intranet der Landesverwaltung SH (SHIP)
 - [sondern auch gemäß §11 Absatz 1 IZG-SH im Transparenzportal]veröffentlicht wird.“

2.3. Abkürzungsverzeichnis / Glossar

Innerhalb der ISMS-Dokumente wird auf ein separates Abkürzungsverzeichnis und Glossar verzichtet. Stattdessen wird auf der SHIP-Seite der Informationssicherheit ein Abkürzungsverzeichnis und Glossar bereitgestellt. Dies dient zum einem der Übersichtlichkeit innerhalb eines Dokuments und zum anderen gewährleistet dieses Vorgehen einen einheitlichen Sprachgebrauch innerhalb der ISMS-Dokumentation.

Anforderung DL.1 ISMS-Dokumente (außer Typ-A-Dokumente) **MÜSSEN** auf das zentrale Abkürzungsverzeichnis und Glossar des ISMS abgestimmt sein.

Insbesondere bei ISMS-Dokumenten einzelner Ressorts kann es notwendig sein, dass ressortspezifische Glossare oder Abkürzungsverzeichnisse als Ergänzung verwendet werden. Es obliegt den jeweiligen Dokumentenverantwortlichen, ob diese Ergänzungen innerhalb der Dokumente oder in einem ressort-zentralen Ort bereitgestellt werden.

2.4. Verwendung von Modalverben in Dokumenten

Strategische und taktische ISMS-Dokumente (Typ D0 und D1) definieren Anforderungen, geben aber auch erläuternde Hinweise. Für die genauere Unterscheidung zwischen normativen und informativen Inhalten ist es daher wichtig, entsprechende Modalverben zu verwenden.

Anforderung DL.2 Für die Definition von Anforderungen **MÜSSEN** die entsprechenden deutschen Schlüsselworte verwendet werden.

Die Schlüsselworte sind wie folgt definiert. Dabei unterscheidet sich die Definition geringfügig vom Standard [3], da innerhalb dieser Richtlinie Mindeststandards definiert werden:

- **MUSS / DARF NUR** Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die nicht zur Disposition steht und dringend erforderlich ist (uneingeschränkte Anforderung).
- **DARF NICHT / DARF KEIN** Dieser Ausdruck bedeutet, es besteht ein uneingeschränktes Verbot, etwas in keinem Fall zu tun.
- **SOLLTE** Dieser Ausdruck bedeutet, dass eine Anforderung immer dann zu erfüllen ist, wenn ein hohes oder sehr hohes Schutzniveau erreicht werden soll. Bei normalem Schutzniveau ist zu erwägen, diese Anforderung ebenfalls umzusetzen.
- **SOLLTE NICHT / SOLLTE KEIN** Dieser Ausdruck bedeutet, dass eine Anforderung besteht, etwas nicht zu tun, wenn ein hohes oder sehr hohes Schutzniveau erreicht werden soll. Bei normalem Schutzniveau ist zu erwägen, dieses Verbot ebenfalls durchzusetzen.

Text ohne diese Schlüsselworte haben grundsätzlich informativen Charakter und dienen dem Zweck eine Anforderung näher zu erläutern. Darüber hinaus werden Texte ohne diese Schlüsselworte verwendet, um eine Vereinheitlichung innerhalb des Geltungsbereichs anzustreben.

2.5. Dokumententypen

Die im Zuge des ISMS zu erstellenden Dokumente dienen verschiedenen Zielsetzungen und verfolgen unterschiedliche Zwecke. Die strukturierte thematische Gliederung der Dokumententypen ist in der folgenden Tabelle 1 zusammengefasst.

