LANDESRECHNUNGSHOF
Mecklenburg-Vorpommern

Landesrechnungshof Mecklenburg-Vorpommern, Mühlentwiete 4, 19059 Schwerin

Einrichtungen der Landesverwaltung
lt. Verteiler

nur per E-Mail

Bearbeitet von: **Steffen Wirks**
Telefon: 0385 7412-113
Fax: 0385 7412-100
E-Mail: swirks@lrh-mv.de

Ihr Zeichen:
Gz.: 32B-2.06.0-1#2 - 11571/2025

Schwerin, 19. September 2025

Rundschreiben Nr. 4/2025
des Landesrechnungshofes Mecklenburg-Vorpommern
Ordnungsmäßigkeit des Einsatzes von Informationstechnik

1 Allgemeines

Der Landesrechnungshof Mecklenburg-Vorpommern informiert in unregelmäßigen Abständen über Themen von über den Einzelfall hinausgehender Bedeutung durch Rundschreiben. Adressat der Rundschreiben sind alle Stellen der öffentlichen Verwaltung in Mecklenburg-Vorpommern, die vom Landesrechnungshof geprüft werden können. Der Versand erfolgt ausschließlich elektronisch, die Rundschreiben werden auch auf der Homepage des Landesrechnungshofes[1] zur Verfügung gestellt.

Der Landesrechnungshof wird die in seinem Rundschreiben mitgeteilten Feststellungen und Wertungen sowie die anliegenden Grundsätze als Maßstab seiner künftigen Prüfungen zugrunde legen und bei den geprüften Stellen als bekannt voraussetzen. Er bittet deshalb die Empfänger, dieses Rundschreiben bekannt zu machen.

Behörden der Landesverwaltung und Rechtspersonen des öffentlichen Rechts in Trägerschaft des Landes sollen die Ausführungen im Rundschreiben beachten. Den Kommunen wird die Anwendung

[1] https://www.lrh-mv.de/Veröffentlichungen/Rundschreiben/.

empfohlen unter der Maßgabe, kommunalspezifische Besonderheiten insbesondere zum Haushaltsrecht zu beachten.

Das Rundschreiben Nr. 1/2023 vom 11. April 2023 findet keine Anwendung mehr und wird durch dieses Rundschreiben einschließlich Anlagen ersetzt.

2 IT-Mindestanforderungen der Rechnungshöfe des Bundes und der Länder

Die Rechnungshöfe des Bundes und der Länder haben ihre IT-Mindestanforderungen überarbeitet. Die überarbeiteten IT-Mindestanforderungen sind auf der Homepage des Landesrechnungshofes veröffentlicht. Sie ersetzen die bisherige Fassung aus dem Jahr 2020.

Die Rechnungshöfe haben die IT-Mindestanforderungen grundlegend neu gefasst. Neu hinzugekommen sind Ausführungen zur IT-Architektur, zum Kontinuitätsmanagement und zum Controlling.

Die IT-Mindestanforderungen sind Prüfungsmaßstab des Landesrechnungshofes Mecklenburg-Vorpommern.

3 Anzuwendende Rechtsvorschriften, Hinweise und Empfehlungen (Anlage 1)

Mit diesem Rundschreiben informiert der Landesrechnungshof Mecklenburg-Vorpommern über die existierenden Rechtsvorschriften und Maßstäbe, welche die Verwaltungen beim Einsatz von Informationstechnik zu beachten bzw. umzusetzen haben.

Die rechtlichen Anforderungen an den ordnungsgemäßen Betrieb von Informationstechnik sind in den letzten Jahren deutlich angestiegen und komplexer geworden. Die zusammenfassende Darstellung in Anlage 1 soll die Verwaltungen als Arbeitshilfe und Nachschlagewerk unterstützen.

Um Informationstechnik ordnungsgemäß einzusetzen, sind die in der Anlage 1 aufgeführten Rechtsvorschriften einzuhalten und die sonstigen Hinweise und Empfehlungen zu beachten. Dies ist nicht nur bei der Inbetriebnahme zu gewährleisten, sondern über den gesamten Lebenszyklus hinweg. Durch regelmäßige Kontrollen ist die Einhaltung der Vorgaben nachzuweisen und das Risiko eines nicht ordnungsgemäßen Einsatzes zu minimieren.

Die dargestellten Rechtsgrundlagen sowie das BSI-Grundschutzkompendium zieht der Landesrechnungshof als grundlegende Prüfungsmaßstäbe heran. Die Hinweise und Empfehlungen nutzt er zur ergänzenden Auslegung und um Verbesserungsmöglichkeiten aufzuzeigen.

Für das Informationssicherheitsmanagement, die digitale Verwaltung (E-Government) und für die Beschaffung von Lieferungen und Leistungen sind einzelne Landesregelungen noch nicht aktualisiert worden (z. B. IT-Landesstandards). Entsprechende Hinweise wurden in den Endnoten der Anlage 1 aufgenommen.

Auf der EU-Ebene hat sich das IT-Recht zwischenzeitlich weiterentwickelt.

Mit der neuen Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) werden der Schutz kritischer Infrastrukturen (z. B. digitale Infrastruktur) in der Europäischen Union (EU), die Cybersicherheit und die Cyber-Sicherheitsstandards weiter verbessert. Die EU-Richtlinie muss von den Mitgliedstaaten in nationales Recht umgesetzt werden. Für Deutschland liegt das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2-UmsuCG) im Entwurf vor, welches voraussichtlich noch 2025 in Kraft treten wird. Den europäischen Vorgaben der NIS-2-Richtlinie entsprechende Landesgesetze[1] für Mecklenburg-Vorpommern liegen noch nicht vor[2].

Die Richtlinie „Critical Entities Resilience " (CER-Richtlinie) regelt die Resilienz von kritischen Infrastrukturen (z. B. digitale Infrastruktur und öffentliche Verwaltung) in der EU durch staatliche Aufsicht und Maßnahmen in Unternehmen. Sie soll im Wesentlichen durch das KRITIS-Dachgesetz umgesetzt werden, das einen bundeseinheitlichen und sektorübergreifenden Mindeststandard für den physischen Schutz der kritischen Infrastrukturen vorsieht und neben das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz treten soll. Die Bundesregierung hat am 28. November 2024 den Regierungsentwurf zum KRITIS-Dachgesetz vorgelegt, dessen weitere Abstimmung im Bundestag noch aussteht. Konkretisierungen für die Länder werden anschließend durch Rechtsverordnungen folgen.[3] Vom KRITIS-Dachgesetz sind Betreiber kritischer Anlagen betroffen, wenn diese über 500.000 Personen mit ihren Anlagen versorgen. Solche Größenordnungen erreicht Mecklenburg-Vorpommern nicht. Die Landesregierung sollte prüfen, ob und inwieweit vergleichbare Sicherheitsstandards dennoch für die Landesverwaltung und die Kommunen im Land geregelt werden sollen.

[1] Zum Anwendungsbereich der Richtlinie für die Länder siehe Art. 2 Abs. 2 lt. f Ziffer ii NIS-2-RL sowie die Erläuterungen dazu von Hornung/Schallbruch, IT-Sicherheitsrecht (2024), § 25 Öffentliche Verwaltung, Rz. 21.

[2] Siehe Sonderbericht „Herausforderungen bei der Digitalisierung der Landesverwaltung", Tz. 58ff. (https://www.lrh-mv.de/Veröffentlichungen/Sonderberichte/).

[3] Gesetzentwurf zum KRITIS-Dachgesetz (https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html).

Die Vorschriften der europäischen Verordnung über künstliche Intelligenz (KI-VO) gelten mit einigen wenigen Ausnahmen ab dem 2. August 2026 unmittelbar in den Mitgliedstaaten.[4] Die Verordnung macht – abhängig von den jeweils potenziellen Risiken – Vorgaben für mögliche Einsatzszenarien. Nach Art. 4b KI-VO müssen z. B. Anbieter und Betreiber sicherstellen, dass ihre Mitarbeiter oder sonstige Personen über einen hinreichenden Grad an Verständnis für Risiken und Potenziale bei der Nutzung eines KI-Systems verfügen („KI-Kompetenz").[5] Diese Pflicht gilt bereits ab dem 1. Februar 2025.

Beim europäischen Datenschutz dient der Angemessenheitsbeschluss der Europäischen Kommission vom 10. Juli 2023 als Grundlage für Datenübermittlungen personenbezogener Daten aus der Europäischen Union an zertifizierte Organisationen in den USA. Mit dem Beschluss wird dem Datenschutz-Rahmenwerk EU-USA [„EU-U.S. Data Privacy Framework" (DPF)] ein angemessenes Schutzniveau attestiert.[6] Es soll Rechtssicherheit für den transatlantischen Datentransfer schaffen. Ein wesentlicher Grundstein hierfür war der Präsidentenerlass 14086 („Executive Order 14086") vom 7. Oktober 2022, welcher den Zugriff US-amerikanischer Nachrichtendienste auf EU-Daten strenger reguliert und EU-Bürgern geeignete Rechtsmittel bei Verstößen zur Verfügung stellt/anbietet.

Unsicherheiten können sich jedoch aus den Absichten der derzeitigen US-Regierung ergeben. Deren neues zugrunde liegendes Staatsverständnis und dessen jüngste politische Entscheidungen über die Entlassung von Mitgliedern der unabhängigen Regierungsbehörde „Privacy and Civil Liberties Oversight Board" (PCLOB) beeinflussen auch die Einhaltung von datenschutzrechtlichen Anforderungen der EU.[7] Das PCLOB beaufsichtigt die US-Nachrichten- und Geheimdienste. Eine Schwächung dieser Behörde oder eine Lockerung bzw. Aufhebung der Executive Order 14086 durch den amtierenden Präsidenten würde weitreichende Folgen für den transatlantischen Datentransfer begründen.

Gemäß Art. 44 der europäischen Datenschutz-Grundverordnung (DS-GVO) ist eine Übermittlung personenbezogener Daten an Empfänger in einem Drittstaat nur zulässig, wenn die Bestimmungen der DS-GVO eingehalten werden. In der Vergangenheit hatte der Europäische Gerichtshof (EuGH) bereits

---

4 Stögmüller: Die Entwicklung des IT-Rechts, NJW 2024, S. 3758. Der Aufsatz liefert einen Überblick über die Entwicklungen und zugleich weitere Fundstellen.

5 Chibanguza/Steege: Die KI-Verordnung – Überblick über den neuen Rechtsrahmen NJW 2024, S. 1769 Rn. 13. Zum zeitlich gestuften Anwendungsbereich siehe Wendt/Wendt, Das neue Recht der Künstlichen Intelligenz (2024), § 3 AI Act Rn, 65.

6 Industrie- und Handelskammer Region Stuttgart: https://www.ihk.de/stuttgart/fuer-unternehmen/recht-und-steuern/datenschutzrecht/datenuebermittlung-usa-4852420.

7 Industrie- und Handelskammer Düsseldorf: https://www.ihk.de/duesseldorf/aussenwirtschaft/auslandsmaerkte/usa/transatlantischer-datenverkehr-4873114.

zweimal Regelungen der EU für Datentransfers zwischen der EU und den USA für unwirksam erklärt.[8] Sollte der aktuelle Angemessenheitsbeschluss vom 10. Juli 2023 aufgehoben werden, wären Behörden und Unternehmen gezwungen, die Nutzung von US-Cloud-Anbietern wie Apple, Google, Microsoft oder Amazon umgehend zu überprüfen.[9]

Personenbezogene Daten können dann nur noch an einen Empfänger in einem Drittstaat übermittelt werden, wenn der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Solche geeigneten Garantien müssen ein Schutzniveau gewährleisten, das mit dem in der Europäischen Union der Sache nach gleichwertig ist[10].

Der EuGH hat hierzu klargestellt, dass eine Übermittlung auszusetzen oder zu beenden ist, wenn das Recht des Drittstaates dem Empfänger der aus der Europäischen Union übermittelten personenbezogenen Daten Verpflichtungen auferlegt, die den genannten Klauseln widersprechen und geeignet sind, den vertraglich garantierten angemessenen Schutz vor Behördenzugriffen zu untergraben[11]. Neben der Einhaltung der DS-GVO hat die Landesverwaltung weitere Schutzvorschriften wie das Dienst-, Sozial- oder Steuergeheimnis zu wahren. Werden nicht datenschutzkonforme IT-Lösungen eingesetzt, sind i. d. R. auch diese Schutzvorschriften nicht eingehalten. Die Umsetzung der DS-GVO allein gewährleistet aber noch nicht, dass diese Schutzvorschriften auch eingehalten werden.

Bei der Durchführung neuer IT-Projekte, der Beschaffung von Hard- und Software sowie dem Abschluss neuer Verträge mit IT-Dienstleistern sind die Vorgaben des EuGH umzusetzen. Eine Datenübermittlung an US-amerikanische Empfänger sollte möglichst vermieden werden. Ist diese unvermeidbar bzw. werden Daten in andere Drittstaaten exportiert, sind bereits bei der Definition der Anforderungen geeignete Sicherheitsmaßnahmen festzulegen, die eine Nutzung personenbezogener Daten entgegen den Vorschriften der DS-GVO ausschließen (Privacy by Design).

Auch für andere Drittstaaten ist im Einzelfall zu prüfen, welche Maßnahmen getroffen werden müssen. Bei zukünftigen Vorhaben ist sicherzustellen, dass Hard- und Software offene Standards einhalten. Hersteller- oder produktbezogene Standards sollten grundsätzlich vermieden werden, wenn sie

[8] EuGH, Urteil vom 6. Oktober 2015 C-362/14 „Schrems-I“, Urteil vom 16. Juli 2020 – C-311/18 „Schrems-II“.

[9] https://www.cloudcomputing-insider.de/eu-us-datenabkommen-trump-rechtliche-grauzone-fuer-eu-unternehmen-a-73409349ad8cd270f433ca5179f424a4/?cmp=nl-5344fd13-49b3-416c-b3f6-2a6c9cd85875; https://www.nytimes.com/2025/01/22/us/trump-privacy-civil-liberties-oversight-board.html?smid=nytcore-ios-share&referringSource=articleShare.

[10] EuGH, Urteil vom 16. Juli 2020 – C 311/18, Rn. 96, Rn. 105.

[11] EuGH, Urteil vom 16. Juli 2020

nicht vollständig offen zugänglich sind. Die Möglichkeit, Open-Source-Produkte einzusetzen, sollte bei allen Vorhaben geprüft werden.

4 Dokumentationsanforderungen (Anlagen 2 und 3)

Die Ordnungsmäßigkeit des Einsatzes von IT setzt Dokumentationen voraus. Darin sind die aus den rechtlichen Grundlagen abgeleiteten organisatorischen und technischen Maßnahmen zu dokumentieren und notwendige behördeninterne Regelungen zu erlassen. Art und Umfang der erforderlichen Dokumentationen sind in den Anlagen 2 (Was ist zu dokumentieren?) und 3 (Wie ist zu dokumentieren?) dargestellt.

5 Beschaffung von Lieferungen und Leistungen (Anlage 4)

Aufgrund seiner Prüfungserfahrungen hat der Landesrechnungshof in der Anlage 4 Anforderungen an die Beschaffung von Lieferungen und Leistungen im IT-Bereich erstellt, die die Basis seiner Prüfungen darstellen.

gez. Dr. Johannsen gez. Hengstenberg

gez. Fuhrmann gez. Dr. Zitscher

Anlagen:

- Anlage 1: Wesentliche anzuwendende Rechtsvorschriften und Prüfungsmaßstäbe
- Anlage 2: Dokumentationsanforderungen beim Einsatz von IT und elektronischer Datenverarbeitung – was ist zu dokumentieren?
- Anlage 3: Grundsätze für die Dokumentation – wie ist zu dokumentieren?
- Anlage 4: Anforderungen an die Beschaffung von Leistungen und Dienstleistungen
- Anlage 5 IT-Mindestanforderungen

Anlage 1 – Wesentliche anzuwendende Rechtsvorschriften, Hinweise und Empfehlungen

1 Mindestanforderungen der Rechnungshöfe des Bundes und der Länder

- IT-Mindestanforderungen in der jeweils aktuellen Fassung[1]

2 Datenschutz

EU-Recht

- Datenschutz-Grundverordnung (DS-GVO)[2]

Gesetze

- Das Zehnte Buch Sozialgesetzbuch (SGB X) – §§ 80 bis 84 Verarbeitung von Sozialdaten[3]
- Landesbeamtengesetz (LBG M-V) – §§ 84 bis 91 Verarbeitung personenbezogener Daten, Führung und Inhalt der Personalakten sowie Zugang zu Personalakten[4]
- Landesdatenschutzgesetz (DSG M-V)[5] und
- Sicherheits- und Ordnungsgesetz (SOG M-V) – §§ 25 bis 49 Verarbeitung personenbezogener Daten[6]

Rechtsverordnungen

- Schuldatenschutzverordnung (SchulDSVO M-V)[7]

Hinweise und Empfehlungen

- Publikationen der Konferenz der unabhängigen Datenschutzbehörden (DSK):

  Entschließungen, Kurzpapiere, Orientierungshilfen, Anwendungshinweise, z. B.:

  - Datenschutz bei Windows 10 – Prüfschema[8]
  - Standard-Datenschutzmodell Version 3.1 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und die Bausteine des Maßnahmenkatalogs[9] und
  - Orientierungshilfe Videokonferenzsysteme[10]

3 Informationssicherheitsmanagement

EU-Recht

- Richtlinie über die Resilienz kritischer Einrichtungen (engl. „Critical Entities Resilience Directive“) (CER-Richtlinie)[11] und
- Richtlinie zur Netzwerk- und Informationssicherheit (engl. „Network and Information Security Directive 2“) (NIS-2-Richtlinie)[12]

Gesetze

- BSI-Gesetz (BSIG)[13] - § 8 Abs. 1 Vorgaben des Bundesamtes (Mindeststandards)[14]

Rechtsverordnungen

- IT-Sicherheitsverordnung Portalverbund (ITSiV-PV)[15]

Verwaltungsvorschriften

- Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung[16]
- Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V)[17]
- Anschlussbedingungen für das Verbindungsnetz Version 2.0 einschließlich des IT-Grundschutzprofils (Beschluss IT-Planungsrat vom 25. März 2020)[18]
- Anschlussbedingungen für das Corporate Network Landeskommunikationsvermittlungs- und Informationsnetz (CN-LAVINE) des Landes Mecklenburg-Vorpommern (AB CNL 2.02)[19]
- Standards des Bundesamtes für die Sicherheit in der Informationstechnik (BSI-Standards)[20]:
  - 200-1 Managementsysteme für Informationssicherheit
  - 200-2 IT-Grundschutz-Methodik
  - 200-3 Risikomanagement
  - 200-4 Business Continuity Management
  - 100-4 Notfallmanagement und
  - Print-Version IT-Grundschutz-Kompendium, Reguvis Fachmedien GmbH[21]

Hinweise und Empfehlungen

- Grundsatzpapier zum Informationssicherheitsmanagement der Rechnungshöfe des Bundes und der Länder[22]
- Rundschreiben des Landesrechnungshofes Mecklenburg-Vorpommern[23]
  - Rundschreiben Nr. 2/2016 – Informationssicherheitsmanagement vom 11. Januar 2016
  - Rundschreiben Nr. 1/2017 – IuK-Mindestanforderungen und
  - Rundschreiben Nr. 01/2020 – Grundsatzpapier zum Informationssicherheitsmanagement
- Empfehlungen des BSI zur IT-Sicherheit, insbesondere:
  - Analyse der Telemetriekomponente in Windows 10 (Konfigurations- und Protokollierungsempfehlungen)[24] und
  - Empfehlungen und Hinweise des BSI und der Allianz für Cybersicherheit[25]
- Cyber-Sicherheitsstrategie für Deutschland[26]
- Standards zur Internet-Sicherheit (ISi-Reihe)[27]
- DIN ISO/IEC 27001 – Audits (Informationssicherheit) - Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen[28]
- Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz[29]
- Normenreihe ISO/IEC 20000 – Spezifikationen und Empfehlungen für IT Service Management[30] und
- IT Infrastructure Library (ITIL)[31]

4 Digitale Verwaltung (E-Government)

EU-Recht

- Datenverordnung (engl. „Data Act“)[32]
- Durchführungsverordnung zu Hochwertigen Datensätzen (DVO-HVD)[33]
- Verordnung über digitale Dienste (engl. „Digital Services Act“) (DSA)[34]
- Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS-Verordnung)[35] und
- Verordnung über künstliche Intelligenz (engl. „Artificial Intelligence Act“) (KI-VO oder AI Act)[36]

Gesetze

- Digitale-Dienste-Gesetz (DDG)[37]
- Gesetz zum Ersten IT-Änderungsstaatsvertrag (GGArt91cÄndVtr1G)[38]
- KONSENS-Gesetz (KONSENS-G)[39]
- Onlinezugangsgesetz (OZG)[40]
- Vertrauensdienstegesetz (VDG)[41]
- E-Government-Gesetz Mecklenburg-Vorpommern (EGovG M-V)[42] und
- Landesverwaltungsverfahrensgesetz (VwVfG M-V) – §§ 3a, 35a, 41 Abs. 2a, 98 Abs. 4 bis 7 VwVfG M-V[43]

Rechtsverordnungen

- Landesverordnung über Datenaustauschstandards (DaALVO M-V)[44] und
- E-Government-Basisdienste-Landesverordnung (BasDi LVO M-V)[45]

Verwaltungsvorschriften

- IT-Richtlinie (ITRL M-V) [46]
- IT-Landesstandards[47]

Hinweise und Empfehlungen

- Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung (Organisationshandbuch - Orghandbuch) [48]
- Datenaustauschstandards des IT-Planungsrats[49]
- Mindestanforderungen an den Betrieb von “Einer für Alle“-Services[50]
- Eigenerklärung der „Einer für Alle“-Dienstleister sowie Plausibilitätsprüfung durch die zentrale Stelle des bereitstellenden Landes[51]
- Koordinierungsstelle für IT-Standards (KoSIT)[52]
- Digitalstrategie der EU – Gestaltung der digitalen Zukunft Europas[53]
- Grundsätze für die Verwaltungsorganisation[54]
- Leitsätze für die Personalbedarfsermittlung[55]und
- Architekturrichtlinie für die IT des Bundes[56]

5 Elektronische Aktenführung

Gesetze

- E-Government-Gesetz Mecklenburg-Vorpommern (EGovG M-V)[57] – § 10 Elektronische Aktenführung
- Landesarchivgesetz (LArchivG M-V)[58] und
- Landesbeamtengesetz (LBG M-V)[59] – § 91 Automatisierte Verarbeitung von Personalakten

Rechtsverordnungen

- Dokumentenerstellungs und -übermittlungsverordung (DokErstÜbV)[60]
- Elektronischer-Rechtsverkehr-Verordnung (ERVV)[61] und
- EAkten-Verordnung (EaktVO M-V)[62]

Verwaltungsvorschriften

- 2. Elektronischer-Rechtsverkehr-Bekanntmachung 2022[63] und
- Verwaltungsvorschrift zu § 1 der Verordnung zur elektronischen Aktenführung bei den Gerichten (EAktVV M-V)[64]

Hinweise und Empfehlungen

- Organisationskonzept elektronische Verwaltungsarbeit, verschiedene Bausteine, u. a. zur E-Akte[65] und
- Positionspapier Aktenführung und E-Akte[66]

6 Haushalt

Gesetze

- Grundgesetz für die Bundesrepublik Deutschland (GG) – Art. 91a bis 91d und 104a bis 115 GG[67],
- Haushaltsgrundsätzegesetz (HGrG)[68]
- Verfassung des Landes Mecklenburg-Vorpommern (Verf MV) – Art. 61 bis 68 und 79a[69]
- Haushaltsbegleitgesetz in der jeweils gültigen Fassung (HBeglG M-V)[70]
- Haushaltsgesetz in der jeweils gültigen Fassung (HG M-V)[71]

- Haushaltsbegleitgesetz zum Nachtragshaushaltsgesetz in der jeweils gültigen Fassung[72]
- Landeshaushaltsordnung Mecklenburg-Vorpommern (LHO)[73] und
- Nachtragshaushaltsgesetz in der jeweils gültigen Fassung[74]

Verwaltungsvorschriften

- Verwaltungsvorschriften zur Landeshaushaltsordnung (VV-LHO)[75]
- Verwaltungsvorschriften zur Haushaltssystematik des Landes Mecklenburg-Vorpommern (VV-HS)[76]
- Haushaltstechnische Richtlinien des Landes Mecklenburg-Vorpommern (HRL)[77]
- Haushaltsrunderlass in der jeweils gültigen Fassung[78]
- Bewirtschaftungserlass(e) in der jeweils gültigen Fassung[79]
- Resteerlass in der jeweils gültigen Fassung

Beschaffung von Lieferungen und Leistungen

Gesetze

- Gesetz gegen Wettbewerbsbeschränkungen (GWB) – Teil 4 Vergabe von öffentlichen Aufträgen und Konzessionen[80]
- Datenverarbeitungszentrumsgesetz (DVZG M-V)[81] und
- Tariftreue- und Vergabegesetz Mecklenburg-Vorpommern (TVgG M-V)[82]

Rechtsverordnungen

- Vergabeverordnung (VgV)[83]
- Vergabeverordnung Verteidigung und Sicherheit (VSVgV)[84] und
- Vergabe- und Mindestarbeitsbedingungen-Verfahrensverordnung (VgMinArbV M-V)[85]

Verwaltungsvorschriften

- Unterschwellenvergabeordnung (UVgO)[86] und
- Beschaffungsrichtlinie (BeschaffRL M-V)[87]

Hinweise und Empfehlungen

- Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT)[88]
- Handreichung zum TVgG M-V pp.[89]und
- Leitfäden für produktneutrale Ausschreibungen[90]

7 Entwicklung und Betrieb von IT-Kassenverfahren

Verwaltungsvorschriften

- VV Nr. 6 zu §§ 70 bis 80 Landeshaushaltsordnung (LHO)[91], insbesondere Anlage 6 zu VV Nr. 6 zu §§ 70 bis 80 LHO – Grundsätze ordnungsgemäßer Buchführung bei Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen (GoBIT-HKR)[92] und
- Verfahrensrichtlinie zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen im Land Mecklenburg-Vorpommern (VerfRi-IT-HKR)[93]

8 Arbeits- und Gesundheitsschutz

Gesetze

- Arbeitsschutzgesetz (ArbSchG)[94]
- E-Government-Gesetz Mecklenburg-Vorpommern (EGovG M-V) – § 9 Barrierefreiheit und
- Landesbehindertengleichstellungsgesetz (LBGG M-V)[95] – § 13 Gestaltung von Bescheiden und Vordrucken

Rechtsverordnungen

- Arbeitsstättenverordnung (ArbStättV), insbesondere Anhang Nr. 6 Maßnahmen zur Gestaltung von Bildschirmarbeitsplätzen[96] und
- Barrierefreie-Informationstechnik-Verordnung (BITV 2.0)[97]

Hinweise und Empfehlungen

- Veröffentlichungen der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA), insbesondere zur Softwareergonomie[98]

9 Wirtschaftlichkeit und Erfolgskontrolle

Gesetze

- Haushaltsgrundsätzegesetz (HGrG) – § 6 Wirtschaftlichkeit und Sparsamkeit, Kosten- und Leistungsrechnung[99] und
- Landeshaushaltsordnung Mecklenburg-Vorpommern (LHO) – §§ 6, 7, 24 und 34

Verwaltungsvorschriften

- Verwaltungsvorschriften zur Landeshaushaltsordnung (VV-LHO) – §§ 6, 7, 24 und 34[100] und
- Arbeitsanleitung Einführung in Wirtschaftlichkeitsuntersuchungen[101]

Hinweise und Empfehlungen

- Anforderungen an Wirtschaftlichkeitsuntersuchungen finanzwirksamer Maßnahmen nach § 7 Bundeshaushaltsordnung[102]
- Erfolgskontrolle finanzwirksamer Maßnahmen in der öffentlichen Verwaltung[103]
- Erfolgskontrolle in der öffentlichen Verwaltung[104] und
- WiBe 5.0, Konzept zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT[105]

10 IT-Verbünde und IT-Kooperationen

Hinweise und Empfehlungen

- Rundschreiben Nr. 02/2020 des Landesrechnungshofes Mecklenburg-Vorpommern – IT-Verbünde und IT-Kooperationen[106]

[1] Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik - Leitlinien und gemeinsame Maßstäbe für IT-Prüfungen - (IT-Mindestanforderungen 2025): www.lrh-mv.de/Veröffentlichungen/Gemeinsame-Dokumente-der-Rechnungshöfe/.

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119 vom 4. Mai 2016, S. 1, L 314 vom 22. November 2016, S. 72, L 127 vom 23. Mai 2018, S. 2, L 074 vom 4. März2021, S. 35).

[3] Das Zehnte Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S.130), das zuletzt durch Artikel 8d des Gesetzes vom 19. Juli 2024 (BGBl. I Nr. 245) geändert worden ist.

[4] Beamtengesetz für das Land Mecklenburg-Vorpommern vom 17. Dezember 2009 (GVOBl. M-V S. 687), das zuletzt durch Artikel 5 des Gesetzes vom 14. Mai 2024 (GVOBl. M-V S. 154) geändert worden ist.

[5] Datenschutzgesetz für das Land Mecklenburg-Vorpommern vom 22. Mai 2018 (GVOBl. M-V S. 193).

[6] Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern vom 27. April 2020 (GVOBl. M-V S. 334), das zuletzt durch Gesetz vom 14. Dezember 2023 (GVOBl. M-V S. 891) geändert worden ist.

[7] Verordnung zum Umgang mit personenbezogenen Daten der Schülerinnen und Schüler, Erziehungsberechtigten, Lehrkräften und sonstigem Schulpersonal vom 23.April 2020 (GVOBl. M-V S. 302).

[8] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.pdf.

[9] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf.

[10] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf.

[11] Richtlinie (EU) 2022/2557 des europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27. Dezember 2022, S. 164).

[12] Richtlinie (EU) 2022/2555 des europäischen Parlaments und des Rates vom 14.Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27. Dezember 2022, S. 80, L 90206 vom 22. Dezember 2023, S. 1).

[13] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist.

[14] Bundesamt für die Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html.

[15] Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten vom 6. Januar 2022 (BGBl. I S. 18).

[16] IT-Planungsrat: https://www.it-planungsrat.de/fileadmin/beschluesse/2019/Beschluss2019-04_TOP12_Anlage-Leitlinie.pdf und https://www.it-planungsrat.de/beschluss/beschluss-2019-59.

[17] Ministerium für Inneres, Bau und Digitalisierung Mecklenburg-Vorpommern (IM M-V): Stand 12. Mai 2014, Fortschreibung steht aus (https://wir.m-v.de/dokumentation-und-wissen/informationssicherheit/Leitlinien-

und-Sicherheitsstandards/).

[18] IT-Planungsrat: https://www.it-planungsrat.de/beschluss/beschluss-2020-15.

[19] IM M-V (verwaltungsinterner Zugang): https://wir.m-v.de/dokumentation-und-wissen/informationssicherheit/Leitlinien-und-Sicherheitsstandards/.

[20] Bundesamt für die Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html

[21] Bundesamt für die Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/Bezugsquellen/bezugsquellen_node.html.

[22] Rechnungshöfe des Bundes und der Länder: www.lrh-mv.de/Veröffentlichungen/Gemeinsame-Dokumente-der-Rechnungshöfe.

[23] Landesrechnungshof Mecklenburg-Vorpommern: https://www.lrh-mv.de/Veröffentlichungen/Rundschreiben/.

[24] Bundesamt für die Sicherheit in der Informationstechnik: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Analyse_Telemetriekomponente_1_2.html.

[25] Bundesamt für die Sicherheit in der Informationstechnik: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen.

[26] Bundesministerium des Innern, für Bau und Heimat: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1.

[27] Bundesamt für die Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/ISI-Reihe/isi-reihe_node.html.

[28] Deutsches Institut für Normung e. V. (DIN), International Organization for Standardization (ISO).

[29] Bundesamt für die Sicherheit in der Informationstechnik: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v4.pdf?__blob=publicationFile&v=2.

[30] DIN/ISO.

[31] https://www.axelos.com/certifications/itil-service-management.

[32] Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (ABl. L 2854 vom 22. Dezember 2023, S. 1), L 90790 vom 9. Dezember 2024, S. 1).

[33] Durchführungsverordnung (EU) 2023/138 der Kommission vom 21. Dezember 2022 zur Festlegung bestimmter hochwertiger Datensätze und der Modalitäten ihrer Veröffentlichung und Weiterverwendung (ABl. L 19/43 vom 20. Januar 2023, S. 43).

[34] Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 17. Oktober 2022, S. 1, L 310 vom 1. Dezember 2022, S. 17).

[35] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28. August 2014, S. 73, L 023 vom 29. Januar 2015, S. 19, L 155 vom 14. Juni 2016, S. 44, L 90317 vom 9. April 2025, S. 1), die zuletzt durch die Verordnung (EU) 2024/1183 (ABl. L 1183 vom 30. April 2024, S. 1) geändert worden ist.

[36] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) Nr. 2018/858, (EU) Nr. 2018/1139 und (EU) Nr. 2019/2144 sowie der Richtlinien (EU) 2014/90, (EU) 2016/797 und (EU) 2020/1828 (ABl. L 2024/1689 vom 12. Juli 2024, S. 1).

[37] Digitale-Dienste-Gesetz vom 6. Mai 2024 (BGBl. I Nr. 149).

[38] Gesetz zum Ersten IT-Änderungsstaatsvertrag vom 4. August 2019 (BGBl. I S. 1126).

[39] Gesetz über die Koordinierung der Entwicklung und des Einsatzes neuer Software der Steuerverwaltung vom 14. August 2017 (BGBl. I S. 3122, 3129).

[40] Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen vom 14. August 2017 (BGBl. I S. 3122, 3138), das zuletzt durch Artikel 1 des Gesetzes vom 19. Juli 2024 (BGBl. I Nr. 245) geändert worden ist.

[41] Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das zuletzt durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist.

[42] Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern vom 25. April 2016 (GVOBl. M-V S. 198), das zuletzt durch Artikel 1 des Gesetzes vom 9. April 2024 (GVOBl. M-V S. 110) geändert worden ist (Überarbeitung steht aus, vgl. Anlage 1 des Sonderberichts Herausforderungen bei der Digitalisierung der Landesverwaltung, LRH M-V, https://www.lrh-mv.de/Veröffentlichungen/Sonderberichte/).

[43] Verwaltungsverfahrens-, Zustellungs- und Vollstreckungsgesetz des Landes Mecklenburg-Vorpommern vom 6. Mai 2020 (GVOBl. M-V S. 410), das zuletzt durch Artikel 1 des Gesetzes vom 11. Dezember 2024 (GVOBl. M-V S. 617) geändert worden ist.

[44] Landesverordnung über Datenaustauschstandards vom 7. Januar 2020 (GVOBl. M-V S. 10) (derzeit in Prüfung aufgrund notwendiger Anpassungsbedarfe, vgl. Sonderbericht Herausforderungen bei der Digitalisierung der Landesverwaltung, LRH M-V, https://www.lrh-mv.de/Veröffentlichungen/Sonderberichte/).

[45] Landesverordnung über die Bereitstellung, Ausgestaltung und Nutzung von E-Government-Basisdiensten im Land Mecklenburg-Vorpommern vom 4. Oktober 2021(GVOBl. M-V S. 1356).

[46] Innenministerium Mecklenburg-Vorpommern: IT-Richtlinie der Behörden der Landesverwaltung Mecklenburg-Vorpommern vom 1. September 2021 – VIII 520 - 0251-1000-2015/001 (https://wir.m-v.de/dokumentation-und-wissen/zdmv/richtlinien-beschluesse/).

[47] Innenministerium Mecklenburg-Vorpommern: IT-Landesstandards derzeit unveröffentlicht (Überarbeitung steht nach Aussagen Innenministerium aus, vgl. Anlage 1 des Sonderberichts Herausforderungen bei der Digitalisierung der Landesverwaltung, LRH M-V, https://www.lrh-mv.de/Veröffentlichungen/Sonderberichte/).

[48] Bundesministerium des Innern, für Bau und Heimat: Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung (Online-Version) (https://www.orghandbuch.de/Webs/OHB/DE/startseite/startseite-node.html).

[49] https://docs.fitko.de/fit-standards/.

[50] IT-Planungsrat: https://www.it-planungsrat.de/fileadmin/beschluesse/2023/Beschluss2023-07_EfA_Mindestanforderungen.pdf.

[51] IT-Planungsrat: https://www.it-planungsrat.de/beschluss/beschluss-2024-59_EfA-Nachnutzung-Informationssicherheit_Eigenerklärung_und_Plausibilitätsprüfung.pdf.

[52] KoSIT: www.xoev.de (Startseite).

[53] Europäische Kommission: Fortschrittsbericht zur Umsetzung in 2025 erwartet, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_de.

[54] Rechnungshöfe des Bundes und der Länder: www.lrh-mv.de/Veröffentlichungen/Gemeinsame-Dokumente-der-Rechnungshöfe/.

[55] Rechnungshöfe des Bundes und der Länder: www.lrh-mv.de/Veröffentlichungen/Gemeinsame-Dokumente-der-Rechnungshöfe/.

[56] https://www.publikationen-bundesregierung.de/pp-de/publikationssuche/it-des-bundes-2248438.

[57] Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern vom 25. April 2016 (GVOBl. M-V S. 198), das zuletzt durch Artikel 1 des Gesetzes vom 9. April 2024 (GVOBl. M-V S. 110) geändert worden ist.

[58] Archivgesetz für das Land Mecklenburg-Vorpommern vom 7. Juli 1997 (GVOBl. M-V S. 282), das zuletzt durch Artikel 1 des Gesetzes vom 8. Mai 2018 (GVOBl. M-V S. 172) geändert worden ist.

[59] Beamtengesetz für das Land Mecklenburg-Vorpommern vom 17. Dezember 2009 (GVOBl. M-V S. 687), das zuletzt durch Artikel 5 des Gesetzes vom 14. Mai 2024 (GVOBl. M-V S. 154) geändert worden ist.

[60] Verordnung über die Standards für die Erstellung elektronischer Dokumente und für deren Übermittlung zwischen Strafverfolgungsbehörden und Gerichten vom 28. Februar 2020 (BGBl. I S. 244), das zuletzt durch Artikel 40 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234) geändert worden ist.

[61] Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach vom 24. November 2017 (BGBl. I S. 3803), das zuletzt durch Artikel 43 des Gesetzes vom 12. Juli 2024 (BGBl. I Nr. 234) geändert worden ist.

[62] Verordnung zur elektronischen Aktenführung bei den Gerichten vom 4. August 2018 (GVOBl. M-V S. 307), das zuletzt durch Verordnung vom 4. Dezember 2024 (GVOBl. M-V S. 623) geändert worden ist.

[63] Zweite Bekanntmachung zu § 5 der Elektronischer-Rechtsverkehr-Verordnung vom 10. Februar 2022 im Bundesanzeiger (BAnz AT 18. Februar 2022 B2).

[64] Verwaltungsvorschrift des Justizministeriums vom 16. August 2018 (AmtsBl. M-V 2018 S. 478), zuletzt geändert durch Verwaltungsvorschrift vom 31. März 2024 (AmtsBl. M-V 2025 S. 250).

[65] Bundesministerium des Innern, für Bau und Heimat: https://www.verwaltung-innovativ.de/DE/Verwaltungsdigitalisierung/orgkonzept_everwaltung/orgkonzept_everwaltung_node.html.

[66] Rechnungshöfe des Bundes und der Länder: www.lrh-mv.de/Veröffentlichungen/Gemeinsame-Dokumente-der-Rechnungshöfe/.

[67] Grundgesetz für die Bundesrepublik in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 22. März 2025 (BGBl. I Nr. 94) geändert worden ist.

[68] Gesetz über die Grundsätze des Haushaltsrechts des Bundes und der Länder vom 19. August 1969 (BGBl. I S. 1273), das zuletzt durch Artikel 1 des Gesetzes vom 21. August 2024 (BGBl. I Nr. 361) geändert worden ist.

[69] Verfassung des Landes Mecklenburg-Vorpommern vom 23. Mai 1993 (GVOBl. M-V S. 372), die zuletzt durch Gesetz vom 20. Februar 2025 (GVOBl. M-V S. 58) geändert worden ist.

[70] Haushaltsbegleitgesetz 2024/2025 vom 18. Dezember 2023 (GVOBl. M-V S. 920) (https://www.regierung-mv.de/Landesregierung/fm/Haushalt/Haushaltsplan/Haushaltsrecht/).

[71] Gesetz über die Feststellung des Haushaltsplanes des Landes Mecklenburg-Vorpommern für die Haushalts-

jahre 2024 und 2025 vom 18. Dezember 2023 (GVOBl. M-V S. 894) (https://www.regierung-mv.de/Landesregierung/fm/Haushalt/Haushaltsplan/Haushaltsrecht/).

[72] Haushaltsbegleitgesetz zum Nachtragshauhaltsgesetz 2025 vom 15. Mai 2025 (GVOBl. M-V S. 214).