	Typ	Zeithorizont	Beispiel	Beschreibung
D0	Strategisch	Langfristig (Jahre)	Informationssicherheitsleitlinie, Strategie	Strategische Dokumente beinhalten Aussagen zu Umfeld, Zielen, Leitgedanken und Rahmenwerken des jeweiligen Informationsverbundes. Im Bezug auf einen Informationsverbund gibt es eine Leitlinie. Daneben kann es mehrere Strategien zu unterschiedlichen Aspekten geben.
D1	Taktisch	Mittelfristig (Monate)	Informationssicherheitsrichtlinie	Taktische Dokumentationen konkretisieren die strategischen Vorgaben z. B. aus der Leitlinie für die Informationssicherheit. Die konkrete Umsetzung einer Richtlinie kann durch ein korrespondierendes Konzept ausgearbeitet werden. Die Bausteine des BSI IT-Grundschutz-Kompendiums sind selbst Richtlinien im Sinne dieses Dokuments.
D2	Operativ-Gestaltung	Mittelfristig (Monate)	Konzept	Ein Konzept im Kontext des BSI IT-Grundschutz greift ausgewählte Aspekte aus taktischen Dokumenten auf. Es beschreibt konkret für die jeweiligen Bereiche und Anwendungsfälle, wie die taktischen Vorgaben umgesetzt werden (z.B. Kryptokonzept, Notfallkonzept, Datensicherungskonzept). Es ist möglich, dass es zu einem thematischen Schwerpunkt mehrere Konzepte geben, die sich je nach betrachtetem Zielobjekt in der Umsetzung der taktischen Vorgaben unterscheiden.
D3	Operativ-Vermittlung	Mittelfristig (Monate)	Anweisung, Handbücher, Pläne	Die Dokumente dieser Ebene beinhalten das Regelwerk für die Mitarbeitenden der jeweiligen Institution mit dem die Konzepte umgesetzt werden (z.B. Anweisung, Betriebshandbuch, Prozessabläufe, Notfallpläne, Wiederanlaufpläne, Checklisten).
A	Operativ-Ergebnis	Kurzfristig (Wochen, Tage)	Aufzeichnung	Aufzeichnungen sind festgehaltene Umstände, Arbeitsergebnisse oder Abläufe aus Umsetzungen (z.B. Auditberichte, Ergebnisse eines IT-Grundschutz-Checks, Protokolle, Checklisten).

Tabelle 1: Beschreibung der Dokumentenarten

Anforderung DL.3 D0-, D1- und D2-Dokumente **MÜSSEN** vollumfänglich gelenkt werden (siehe Kapitel 2.6).

Anforderung DL.4 D3-Dokumente **MÜSSEN** mindestens minimal gelenkt werden (siehe Kapitel 2.7).

A-Dokumente können gelenkt werden, wenn die darin enthaltenen Informationen eine Dokumentenlenkung rechtfertigen.

Neben den oben dargestellten Dokumenten werden im ISMS für viele Bereiche und Informationsverbünde Sicherheitskonzepte verlangt und erstellt. Dabei werden Sicherheitskonzepte gemäß IT-Grundschutz aus verschiedenen Perspektiven erstellt, was dazu führt, dass je nach Betrachtung ein unterschiedlicher Schwerpunkt gesetzt wird. Dies spiegelt sich auch in den Inhalten der Sicherheitskonzepte wider. In der folgenden Auflistung werden daher die unterschiedlichen Perspektiven und die Zusammenhänge genannt.

- Die Perspektive eines Anbieters eines Dienstes oder eines Fachverfahrens wird in einem **Fachsicherheitskonzept** betrachtet. Auch die nutzerspezifischen Anpassungen eines Basissicherheitskonzepts oder Betriebssicherheitskonzepts sind ein Fachsicherheitskonzept. In diesem besteht der Informationsverbund aus dem Fachverfahren, seiner betrieblichen Aspekte, den Geschäftsprozessen, den genutzten zentralen Diensten, der Infrastruktur, in denen die Geschäftsprozesse ablaufen und gegebenenfalls weiteren Aspekten. Somit kann ein Fachsicherheitskonzept aus einem oder mehreren Betriebssicherheitskonzepten, an das individuelle Fachverfahren angepasste Basissicherheitskonzepte und weiteren Teilen der Grundschutzmethodik bestehen.
- Das **Betriebssicherheitskonzept** oder **SSLA (Teil A oder B)** wird aus der Perspektive des Betriebs geschrieben, wobei hiermit regelmäßig der Betrieb im Rechenzentrum von einem Dienstleister (z.B. Dataport) gemeint ist. Im Betriebssicherheitskonzept werden daher nur Aspekte betrachtet, die direkt durch den Betrieb motiviert sind, wie beispielsweise die Infrastruktur des Rechenzentrums. Die Aspekte aus Kunden- bzw. Nutzersicht werden in einem Betriebssicherheitskonzept regelmäßig nicht betrachtet.
- Werden in einem Informationsverbund durch zentrale Stellen Dienste oder Services zur Verfügung gestellt, die von mehreren Fachverfahren genutzt werden, dann bietet es sich an, für diese jeweils ein Sicherheitskonzept zu erstellen. Aus Sicht des Nutzers dieser Dienste ergibt sich jedoch regelmäßig die Pflicht, dieses Sicherheitskonzept an die eigenen Gegebenheiten und Prozesse anzupassen. Aus diesem Grund spricht man bei diesen Sicherheitskonzepten von **Basissicherheitskonzepten**, die grundsätzliche Annahmen treffen, wie in einem ausgelieferten Zustand die Nutzungen vorstellbar sind.

Basissicherheitskonzepte bieten sich insbesondere für Betrachtungen innerhalb eines Ministeriums oder einer nachgeordneten Behörde an, da sich z.B. die Bausteine für Infrastrukturzielobjekte nicht bei einzelnen Fachverfahren unterscheiden.

2.6. Dokumenteninformationen für vollumfängliche Lenkung

Anforderung DL.5 Für eine vollumfängliche Lenkung MÜSSEN in jedem Dokument die nachfolgenden Informationen angegeben werden [1].

- Dokumententitel
- Version
Hinweis: Siehe Kapitel 2.8
- Dokumententyp
Hinweis: Der Dokumententyp ist in Kapitel 2.5 definiert. Die verwendeten Abkürzungen sind in Tabelle 2 zu finden.
- Vertraulichkeitsstufe / TLP-Klassifizierung
Hinweis: Siehe Kapitel 2.9 und Kapitel 2.10
- Konformität
Hinweis: An dieser Stelle ist die Konformität zu einem Standard (z.B. Grundschatz oder ISO 27001) gemeint, da es auf Grund von externen Vorgaben sein kann, dass über den Grundschatz hinaus noch andere Standards unterstützt werden müssen.
- Zuständige Instanz
Hinweis: Im Allgemeinen entspricht diese Angabe dem Autor bzw. inhaltlichen Ansprechpartner des Dokuments
- Letzte Änderung
- Revisionszyklus / nächste Überprüfung
- Berechtigte Rollen (Verteilerkreis)
Hinweis: An dieser Stelle sind der Verteilerkreis gemeint, dem dieses Dokument zur Kenntnis gegeben werden soll. Oftmals korrespondiert diese Liste mit dem Geltungsbereich des Dokuments, so dass landesweit gültige ISMS-Dokumente „alle Beschäftigten der Landesverwaltung“ als Verteilerkreis haben.
- Verantwortliche Instanz (Name / Funktion)
- Ablageort (VIS-Akte / Vorgang)

- Ablageort (Veröffentlichung)
- BCM-Relevanz
Hinweis: Im Notfall ist es ggf. notwendig, auf das aktuelle Dokument zuzugreifen, auch wenn die offiziellen Ablageorte nicht mehr erreichbar sind. Ist dies nicht der Fall, dann reicht hier die Angabe „nein“. Ansonsten ist hier zu spezifizieren, wie man im Notfall auf das Dokument zugreifen kann (z.B. „aktueller Ausdruck wird im Tresor in der StK hinterlegt“).
- Änderungshistorie mit:
 - Datum
 - Version
 - Geänderte Kapitel
 - Beschreibung der Änderungen
 - Autorin bzw. Autor

Für Dokumente, die in einem Textverarbeitungsprogramm erstellt werden und grundsätzlich für das Ausdrucken optimiert sind, ist es zweckmäßig, die genannten Angaben am Anfang des Dokuments als Dokumenteneigenschaften mit einzufügen. Es ist jedoch ebenfalls konform, die Informationen neben dem Dokument zu pflegen, wenn eine nachvollziehbare Verknüpfung sichergestellt werden kann.