[73] Landeshaushaltsordnung Mecklenburg-Vorpommern in der Fassung der Bekanntmachung vom 10. April 2000 (GVOBl. M-V S. 159), die zuletzt durch Artikel 2 des Gesetzes vom 18. Dezember 2023 (GVOBl. M-V S. 934) geändert worden ist.

[74] Gesetz über die Feststellung eines Nachtrags zum Haushalt für das Haushaltsjahr 2025 vom 15. Mai 2025 (GVOBl. M-V S. 206)

[75] Verwaltungsvorschriften zur Landeshaushaltsordnung vom 22. September 2005 (AmtsBl. M-V S. 1121), die zuletzt durch Verwaltungsvorschrift des Finanzministeriums vom 11. Dezember 2024 (AmtsBl. M-V S. 1120) geändert worden sind (https://www.regierung-mv.de/Landesregierung/fm/Haushalt/Haushaltsplan/Haushaltsrecht/).

[76] Verwaltungsvorschrift zur Haushaltssystematik des Landes Mecklenburg-Vorpommern vom 11. Dezember 2024 – IV 200 -2H 1005-VV-HS-2010/019-010 – (AmtsBl. M-V S. 1050).

[77] Verwaltungsvorschrift des Finanzministeriums vom 2. Dezember 2002 (AmtsBl. M-V S. 1509), die zuletzt durch Verwaltungsvorschrift vom 2. Dezember 2020 (AmtsBl. M-V S. 596) geändert worden ist (https://www.regierung-mv.de/Landesregierung/fm/Haushalt/Haushaltsplan/Haushaltsrecht/).

[78] Finanzministerium Mecklenburg-Vorpommern: Erlass Haushaltsvoranschläge/Beiträge zum Entwurf des Haushaltsplans 2024/2025 sowie zum Finanzplan 2023 bis 2028 (https://www.regierung-mv.de/Landesregierung/fm/Haushalt/Haushaltsplan/Haushaltsrecht/).

[79] Finanzministerium Mecklenburg-Vorpommern: Verwaltungsvorschriften zur Haushalts- und Wirtschaftsführung der Landesverwaltung im jeweiligen Haushaltsjahr (https://www.regierung-mv.de/Landesregierung/fm/Haushalt/Haushaltsplan/Haushaltsrecht/).

[80] Gesetz gegen Wettbewerbsbeschränkungen vom 26. Juni 2013 (BGBl. I S. 1750, 3245), das zuletzt durch Artikel 6 des Gesetzes vom 5. Dezember 2024 (BGBl. 2024 I Nr. 400) geändert worden ist.

[81] Gesetz über die Rechtsstellung des Datenverarbeitungszentrums Mecklenburg-Vorpommern vom 1. November 2000 (GVOBl. M-V S. 522), das zuletzt durch Art. 22 des Gesetzes vom 19. Dezember 2005 (GVOBl. M-V S. 640) geändert worden ist (Überarbeitung angekündigt, vgl. Sonderbericht Herausforderungen bei der Digitalisierung der Landesverwaltung, LRH M-V, https://www.lrh-mv.de/Veröffentlichungen/Sonderberichte/).

[82] Tariftreue- und Vergabegesetz Mecklenburg-Vorpommern vom 18. Dezember 2023 (GVOBl. M-V S. 934).

[83] Verordnung über die Vergabe öffentlicher Aufträge vom 12. April 2016 (BGBl. I S. 624), die zuletzt durch Artikel 1 der Verordnung vom 7. Februar 2024 (BGBl. 2024 I Nr. 39) geändert worden ist.

[84] Vergabeverordnung für die Bereiche Verteidigung und Sicherheit zur Umsetzung der Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Koordinierung der Verfahren zur Vergabe bestimmter Bau-, Liefer- und Dienstleistungsaufträge in den Bereichen Verteidigung und Sicherheit und zur Änderung der Richtlinien 2004/17/EG und 2004/18/EG vom 12. Juli 2012 (BGBl. I S. 1509), die zuletzt durch Artikel 2 der Verordnung vom 7. Februar 2024 (BGBl. 2024 I Nr. 39) geändert worden ist.

[85] Verordnung über das Vergabeverfahren und das Verfahren zur Festlegung und Kontrolle von Mindestarbeitsbedingungen vom 19. April 2024 (GVOBl. M-V S. 127).

[86] Bekanntmachung der Verfahrensordnung für die Vergabe öffentlicher Liefer- und Dienstleistungsaufträge un-

terhalb der EU-Schwellenwerte vom 2. Februar 2017 (Banz. AT 7. Februar 2017 B1, ber. Banz AT 8. Februar 2017 B1).

[87] Richtlinie für das Verfahren bei Beschaffungen durch das Landesamt für innere Verwaltung vom 11. Dezember 2017 (AmtsBl. M-V S. 866).

[88] Der Beauftragte der Bundesregierung für Informationstechnik (engl. Chief Information Officer (CIO)): https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-einkauf/evb-it-und-bvb/evb-it/evb-it-node.html.

[89] https://www.regierung-mv.de/Landesregierung/wm/Wirtschaft/Öffentliches-Auftragswesen/.

[90] Bitkom e.V.: https://www.bitkom.org/ITK-Beschaffung/Alle-Leitfäden.

[91] Verwaltungsvorschriften zur Landeshaushaltsordnung vom 22. September 2005 (AmtsBl. M-V S. 1121), die zuletzt durch Verwaltungsvorschrift des Finanzministeriums vom 11. Dezember 2024 (AmtsBl. M-V S. 1120) geändert worden sind.

[92] Ebd.

[93] Finanzministerium Mecklenburg-Vorpommern: Richtlinie vom 24. Mai 2017 (https://www.regierung-mv.de/Landesregierung/fm/Haushalt/Haushaltsplan/Haushaltsrecht/).

[94] Gesetz über die Durchführung von Maßnahmen des Arbeitsschutzes zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Beschäftigten bei der Arbeit vom 7. August 1996 (BGBl. I S. 1246), das zuletzt durch Artikel 32 des Gesetzes vom 15. Juli 2024 (BGBl. I Nr. 236) geändert worden ist.

[95] Gesetz zur Gleichstellung, gleichberechtigten Teilhabe und Integration von Menschen mit Behinderungen vom 10. Juli 2006 (GVOBl. M-V S.539), das zuletzt durch Artikel 10 des Gesetzes vom 14. Mai 2024 (GVOBl. M-V S. 154) geändert worden ist.

[96] Verordnung über Arbeitsstätten vom 12. August 2004 (BGBl. I S. 2179), die zuletzt durch Artikel 10 des Gesetzes vom 27. März 2024 (BGBl. I Nr. 109) geändert worden ist.

[97] Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BGBl. I S. 1843), die zuletzt durch Artikel 1 der Verordnung vom 24. Oktober 2023 (BGBl. I Nr. 286) geändert worden ist.

[98] BauA: https://www.baua.de/DE/Angebote/Publikationen/Praxis/A72.

[99] Gesetz über die Grundsätze des Haushaltsrechts des Bundes und der Länder vom 19. August 1969 (BGBl. I S. 1273), das zuletzt durch Artikel 1 des Gesetzes vom 21. August 2024 (BGBl. I Nr. 361) geändert worden ist.

[100] Verwaltungsvorschriften zur Landeshaushaltsordnung vom 22. September 2005 (AmtsBl. M-V S. 1121), die zuletzt durch Verwaltungsvorschrift des Finanzministeriums vom 11. Dezember 2024 (AmtsBl. M-V S. 1120).

[101] Rundschreiben des Bundesministeriums für Finanzen (BMF) vom 12. Januar 2011, in der Fassung der Änderung durch Rundschreiben des BMF vom 17. Mai 2024 – II A 3 – H 1012-6/23/10003:006 (https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_20122013_IIA3H1012100810004.htm).

[102] Empfehlungen des Präsidenten des Bundesrechnungshofes als Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung, Band 18, 2013 (www.bundesrechnungshof.de und https://wibe.de/wp-content/uploads/bwv-band18-Anford_an_WU_2013.pdf).

[103] Gutachten des Beauftragten für die Wirtschaftlichkeit in der Verwaltung, Band 2, 1998 (www.bundesrechnungshof.de).

[104] Finanzministerium Mecklenburg-Vorpommern: https://www.regierung-mv.de/Landesregierung/fm/Service/Publikationen/.

[105] Bundesamt für die Sicherheit in der Informationstechnik: https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-beschaffung/wirtschaftlichkeitsbetrachtung/wibe5-0/wibe-fachkonzept-5-0.pdf?__blob=publicationFile&v=5.

[106] Landesrechnungshof Mecklenburg-Vorpommern: www.lrh-mv.de/Veröffentlichungen/Rundschreiben/.

Anlage 2 – Dokumentationsanforderungen beim Einsatz von IT und elektronischer Datenverarbeitung

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
I Übergreifende Regelungen		
I a Basisregeln		
Hausordnung, Geschäftsordnung/-anweisung, Brandschutzordnung, Geschäftsverteilungsplan, Organigramm	Art. 5 Absatz 2 DS-GVO[1]: Rechenschaftspflicht Art. 24 Absatz 1 DS-GVO: Nachweis DS-GVO-konformer Datenverarbeitung	• übergreifende organisatorische Maßnahmen des Datenschutzes festlegen, soweit nicht eigenständig geregelt
	SDM[2] M 42.P07	• Organigramm und GVP
	SDM M42.P13 (Art. 24 Abs. 1 DS-GVO)	• Dokumentation der Datenschutzorganisation gemäß Art. 24 Abs. 1 DS-GVO
	IT-Grundschutz-Kompendium[3] CON.2.A1 MUSS, R 2	• Umsetzung Standard-Datenschutzmodell (SDM): (Einhaltung gesetzlicher Bestimmungen zum Datenschutz) • Wird das SDM nicht verwendet, so ist dies zu begründen
	IT-Grundschutz-Kompendium ORP.1.A1 MUSS, R 1	• Verantwortlichkeiten und Befugnisse für sicherheitsrelevante Aufgaben festlegen • verbindliche Regelungen zur Informationssicherheit für verschiedene betriebliche Aspekte übergreifend festlegen • verbindliche Regelungen anlassbezogen überarbeiten
	IT-Grundschutz-Kompendium ORP1.A2 MUSS, R 1	• für alle Informationen, Geschäftsprozesse, Anwendungen und IT-Komponenten Verantwortliche festlegen und Verantwortlichkeiten veröffentlichen
	IT-Grundschutz-Kompendium INF.7.A6 SOLL , R 2	• regeln, dass an unbeaufsichtigten Arbeitsplätzen sensible Informationen und IT-Systeme nicht frei zugänglich sein dürfen • Einhaltung der Regelung anlassbezogen prüfen
Übersicht der vorhandenen Dokumentation, Regelungen zur Erstellung	SDM (Bausteine wie angegeben)	• Strukturierung der Gesamtdokumentation (M42.P01) • Aufbewahrungsorte und -medien festlegen

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
2 Standard-Datenschutzmodell vom 24. November 2022 (Version 3.0)
3 IT-Grundschutz-Kompendium Edition 2023

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
Änderung und Aufbewahrung von Dokumentationen		(M42.P06) • Festlegung zur Form der Dokumentation (Papier/Datei/Datenbank) (M42.P02) • Regelung zum Vertraulichkeitsgrad und zu Zugriffsrechten treffen (M42.P05) • Aktualisierungs- und Fortschreibungsregeln festlegen (M42.P04)
	BSI Standard 200-2 Abschnitt 5.2.3 Anforderungen an die Dokumentationen (Mindestanforderung an die Kennzeichnung der Dokumente zum Sicherheitsmanagement)	• Mindestangaben zur Beschreibung der Dokumente (Metadaten) festlegen
I b Geschäftsprozessdarstellungen		
Prozesslandkarte	Voraussetzung für Geschäftsprozessdarstellung Voraussetzung für Qualitätsmanagement	• Hauptprozesse in ihrer Wirkung als Managementprozesse, Wertschöpfungsprozesse und Supportprozesse grafisch beschreiben
Prozessdarstellungen	IT-Grundschutz-Kompendium	• Sicherheitsprozess ISMS.1.A13, SOLL, R 1 • Prozess zur Beseitigung von Restinformationen vor Weitergabe CON.9.A5 , SOLL , R 2 • Patch- und Änderungsmanagement, OPS.1.1.3.A1, MUSS, R 1 i.V.m. OPS.1.1.3.A11, SOLL, R 1 • Identitäts- und Berechtigungsmanagement, ORP.4.A15, SOLL, R 1; ORP.5.A4, SOLL, R 3 • Compliancemanagement, ORP.5.A4, MUSS, R 3 • Prozesse zur Behandlung von Sicherheitsvorfällen, DER.2.1.A7, SOLL • Prozesse zur Meldung, Eskalation und Alarmierung bei Notfällen, Anforderungskatalog zu BSI 200-4 Nr. 5.2.3
	Art. 12 Abs. 1 DS-GVO Art. 33 Abs. 1 DS-GVO	• Implementierung und Dokumentation von Prozessen zur Sicherstellung von Informationspflichten (insbes. Art. 13 – 19 DS-GVO) • Implementierung und Dokumentation eines Prozesses zur Sicherstellung der Meldepflicht aus Art. 33 DS-GVO
	SDM M42.P33	• Dokumentation der Prozesse und ggf. Querverweise in M42.P20 (Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO)
	Nr. 5.1.1 VerfRi-IT-HKR	• Prozess für die Verwaltungen von Berechtigungen (Einrichten, Verändern, Entzug gem. Ord-

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
		nungsmäßigkeitskonzept) • Berechtigungen dürfen nur eingerichtet werden, soweit dies zur Aufgabenerfüllung zwingend erforderlich ist (Prinzip der minimalen Berechtigung) • zu jedem Zeitpunkt muss festgestellt werden können, welche Person zu welchem Zeitpunkt mit welcher Berechtigung ausgestattet gewesen ist/war
I c Anforderungen der DS-GVO		
Datenschutzleitlinie und -konzept	Art. 5 Abs. 2 , Art. 24 Abs. 1 DS-GVO	• Erklärung der Behördenleitung zum Stellenwert des Datenschutzes und zum Umgang mit personenbezogenen Daten • Schutz- und Sicherheitsziele definieren • Rechtsgrundlagen aufführen • Begriffe definieren • Verantwortlichkeiten benennen • kontinuierliche Verbesserung regeln
Dienstanweisung Datenschutz	Art. 5 Abs. 2, Art. 24 Abs. 1 DS-GVO	• organisatorische Maßnahmen des Datenschutzes verbindlich festlegen (soweit nicht in Basisregeln geregelt) • Umgang mit Melde-, Informations- und Auskunftspflichten nach DS-GVO regeln • Verantwortlichkeiten festlegen • festlegen, wie mit Verstößen umgegangen wird
	Eg. 39 DS-GVO, SDM M42.P21	• Dokumentation der Umsetzung der Betroffenenrechte gemäß Erwägungsgrund 39 DS-GVO
	SDM M42.P11	• Dienst-/Betriebsanweisungen und -vereinbarungen
Verzeichnis der Verarbeitungstätigkeiten	SDM M42.P09, M42.P20 i.V.m. Art. 30 DS-GVO	• Dokumentation der Bestellung des/der Datenschutzbeauftragten • fortlaufende Darstellung der Beschreibung der jeweiligen Verarbeitungstätigkeit im Verzeichnis der Verarbeitungstätigkeiten
	SDM M41.D01	• Spezifikation der Daten, die verarbeitet werden
Rahmen-Datenschutzkonzept	SDM M42.P12	• übergreifende Schutzmaßnahmen darstellen • Verantwortliche und Ansprechpartner benennen • Handbücher, übergreifende Schutzmaßnahmen, Verantwortliche und Ansprechpartner
Protokollierungskonzept	SDM M42.P32 SDM M41.S04	• regeln, welche Protokolle genutzt und was protokolliert werden soll • Aufbewahrungsorte, -Aufbewahrungsfristen und Zugriffsregelungen festlegen
Darstellung der IT-Infrastruktur	SDM M42.P15 SDM M41.D01	• IT-Konzept: Darstellung aller in die Verarbeitung personenbezogener Daten involvierter Systeme • Spezifikation der Daten, die von der Verarbei-

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
	SDM M41.S05	tungstätigkeit verarbeitet werden • Spezifikation der IT-Infrastruktur und IT-Systeme in Bezug auf Erfüllung des Zwecks und der technischen und organisatorischen Maßnahmen
Dokumentieren	SDM M42.P31	• Dokumentation von Sicherheitsvorfällen gemäß Art. 33 Abs. 2 DS-GVO
	SDM M42.P03	• Festlegungen für ein in Notfällen verfügbares und aktuelles Backup der Dokumentation
Planen und Spezifizieren	SDM M41.P01	• Durchführen einer Risikoanalyse, die der Durchführung einer Datenschutz-Folgenabschätzung (DSFA) vorausgeht („Schwellwertanalyse“)
	SDM M41.P25	• Durchführen einer DSFA, wenn sich aus M41.P01 Notwendigkeit ergibt
Trennen	SDM M50.P10	• Dokumentation von Restrisiken
Aufbewahren	SDM M11.D06	• Einhaltung der Vorkehrungen der eIDAS-Verordnung sowie des Vertrauensdienstegesetzes zur Sicherung der Authentizität und des Beweiswertes von Daten
Berichtigen	SDM M61.P01	• Berichtigungskonzept
Einschränken der Verarbeitung	SDM M62.P01	• Konzept zur Einschränkung der Verarbeitung
	SDM M42.P26	• Dokumentation der eingeholten Einwilligungen gemäß Art. 7 Abs. 1 DS-GVO
	SDM M42.P30	• Dokumentation für Ausnahmen für bestimmte Fälle von Übermittlungen gemäß Art. 49 Abs. 6 DS-GVO
I d Anforderungen aus dem IT-Grundschutz-Kompendium des BSI		
Baustein ISM Informationssicherheitsmanagement		
Leitlinie zur Informationssicherheit	ISMS.1.A3, MUSS, R 1	• Stellenwert der Informationssicherheit, die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit beschreiben • Verantwortung der Behördenleitung festschreiben • Stellenwert der Informationssicherheit und Bedeutung der wesentlichen Informationen, Geschäftsprozesse und IT für Institution darstellen • Geltungsbereich festlegen • Sicherheitsziele und Bezug zu den Geschäftszielen und Aufgaben der Institution darstellen • Kernelemente der Sicherheitsstrategie benennen

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
		• Leitaussagen zur Erfolgskontrolle treffen • Organisationsstruktur zur Umsetzung des Sicherheitsprozesses beschreiben • Sicherheitsleitlinie regelmäßig aktualisieren
Basis- bzw. Rahmensicherheitskonzept (zentrale Infrastruktur und Dienste)	ISMS1.A7, MUSS, R 1	• alle Sicherheitsmaßnahmen systematisch im Sicherheitskonzept dokumentieren • Sicherheitsmaßnahmen festlegen und konkret beschreiben • Dringlichkeit und Zeitplan der Umsetzung der Sicherheitsmaßnahmen festlegen • festgelegte Sicherheitsmaßnahmen systematisch dokumentieren
Regelungen zu Dokumentationen im Sicherheitsprozess	ISMS.1.A.13, SOLL, R 1	• Vorgehensweise für Erstellung und Archivierung von Dokumentationen im Rahmen des Sicherheitsprozesses regeln • Sicherstellung von Aktualität und Vertraulichkeit der Dokumentationen regeln • zentrale Archivierung aller Vorgängerversionen sicherstellen
Baustein ORP Organisation und Personal		
Berechtigungskonzept	ORP.4.A3, MUSS, R 1	• zugelassene Kennungen für Benutzende, angelegte Gruppen für Benutzende und Rechteprofile dokumentieren • Zugriffsrechte auf die Dokumentation festlegen und kontrollieren • anlassbezogen Aktualität prüfen • Dokumentation in Backup aufnehmen
Authentisierungskonzept	ORP.4.A12, SOLL, R 1	• für jedes IT-System und jede Anwendung definieren, welche Funktions- und Sicherheitsanforderungen an die Authentisierung gestellt werden • festlegen, dass Authentisierungsinformationen kryptografisch geschützt übertragen und gespeichert werden
Regelungen zum Umgang mit Passwörtern (Passwortrichtlinie)	ORP.4.A8, MUSS, R 1 ORP.4.A11, SOLL, R 1	• Passwortgebrauch verbindlich vorschreiben (ein Passwort pro System oder Anbindung an zentralen Verzeichnisdienst) • Anforderungen zu Länge und Komplexität (Passwortqualität) sowie zum Wechsel von Passwörtern festlegen • Regelungen zum Zurücksetzen von Passwörtern erlassen
Richtlinie für die Zugriffs- und Zugangskontrolle von IT-Systemen, IT-Komponenten und Netzen	ORP.4.A16, SOLL, R 1	• eingerichtete Benutzende und vergebene Rechte dokumentieren • regeln, dass Benutzende nur auf IT-Systeme und Dienste zugreifen können, wenn sie vorher angemessen identifiziert und authentisiert wurden • Standard-Rechteprofile vorgeben, die den

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
		Funktionen und Aufgaben der Mitarbeiter entsprechen • schriftliche Zugriffsregelungen für jedes IT-System und jede IT-Anwendung
Sensibilisierung- und Schulung zur Informationssicherheit	ORP.3.A4, SOLL, R 1	• zielgruppenorientierte Informationen und Fähigkeiten vermitteln, die erforderlich sind, um in der Institution geltende Sicherheitsregelungen und -maßnahmen umsetzen zu können
Betriebsmittel- und Geräteverwaltung	ORP.1.A8, SOLL, R 1	• Geräte und Betriebsmittel in ausreichender Menge vorhalten • geeignete Prüf- und Genehmigungsverfahren vor Einsatz der Geräte und Betriebsmittel • Inventarisierung (Bestandsverzeichnisse führen)
Dokumentation der rechtlichen Rahmenbedingungen	ORP.5.A1, MUSS, R 3	• rechtliche Rahmenbedingungen mit Auswirkungen auf das Sicherheitsmanagement identifizieren • strukturierte Übersicht der für die einzelnen Bereiche relevanten gesetzlichen und vertraglichen Vorgaben (SOLL)
	BSI 200-1, S. 43	• Strukturanalyse zur Identifikation von Schutzobjekten
Baustein CON Konzepte und Vorgehensweisen		
Datensicherungskonzept	CON.3.A1 Erhebung der Einflussfaktoren für Datensicherungen MUSS, R 1	• Der IT-Betrieb MUSS mindestens die nachfolgenden Rahmenbedingungen berücksichtigen: • zu sichernde Daten • Speichervolumen • Änderungsvolumen • Änderungszeitpunkte • Verfügbarkeitsanforderungen • Integritätsbedarf sowie • rechtliche Anforderungen • nachvollziehbare Ergebnis- und Anforderungsdokumentation
	SDM M11.P07 Sicherungs- und Rücksicherungs-Strategien	
	CON.3.A4 Erstellung von Datensicherungsplänen CON.3.A6 Datensicherungskonzept SOLL, R 1	Dokumentation erforderlich • zu sichernde und beteiligte Systeme • Verfahrensweise für Datensicherung und Wiederherstellungstests festlegen • Verantwortlichkeiten festlegen
Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen	CON.6.A1, MUSS, R 1 als Richtlinie für die Löschung und Vernichtung von Informationen CON.6.A8, SOLL, R 1	• regeln, welche Informationen und Betriebsmittel unter welchen Voraussetzungen gelöscht und entsorgt werden dürfen (MUSS) • festlegen, in welchen räumlichen Bereichen Entsorgungs- und Vernichtungseinrichtungen aufgebaut werden sollen (MUSS) • Verantwortlichkeiten festlegen (MUSS) • Informationsfluss mit Outsourcing-Dienstleistern regeln (MUSS)
	SDM M11.P09 Prozess zur automatisierten Löschung	
	SDM M60.P03	

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
	Löschkonzept	• geeignete Verfahren nach dem Stand der Technik auswählen CON.6.A4, SOLL, R 1 • Außerbetriebnahme von IT-Systemen und Datenträgern regeln CON.6.A5, SOLL, R 1
Baustein OPS Betrieb		
Archivierungskonzept	OPS.1.2.2.A2, MUSS, R 3	• Ziele der Archivierung definieren • Verantwortlichkeiten sowie Funktions- und Leistungsumfang festlegen
Dienstanweisung IT-Administration	OPS.1.1.2.A7, SOLL, R 1	• Befugnisse, Aufgaben und Pflichten der IT-Administratoren festschreiben • Aufgabenverteilung festlegen, insbesondere auch Abgrenzung zwischen Fach- und Systemadministration vornehmen • Vertretungen in der Notfallplanung berücksichtigen
Konzept für den Schutz vor Schadprogrammen	OPS.1.1.4.A1, MUSS, R 1	• darstellen, welche IT-Systeme vor Schadprogrammen geschützt werden müssen • darstellen, wie Schutz zu erfolgen hat
Konzept für das Patch- und Änderungsmanagement	OPS.1.1.3.A1, MUSS, R 1	• Verantwortlichkeiten und Vorgehensweise (Planung, Test, Genehmigung, Dokumentation, Rückfall-Lösungen) festlegen • Umgang mit Update-Mechanismen regeln • Prüfung von Softwarepaketen auf Integrität und Authentizität anordnen • Änderungsmanagementprozess festlegen • Anforderungen und Rahmenbedingungen für Werkzeugauswahl einschließlich Sicherheitsrichtlinien festlegen • Umgang mit Änderungsanforderungen unter Beteiligung des ISB regeln
Outsourcing-Strategie	OPS.2.3.A8, SOLL, R 2	• wirtschaftliche, rechtliche, technische, organisatorische und sicherheitsrelevante Rahmenbedingungen definieren • Ziele, Chancen und Risiken des Outsourcing beschreiben • Geschäftsprozesse, Aufgaben oder Anwendungen festlegen, die für Outsourcing in Frage kommen • notwendige Fähigkeiten, Kompetenzen und Ressourcen eines Outsourcing-Dienstleisters definieren • notwendige eigene Fähigkeiten, Kompetenzen und Ressourcen definieren, die vorgehalten werden müssen
Festlegung von Sicherheitsanforderungen und Erstellung eines Sicherheitskonzeptes für das	OPS.2.3.A6, SOLL, R 2	• Sicherheitsanforderungen festlegen • Prüfung der Sicherheitskonzepte der Outsourcing-Partner auf Konsistenz und Aktualität sowie Kontrollen der Sicherheitsmaßnahmen fest-

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
Outsourcing-Vorhaben		legen • Durchführung regelmäßiger Übungen und Tests zur Aufrechterhaltung des Sicherheitsniveaus festlegen • Informationsfluss bei Sicherheitsvorfällen regeln
Regelungen für den Einsatz des Personals des Outsourcing-Dienstleisters	OPS.2.3.A17, SOLL, R 2	• Mitarbeiter des Outsourcing-Dienstleisters schriftlich auf Einhaltung der einschlägigen Gesetze, Vorschriften und der beim Outsourcing-Kunden gültigen Regelungen verpflichten • Einweisung in die Aufgaben regeln • Regelungen für den einmaligen bzw. kurzfristigen Einsatz von Mitarbeitern des Outsourcing-Dienstleisters erlassen (Aufsicht, Zugangsbeschränkungen usw.) • Vertretungen regeln
Vereinbarung über Anbindung an Netze der Outsourcing-Partner	OPS.2.3.A15, SOLL, R 2	• sicherheitsrelevante Aspekte regeln, z. B. Zugriffsrechte auf Bereiche und Dienste • Ansprechpartner für organisatorische und technische Fragen der Netzanbindung benennen • Sicherheitsniveau festlegen und vor Aktivierung der Netzwerkverbindung prüfen • Informationspflichten und Eskalationsschritte bei Sicherheitsproblemen regeln
Berücksichtigung von Outsourcing im Notfallkonzept	OPS.2.3.A20, SOLL, R 2	• Ansprechpartner für organisatorische und technische Probleme sowie sicherheitsrelevante Ereignisse benennen • Verfügbarkeiten und Reaktionszeiten vereinbaren • standardisierte Protokolle und Berichte zur Meldung von Sicherheitsvorfällen etablieren
Baustein OPS.2.2 Cloud-Nutzung		
Cloud-Nutzungs-Strategie erstellen	OPS.2.2.A1, MUSS, R 2	• Cloud-Nutzungs-Strategie erstellen • Ziele, Chancen und Risiken definieren • rechtliche und organisatorische Rahmenbedingungen sowie technische Anforderungen untersuchen • Machbarkeitsstudie für die Nutzung von Cloud-Diensten erstellen • festlegen des Bereitstellungsmodells für zukünftig vom Cloud-Dienstanbieter bereitgestellten Dienste • bereits während Planungsphase TOM‘s zu Sicherheitsaspekten berücksichtigen
	OPS.2.2.A1, SOLL, R 2	• grobe individuelle Sicherheitsanalyse durchführen • Wiederholung, wenn sich die Rahmenbedingungen für die technischen und organisatorischen Maßnahmen ändern • Roadmap zur Einführung von Cloud-Diensten

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
		planen
Sicherheitsrichtlinie für die Cloud-Nutzung	OPS.2.2.A2, MUSS, R 2	• Sicherheitsrichtlinie für die Cloud-Nutzung auf Basis der Cloud-Nutzungs-Strategie • konkrete Sicherheitsvorgaben zur Umsetzung der Cloud-Dienste • Definition der Sicherheitsanforderungen an den Cloud-Dienstanbieter • festgelegtes Schutzniveau für Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentieren • Berücksichtigung der länderspezifischen Anforderungen und gesetzlichen Bestimmungen bei Nutzung von internationalen Dienstanbietern
Service-Definition für Cloud-Dienste durch den Anwender	OPS.2.2.A3, MUSS, R 2	• erarbeiten einer Service-Definition für jeden Cloud-Dienst
	OPS.2.2.A3, SOLL, R 2	• Dokumentation aller geplanten und benutzten Cloud-Dienste
Planung der sicheren Migration zu einem Cloud-Dienst	OPS.2.2.A5, SOLL, R 2	• Erstellung eines Migrationskonzepts • Festlegung von organisatorischen Regelungen und Aufgabenverteilungen • Identifikation und Anpassung bestehender Betriebsprozesse für die Cloud-Nutzung • Berücksichtigung der eigenen IT im Migrationsprozess • Schulungsbedarfe der Mitarbeiter durch Migrationsverantwortliche ermitteln lassen
Sicherheitskonzept für die Cloud-Nutzung	OPS.2.2.A7, SOLL, R 2	• Sicherheitskonzept für die Nutzung von Cloud-Diensten auf Basis der identifizierten Sicherheitsanforderungen aus OPS.2.2.A2 erstellen
Sorgfältige Auswahl eines Cloud-Dienstanbieters	OPS.2.2.A8, SOLL, R 2	• Detailliertes Anforderungsprofil für einen Cloud-Dienstanbieter erstellen • Leistungsbeschreibung und Lastenheft erstellen • Service-Beschreibungen des Cloud-Dienstanbieters sorgfältig prüfen und hinterfragen
Vertragsgestaltung mit dem Cloud-Dienstanbieter	OPS.2.2.A9, SOLL, R 2	• vertragliche Regelungen sollen in Art, Umfang und Detaillierungsgrad dem Schutzbedarf der Informationen angepasst sein, die im Zusammenhang mit der Cloud-Nutzung stehen • schriftliche Fixierung der Kündigungsregelungen
Sichere Migration zu einem Cloud-Dienst	OPS.2.2.A10, SOLL, R 2	• Migration zu einem Cloud-Dienst auf Basis des Migrationskonzepts aus OPS.2.2.A5 • Prüfung des Sicherheitskonzepts für die Cloud-Nutzung (OPS.2.2.A7) auf etwaige Anpassungsbedarfe
Notfallkonzept für einen Cloud-Dienst	OPS.2.2.A11, SOLL, R 2	• Notfallkonzept erstellen

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb	OPS.2.2.A12, SOLL, R 2	• Regelmäßige Aktualisierung der für die Cloud-Dienste erstellten Dokumentationen und Richtlinien • Monitoring der zu erbringenden Leistung
Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses	OPS.2.2.A14, SOLL, R 2	• Vertrag mit dem Cloud-Dienstanbieter soll geordnete Auflösung des Dienstverhältnisses vorsehen
Anforderungen bei erhöhtem Schutzbedarf		
Durchführung eigener Datensicherungen	OPS.2.2.A16, SOLL, R 2, (IA)	• Anforderungen an Backup-Service detailliert beschreiben
Einsatz von Verschlüsselung bei Cloud-Nutzung	OPS.2.2.A17, SOLL, R 2, (IA)	• bei Verschlüsselung von Daten durch einen Cloud-Dienstanbieter vertraglich regeln, welche Verschlüsselungsmechanismen und welche Schlüssellängen eingesetzt werden dürfen
Baustein OPS.1.2.4 Telearbeit		
Sicherheitskonzept für Telearbeit	OPS.1.2.4.A6, SOLL, R 3	• Sicherheitsziele, Schutzbedarf, Sicherheitsanforderungen sowie Risiken beschreiben • sicherheitstechnische Anforderungen an Telearbeitsrechner und Kommunikationsverbindung festlegen
Betreuungs- und Wartungskonzept Telearbeit	OPS.1.2.4.A9, SOLL, R 3	• Ansprechpartner für den IT-Service, Wartungstermine, Fernwartung, Transport der IT-Geräte und Einführung von Standard-Telearbeitsrechnern, Hard- und Software-Probleme benennen
Anforderungsanalyse für den Telearbeitsplatz	OPS.1.2.4.A10, SOLL, R 3	• Schutzbedarf der am Telearbeitsplatz verarbeiteten Informationen feststellen und dokumentieren • Bedarf an Hard- und Software-Komponenten bestimmen
Baustein DER Detektion und Reaktion		
Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen	DER.1.A1, MUSS, R 2	• nachvollziehbar Anforderungen und Vorgaben beschreiben, wie die Detektion von sicherheitsrelevanten Ereignissen sicher geplant, aufgebaut und betrieben werden kann • ISB nachweislich beteiligen • Revisionen planen und dokumentieren
Baustein APP Anwendungen		
Sicherheitsleitlinie für den Verzeichnisdienst	APP.2.1.A1, MUSS, R 2	• Regelungen des Verzeichnisdienstes in eigener Sicherheitsrichtlinie dokumentieren
Regelung für die	APP.6.A4, MUSS, R 2	• erstellen und dokumentieren einer an den Be-

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
Installation und Konfiguration von Software		darf der Institution angepassten Standardkonfiguration
Regelung der Software-Entwicklung mittels Office-Produkten durch Endbenutzende	APP.1.1.A10, SOLL, R 2	• Grundsatzentscheidung, ob Eigenentwicklungen erwünscht sind • Verfahren und Verantwortlichkeiten festlegen, Dokumentation vorschreiben, Test und Freigabe regeln
Baustein SYS IT-Systeme		
Richtlinien zum Umgang mit IoT-Komponenten	SYS.4.4.A6, SOLL, R 2	• verbindliche, verständliche, aktuelle und verfügbare Richtlinien • in den sicheren Umgang mit den jeweiligen Komponenten einweisen
I e Anforderungen beim Ersetzenden Scannen		
Verfahrensdokumentation einschließlich Verfahrensanweisung und Sicherheitskonzept beim ersetzenden Scannen	TR-RESISCAN[4] Anforderung A.G.1 MUSS	• Art der verarbeiteten Dokumente festlegen • Umgang mit nicht verarbeitbaren Dokumenten regeln • Verantwortlichkeiten, Abläufe und Aufgaben im Scan-Prozess festlegen • Anforderungen an die in den Scan-Prozess involvierten Räume, IT-Systeme, Anwendungen und Sicherungsmittel entsprechend festgelegten Schutzbedarfe beschreiben • Administration und Wartung der IT-Systeme und Anwendungen regeln • geeignete Sicherheitsmaßnahmen für IT-Systeme, Netze und Anwendungen festlegen
Dienstanweisung ersetzendes Scannen beim Einsatz von IT-Verfahren im Haushalts-, Kassen und Rechnungswesen	Nr. 6.4.3 GoBIT-HKR[5]-+	• Festlegen, wer nach dem Berechtigungskonzept scannen darf • Scan-Zeitpunkt festlegen • Festlegen, welche Unterlagen gescannt werden und welche Unterlagen nach dem Scannen nicht vernichtet werden dürfen • Qualitätskontrolle auf Lesbarkeit und Vollständigkeit regeln • Zuordnung der elektronischen Unterlage zu einem Geschäftsvorgang regeln • Fehlerprotokollierung regeln
Verfahrensdokumentation ersetzendes Scannen beim Einsatz von IT-Verfahren im Haushalts-, Kassen und Rechnungswesen	Nr. 6.4.3 GoBIT-HKR	• Verfahren zur Übertragung der Unterlagen in elektronische Form beschreiben
I f Anforderungen aus dem Notfallmanagement		

4 BSI Technische Richtlinie 03138 Ersetzendes Scannen (RESISCAN) Version 1.5 vom 21. November 2024
5 VV-LHO Anlage 6 zu VV zu §§ 70 bis 80 (Nr. 6.1.1.4) Stand 2. September 2021

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
Leitlinie BCMS	BSI 200-4 Nr. 4.8.1	• die Übernahme der Verantwortung durch die Institutionsleitung dokumentieren • Begriffe definieren, Stellenwert des BCM beschreiben • Geltungsbereich festlegen • zu beachtende Gesetze, Richtlinien und Vorschriften aufzählen • Kernpunkte der Notfallstrategie darstellen • Rahmen für die Konzeption, den Aufbau und die Aufrechterhaltung des Notfallmanagements festlegen • Ziele des Notfallmanagements beschreiben • Aufbauorganisation mit den wichtigsten Rollen und deren Zuständigkeiten darstellen
Notfallvorsorgekonzept	BSI 200-4, Nr. 4.4.1	• Kontinuitätsstrategien darstellen • Notfallszenarien und ihre Auswirkungen auf kritische Geschäftsprozesse beschreiben • Wiederanlaufanforderungen für die Geschäftsprozesse festlegen • organisatorische und konzeptuelle Aspekte sowie alle Maßnahmen und Tätigkeiten des Notfallmanagements, die nicht zur direkten Bewältigung eines Notfalls beitragen, beschreiben
	SDM M42.P19	
Notfallhandbuch	DER.4.A1 SOLL, R 3	• Informationen zu Rollen, Sofortmaßnahmen, Alarmierung und Eskalation sowie Kommunikations-, Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungsplänen • Zuständigkeiten und Befugnisse regeln
	BSI 200-4 Nr. 4.4.1	• benötigte Strukturen, Informationen sowie die erforderlichen Maßnahmen und Aktionen nach Eintritt eines Notfalls und zur Wiederaufnahme des Geschäfts zusammenfassen • Kommunikationsplan, Geschäftsfortführungspläne, Wiederanlaufpläne, Alarmierungspfade, Verhaltenskodex in Geschäftsordnung der Besonderen Aufbauorganisation dokumentieren
II Bereichs-/ Verfahrensspezifische Regelungen		
II a Vertragliche Regelungen		
Verträge mit *Dienstleistern)*	Bewirtschaftungserlass: Empfehlung EVB-IT Verträge zu nutzen	• Festlegen der Anforderungen in einem Lasten- und Pflichtenheft • Vertragsgegenstand beschreiben (Leistungsbeschreibung als Anlage zum Vertrag) • Vertragsbestandteile dokumentieren • Laufzeit und Kündigungsbedingungen sowie Pflichten nach Vertragsende regeln • Vergütung und Zahlungsbedingungen festlegen • Nutzungsrechte regeln

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
		• Haftungsregelungen treffen • zu beachtende Regelungen zur IT-Sicherheit und ggf. zum Geheimschutz festlegen (Anlagen zum Vertrag) • schriftliche Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO zum Vertragsbestandteil machen (Anlage zum Vertrag)
Leistungsbeschreibung, Service-Level-Agreement (Anlage zum Vertrag)		• detaillierte Leistungsbeschreibung • Ansprechpartner • Verfügbarkeiten der Services • Reaktions-/Wiederherstellungszeiten
schriftliche Vereinbarung zur Auftragsverarbeitung (Anlage zum Vertrag)	Art. 28 Abs. 3 DS-GVO Vertragsbestandteil EVB-IT Vertrag SDM M42.P23 – M42.P25 SDM M50.P15 – M50.P16	• Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festlegen • Art. 28 Abs. 3 lit. a) bis h) DS-GVO • Vereinbarungen zwischen Beteiligten an gemeinsam genutzter Informationstechnik gemäß Art. 26 DS-GVO treffen • Konzept der Verarbeitung aus der Planungsphase (u. a. Lasten- und Pflichtenheft)
schriftliche Regelung zur Informationssicherheit beim Outsourcing (Anlage zum Vertrag)	OPS.2.3.A4 MUSS, R 2	• Rechte und Pflichten der Vertragsparteien festlegen (Aspekte der Informationssicherheit, einen Zustimmungsvorbehalt bei Weiterverlagerung sowie ein Recht auf Prüfung, Revision und Audit) • Rollen und Mitwirkungspflichten zur Erstellung, Prüfung und Änderung des Sicherheitskonzeptes regeln • Geltung des Sicherheitskonzeptes vereinbaren
II b Allgemeine organisatorische Regelungen		
Dienst- und Arbeitsanweisungen (aufbau- und ablauforganisatorische Regelungen)	ISMS.1.A6 MUSS, R 1	• Aufgaben, Verantwortung und Kompetenzen im Sicherheitsmanagement durch Arbeitsanweisungen und organisatorische Regelungen nachvollziehbar dokumentieren • Arbeitsabläufe, organisatorische Vorgaben und technische Sicherheitsmaßnahmen so dokumentieren, dass Sicherheitsvorfälle durch Unkenntnis oder Fehlhandlungen vermieden werden • sicherheitsrelevante organisatorische Maßnahmen festlegen, die erforderlich sind, um technische Sicherheitsdefizite zu kompensieren
	Rechtsstaatsgebot, Compliance: Sicherung rechtskonformer, einheitlicher und per-	• detaillierte Weisungen des Arbeitgebers/ Dienstherrn an seine Arbeitnehmer/Beamte, wie eine bestimmte Arbeitsaufgabe an einem Arbeitsplatz zu verrichten ist (Ausführungsebene) • Verantwortlichkeiten festlegen (Durchführung,