2.7. Dokumenteninformationen für minimale Lenkung

Anforderung DL.6 Für Aufzeichnungen und Dokumente, die minimal gelenkt werden, **MÜSSEN** die folgenden Mindestinformationen angegeben werden.

- Version
Hinweis: Siehe Kapitel 2.8
- Dokumententyp
Hinweis: Der Dokumententyp ist in Kapitel 2.5 definiert. Die verwendeten Abkürzungen sind in Tabelle 2 zu finden.
- Vertraulichkeitsstufe / TLP-Klassifizierung
Hinweis: Siehe Kapitel 2.9 und Kapitel 2.10
- Zuständige Instanz
Hinweis: Im Allgemeinen entspricht diese Angabe dem Autor bzw. inhaltlichen Ansprechpartner des Dokuments
- Letzte Änderung

- **Berechtigte Rollen (Verteilerkreis)**
Hinweis: An dieser Stelle sind der Verteilerkreis gemeint, dem dieses Dokument zur Kenntnis gegeben werden soll. Oftmals korrespondiert diese Liste mit dem Geltungsbereich des Dokuments, so dass landesweit gültige ISMS-Dokumente „alle Beschäftigten der Landesverwaltung“ als Verteilerkreis haben.
- **Ablageort (Veröffentlichung)**
- **BCM-Relevanz**
Hinweis: Im Notfall ist es ggf. notwendig, auf das aktuelle Dokument zuzugreifen, auch wenn die offiziellen Ablageorte nicht mehr erreichbar sind. Ist dies nicht der Fall, dann reicht hier die Angabe „nein“. Ansonsten ist hier zu spezifizieren, wie man im Notfall auf das Dokument zugreifen kann (z.B. „aktueller Ausdruck wird im Tresor in der StK hinterlegt“).

Systemisch erzeugte Aufzeichnungen (z.B. Logfiles) sind in der Regel nach ihrer Erstellung keinem Ansprechpartner zugewiesen. Es gilt jene Instanz als zuständig, die das Dokument einem Prozess zugeführt hat. Als Datum der letzten Änderung gilt das Datum der Bereitstellung. Können diese Informationen nicht im Dokument selber hinterlegt werden, so kann das Dokument um ein Deckblatt erweitert werden, welches diese Information beinhaltet.

2.8. Aufbau des Dateinamens

Für ISMS-Dokumente, die nicht systemisch erzeugt werden, wird die Übersicht erhöht, wenn der Dateiname durch ein definiertes Schema einheitlich vergeben wird. Dies erleichtert den Austausch von Dokumenten und beugt Missverständnisse und Fehler vor.

Jedes Dokument mit Bezug zum Informationssicherheitsmanagementsystem sollte nach dem folgenden Schema benannt werden:

ISMS_<Geltungsbereich>_<Dokumentart>_<Dokumentenbezeichnung>_<Version>.Dateiendung

<Geltungsbereich> Die Angabe des Geltungsbereichs im Dateinamen erleichtert die Zuordnung. Dabei sind folgende Fälle möglich, wobei die Aufzählung nicht abschließend ist:

- „LandSH“, falls der Geltungsbereich analog zur ISLL SH ist.
- „GB-<Kürzel Ministerium>“, falls der Geltungsbereich den kompletten Geschäftsbereich inkl. der nachgeordneten Bereiche eines Ministeriums umfasst.
- „<Kürzel Behörde>“, falls der Geltungsbereich eine einzelne Behörde umfasst. Dabei sind die offiziellen Behördenkürzel zu verwenden.

- „<Projekt / Dienst / Verfahren / o.ä.>“, falls der Geltungsbereich für einen kleinen definierten Bereich gilt.

<Dokumentart> Um die Art eines Dokumentes in seinem Namen kenntlich zu machen, werden bevorzugt Kürzel verwendet um die Länge des Dateinamens zu begrenzen. Die folgende Tabelle hat keinen Anspruch auf Vollständigkeit und sollte bei Bedarf erweitert werden.

Kürzel	Dokumentart
ANL	Anlage
AUFZ	Aufzeichnung
AW	Arbeitsanweisungen
HB	Handbuch
ISLL	Informationssicherheitsleitlinie
ISRL	Informationssicherheitsrichtlinie
KO	Konzept
LF	Leitfaden
MBL	Merkblatt
PL	Plan
PZS	Prozesssteckbrief
PZV	Prozessvisualisierung in BPMN
ST	Strategie
VO	Vorlage

Tabelle 2: Abkürzungen der Dokumentarten

<Dokumentenbezeichnung> Dies ist ein beliebiger sprechender Name zur Bezeichnung des Dokumentes. Diese sollte eindeutig, jedoch nicht zu lang sein.

<Version> Die Angabe der Version unterscheidet sich, in welchem Lebenszyklus sich ein Dokument befindet.

- In einem Dokument, das einen Freigabeprozess durchlaufen hat, wird nur eine **<Hauptversionsnummer>** (vierstellige Jahreszahl der Freigabe) angegeben, da eine Revision in der Regel jährlich oder länger stattfindet. Kommt der seltene Fall vor, dass unterjährig eine Aktualisierung vorgenommen werden muss, ergänzt man **<Hauptversionsnummer>.<Nebenversionsnummer>**, wobei die Nebenversionsnummer eine bei 0

beginnende hochgezählte Zahl ist. Bei Dokumenten mit einer höheren Revisionsfrequenz kann man grundsätzlich die Nebenversionsnummer angeben.

- Dokumente, die sich in Bearbeitung oder Prüfung befinden, haben das Schema <freigegebene Version>.beta<Nummer>. Die <freigegebene Version> entspricht dabei der Version der letzten freigegebenen Veröffentlichung. Wird ein Dokument initial erstellt, so dass es noch keine freigegebene Vorgängerversion gibt, so ist <freigegebene Version> mit „0“ zu setzen. Die abschließende Nummer ist eine bei 0 beginnende hochgezählte Zahl, die immer dann hochgezählt wird, wenn im Dokument beschriebene Sachverhalte verändert wurden.

2.9. Einstufung der Vertraulichkeit

Im Rahmen des ISMS dürfen Dokumente nur von den Personen eingesehen oder offengelegt werden, die dazu auch berechtigt sind.

Anforderung DL.7 Um das Schutzziel der Vertraulichkeit einzuhalten, **MÜSSEN** vollständig gelenkte Dokumente eingestuft werden.

Folgende Vertraulichkeitsstufen stehen zur Verfügung. Dabei ist zu beachten, dass diese Einstufung sowohl für ein Dokument als Ganzes als auch für Teile des Dokuments gilt.

- **Öffentlich:** Diese Information hat keine Vertraulichkeitsanforderungen. Dokumente mit dieser Klassifikation können im Amtsblatt oder über eine andere öffentliche Quelle (z.B. Transparenzportal) bereitgestellt werden. Vor einer Veröffentlichung außerhalb der Landesverwaltung ist dies analog §11 Absatz 1 IZG-SH ohne Angaben von personenbezogenen Daten und Geschäfts- und Betriebsgeheimnissen durchzuführen.
Beispiel: Rede des Ministers nach der Landtagsdebatte
- **Intern:** Diese Information ist nicht für die Öffentlichkeit bestimmt. Dokumente dieser Klassifikation werden beispielsweise im SHIP abgelegt oder innerhalb der Landesverwaltung geteilt. Bei einer Veröffentlichung sind negative Auswirkungen nicht auszuschließen.
Beispiel: Aktuelle Informationen des Personalrats
- **Vertraulich:** Diese Information ist nur für einen intern und beschränkten Adressatenkreis vorgesehen. Kenntnis von ihr sollte nur die Person erlangen, die diese benötigt. Dokumente werden in einem System mit eingeschränkten Zugriffsrechten abgelegt. Eine Veröffentlichung hat negative Auswirkungen.
Beispiel: Staatssekretärsrunden, Personalangelegenheiten

Neben diesen Einstufungen gibt es die Einstufung als Verschlussache. Regelungen dazu werden in der VSA SH definiert.