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
	sonenunabhängiger Aufgabenwahrnehmung Korruptionsprävention Risikomanagement Wirtschaftlichkeitsgebot § 7 LHO: Effizienz des Verwaltungshandelns	Entscheidung, Mitwirkung, Information) • Risiken darstellen und Kontrollen festlegen • als Dienstanweisung oder sonstige schriftliche Weisung erlassen • verbindlich, einheitlich, fachlich geprüft
Handbücher, Anleitungen und Richtlinien	ISMS.1.A3	• Leitlinie zur Informationssicherheit • Beschäftigte zum verantwortungsvollen Umgang mit internen Informationen, für die sichere Nutzung von IT-Systemen und Anwendungen sowie zum Verhalten bei Sicherheitsvorfällen informieren und sensibilisieren • Handbücher und Anleitungen für die eingesetzten IT-Systeme und Anwendungen erarbeiten und/oder zur Verfügung stellen
	SDM M42.P17	• Sicherheitsrichtlinie
Darstellung der durch das IT-Verfahren unterstützten Fachprozesse	Art. 5 Abs. 2 DS-GVO Art. 24 Abs. 1 DS-GVO SDM M42.P34 – M42.P35	• Dokumentation der Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DS-GVO) in den Geschäftsprozessen, bei denen personenbezogene Daten verarbeitet werden • Nachweis, das Verarbeitung gemäß DS-GVO erfolgt • Darstellung aller in die Verarbeitung personenbezogener Daten involvierter Prozesse und deren funktionale Beschreibung (Sachbearbeitung und Administration)
	ISMS.1.A9, MUSS, R 1	• Integration von Informationssicherheit in alle Geschäftsprozesse • Zuweisung der Verantwortung für Geschäftsprozesse, Informationen, Anwendungen und IT-Systeme • Einbeziehung von Sicherheitsaspekten in alle Geschäftsprozesse • Überblick über geschäftskritische Informationen, Fachaufgaben und Geschäftsprozesse
	Risikomanagement	• zu den Prozessschritten gehörige Risiken und Kontrollen darstellen
II c Datenschutz		
Beschreibung des Verfahrens als Teil des Verzeichnisses der Verarbeitungs-	Art. 30 DS-GVO SDM M42.P20	• Angaben gemäß Art. 30 Abs. 1 lit. a bis g DS-GVO, insbesondere Angabe des Verantwortlichen, Verarbeitungszweck, Beschreibung

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
tätigkeiten		der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Löschfristen und Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DS-GVO
Dokumentation der verarbeiteten personenbezogenen Daten, Datenmodell	SDM M42.D01 und M42.S01	• detaillierte Beschreibung der Struktur und der Syntax der verarbeiteten Daten (Datenebene) • Angabe, wo Daten verarbeitet, ggf. gelöscht bzw. berichtigt werden (Systemebene)
II d Ergänzende Regelungen für IT-Management und Fachbereich		
Sicherheitskonzept	folgt aus Art. 24 Abs. 1 DS-GVO i. V. m. Eg. 74 S. 2 SDM M42.P18	• Dokumentation der durch den Verantwortlichen zu treffenden geeigneten technischen und organisatorischen Maßnahmen • Sicherstellung der Überprüfung • Nachweis DS-GVO-konformer Datenverarbeitung
	ISMS.1.A7, ISMS.1.A10 SOLL, R 1	• Sicherheitsmaßnahmen festlegen und konkret beschreiben • Dringlichkeit und Zeitplan der Umsetzung der Sicherheitsmaßnahmen festlegen • festgelegte Sicherheitsmaßnahmen systematisch dokumentieren
vorhabenbezogenes Sicherheitskonzept Outsourcing	OPS.2.3.A6, MUSS, R 2	• individuelles Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben • Zusammenführen mit Sicherheitskonzept des Outsourcing-Dienstleisters in einem Gesamtsicherheitskonzept
Rechte- und Rollenkonzept	SDM M42.P34-M42.P35	• Dokumentation der Sachbearbeitung sowie Administration und ggf. Querverweise in M42.P20 (Verzeichnis der Verarbeitungstätigkeiten)
	SDM M51.S04	• Zugriffsrechte auf der Basis eines Identitätsmanagements und sicherer Authentisierungsverfahren festlegen
Festlegung benötigter Sicherheitsfunktionen bei Entwicklung und Einsatz von Individualsoftware	APP.7.A3, MUSS, R 3	• notwendige Sicherheitsfunktionen bei der fachlichen Auswahl und der Integration in die IT-betrieblichen Infrastrukturen und Betriebsprozesse festlegen und dokumentieren
Erstellung eines Anforderungskatalogs für Software	APP.6.A2, SOLL, R 3	• alle relevanten Anforderungen dokumentieren (Fachkonzept, Lastenheft)
Ordnungsgemäße IT-Administration	OPS.1.1.2.A7, MUSS, R 1	• korrekte Nutzung und Administration der Anwendung einschließlich der Sicherheitsfunktionen beschreiben und schulen • Verantwortlichkeiten festlegen
	SDM M43.P03	• Aktivitäten der Systemadministration protokollieren

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
Regelung für die Installation und Konfiguration von Software	APP.6.A4, MUSS, R 2	• benötigte Anwendungsmodule, Installations-reihenfolge und sichere Konfiguration der An-wendungsmodule dokumentieren
Freigabeerklärung	OPS.1.1.6.A4, MUSS, R 1	• prüfen und bestätigen, ob Software gemäß den Anforderungen getestet wurde und dabei recht-liche und organisatorische Vorgaben eingehalt-en wurden • Freigabeerklärung dokumentieren
	Nr. 5.9.3 VerfRi-IT-HKR[6]	• IT-Verfahren fachlich und technisch prüfen und Gewährleistung der Datenintegrität bestätigen • nur dokumentierte und nach einem erfolgrei-chen Testverfahren durch eine bevollmächtigte Person freigegebene Software einsetzen
Geregelte Außerbetrieb-nahme von Software	APP.6.A12, SOLL, R 2	• Planung der Außerbetriebnahme • Migrationsszenarien, Datensicherung, sichere Löschung
II e Zusätzliche kassenrechtliche Anforderungen		
Nachweis der Unterlagen gemäß Nr. 6. VV zu §§ 70 bis 80 LHO und 7.2 i. V. m. 7.4 VerfRi-IT-HKR Verwendung Musterunterlagen in Verf-IT-HKR empfohlen		
Verfahrensdokumentation	Nr. 7.4.1	• übersichtlich gegliedert • vollständige und schlüssige Beschreibung von Inhalt, Aufbau, Ablauf und Ergebnissen beim Einsatz des IT-Verfahrens • verständliche Beschreibung, so dass Verfahren für einen sachverständigen Dritten in angemes-sener Zeit nachprüfbar ist • Dokumentation, wie elektronische Belege er-fasst, empfangen, verarbeitet, ausgegeben und aufbewahrt werden (Nr. 4 GoBIT-HKR) • Prozessbeschreibung • Versionierung und Änderungshistorie
Gefährdungsanalyse	Nr. 7.4.2	• Risiken, Sicherheitsmaßnahmen zur Risikoverringerung, verbleibende Eintrittswahr-scheinlichkeit und potenzielle Schadenshöhe beschreiben • Verzicht auf weitergehende Schutzmaßnahmen erläutern
Ordnungsmäßigkeitskon-zept	Nr. 7.4.3	• Abgrenzung der Verantwortlichkeiten und Fest-legung von Befugnissen (Berechtigungskon-zept) • Vier-Augen-Prinzip • Regelung der Anwendung vollautomatisierter Verfahrensabläufe (Dunkelverarbeitung) • zusätzliche Prüfverfahren oder Sicherheitsmaß-

6 VerfRi-IT-HKR (Stand Mai 2017) - Verfahrensrichtlinie zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen im Land Mecklenburg-Vorpommern

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
		nahmen
Prüfliste zur Einhaltung der kassenrechtlichen Vorschriften	Nr. 7.4.4	• detaillierte Erklärung darüber, ob und inwieweit kassenrechtliche Vorschriften eingehalten werden
Gewährung der Richtigkeit und Vollständigkeit der erfassten und verarbeiteten Daten Nr. 5 VerfRi-IT-HKR		
Dokumentation der Verantwortungsbereiche	Nr. 5.1.2	• Dokumentation der Übertragung der im Ordnungsmäßigkeitskonzept festgelegten Verantwortungsbereiche und Zugriffsberechtigungen durch BfH
Bescheinigung der Verantwortungsbereiche	Nr. 5.1.3	• schriftliche oder elektronische Dokumentation der ordnungsgemäßen Wahrnehmung der Verantwortungsbereiche gemäß Ordnungsmäßigkeitskonzept
Wartungsvertrag	Nr. 5.9.4	• sicherstellen, dass Programmfehler oder Sicherheitslücken in angemessener Zeit beseitigt werden
Nachweis Programmidentität	Nr. 5.10	• kontrollieren, ob das eingesetzte IT-Verfahren dem dokumentierten und genehmigten Verfahren entspricht, systematische und manuelle Kontrolle (IKS – Internes Kontroll System)
Zu erbringende Nachweise gemäß VerfRi-IT-HKR		
Testbescheinigungen	Nr. 6.4.1	• Bescheinigung des LZK über den Batch-Input-Test • Bescheinigung des Finanzministeriums über den Test der Schnittstelle zwischen Fachverfahren und CBPay
Nachweis der Änderung genehmigter IT-Verfahren	Nr. 7.3, 10.2	• Änderungen beschreiben und mit der Änderung verbundene Risiken benennen und analysieren
Vorgeschriebene Anlagen zu den Verfahren gemäß VerfR-IT-HKR		
Einwilligung	Nr. 8.1 i.V.m. Nr. 8.3	• Antrag auf Einwilligung
Erhebungsbogen IT-Verfahren	Nr. 10.3 Anlage 5	• jährliche Berichtspflicht bis zum 30. März jeden Jahres
II f Risikomanagement		
Risikobewertung	EG 76, Art. 24, 32 DS-GVO SDM M42.P28-M42.P29	• Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten abschätzen, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht • Bericht zur Datenschutz-Folgeabschätzung und

Dokumentations-anforderungen	Grundlage	Beschreibung/ Anforderungen
		Nachweis der Wirksamkeit der ergriffenen Schutzmaßnahmen
Risikoanalyse	BSI-Standard 200-3	• Zielobjekte feststellen, für die über den IT-Grundschutz hinaus Handlungsbedarf besteht • Risiken identifizieren, einschätzen, bewerten und behandeln • Sicherheitsmaßnahmen zur Risikoreduktion ermitteln • Maßnahmen in das Sicherheitskonzept integrieren

Legende

	übergreifend
	Datenschutz
	Informationssicherheitsmanagement
	Haushaltsrecht

Die dargestellten Anforderungen aus dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (Informationssicherheitsmanagement) umfassen die Basis- und Standardanforderungen. Erhöhte Anforderungen können zusätzliche Dokumentationen erforderlich machen. Aufgeführt sind die Anforderungen aus den einzelnen Bausteinen. Zusätzlich sind Angaben zu den notwendigen Inhalten der Dokumente aufgeführt.

R 1	Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.
R 2	Diese Bausteine sollten als nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbundes für nachhaltige Sicherheit erforderlich sind.
R 3	Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden, es wird aber empfohlen, diese erst nach den anderen Bausteinen zu betrachten.

Anlage 3 – Grundsätze für die Dokumentation – wie ist zu dokumentieren?

Grundsatz der Angemessenheit und Wirtschaftlichkeit

Dokumentationen müssen die bestehenden rechtlichen Anforderungen erfüllen. Ein Übermaß an Dokumentation sollte vermieden werden. Der Umfang der Dokumentation wird durch die Sicherheitsziele, die identifizierten Schutzbedarfe und die Risikobewertungen bestimmt.

Die Erstellung und Fortschreibung der Dokumentation sollte durch den Einsatz von IT-Verfahren unterstützt werden.

Alle Maßnahmen, Strukturen und Prozesse, die Regelkonformität sicherstellen sollen, sollten in einem IT-unterstützten Compliance-Management-System verwaltet und gesteuert werden.

Grundsatz der Vollständigkeit und Aktualität

Alle Verarbeitungsprozesse sind zu dokumentieren. Sie sind mit allen rechtlichen Forderungen und allen Informationen, Daten, Systemen und Prozessen zu erfassen. Der Betrieb in einer Organisation ist hinreichend genau und den tatsächlichen Gegebenheiten entsprechend zu beschreiben. Alle Maßnahmen sind entsprechend dem festgestellten Schutzbedarf mit ihrem Erfüllungsgrad darzustellen.

Im Rahmen des Änderungsmanagements muss durch definierte Prozesse sichergestellt werden, dass fachliche, technische oder organisatorische Änderungen zu einer Überarbeitung der Dokumentation führen.

Sofern auf Zertifikate eines Dienstleisters verwiesen wird[1], hat der Verfahrensbetreiber zu prüfen, inwieweit das Zertifikat für den jeweiligen Informationsverbund rele-

1 z. B. eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz.

vant ist und diesen tatsächlich sowie vollumfänglich abdeckt. Etwaige Auflagen aus dem Zertifizierungsverfahren sind vorab durch geeignete und ausreichende Maßnahmen des Dienstleisters zu erfüllen und durch Dokumentation nachzuweisen, damit die Schutzziele der Landesverwaltung gewährleistet werden.

Grundsatz der Transparenz und Übersichtlichkeit

Die Dokumentation soll vollständig und strukturiert sein. Der Bestand an Einzeldokumenten sollte übersichtlich dargestellt sein. Der Kontext, in dem die jeweiligen Dokumente stehen und die Beziehungen der Dokumente untereinander sollten klar erkennbar sein. Es sollte eine Rahmendokumentation mit Übersichten und Beschreibungen des Aufbaus der Dokumentation sowie der verwendeten Aufbewahrungs- bzw. Speicherorte erstellt werden. Die vorhandenen Dokumente können in einem Dokumentenmodell dargestellt werden. Mit einer Dokumentationsrichtlinie sollte ein einheitlicher Dokumentenstandard festgeschrieben werden.

Dokumente sollten so beschrieben sein, dass sie im Bedarfsfall schnell gefunden und zugeordnet werden können.

Sie sollten mit mindestens folgenden Angaben beschrieben werden:

- eindeutige Bezeichnung (aussagekräftiger Titel),
- Ersteller/Autor/Dokumenteninhaber einschließlich ihrer Funktion,
- Versionsnummer,
- letzte Überarbeitung, nächste geplante Überarbeitung,
- freigegeben am/durch,
- Vertraulichkeitsgrad und berechtigte Rollen (Verteilerkreis),
- Änderungsübersicht bzw. -historie,

- Angaben zur letzten Überprüfung (Datum, Prüfer, Ergebnis) und
- Aufbewahrungszeitraum.

Grundsatz der Revisionsfestigkeit

Dokumentationen müssen revisionssicher sein. Sie müssen nach den gesetzlichen und verwaltungsinternen Vorschriften ordnungsgemäß aufbewahrt werden. Der aktuelle Stand der Dokumentation muss jederzeit nachgewiesen werden können. Nur berechtigte Personen dürfen Dokumente einsehen oder Änderungen vornehmen. Die Änderungen sind zu dokumentieren. Hierzu sollten Versionierungsregeln erlassen werden.

Die Dokumentation muss in einer angemessenen Zeit und für eine sachverständige (dritte) Person prüffähig zur Verfügung gestellt werden können.

Bei einem hohen Schutzbedarf ist ein geeigneter und angemessener Manipulationsschutz der Dokumentation erforderlich. Dies verlangt entweder eine Signatur der Dokumentation oder den Betrieb eines Dokumentationssystems, dessen Zugriff mit einem dokumentationsspezifischen Rechte- und Rollenkonzept geregelt ist.

Anlage 4 – Anforderungen an die Beschaffung von Leistungen und Dienstleistungen

1 Nachweis der Notwendigkeit (§§ 6, 34 LHO)

Gemäß § 6 LHO sind bei der Aufstellung und Ausführung des Haushaltsplans nur Ausgaben und Verpflichtungsermächtigungen zu berücksichtigen, die zur Erfüllung der Aufgaben des Landes notwendig sind.

Der Nachweis der Notwendigkeit ist bereits vor Abschluss eines Vertrages zu erbringen.

2 Anforderungsmanagement

Die Behörden haben vor dem Abschluss von Verträgen die Anforderungen systematisch herzuleiten und auf deren Basis die notwendigen Leistungen zu bestimmen.

Ohne eine dokumentierte Bedarfsfeststellung sowie eine Bedarfsbegründung lassen sich Anforderungen für ein Pflichtenheft nicht ableiten.

Zu den Anforderungen gehören insbesondere:

- Anforderungen aus allgemeinen rechtlichen Regelungen (z. B. Datenschutz, Informationssicherheit, IT-Compliance),
- zu berücksichtigende Standards (z. B. IT-Planungsrat, landesspezifische Standards),
- fachrechtliche Vorgaben,
- Anforderungen aus der Aufgabenerfüllung (Aufbau- und Ablauforganisation, Geschäftsprozesse) und
- sonstige unbedingt notwendige funktionale und nicht funktionale Anforderungen.

3 Nachweis der Wirtschaftlichkeit

Bei der Aufstellung sowie bei der Ausführung des Haushaltsplans sind gemäß § 7 Abs. 1 LHO die Grundsätze der Wirtschaftlichkeit und Sparsamkeit zu beachten. Die Umsetzung wird in den Verwaltungsvorschriften zu § 7 LHO konkretisiert und ist bei allen Maßnahmen des Landes, die die Einnahmen und Ausgaben des Landeshaushalts unmittelbar oder mittelbar beeinflussen, zu beachten.[1]

Aufwand und Umfang der Wirtschaftlichkeitsbetrachtungen sind an den Erfordernissen des Einzelfalls auszurichten.

Wirtschaftlichkeitsbetrachtungen sind durch die Organisationseinheit zu erstellen, die mit der Durchführung der Maßnahme befasst ist.

Sie sind nicht nur in der Planungsphase, sondern auch während und nach der Durchführung einer Maßnahme durchzuführen.[2] Dabei ist festzustellen, ob und in welchem Umfang die Maßnahme ursächlich für die Zielerreichung war. Die Beauftragten für den Haushalt entscheiden, welche Untersuchungen ihnen vorzulegen sind.[3]

In der Planungsphase muss die Wirtschaftlichkeitsuntersuchung Aussagen zu den in VV Nr. 2.1 aufgeführten Teilaspekten enthalten, wenn die dort angegebenen Werte zum Mittelbedarf erreicht werden.

In der Wirtschaftlichkeitsbetrachtung sind auch Ausgaben bzw. Kosten zu berücksichtigen die entstehen, wenn der rechtmäßige Betrieb einer Hard- oder Software nur durch zusätzliche technische oder organisatorische Maßnahmen sichergestellt werden kann.

1 VV Nr. 1 zu § 7 LHO.
2 Ebenda.
3 VV Nr 2.4 zu § 7 LHO.

Bei größeren Beschaffungen und größeren Entwicklungsvorhaben i. S. v. § 24 LHO sind die Planungsunterlagen gemäß VV Nr. 2 zu § 24 LHO zu erstellen. Ausgaben und Verpflichtungsermächtigungen sind gemäß § 24 Abs. 3 LHO gesetzlich gesperrt, solange diese Unterlagen noch nicht vorliegen. Das heißt, es dürfen keine Ausgaben geleistet bzw. Verpflichtungen eingegangen werden, bis die Unterlagen erstellt wurden.

4 Informationssicherheit und Datenschutz

Vor Abschluss von Verträgen ist der Schutzbedarf nach IT-Grundschutz sowie der datenschutzrechtliche Schutzbedarf festzustellen und als Anforderung in die Leistungsbeschreibung aufzunehmen.

Vor der Beschaffung ist zu prüfen, ob ein bestimmtes Produkt unbedenklich eingesetzt werden kann. Es sollte vorab eine Freigabe durch den behördlichen Datenschutzbeauftragten und den Informationssicherheitsbeauftragten eingeholt werden. Wird ein Produkt beschafft, das aufgrund von Bedenken hinsichtlich der Rechtmäßigkeit nicht eingesetzt werden kann, verstößt dies auch gegen den Grundsatz der Wirtschaftlichkeit.

Bereits bei der Definition der Anforderungen (vgl. Nr. 2) sind Sicherheitsmaßnahmen vorzusehen, die eine rechtswidrige Nutzung personenbezogener Daten ausschließen (Privacy by Design). Informationssicherheit ist bereits bei der Entwicklung von Hard- und Softwareprodukten zu berücksichtigen und über deren gesamten Lebenszyklus zu gewährleisten (Security by Design).

5 Leistungsbeschreibung

Eine konkrete und vollständige Leistungsbeschreibung ist Voraussetzung dafür, dass das gewünschte Ziel im vorgegebenen Zeit- und Kostenrahmen sowie in der vereinbarten Qualität erreicht wird. Als Vertragsbestandteil bindet sie alle Vertragsparteien

über die gesamte Vertragslaufzeit und stellt die Grundlage für die Leistungsabrechnung dar. Sie ist als zahlungsbegründende Unterlage die Basis für die Feststellung der rechnerischen und sachlichen Richtigkeit durch die Landesverwaltung.

Die Leistung ist so eindeutig und erschöpfend zu beschreiben, dass die vom Auftraggeber geschuldete Leistung klar erkennbar ist. Dabei sollte sich die Verwaltung auf das Notwendige beschränken. Unvereinbarkeiten mit oder Widersprüche zu anderen Vertragsbestandteilen sind zu vermeiden.

Gesetzliche Regelungen zu Leistungsbeschreibungen ergeben sich beispielsweise aus § 121 Gesetz gegen Wettbewerbsbeschränkungen[4] oder aus §§ 31, 32 Verordnung über die Vergabe öffentlicher Aufträge (Oberschwellenbereich)[5] und im Unterschwellenbereich aus § 23 der Unterschwellenvergabeordnung (UVgO). Außerdem enthält der international gültige Standard „ISO/IEC/IEEE 29148:2018-11 – System-und Software-Engineering - Lebenszyklus-Prozesse - Requirements Engineering“ Hinweise zur Beschreibung von Leistungen.

6 Vertragsgestaltung

6.1 Vertragsübersicht

Leistungsbeziehungen können nicht aktiv gesteuert werden, wenn keine Übersicht über die Verträge existiert.

Es sollte ein Vertragsmanagement einschließlich eines IT-Controllings eingeführt werden, in dem Vertragsbeziehungen hinterlegt und Kennzahlen zur Steuerung festgelegt werden.

4 Gesetz gegen Wettbewerbsbeschränkungen vom 26. Juni 2013, BGBl. I S. 1750, 3245, zuletzt geändert durch Artikel 2 des Gesetzes vom 19. Juli 2022, BGBl. I S. 1214.

5 Vergabeverordnung vom 12. April 2016, BGBl. I S. 624, zuletzt geändert durch Artikel 2 des Gesetzes vom 9. Juni 2021, BGBl. I S. 1691.

6.2 Schriftliche oder elektronische Dokumentation

Aus dem Grundsatz der Aktenmäßigkeit der Verwaltung hat das Bundesverwaltungsgericht eine Pflicht zur Aktenführung abgeleitet[6]. Die öffentliche Verwaltung ist verpflichtet, ihr Handeln in Akten vollständig, transparent und nachvollziehbar zu dokumentieren.

Die Verfahrensschritte und Entscheidungen im Lebenszyklus eines Vertrages und alle entscheidungsrelevanten Tatsachen sind schriftlich oder elektronisch zu dokumentieren.

In der Regel sind Verträge vor Leistungsbeginn schriftlich oder elektronisch zu schließen. Insbesondere sind dabei die geschuldeten Leistungen zu dokumentieren.

Ist dies ausnahmsweise nicht möglich, sind die wesentlichen Vertragsinhalte eines zunächst mündlich geschlossenen Vertrages unverzüglich schriftlich oder elektronisch zu dokumentieren. Eine schriftliche oder elektronische Ausfertigung des Vertrages ist zeitnah anzufertigen. Diese sollte spätestens vor der ersten Rechnungslegung vorliegen.

6.3 Laufzeiten

Verträge mit unbegrenzter Laufzeit können Regelungen enthalten, die nicht mehr notwendig, zweckmäßig oder wirtschaftlich sind. Die Vertragslaufzeit sollte daher auf einen überschaubaren Zeitraum beschränkt werden. Werden Verträge verlängert, sollten die Vertragspartner prüfen, ob die ursprünglich vereinbarten Vertragsinhalte noch notwendig, zweckmäßig und wirtschaftlich sind. Eine automatische Vertragsverlängerung ohne diese Prüfung ist zu vermeiden. Rahmenverträge sollten maximal mit einer Laufzeit von vier bis sechs Jahren geschlossen werden.

6 Bundesverwaltungsgericht, Beschluss vom 16. März 1988, Az.: BVerwG 1 B 153.87. Vgl. hierzu auch Landesrechnungshof Mecklenburg-Vorpommern 2016: Rundschreiben Nr. 3/2016 Aktenführung.

6.4 Verwendung von EVB IT-Vertragsvorlagen

Der IT-Planungsrat hat die Anwendung der EVB-IT empfohlen[7].

Seit dem Bewirtschaftungserlass 2025 sind für die Beschaffung von IT-Leistungen zu berücksichtigen:

- die „Ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik“ (EVB-IT),
- die „Besonderen Vertragsbedingungen für die Beschaffung und den Betrieb von DV-Anlagen und -Geräten sowie von DV-Programmen“ (BVB) und
- die Hinweise zu den EVB-IT zu berücksichtigen.

In begründeten Ausnahmefällen kann hiervon abgewichen werden, sofern die Wirtschaftlichkeit der Beschaffung nachgewiesen ist und die Wertgrenzen für eine Beschränkte Ausschreibung gemäß Unterschwellenvergabeverordnung – UVgO nicht überschritten werden.“[8] Auf Individualverträge sollte verzichtet werden.

Die Landesverwaltung sollte nur Verträge abschließen, die auf Grundlage der jeweils aktuellen EVB-IT-Vertragsvorlagen erstellt werden. Anderenfalls hat die Behörde die Gründe in Vermerken zu dokumentieren und sicherzustellen, dass die Verwendung von Individualverträgen die Landesverwaltung nicht benachteiligt.

Änderungen an den EVB-IT-Vertragsvorlagen sollten grundsätzlich unterbleiben. Sie sind nur in begründeten Ausnahmefällen vorzunehmen und entsprechend hervorzuheben.

7 Vgl. IT-Planungsrat, Entscheidung 2018/01 vom 1. Februar 2018.

8 Beispielsweise 1. Bewirtschaftungserlass 2025 vom 16. Dezember 2024, S. 22.

6.5 Regelungen zu Nutzungs- und Verwertungsrechten bei Entwicklungsvorhaben

Trägt die Landesverwaltung die wesentlichen Kosten eines Entwicklungsvorhabens, sind der Landesverwaltung grundsätzlich dauerhafte, unwiderrufliche, unkündbare, unterlizensierbare und übertragbare Nutzungs- und Verwertungsrechte einzuräumen[9].

Die Behörden des Landes sollten bereits im Anforderungsmanagement erforderliche Nutzungsrechte ermitteln. Sie haben sicherzustellen, dass diese Rechte in den vertraglichen Vereinbarungen gewährt werden. Ausnahmsweise kann auf Nutzungsrechte verzichtet werden, wenn ein überwiegendes Landesinteresse besteht. Dies ist zu begründen.

6.6 Regelungen zur Auftragsverarbeitung

Auftragsverarbeitung ist die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Auftragsverarbeiter gemäß den Weisungen des für die Datenverarbeitung Verantwortlichen auf Grundlage eines Vertrages. Damit eine Auftragsverarbeitung wirksam vereinbart wird, ist gemäß Art. 28 Abs. 3 DS-GVO ein entsprechender Vertrag oder ein anderes Rechtsinstrument erforderlich.

Es sind Verträge zur Auftragsverarbeitung mit den in Art. 28 Abs. 3 DS-GVO aufgeführten Regelungen zu schließen.

7 Preiskalkulation

Bei der Vergabe öffentlicher Aufträge ist die Verordnung PR Nr. 30/53 über die Preise bei öffentlichen Aufträgen (PreisV 30/53) zu beachten. Bei der Vergabe von Aufträgen

9 Siehe auch Landesrechnungshof Mecklenburg-Vorpommern (2020), Rundschreiben Nr. 2/2020 – IT-Verbünde und IT-Kooperationen, S. 3.

an die DVZ M-V GmbH ist diese Verordnung gemäß § 3 Abs. 1 DVZG M-V anzuwenden. Beide Vertragsparteien haben dafür Sorge zu tragen, dass

- dem Marktpreis Vorrang vor Selbstkostenpreisen eingeräumt wird (§ 4 PreisV 30/53) und
- keine höheren Preise gefordert, versprochen, vereinbart, angenommen oder gewährt werden, als nach den Bestimmungen der Verordnung zulässig sind (§ 1 Abs. 3 PreisV 30/53).

Soweit es die Verhältnisse des Auftrages ermöglichen, ist mit dem Angebot eine Selbstkostenpreisberechnung vorzulegen. Zu allen Angeboten der DVZ M-V GmbH ist eine entsprechende Kalkulation gemäß den Leitsätzen für die Preisermittlung auf Grund von Selbstkosten einzuholen.

Für marktgängige Leistungen dürfen die im Verkehr üblichen preisrechtlich zulässigen Preise nicht überschritten werden.

Marktgängig ist eine Leistung, für die zum Zeitpunkt der Auftragsvergabe ein Markt aus Angebot und Nachfrage mit funktionierendem Wettbewerb besteht. Ebenfalls marktgängig ist eine Leistung, wenn durch ein Vergabeverfahren ein Markt geschaffen wurde, auf dem mindestens zwei Anbieter zuschlagsfähige Angebote eingereicht haben.

Im Verkehr üblich ist der Preis, den der betreffende Anbieter für die Leistung im Wettbewerb regelmäßig durchsetzen kann. Gibt es für eine Leistung einen verkehrsüblichen Marktpreis auf dem allgemeinen Markt, so ist dieser maßgeblich. Das heißt, für Leistungen der DVZ M-V GmbH, die auch auf dem allgemeinen Markt angeboten

werden, darf nur der dort verkehrsübliche Preis kalkuliert werden. Die öffentlichen Auftraggeber haben dies zu prüfen.[10]

8 Abrechnung vertraglicher Leistungen

Leistungsnachweise sind ein zentrales Element der Rechnungsprüfung. Die EVB-IT-Vertragsvorlagen enthalten für jeden Vertragstyp spezifische Regelungen und Muster zum Nachweis der erbrachten Leistungen. Mit den Rechnungen sind die vereinbarten Nachweise einzuholen. Sie sind Grundlage der rechnerischen und sachlichen Prüfung. Ohne Leistungsnachweis darf die Rechnung nicht bearbeitet werden.

Rechnungen sind gemäß den vertraglich vereinbarten Regelungen zur Fälligkeit zu bearbeiten. Rechnungen mit Fälligkeiten, die von der vertraglichen Vereinbarung abweichen, sind zurückzuweisen. Zahlungsziele sind einzuhalten. Dies ist organisatorisch zu gewährleisten.

9 Erfolgskontrolle

Die Erfolgskontrolle ist ein systematisches Prüfungsverfahren um festzustellen:

- ob und in welchem Ausmaß die angestrebten Ziele erreicht wurden,
- ob die Maßnahme ursächlich für die Zielerreichung war und
- ob die Maßnahme wirtschaftlich war.

Erfolgskontrollen sind während der Durchführung und nach Abschluss einer Maßnahme durchzuführen. Sie sind auch dann durchzuführen, wenn die Dokumentation in der Planungsphase unzureichend war. Benötigte Informationen sind in solchen Fällen nachträglich zu beschaffen.[11]

10 Vgl. Ley, Altus, Müller: Handbuch für umweltfreundliche Beschaffung, 1.8 Geltung des Preisrechts bei öffentlichen Aufträgen.

11 Vgl. VV Nr. 2.2 zu § 7 LHO.

Die Beauftragten für den Haushalt der Ressorts haben durch organisatorische Maßnahmen sicherzustellen, dass die vorgeschriebenen Erfolgskontrollen mit den geforderten Inhalten erstellt werden. Sie sollten regelmäßig durch die Beauftragten für den Haushalt ausgewertet werden, um mögliche interne Defizite zu erkennen und mit geeigneten Maßnahmen gegenzusteuern.

Rechnungshöfe des
Bundes und der Länder

Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik

- Leitlinien und gemeinsame Maßstäbe für IT-Prüfungen -

(IT-Mindestanforderungen 2025)

Stand: Mai 2025

Inhalt

1. Zweck der IT-Mindestanforderungen

In den IT-Mindestanforderungen benennen die Rechnungshöfe des Bundes und der Länder die grundlegenden Voraussetzungen und Anforderungen für den IT-Einsatz in der Bundes- und den Landesverwaltungen. Die Kommunen, Körperschaften, Anstalten und Stiftungen, die den Prüfungsrechten der Rechnungshöfe unterliegen, sollten die IT-Mindestanforderungen entsprechend anwenden.

Die IT-Mindestanforderungen basieren auf den Prüfungserkenntnissen der Rechnungshöfe und schaffen gemeinsame, transparente Prüfungsmaßstäbe.

Sie enthalten grundlegende Anforderungen zu Wirtschaftlichkeit, Ordnungsmäßigkeit und Informationssicherheit. Es folgen Anforderungen zu den übergreifenden Themen IT-Strategie und Organisation sowie zu ausgewählten Einzelthemen, die sowohl die strategische als auch die operative Ebene betreffen. Den Abschluss bilden Ausführungen zu IT-Projekten.

Die Normen, Standards und Empfehlungen zu den im Text *kursiv* hervorgehobenen Stichworten sind in der Anlage enthalten.

2. Wirtschaftlichkeit

Nach den im Haushaltsrecht des Bundes und der Länder verankerten Grundsätzen der *Wirtschaftlichkeit und Sparsamkeit* ist bei jeglichem Verwaltungshandeln die günstigste Relation zwischen dem verfolgten Zweck und den eingesetzten Ressourcen anzustreben. Für alle finanzwirksamen Maßnahmen sind daher angemessene *Wirtschaftlichkeitsuntersuchungen* durchzuführen (§/Artikel 7 BHO/LHO). Dies gilt auch für Maßnahmen der IT.

*Wirtschaftlichkeitsuntersuchunge*n sind zu folgenden Zeitpunkten zu erstellen:

Zeitpunkt	Zweck
während der Planung (vor Maßnahmenbeginn und bei Änderungen von laufenden Maßnahmen)	Entscheidungsgrundlage für die Realisierung der Maßnahme
während der Realisierung, ggf. mehrfach	begleitende *Erfolgskontrolle* bei zeitlich oder inhaltlich umfangreichen Maßnahmen
nach Abschluss	abschließende *Erfolgskontrolle*

Wirtschaftlichkeitsuntersuchungen in der Planungsphase müssen die in den Verwaltungsvorschriften zu §/Art. 7 BHO/LHO geforderten Mindestaussagen beinhalten. Dabei ist insbesondere darauf zu achten, dass

- Ziele operationalisiert/konkretisiert werden,
- sämtliche im Betrachtungszeitraum voraussichtlich entstehende Kosten - auch nicht haushaltswirksame - einbezogen werden,
- der Nutzen einbezogen wird, der von der Maßnahme ausgeht,
- die mit der Maßnahme verbundenen Risiken berücksichtigt werden
- relevante Lösungsmöglichkeiten aufgezeigt werden und
- die monetäre Betrachtung im Vordergrund steht.

Im Rahmen von *Erfolgskontrollen* ist zu prüfen, inwieweit die mit der Maßnahme verfolgten Ziele erreicht worden sind und ob die Maßnahme hierfür ursächlich und wirtschaftlich war (Zielerreichungs-, Wirkungs- und Wirtschaftlichkeitskontrolle).

Bei Maßnahmen von *IT-Verbünden* sind auch die Auswirkungen auf die einzelnen Verbundpartner zu betrachten. Näheres ergibt sich aus der gemeinsamen *„Handreichung IT-Verbünde und IT-Kooperation“* der Rechnungshöfe des Bundes und der Länder.

3. Ordnungsmäßigkeit

Ordnungsmäßigkeit umfasst die Einhaltung der geltenden Normen, insbesondere der Gesetze, Haushaltsgrundsätze und Verwaltungsvorschriften.

Beim IT-Einsatz in der öffentlichen Verwaltung sind insbesondere die Regelungen zur *Revisionsfähigkeit*, zur *Informationssicherheit*, zum *Datenschutz*, zur *Verwaltungsdigitalisierung*, zum *Arbeitsschutz* und zur *Barrierefreiheit* zu beachten.

Um einen ordnungsgemäßen IT-Einsatz sicherzustellen, sind *interne Kontrollsysteme* zu etablieren.

Planung und Einsatz der IT sowie Maßnahmen der internen Kontrolle sind zu dokumentieren. Die *Dokumentation* muss vollständig, aktuell und verständlich sein sowie alle Änderungen und Entscheidungen nachweisen.

Hierzu gelten die im *„Positionspapier Aktenführung- und E-Akte“* der Rechnungshöfe des Bundes und der Länder aufgeführten Grundsätze, auch während der gesetzlichen Aufbewahrungsfristen (*Langzeitspeicherung*) und ggf. dauerhaft im Rahmen der *Archivierung*.

4. Informationssicherheit

Die Gewährleistung der *Informationssicherheit* ist eine Daueraufgabe. Der Schutz der Informationen vor

- unberechtigter Kenntnisnahme (Verlust der Vertraulichkeit),
- unberechtigter Veränderung oder Verfälschung (Verlust der Integrität) und
- Beeinträchtigung oder Verlust der Verfügbarkeit

ist im gesamten Lebenszyklus sicherzustellen.

Die Leitung der Behörden, Stellen und Einrichtungen ist für die *Informationssicherheit* verantwortlich und hat sicherzustellen, dass die hierfür erforderlichen finanziellen, personellen und zeitlichen Ressourcen zur Verfügung stehen.

Zur Gewährleistung der Informationssicherheit ist ein angemessenes und einheitliches *Informationssicherheitsmanagement* aufzubauen und zu unterhalten.

Innerhalb von Gebietskörperschaften ist dafür eine *zentrale Stelle* mit Durchgriffsmöglichkeiten erforderlich. Ebenen- bzw. länderübergreifende Kooperationen sollten angestrebt werden. Von allen Beteiligten ist ein angemessenes und einheitliches Sicherheitsniveau zu definieren und zu gewährleisten.

Die konkreten infrastrukturellen, organisatorischen, personellen und technischen Maßnahmen zur *Informationssicherheit* sind aus regelmäßigen *Schutzbedarfsfeststellungen* und *Risikoanalysen* abzuleiten. Dabei ist der *Stand der Technik* zu berücksichtigen.

Konkrete Empfehlungen für die Ausgestaltung des *Informationssicherheitsmanagements* ergeben sich aus dem „*Grundsatzpapier zum Informationssicherheitsmanagement*“ der Rechnungshöfe des Bundes und der Länder.

5. IT-Strategie

Die Prinzipien, Leitlinien und Ziele für den Einsatz der IT sind für die verschiedenen Ebenen verbindlich festzulegen (*IT-Strategie*). Dabei ist zu beschreiben, welchen Beitrag die IT zur Aufgabenwahrnehmung der Verwaltung leisten soll.

IT-Strategien sollen Ziele festlegen und Aussagen enthalten zu folgenden Themen:

- Strukturen und Organisation,
- Finanzierung,
- *IT-Architektur*,
- IT-Infrastruktur,
- *Informationssicherheitsmanagement*,
- *IT-Servicemanagement*,
- *IT-Risikomanagement*,
- *Kontinuitätsmanagement*,
- ebenenübergreifende IT (z. B. Kooperationen in *IT-Verbünden*) sowie
- technische und wirtschaftliche Abhängigkeiten (*digitale Souveränität*).

Aus der *IT-Strategie* sind konkrete IT-Maßnahmen abzuleiten und zu priorisieren sowie mit operationalisierten Kennzahlen zu verbinden. Die *IT-Strategie*, IT- Maßnahmen und Kennzahlen sind zu dokumentieren, transparent zu machen, zu evaluieren und regelmäßig fortzuschreiben.