2.10. Austausch mit Externen / TLP-Klassifizierung

Für den Austausch von schützenswerten Informationen mit Externen außerhalb der Landesverwaltung (z.B. Dienstleister) ist es notwendig, eine **Geheimhaltungsvereinbarung** oder **Vertraulichkeitsvereinbarung** von der Gegenstelle unterzeichnen zu lassen. Dies ermöglicht, die Gegenstelle zu verpflichten, mit den schützenswerten Informationen entsprechend sorgsam umzugehen. Um zu vermeiden, dass bei jedem Informationsaustausch eine neue Vertraulichkeitsvereinbarung erstellt werden muss, wird für diesen Zweck das Traffic Light Protocol (TLP 2.0) verwendet.

Anforderung DL.8 Der Versender MUSS das zu versendende Dokument gemäß TLP-Klassifizierung nach den Vorgaben von [2] kennzeichnen, wenn dieses nicht als „öffentlich“ eingestuft wurde. Das gilt nicht für die Weitergabe von Informationen an andere Landesverwaltungen oder die Bundesverwaltung, soweit die Kooperation durch Gesetz oder Staatsvertrag geregelt ist.

Informationen der Vertraulichkeitsstufe „öffentlich“ müssen nicht klassifiziert werden, da in dem Fall durch die unbegrenzte Weitergabeberechtigung die TLP-Verpflichtung der Empfänger nicht nachgeprüft werden können. Welche TLP-Klasse für ein Dokument passend ist, regeln die Vorgaben aus [2]. In Tabelle 3 wird eine grobe Zuordnung der Vertraulichkeitsstufen zu den TLP-Klassen vorgenommen, die als erste Einschätzung zweckmäßig ist.

TLP-Klassifizierung	Geeignet für Vertraulichkeitsstufe
TLP:CLEAR	Nur für die Einstufung öffentlich
TLP:GREEN	Für die Einstufung intern
TLP:AMBER	Für die Einstufung intern oder vertraulich
TLP:AMBER+STRICT	Wahrscheinlich für die Einstufung vertraulich
TLP:RED	Nur für die Einstufung vertraulich

Tabelle 3: Zuordnung TLP-Klassen zu Vertraulichkeitsstufen

Durch die Unterschrift auf der TLP-Verpflichtung erklären natürliche Personen ihre Verpflichtung, die Regeln des TLP einzuhalten. Diese Verpflichtung endet nicht mit ihrer Zugehörigkeit zu einer bestimmten am TLP-basierten Informationsaustausch teilnehmenden Organisation (vgl. [2]).

Anforderung DL.9 Der Versender MUSS vor Versand prüfen, ob beim Empfänger eine TLP-Verpflichtung erfolgte.

Anforderung DL.10 Die oder der ISB MÜSSEN eine Übersicht führen, welche TLP-Verpflichtungen erfolgten.

Weiterführende Informationen zur TLP-Spezifikation ist [2] zu entnehmen.

3. Prozessbeschreibung

3.1. Überblick

In der Dokumentenlenkung wird der PDCA-Zyklus eingesetzt, um einen ganzheitlichen und kontinuierlichen Prozess für die Lenkung von Dokumenten zu gewährleisten. In der Planungsphase (Plan) werden die Anforderungen an das Dokument festgelegt. Dies beinhaltet auch die Festlegung einer zuständigen Instanz, die den PDCA-Prozess für das gesamte Leben eines Dokumentes begleitet und verantwortet. Darüber hinaus werden der Dokumententyp, Geltungsbereich des Dokumentes und die Inhalte festgelegt. Die zuständige Instanz erzeugt den Inhalt entweder neu oder setzt die aus einer früheren Iteration entstandenen oder aus geänderten Anforderungen resultierenden Änderungen um (Do). Die Prüfung des Dokumentes wird während der Freigabe durchgeführt, so dass die verantwortliche Instanz die Freigabe erteilen kann (Check). Als letzte Aufgabe in der Umsetzungsphase wird das Dokument bekannt gegeben und die neue Version des Dokumentes in der Dokumentenübersicht (siehe Kapitel 3.7) vermerkt. Mit Bekanntgabe tritt das Dokument in Kraft (Act). Es folgt die turnusmäßige Revision des Dokumentes bis der Prozess in einer Aussonderung des Dokumentes endet.