Die in den „*Grundsätzen für die Verwaltungsorganisation*“ der Rechnungshöfe des Bundes und der Länder aufgeführten Anforderungen an eine Strategie sind zu berücksichtigen.

Die *IT-Governance* sollte gewährleisten, dass die *IT-Strategie* sowie deren operative Umsetzung im Einklang mit den Aufgaben und Zielen der Verwaltung steht und die vorhandenen Ressourcen effizient genutzt werden.

6. Organisatorische Anforderungen

Die Entwicklung der *IT-Strategie*, die (ressort-)übergreifende IT-Koordinierung, die Planung und Kontrolle strategischer Aufgaben, IT-Querschnittsaufgaben und die Bereitstellung und Gewährleistung der erforderlichen Infrastrukturen müssen aufeinander abgestimmt sein.

Dazu bedarf es vor allem einer übergreifenden IT-Steuerung durch eine *zentrale Stelle*. Diese hat darüber hinaus Standards für *IT-Architekturen* (z. B. IT-Systemkomponenten, *Datenaustausch* und Benutzerschnittstellen) sowie *IT-Projektmanagement*, IT-Betrieb und *IT-Beschaffungen* festzulegen.

Die *zentrale Stelle* muss mit den zur Bewältigung der Aufgaben benötigten Befugnissen ausgestattet sein. Das *Ressortprinzip* steht dem grundsätzlich nicht entgegen. Denn die IT erfüllt lediglich unterstützende Aufgaben. Die fachliche Zuständigkeit der Ressorts und wie diese ihre Fachaufgaben erfüllen, ist davon unbenommen. Diese wird durch aufgabenneutrale Vorgaben einer übergreifenden IT-Steuerung in der Regel nicht berührt.

Die *zentrale Stelle* und die Leitungen der Behörden bzw. Einrichtungen haben insbesondere sicherzustellen, dass

- die Fach-, Entwicklungs- und Betriebsverantwortung unter Beachtung des Prinzips der *Funktionstrennung* abgegrenzt ist,
- interne Vorgaben aus *Rahmenwerken* bedarfsgerecht entwickelt werden,
- das erforderliche Personal mit den benötigten Fähigkeiten und Kompetenzen vorhanden ist,
- Prozesse definiert sind,
- ein Berichtswesen mit geeigneten Kennzahlen eingerichtet ist (IT-Controlling),
- IT-Leistungen wie Dienste, Infrastruktur und Verfahren einschließlich deren Lebens- und Beschaffungszyklen definiert sind,

- die Fähigkeiten zur Anforderungsdefinition, Steuerung und Überwachung externer Leistungen vorhanden sind (Auftraggeberfähigkeit),
- *verbindliche Vereinbarungen* für die auf IT-Dienstleister übertragenen Aufgaben getroffen wurden sowie
- bei Verfahren, in denen mehrere Einheiten zusammenwirken, Verantwortlichkeiten zugewiesen sind.

Alle Vorgaben sind kontinuierlich zu überprüfen, fortzuschreiben und bekanntzugeben.

Die erforderlichen Personalressourcen für die IT sind durch *Personalbedarfsermittlungen* festzustellen. Die Anforderungen dazu ergeben sich aus den „*Leitsätzen für die Personalbedarfsermittlung*“ der Rechnungshöfe des Bundes und der Länder.

Im Übrigen gelten die allgemeinen organisatorischen Anforderungen aus den „*Grundsätzen für die Verwaltungsorganisation*“ der Rechnungshöfe des Bundes und der Länder.

7. Schwerpunktthemen

7.1. IT-Architektur

IT-Architekturen sind organisations- und ebenenübergreifend abzustimmen. Durch die Verwendung offener, interoperabler Standards soll sichergestellt werden, dass die Elemente der verschiedenen *IT-Architekturen* kompatibel und nachnutzbar sind.

Vorgaben für die *IT-Architektur* sind aus den jeweiligen strategischen Zielen abzuleiten und müssen insbesondere Aussagen zur:

- Facharchitektur,
- Anwendungsarchitektur,
- technische Architektur sowie
- Informations- und Datenarchitektur

enthalten.

Die Vorgaben sind kontinuierlich unter Berücksichtigung der sich wandelnden Anforderungen und dem *Stand der Technik* weiterzuentwickeln und deren Einhaltung zu überwachen.

7.2. IT-Controlling

Für die Steuerung des IT-Einsatzes ist ein angemessenes IT-Controlling einzurichten. Das IT-Controlling soll bestehen aus:

- Zieldefinitionen: Messbarkeit durch Kennzahlen, Festlegen entsprechender Zielgrößen,
- Überwachung: fortlaufender Soll-Ist-Vergleich der Kennzahlen,
- Analyse: Untersuchen von Soll-Ist-Abweichungen und Identifizieren von Optimierungspotenzialen sowie
- Information: Kommunizieren der Ergebnisse (Berichtswesen).

Es soll insbesondere

- die Gesamtheit der IT-Vorhaben einer Organisation (Portfoliomanagement),
- die einzelnen IT-Projekte inklusive der Projekte mit IT-Bezug aus den Fachbereichen (Projektcontrolling),
- die eingesetzten IT-Produkte (Produktcontrolling) und
- die betriebene IT-Infrastruktur

umfassen.

Die Kosten des IT-Einsatzes sollen identifiziert, erfasst, überwacht, bewertet und verursachungsgerecht zugeordnet werden.

7.3. IT-Servicemanagement

Es ist ein angemessenes *IT-Servicemanagement* zu betreiben. Wichtige Prozesse sind dabei:

- *Service Level Management* zur Definition, Überwachung und Optimierung von Dienstleistungen,
- *Incident Management* zur schnellstmöglichen Wiederherstellung eines *IT-Services* nach einer Betriebsstörung,
- *Problem Management* zur Analyse von Betriebsstörungen (reaktiv und proaktiv) mit dem Ziel einer dauerhaften Problemlösung,
- *Change Management* zur Steuerung sämtlicher Veränderungen der IT-Infrastruktur und *IT-Services* sowie
- *Asset Management* zur Überwachung und Verwaltung von IT-Vermögenswerten über den gesamten Lebenszyklus.

Es sollte eine zentrale Serviceeinheit (*Service Desk*), u. a. als Schnittstelle zu den Endanwendern, eingerichtet sein. Erforderliche Informationen über die IT-Komponenten und deren Beziehungen untereinander sind zentral und strukturiert in einer *Configuration Management Database* vorzuhalten und zu pflegen.

7.4. IT-Risikomanagement

Zur systematischen Behandlung der aus dem IT-Einsatz resultierenden Risiken ist ein *IT-Risikomanagement* einzurichten. Dieses muss in das organisationsweite Risikomanagement eingebettet sein. Die Vorgaben aus der *IT-Strategie* sind zu beachten.

Das *IT-Risikomanagement* soll die strategischen sowie operationellen Risiken insbesondere aus den Bereichen

- *Informationssicherheit* und *Datenschutz*,
- IT-Betrieb und IT-Infrastrukturen,
- IT-Dienste, IT-Systeme und IT-Verfahren,
- personelle (inkl. Fähigkeiten und Kompetenzen) und finanzielle Ressourcen,
- IT-Projekte sowie

- IT-Umfeld (bspw. Gesetzesänderungen, externe Beziehungen, aufbauorganisatorische Belange)

angemessen behandeln und fortlaufend Änderungen berücksichtigen. Dazu ist ein kontinuierlicher Risikomanagement-Prozess zu etablieren.

Weitere allgemeine Anforderungen an ein IT-Risikomanagement ergeben sich aus den „Grundsätzen für die Verwaltungsorganisation“ der Rechnungshöfe des Bundes und der Länder.

7.5. Kontinuitätsmanagement

Die Verwaltungen bzw. Behörden müssen die Verfügbarkeit ihrer kritischen Geschäftsprozesse sichern und ggf. wiederherstellen.

Dazu sollen sie im Rahmen eines *Business Continuity Management* Maßnahmen zur Vorsorge treffen sowie Strategien und Planungen zur Notfallbewältigung erarbeiten.

Bei IT-unterstützten kritischen Geschäftsprozessen müssen die IT-Verantwortlichen von den Prozessverantwortlichen eingebunden werden.

Die Prozessverantwortlichen haben sicherzustellen, dass

- die den kritischen Geschäftsprozessen zugrundeliegenden IT-Dienste, IT-Systeme und IT-Verfahren dokumentiert sind,
- *Vorsorgekonzepte*, Notfallhandbücher, Wiederherstellungspläne und Wiederanlaufpläne vorhanden sind sowie überprüft und kontinuierlich fortgeschrieben werden sowie
- Notfallszenarien regelmäßig geübt werden.

8. IT-Projekte

8.1. Planung

Zur Planung eines IT-Projekts[1] gehört es

- die Ziele festzulegen,
- die Anforderungen systematisch zu analysieren,
- das erforderliche Budget bzw. die notwendigen Ressourcen zu ermitteln sowie
- Lösungsalternativen einschließlich der Risiken in einer *Wirtschaftlichkeitsuntersuchung* zu bewerten.

Bereits bei der Anforderungsanalyse sind neben den rechtlichen und strategischen Rahmenbedingungen insbesondere

- vorrangig *IT-Standards* zu berücksichtigen,
- die Kompatibilität und Interoperabilität mit vorhandener Infrastruktur zu prüfen,
- notwendige Datenmigrationen einzubeziehen,
- Produkt- und Anbieterabhängigkeiten (*„Lock-In"-Effekte*) zu vermeiden,
- Energieeffizienz, Lebenszyklus und Nachnutzung zu berücksichtigen,
- Betrieb, Wartung und Pflege mitzubetrachten sowie
- *Test- und Abnahmeverfahren* vorzusehen.

Bei der Detailplanung sind insbesondere folgende Lösungsalternativen zu vergleichen

- die Übernahme von in anderen Verwaltungen vorhandenen Produkten,
- die Beteiligung an oder Initiierung von *IT-Verbünden*,
- der Einsatz von marktgängigen Produkten,
- die Entwicklung durch Externe und
- die Entwicklung durch eigene Bedienstete.

[1] IT-Projekte (auch bezeichnet als IT-Vorhaben, IT-Maßnahmen) umfassen die Konzeption, Entwicklung, Beschaffung und Einführung von IT-Verfahren, IT-Infrastruktur und IT-Diensten sowie wesentliche Änderungen im IT-Betrieb.

Es ist ein geeigneter Projektmanagementstandard anzuwenden. Dieser sollte insbesondere beinhalten:

- Projektorganisation,
- Zeitplanung,
- Controlling,
- *Qualitätsmanagement*,
- Veränderungsmanagement,
- Kommunikationsmanagement sowie
- *Risikomanagement*.

Die gesamte Planung ist systematisch und vollständig zu dokumentieren.

8.2. IT-Beschaffungen und Einsatz Externer

Die (vergabe-)rechtlichen Anforderungen sind im Rahmen von *IT-Beschaffungen* zu erfüllen. Dabei sind insbesondere

- Bedarfe systematisch zu erheben und (ggf. auch ebenenübergreifend) zu bündeln,
- eindeutige und erschöpfende Leistungsbeschreibungen zu erstellen,
- Rahmenvereinbarungen zu nutzen und In-House-Vergaben zu prüfen,
- standardisierte Vertragsmuster (z. B. EVB-IT) anzuwenden,
- *Test- und Abnahmeverfahren* zu den Anforderungen vertraglich zu vereinbaren,
- die Leistungserbringung zu kontrollieren und zu steuern und
- Verfahren und Entscheidungen nachvollziehbar zu dokumentieren.

IT-Beschaffungen sollen über zentrale darauf spezialisierte Beschaffungsstellen durchgeführt werden.

Falls externe Dienstleister beauftragt werden, sind folgende Anforderungen zu beachten:

- Die Notwendigkeit und die Wirtschaftlichkeit des Einsatzes sind nachzuweisen.
- Entscheidungsbefugnisse und Kernaufgaben sind bei internem Personal zu belassen.
- Die Steuerung und Erfolgskontrolle sind sicherzustellen.
- Der fachliche Austausch und Wissenstransfer sind zu gewährleisten.
- Die Abhängigkeit von Externen ist zu vermeiden.

Bei der *Entwicklung* von Software sind der Zugriff auf den Quellcode und die *Nutzungsrechte* für diesen vertraglich sicherzustellen. Dies gilt auch für sonstige Ergebnisse des Entwicklungsprozesses.

8.3. Entwicklung, Test, Abnahme und Freigabe

Die Entwicklung ist anhand der Planungsvorgaben engmaschig zu kontrollieren und zu steuern.

Details des *Test- und Abnahmeverfahrens* sind zu regeln. Die Testszenarien sollten funktionale wie auch nicht-funktionale Anforderungen und die Datenmigration erfassen. Test- und Produktivumgebung sind zu trennen. Die Nutzenden und die fachlich zuständigen Stellen sind zu beteiligen.

Es ist zu prüfen, ob gesetzliche Vorgaben oder andere Richtlinien eine *Freigabe* der entwickelten Produkte erfordern und welche Voraussetzungen dafür zu erfüllen sind.

Entwicklung, Test und Abnahme sowie ggf. Freigabe sind zu dokumentieren. Die *Dokumentation* muss die Pflege, die Wartung und einen ordnungsgemäßen IT-Betrieb unterstützen.

8.4. Inbetriebnahme

Vor der Inbetriebnahme ist zu gewährleisten, dass

- das neue IT-System in das *IT-Servicemanagement* und das *Informationssicherheitsmanagement* eingebunden wurde,
- die erforderliche Hard- und Softwareumgebung eingerichtet ist,
- die notwendigen Datenbestände übernommen wurden,
- die Benutzer bedarfsgerecht und zeitnah geschult werden und
- die erforderlichen Tests durchgeführt wurden und alle Freigaben vorliegen.

Eine im Umfang angemessene und auf die jeweilige Zielgruppe ausgerichtete *Dokumentation* ist bereitzustellen.

IT-Mindestanforderungen 2025

Anlage:
Fundstellen zu Normen, Standards und Empfehlungen

Stand: Mai 2025

Für eine Vielzahl von Anforderungen existieren Normen, Standards und Empfehlungen. Sie sind für den jeweiligen Adressaten von unterschiedlicher Verbindlichkeit.

Die nachfolgenden Links und Versionsangaben geben den Stand zum Zeitpunkt der Erstellung des Dokuments wieder. Sollten danach neue Versionen der entsprechenden Unterlagen und Regelwerke veröffentlicht werden, so werden auch diese von den Rechnungshöfen des Bundes und der Länder berücksichtigt.

Bei Rechtsgrundlagen ist auf die jeweils geltende Fassung zu achten.

Die nachfolgende Aufzählung erhebt keinen Anspruch auf Vollständigkeit.

Bei vergleichbaren Normen, Standards und Empfehlungen, die sowohl vom Bund wie auch von den Ländern herausgegeben wurden, wird aus Platzgründen auf eine Quelle der Bundesebene verwiesen.

Sollte ein Link nicht mehr funktionieren, so kann mit den in der Spalte „Quelle, Bemerkung“ angegebenen Stichworten gesucht werden.

Stichworte

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
A			
Arbeitsschutz	3	Arbeitsschutzgesetz (ArbSchG)	www.gesetze-im-internet.de | ArbSchG
		Verordnung über Arbeitsstätten (ArbStättV), Anlage Nr. 6 - Maßnahmen zur Gestaltung von Bildschirmarbeitsplätzen	www.gesetze-im-internet.de | ArbStättV
Archivierung	3		Zeitraum nach Abschluss der Langzeitspeicherung
		§ 31 Verschlusssachenanweisung (VSA), Archivierung von Verschlusssachen	www.verwaltungsvorschriften-im-internet.de | VSA
		Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)	Bundesfinanzministerium (BMF), www.bundesfinanzministerium.de | GoBD
		Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)	Institut der Wirtschaftsprüfer in Deutschland e. V. (IDW)
Asset Management	7.3	Information technology - IT asset management - Part 1: IT asset management systems - Requirements (ISO/IEC 19770-1:2017-12)	ISO
B			
Barrierefreiheit	3	Gesetz zur Gleichstellung behinderter Menschen (BGG)	www.gesetze-im-internet.de | BGG
		Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie Informationstechnik-Verordnung - BITV) und vergleichbare Landesregelungen	www.gesetze-im-internet.de | BITV
Beauftragung und Einsatz Externer	8.2	Einsatz externer Berater in der Bundesverwaltung	Diverse Veröffentlichungen des Bundesrechnungshofs www.bundesrechnungshof.de | externe Berater

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Leitsatz der externen Finanzkontrolle (09/03) – Einsatz externer Berater – Grundsatz	Bundesbeauftragter für Wirtschaftlichkeit in der Verwaltung, www.bundesrechnungshof.de | BWV-Leitsatz Nummer 09/03
		Eckpunkte „Einsatz Externer in der Informationstechnik der Bundesverwaltung“ Empfehlungen zur Inanspruchnahme von externen Unterstützungsleistungen durch Bundesbehörden im IT-Bereich	IT-Rat Bund, Beschluss 2016/8 vom 29. Juni 2016, www.cio.bund.de | 2016/8
Business Continuity Management	7.5	siehe Kontinuitätsmanagement	
C			
Change Management	7.3		Der ITIL-Prozess Change Management hat das Ziel, Veränderungen in Organisationen durch standardisierte Maßnahmen zu gestalten.
Configuration Management Database	7.3		Die Configuration Management Database ist ein Speicherort für Daten über alle Betriebsmittel der IT (Configuration Items - CIs).
		Spezifikationen und für IT Service Management (Normenreihe ISO/IEC 20000)	DIN, ISO
		siehe Rahmenwerke, ITIL	
		Standardfamilie für ein „leichtgewichtiges IT Service Management“ (FitSM)	Frei verfügbare Ergebnisse des EU-geförderten Projekts „Implementing service management in federated e-Infrastructures“ (FedSM), www.FitSM.eu | FitSM Standard | Downloads

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
D			
Datenaustausch	6		Datenaustausch bezeichnet die informationstechnische Umsetzung des Verfahrens zur Übergabe von maschinell und automatisiert weiterverwendeten Informationen zwischen dazu berechtigten Informationssystemen oder -subsystemen auf Basis lesender oder schreibender Zugriffe auf die entsprechenden Schnittstellen. Datenaustausch im Sinne der IT ist vom Datenabruf aus einem Informationssystem durch menschliche Akteure zu unterscheiden.
		Standards des IT-Planungsrats	IT-Planungsrat, www.it-planungsrat.de | Standards
		Koordinierungsstelle für IT-Standards (KoSIT)	KoSIT, www.xoev.de (Startseite)
		Standards der XLeitstelle	www.XLeitstelle.de
Datenschutz	3, 7.4	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)	ABl. L 119 vom 04.05.2016 www.eur-lex.europa.eu | DSGVO
		Bundesdatenschutzgesetz (BDSG), und entsprechende Ländergesetze	www.gesetze-im-internet.de | BDSG
		Standard-Datenschutzmodell	Abrufbar in der jeweils aktuellen Version auf den Seiten der Datenschutzbeauftragten des Bundes und der Länder, z. B. www.bfdi.bund.de | Standard-Datenschutzmodell
		IT-Grundschutz Grundschutzkompendium Baustein CON.2: Datenschutz	BSI, www.bsi.bund.de | CON.2

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Orientierungshilfen der Beauftragten für den Datenschutz zu verschiedenen Themen	Datenschutzkonferenz, www.datenschutzkonferenz-online.de | Infothek | Orientierungshilfen
Digitale Souveränität	5		Digitale Souveränität beschreibt die Fähigkeit, zum kompetenten Handeln in Abgrenzung zu den Extremen der digitalen Abhängigkeit („Andere entscheiden“) und zur digitalen Autarkie („Alles selbst machen“).
		Kompetenzzentrum Öffentliche IT: Bericht zum „Digitalpolitisches Dossier“ im Deutschen Bundestag mit Whitepaper „Digitale Souveränität“	www.oeffentliche-it.de | Veranstaltungen | Digitale Souveränität
		Bedeutung „Digitale Souveränität“ und Eckpunktepapier	IT-Planungsrat, www.it-planungsrat.de | Eckpunktepapier Digitale Souveränität
		Antwort der Bundesregierung auf die Kleine Anfrage „Digitale Souveränität in der Digitalstrategie der Bundesregierung“, BT-Drs. 20/4500	Deutscher Bundestag https://dip.bundestag.de | Bundestagsdrucksache 20/4500
Dokumentation	3, 8.3, 8.4	Grundsatz der Schriftlichkeit (Aktenmäßigkeit)	Online-Verwaltungslexikon, www.olev.de | Schriftlichkeit
		§ 12 Abs. 2 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) und vergleichbare Landesvorschriften	Bundesministerium des Innern (BMI), www.bmi.bund.de | GGO
		Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien und vergleichbare Landesvorschriften	BMI, www.bmi.bund.de | Registraturrichtlinie
		Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) - insbesondere Nr. 10	BMF, www.bundesfinanzministerium.de | GoBD

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Verwaltungsvorschrift für Zahlungen, Buchführung und Rechnungslegung (§§ 70 bis 72 und 74 bis 80 BHO) – VV-ZBR BHO, Nr. 4.7 Aufbewahrungsbestimmungen und vergleichbare Landesregelungen	www.verwaltungsvorschriften-im-internet.de | VV-ZBR BHO
		Anlage zur VV Nr. 6.1 ZBR BHO (Anlage 1 zur VV-ZBR BHO) Grundsätze ordnungsgemäßer Buchführung bei Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (GoBIT-HKR), Nr. 6 Aufbewahrung von Elektronischen Unterlagen und vergleichbare Landesregelungen	www.verwaltungsvorschriften-im-internet.de | VV-ZBR BHO
		DIN ISO 15489-1 Information und Dokumentation - Schriftgutverwaltung	DIN
		IT-Grundschutz-konforme Dokumentation (Entwurfsfassung)	BSI, www.bsi.bund.de | IT-Grundschutz-konforme Dokumentation
E			
Erfolgskontrolle	2, 8.2	Verwaltungsvorschriften zu § / Artikel 7 der Haushaltsordnungen des Bundes und der Länder	z. B. Verwaltungsvorschriften zur BHO, www.verwaltungsvorschriften-im-internet.de | VV-BHO
		Arbeitsanleitung Einführung in Wirtschaftlichkeitsuntersuchungen	BMF, www.verwaltungsvorschriften-im-internet.de | Wirtschaftlichkeitsuntersuchungen
		Bericht nach § 88 Absatz 2 BHO an den Haushaltsausschuss des Deutschen Bundestages „Erfolgskontrollen als Voraussetzung für eine wirkungsorientierte Haushaltsführung“	Bundesrechnungshof, www.bundesrechnungshof.de | Bericht Erfolgskontrolle
		Erfolgskontrolle in der öffentlichen Verwaltung	Finanzministerium des Landes Mecklenburg-Vorpommern, www.regierung-mv.de | Erfolgskontrolle

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
F			
Freigabe	8.3, 8.4	IT-Grundschutz-Kompendium des BSI, hier: IT-Grundschutz-Baustein (OPS.1.1.6) Software-Tests und -Freigaben	BSI, www.bsi.bund.de | Freigabe
		Bestimmungen über die Mindestanforderungen für den Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (BestMaVB - HKR) und vergleichbare Landesregelungen	www.verwaltungsvorschriften-im-internet.de | BestMaVB-HKR
Funktionstrennung	6		Organisationsgrundsatz, nach dem unvereinbare Aufgaben (z. B. im Zusammenhang mit der Berechtigungsvergabe oder der Protokollierung) nicht auf einem Arbeitsplatz zusammengeführt werden dürfen. Dies betrifft auch Vertretungssituationen.
		BSI: IT-Grundschutz – Baustein ORP.1 Organisation (hier: ORP.1.A4)	BSI, www.bsi.bund.de | ORP.1
G			
Grundsätze für die Verwaltungsorganisation	5, 6, 7.4	Grundsätze für die Verwaltungsorganisation	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Grundsätze Verwaltungsorganisation
Grundsatzpapier Informationssicherheits-management	4	Grundsatzpapier Informationssicherheitsmanagement	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Grundsatzpapier Informationssicherheitsmanagement
I			
Incident Management	7.3		Der ITIL-Prozess Incident-Management hat das Ziel, Störungen schnellstmöglich zu beseitigen oder zu umgehen, um Services wieder zur Verfügung zu stellen.
Informationssicherheit	3, 4, 7.4	Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung und vergleichbare Landesregelungen	IT-Planungsrat, www.it-planungsrat.de | Informationssicherheitsleitlinie

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Standards, technische Richtlinien und sonstige Dokumente des BSI	BSI, www.bsi.bund.de (Startseite)
		Grundsatzpapier zum Informationssicherheits-management mit Fragenkatalog	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Grundsatzpapier Informationssicherheitsmanagement
		Cyber-Sicherheitsstrategie für Deutschland	BMI; www.bmi.bund.de | Cyber-Sicherheitsstrategie
		Informationssicherheitsmanagementsystem in 12 Schritten (CISIS12)	SWI-Informationssicherheit für den Mittelstand GmbH, https://cisis12.de/
		Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (DIN ISO/IEC 27000 Normenreihe)	DIN, ISO
Informationssicherheits-management	4, 5	Siehe Informationssicherheit	Planungs- und Lenkungsaufgabe, die erforderlich ist, um einen durchdachten und planmäßigen Informationssicherheitsprozess aufzubauen und kontinuierlich umzusetzen.
Internes Kontrollsystem	3	Empfehlungen für Interne Revisionen in der Bundesverwaltung	BMI, www.bmi.bund.de | Interne Revisionen
		Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)	BMF, www.bundesfinanzministerium.de | GoBD
		Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz -	BSI, www.bsi.bund.de | Leitfaden IS-Revision
		Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)	IDW
		Grundsätze ordnungsmäßiger Buchführung beim Ein-satz elektronischer Archivierungsverfahren (IDW RS FAIT 3)	IDW

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330)	IDW
		siehe Rahmenwerke, COBIT	
IT-Architektur	5, 6, 7.1	Föderale Architekturrichtlinien, Beschluss 2021/37 des IT-Planungsrates	IT-Planungsrat www.it-planungsrat.de | 2021/37
		IT-Architektur Bund	BMI, Architekturrichtlinie des Bundes in der jeweils aktuellen Version abrufbar, www.cio.bund.de | IT-Architektur
		Standards und Architekturen für E-Government-Anwendungen (SAGA) für die Bundesverwaltung (IT-Rat Bund, Beschluss vom 03.11.2011), und landesspezifische Regelungen und Vorgaben	CIO Bund www.cio.bund.de | Architekturen und Standards | SAGA
		Föderale IT-Architektur (FITKO)	FITKO www.fitko.de | Föderale IT-Architektur
		Enterprise Architecture Management – neue Disziplin für die ganzheitliche Unternehmensentwicklung des Bundesverbands Informationswirtschaft Telekommunikation und neue Medien e.V. (BITKOM)	Bitkom www.bitkom.org
IT-Beschaffung	6, 8.2	Umfassende Liste von Normen und Rechtsgrundlagen	Beschaffungsamt des BMI, www.bescha.bund.de | Normen und Rechtsvorschriften
		Regeln und Vorschriften für die öffentliche Vergabe	Bundesministerium für Wirtschaft und Klimaschutz, www.bmwk.de | Regeln Vorschriften öffentliche Vergabe
		Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT)	CIO Bund, www.cio.bund.de | EVB-IT
		Leitfäden für produktneutrale Ausschreibungen	bitkom, www.itk-beschaffung.de (Startseite)
		Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB)	CIO Bund, www.cio.bund.de | UfAB

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
IT-Governance	5		IT-Governance ist ein formales Rahmenwerk das sicherstellt, dass die IT-Investitionen einer Organisation die Geschäftsziele unterstützen. Es umfasst Prozesse und Strukturen die notwendig sind, um die effektive und effiziente Nutzung von IT zu gewährleisten.
		Informationstechnik - Unternehmensführung in der Informationstechnik (ISO/IEC 38500)	DIN, ISO
		siehe Rahmenwerke, COBIT	
		siehe Rahmenwerke, ITIL	
		siehe Informationssicherheit	
		siehe IT-Servicemanagement	
IT-Projektmanagement	6	Projektmanagementmethoden V-Modell XT und V-Modell XT Bund	CIO Bund, www.cio.bund.de | V-Modell XT, www.cio.bund.de | V-Modell XT Bund
		Praxisleitfaden „Projektmanagement für die öffentliche Verwaltung“	BMI www.bmi.bund.de | Praxisleitfaden Projektmanagement
		HERMES	Schweizerische Eidgenossenschaft, www.isb.admin.ch | Themen | Projektmanagement | HERMES
		Projektmanagementsysteme (Normenfamilie DIN 69901)	DIN
		Qualitätsmanagementsysteme - Leitfaden für Qualitätsmanagement in Projekten (ISO 10006)	DIN, ISO
		S-O-S-Methode© für Großprojekte	Bundesverwaltungsamt (BVA), www.bva.bund.de | SOS-Methode
		Projektmanagementstandard PMflex	BVA, https://www.bva.bund.de | PMflex

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
IT-Service / IT-Servicemanagement	5, 7.3, 8.4		IT-Servicemanagement (ITSM) bezeichnet die Gesamtheit von Maßnahmen und Methoden, die nötig sind, um die bestmögliche Unterstützung von Geschäftsprozessen durch die IT-Organisation zu erreichen.
		siehe Rahmenwerke, ITIL	
		Standardfamilie für ein „leichtgewichtiges IT Service Management“ (FitSM)	Frei verfügbare Ergebnisse des EU-geförderten Projekts „Implementing service management in federated e-Infrastructures“ (FedSM), www.fitsm.eu | Downloads
		Spezifikationen und Empfehlungen für IT Service Management (Normenreihe ISO/IEC 20000)	DIN, ISO
		Sicherheit und Schutz des Gemeinwesens - Business Continuity Management System - Anforderungen (ISO 22301)	DIN, ISO
		Qualitätsmanagementsysteme - Grundlagen und Begriffe (DIN EN ISO 9000)	DIN, ISO
		siehe Operational Level Agreement (OLA), Service Level Agreement (SLA)	
IT-Standards	8.1	IT-Interoperabilitäts- und IT-Sicherheitsstandards gemäß § 2 IT-Staatsvertrag	IT-Planungsrat, www.it-planungsrat.de | föderale IT-Standards
IT-Strategie	5, 6, 7.4	IT-Strategie Bund oder vergleichbare Grundlagen in den Ländern	BMI, www.cio.bund.de | IT-Strategie Bund

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
IT-Verbund	2, 5, 8.1		Insbesondere zum gemeinsamen Einkauf, zur Entwicklung, zur Pflege und zum Betrieb von Software haben sich IT-Verbünde, IT-Kooperationen und sonstige Formen der Zusammenarbeit der öffentlichen Verwaltung zwischen Bund, Ländern und Kommunen etabliert. Beispiele sind der Entwicklungsverbund KONSENS, die IT-Verbünde der Justiz sowie die Projekte und Anwendungen des IT-Planungsrats.
		Gutachten zur Evaluierung der Kieler Beschlüsse	IT-Planungsrat, Beschluss vom 16.10.2014 www.it-planungsrat.de | evakb
		Leitfaden zur Gestaltung von Softwarekooperationen vom 20.08.2014	IT-Planungsrat, Beschluss vom 16.10.2014 www.it-planungsrat.de | Leitfaden Softwarekooperationen
		Handreichung „IT-Verbünde und IT-Kooperationen“ der Rechnungshöfe des Bundes und der Länder vom Mai 2020	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Handreichung IT-Verbünde und IT-Kooperationen
K			
Kontinuitätsmanagement	5	BSI-Standard 200-4 Business Continuity Management	BSI, www.bsi.bund.de | BSI-Standard 200-4
		ISO/IEC 27031:2011 Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity	ISO
		ISO 22300:2021 Security and resilience - Vocabulary	ISO
		ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements	ISO
		ISO 22313:2020 Security and resilience - Business continuity management systems - Guidance on the use of ISO 22301	ISO

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
L			
Langzeitspeicherung	3	Organisationskonzept elektronische Verwaltungsarbeit, verschiedene Bausteine, u. a. zur E-Langzeitspeicherung	Bundesregierung, www.verwaltung-innovativ.de | Organisationskonzept
		Technische Richtlinie: Vertrauenswürdige elektronische Langzeitspeicherung; Beweiswerterhaltung kryptographisch signierter Dokumente	BSI, www.bsi.bund.de | TR-03125
Leitsätze für die Personalbedarfsermittlung	6	Leitsätze für die Personalbedarfsermittlung	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Personalbedarfsermittlung
Lock-In-Effekt	8.1		Abhängigkeitsverhältnis von Kunden zu Anbietern oder Produkten, das dadurch gekennzeichnet ist, dass hohe Kosten einen Wechsel unwirtschaftlich machen.
N			
Nachhaltigkeit		Leitprinzip Nachhaltigkeit im Haushaltskreislauf, Die Grundsätze der umweltpolitischen Digitalagenda	BRH, www.bundesrechnungshof.de | Bundeshaushalt-Nachhaltigkeit
		Umweltpolitische Digitalagenda	Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV), www.bmuv.de | Digitalisierung-Digitalagenda
Nutzungsrechte	8.2	siehe IT-Beschaffungen, EVB-IT	
P			
Personalbedarfsermittlung	6	Organisationshandbuch	BMI, www.orghandbuch.de (Startseite)
		Leitsätze für die Personalbedarfsermittlung	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Personalbedarfsermittlung
Positionspapier Aktenführung- und E-Akte	3	Positionspapier Aktenführung- und E-Akte	Rechnungshöfe des Bundes und der Länder, z. B. www.bundesrechnungshof.de | Positionspapier Aktenführung

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Problem Management	7.3		Der ITIL-Prozess Problem-Management hat das Ziel, Ursachen für eine oder mehrere Störungen zu ermitteln sowie Wege zu deren Behebung und Vorbeugung zu finden.
Q			
Qualitätsmanagement	8.1	Qualitätsmanagementsysteme - Grundlagen und Begriffe (DIN EN ISO 9000)	DIN, ISO
R			
Rahmenwerke	6	siehe IT-Servicemanagement und IT-Servicemanagement	Rahmenwerke bezeichnet in der IT einen sektoren- und branchenunabhängigen Überbau für die IT-Ablauforganisation, der Prinzipien, Konzepte, einheitliche Terminologie sowie Anleitungen und Hilfestellungen auf Basis langer (Fach-)Studien und Diskussionen bereitstellt.
		ISO 27001; Detaillierter: BSI-Grundschutz	BSI, BSI - IT-Grundschutz (bund.de) BSI - veröffentlichte Profile (bund.de)
		ITIL, Verfeinerung der ISO 20000	AXELOS, www.axelos.com | ITIL®, PRINCE2® and MSP® siehe auch it-processmaps.com | ITIL 4 | IT Process Wiki
		COBIT,	Verfeinerung der ISO 38500 ISACA, ISACA Germany Chapter e. V. www.isaca.org, www.isaca.de
		Standardfamilie für ein „leichtgewichtiges IT Service Management“ (FitSM)	Frei verfügbare Ergebnisse des EU-geförderten Projekts „Implementing service management in federated e-Infrastructures“ (FedSM), www.fitsm.eu | Downloads
		siehe Datenschutz	

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
Ressortprinzip	6		Aufgabenverteilungen der Regierungen nach Richtlinienkompetenz, Ressortprinzip und Kollegialprinzip
		Grundgesetz Art. 65 und vergleichbar Landesverfassung	www.gesetze-im-internet.de | Art 65 GG
Revisionsfähigkeit	3	IT-Grundschutz, Grundschutzkompendium DER.3.2 (Revision auf Basis des Leitfadens IS-Revision) mit Umsetzungshinweisen	www.bsi.bund.de | Revision auf Basis
		BSI Leitfaden für die Informationssicherheitsrevision (IS-Revision)	www.bsi.bund.de | Leitfaden IS-Revision
		Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)	BMF, www.bundesfinanzministerium.de | GoBD
		Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)	IDW
		Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3)	IDW
		Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PS 330)	IDW
		§ 9 BDSG i. V. m. der Anlage zu § 9 und vergleichbare Landesvorschriften	www.gesetze-im-internet.de | BDSG
Risikomanagement	5, 7.4, 8.1	BSI-Standard 200-3: Risikomanagement	BSI www.bsi.bund.de | Standard 200-3
		Organisationshandbuch	BMI www.orghandbuch.de | Risikomanagement
		Informationssicherheits-Risikomanagement (ISO/IEC 27005)	DIN, ISO

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		Risikomanagement — Leitfaden zur Implementierung der ISO 31000 (ISO/TR 31004)	DIN, ISO
		COBIT 5 for Risk, COBIT 2019	ISACA
		Risikoanalyse bei automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen	Verwaltungsvorschriften Nr. 6.3 zu §§ 70 bis 72 und 74 bis 80 BHO und vergleichbare Landesregelungen, z. B. www.verwaltungsvorschriften-im-internet.de | VV-ReVuS
S			
Schutzbedarfsfeststellung	4	BSI-Standard 200-2, IT-Grundschutz-Methodik, hier Nr. 7.5: Schutzbedarfsfeststellung	BSI, www.bsi.bund.de | 200-2
		Modell XT (Bund), Checkliste für das Interview zur Schutzbedarfsfeststellung, hier Nr. C.1.10.4: Schutzbedarfsfeststellung	CIO Bund, www.cio.bund.de | V-Modell XT, www.cio.bund.de | V-Modell XT Bund
Service Desk	7.3		Der Service Desk bildet die zentrale operative Schnittstelle zwischen Benutzerinnen und Benutzern und der IT-Organisation.
Service Level Management	7.3		Der ITIL-Prozess Service Level Management hat das Ziel, IT-Dienstleistungen zu definieren, zu überwachen und zu optimieren.
Stand der Technik	4, 7.1	Handbuch der Rechtsförmlichkeit, Rd-Nr. 256	Bundesjustizministerium, www.bmj.de | Handbuch der Rechtsförmlichkeit
		Handreichung zum „Stand der Technik“ im Sinne des IT-Sicherheitsgesetzes und der Datenschutz-Grundverordnung	Bundesverband IT-Sicherheit e.V., Handreichung zum „Stand der Technik“
T			
Test- und Abnahmeverfahren	8.1, 8.2, 8.3	siehe IT-Projektmanagement	

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
V			
verbindliche Vereinbarungen	6		Verbindliche Vereinbarungen entstammt dem IT-Servicemanagement und bezeichnet anspruchsbegründende Zusicherungen mit Rechtscharakter über die wesentlichen Eigenschaften (bspw. Verfügbarkeiten, Antwortzeiten, Reaktionszeiten, Mengen, Preise) der Erbringung von spezifischen IT-Leistungen und dem Vorgehen im Falle einer Abweichung vom vereinbarten Standard.
		siehe IT-Service / IT-Servicemanagement	
Verwaltungsdigitalisierung	3	Digitalstrategie der EU Gestaltung der digitalen Zukunft Europas	Europäische Kommission, www.ec.europa.eu | Deutsch | Ein Europa für das digitale Zeitalter
		Gesetz zur Förderung der elektronischen Verwaltung (EGovG) und vergleichbare Landesvorschriften	www.gesetze-im-internet.de | EGovG
		Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG)	www.gesetze-im-internet.de | OZG
		Digitalstrategie des Bundes und vergleichbaren Strategien in den Ländern	Bundesregierung, www.bundesregierung.de | Digitalstrategie
Vorsorgekonzept	7.5	BSI-Standard 200-4 Hilfsmittel - Dokumentenvorlage für ein Notfallvorsorgekonzept	BSI, www.bsi.bund.de | Vorlage Notfallvorsorgekonzept
W			
Wirtschaftlichkeit und Sparsamkeit / Wirtschaftlichkeitsunter-suchung	2, 8.1	Verwaltungsvorschriften zu § / Artikel 7 der Haushaltsordnungen des Bundes und der Länder	z. B. Verwaltungsvorschriften zur BHO, www.verwaltungsvorschriften-im-internet.de | VV-BHO
		Einführung in Wirtschaftlichkeitsuntersuchungen	BMF, www.verwaltungsvorschriften-im-internet.de | Wirtschaftlichkeitsuntersuchungen

Stichwort	Zu Nr.	Norm, Standard, Empfehlung	Quelle, Bemerkung
		WiBe 5.0, Konzept zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT und vergleichbare Landesregelungen	IT-Rat Bund, Anwendung für die Bundesverwaltung vorgesehen nach Beschluss vom 19.02.2015, www.cio.bund.de | WiBe Fachkonzept IT
		Quellen, Informationen und Einzelbeispiele	WiBe-Team, www.wibe.de | WiBe Quellen
		Erfolgskontrolle in der öffentlichen Verwaltung	Finanzministerium des Landes Mecklenburg-Vorpommern, www.regierung-mv.de | Erfolgskontrolle
		siehe Nachhaltigkeit	
Z			
Zentrale S	4, 6		Der zentralen Stelle sind koordinierende und steuernde Aufgaben innerhalb der Gebietskörperschaft entsprechend der Zuständigkeitsnormen zugewiesen.