Eine genaue Prozessbeschreibung in Form eines Steckbriefs und einer BPMN-Darstellung ist dieser Richtlinie beigelegt.

3.2. Rollen

Damit die Verantwortlichkeiten im Lebenszyklus von Dokumenten geklärt sind, werden die folgenden Rollen definiert:

- Die **verantwortliche Instanz** ist für ein Dokument verantwortlich und initiiert seine Erstellung. Sie ist dementsprechend diejenige Instanz, die einen fertigen Entwurf freigibt und damit die Gültigkeit des Dokuments bestätigt.
- Da die verantwortliche Instanz üblicherweise der Leitungsebene zuzuordnen ist, die konkrete Erstellung des Dokuments aber in der Fachlichkeit zu verorten ist, ist die **zuständige Instanz** diejenige, die das Dokument in seinem Lebenszyklus begleitet und somit das Dokument verfasst und pflegt. Die zuständige Instanz wird durch die verantwortliche Instanz ernannt und ist auch für fachliche Fragen anderer Organisationsbereiche erste Ansprechpartnerin. Die zuständige Instanz initiiert die Prüfung, Freigabe und Bekanntgabe und startet bei Bedarf den Review-Prozess.

Auch wenn in den Rollen von Instanzen die Rede ist, können Personen oder auch Teams hinter der Rolle stehen.

Die Prüfung sachlich auf inhaltliche Richtigkeit, Vollständigkeit und Stimmigkeit und fachlich auf Korrektheit bzgl. verwendete Begriffe, Methoden und Aussagen sowie qualitativ auf Fachwissen, Präzision und Relevanz wird üblicherweise im Rahmen eines Freigabeprozess durchgeführt und muss daher hier nicht weiter spezifiziert werden.

Anforderung DL.11 Dokumente vom Typ D0, D1 und D2 MÜSSEN von der verantwortlichen Instanz in VIS freigegeben werden.

Für Mindeststandards gemäß §4 Absatz 4 Satz 2 EGovG SH ist das AG ISM die verantwortliche Instanz.

3.3. Lebenszyklus

Für Dokumente wird folgender Lebenszyklus definiert. Dokumente besitzen erst Gültigkeit und gelten als verbindlich, wenn diese bekanntgegeben wurden. Der Freigabeprozess wird über einen VIS-Geschäftsgang gesteuert.

- Ein Dokument im Status „**in Bearbeitung**“ ist entweder in der initialen Erstellung oder es wird eine Revision eines bereits freigegebenen Dokuments durchgeführt. Falls dies durch einen verlängerten Zeitraum sinnvoll ist, kann der Status „**in Prüfung**“ den Status „in Bearbeitung“ näher definieren.
- Nachdem die verantwortliche Instanz ein Dokument durch die Zeichnung im VIS formal „**freigegeben**“ hat, wird es anschließend bekanntgegeben. Es ist nun gültig und muss verwendet werden.
- Dokumente verlieren entweder durch zurückziehen oder durch eine neue freigegebene Versionen ihre Gültigkeit und werden dadurch „**ungültig**“.

Anforderung DL.12 Ein ungültiges Dokument DARF NICHT mehr verwendet werden.

Mit Freigabe wird die Dokumentenübersicht aktualisiert (siehe Kapitel 3.7). Die Aktualisierung wird durch die zuständige Instanz initiiert und ist im VIS-Geschäftsgang mit integriert.

3.4. Ablageort, Bekanntgabe und Inkrafttreten

Für jedes Dokument muss geprüft werden, welche Ablageorte für den Bearbeitungsstand, für den Freigabeprozess und für die Bekanntgabe verwendet werden soll. Bei systemisch erzeugten Dokumenten wird dies zumeist durch das verwendete System vorgegeben.

Standardmäßig wird der Bearbeitungsstand und der Freigabeprozess in VIS abgelegt und die Bekanntgabe erfolgt über das Intranet bzw. SHIP. Bei vollständig gelenkten Dokumenten sind die Ablageorte in den Dokumenteneigenschaften hinterlegt.

ISMS-Dokumente treten, wenn dies nicht anders innerhalb der Dokumente geregelt ist, mit Bekanntgabe in Kraft.

3.5. Änderungsmanagement

Zu jeder Freigabe ist aus Gründen der Nachvollziehbarkeit zu dokumentieren, welche wesentlichen Änderungen es gegenüber der Vorversion gab.

Anforderung DL.13 Wesentliche Änderungen in vollumfänglich gelenkten Dokumenten **MÜSSEN** durch einen zusammenfassenden Änderungsvermerk in der Änderungshistorie erfasst werden.

3.6. Fortschreibung und Revision

Jedes Dokument ist, soweit nicht anderweitig geregelt, im Rahmen des PDCA-Zyklus auf Aktualität zu prüfen und bei Bedarf fortzuschreiben (siehe Kapitel 3.1). Ein besonderer (unverzögerlicher) Überarbeitungsbedarf ergibt sich insbesondere bei Änderungen des Geltungsbereichs wie beispielsweise der Organisationsstrukturen oder bei Änderungen der verwendeten Standards und Normen.

Der PDCA-Zyklus von D0-Dokumente ist in der Regel drei Jahre lang, von D1- und D2-Dokumente in der Regel ein Jahr, so dass diese Dokumente jährlich einer Revision zu unterziehen sind.

Die Aktualisierung des Dokumentes wird durch die zuständigen Instanz gestartet, d.h. sie initiiert die notwendigen Schritte, die Prüfung, Freigabe und Bekanntgabe.

Anforderung DL.14 In vollumfänglich gelenkten Dokumenten **MUSS** eine vollständig durchgeführte Revision in der Änderungshistorie erfasst werden.

Wurden bei der Revision Änderungen durchgeführt, die in der Änderungshistorie bereits erwähnt sind, dann reicht es aus, die Änderungshistorie durch einen Verweis auf die durchgeführte Revision zu präzisieren.

3.7. Dokumentenübersicht

Die Geschäftsstelle des AG ISM pflegt eine Seite im SHIP im Bereich Informationssicherheit mit den Dokumenten des übergreifenden ISMS, die zum aktuellen Zeitpunkt gültig sind. Die Aktualisierung der Liste wird nach Freigabe eines Dokumentes durch die Geschäftsstelle des AG ISM durchgeführt.

3.8. Aufbewahrungsfristen

Nicht mehr gültige aktenrelevante Dokumente und Aufzeichnungen werden bis zum Ende der Aufbewahrungsfrist gemäß Aktenordnung aufbewahrt. Sie beträgt 5 Jahre, sofern sich aus der jeweils

gültigen Aktenordnung keine abweichenden Anforderungen ergeben. Längere Aufbewahrungsfristen können individuell festgelegt werden.

3.9. Aussonderung und Löschen

Nach Ablauf der Aufbewahrungsfrist werden ungültige Dokumente gelöscht, sofern sie nicht nach der jeweils gültigen Aktenordnung zur Archivierung angeboten werden müssen. Die Vorgaben zum Löschen und Vernichten von Dokumenten werden in der „Informationssicherheitsrichtlinie für die Löschung und Vernichtung von Informationen“ geregelt.

4. Quellenverzeichnis

- [1] IT-Grundschutz-Kompodium - Bundesamt für Sicherheit in der Informationstechnik (BSI) - Stand Februar 2023 - https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium_node.html
- [2] Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP), Version 2.0 - Bundesamt für Sicherheit in der Informationstechnik (BSI) – 26.06.2023 - <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/TLP/merkblatt-tlp.html>
- [3] BSI-Standard 200-2 - Bundesamt für Sicherheit in der Informationstechnik (BSI) - 15.11.2017 - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2#page=18

5. Anhänge

- ISMS_LandSH_PZV_PDCA-ISMS-Dokumentation_2026.bpmn – Prozessvisualisierung eines generischen PDCA-Prozesses, der Kapitel 3 umsetzt. Die Visualisierung kann als Vorlage für einen eigenen Prozess benutzt werden.
- ISMS_LandSH_PZS_PDCA-ISMS-Dokumentation_2026.odt – Prozesssteckbrief eines generischen PDCA-Prozesses, der Kapitel 3 umsetzt. Der Steckbrief kann als Vorlage für einen eigenen Prozess benutzt werden.