Landesrechnungshof Mecklenburg-Vorpommern

Landesrechnungshof Mecklenburg-Vorpommern, Mühlentwiete 4, 19059 Schwerin

Einrichtungen der Landesverwaltung
lt. Verteiler

nur per E-Mail

Bearbeiter: Referat 33
Telefon: +49 (0) 385 74 12 -0
Fax: +49 (0) 385 74 12 -100
E-Mail: poststelle@lrh-mv.de
Ihr Zeichen:
GZ: 33-11.025-21 - 19218/2019

Schwerin, 16. April 2019

Rundschreiben Nr. 1/2019 des Landesrechnungshofes Mecklenburg-Vorpommern
Ordnungsmäßigkeit des Einsatzes von Informationstechnik

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 zur Verfügung gestellt.

Der Landesrechnungshof wird die in seinen Rundschreiben mitgeteilten Feststellungen und Wertungen seiner künftigen Prüfungstätigkeit zugrunde legen und bei den geprüften Stellen als bekannt voraussetzen. Er bittet deshalb die Empfänger, in geeigneter Weise sicherzustellen, dass die Rundschreiben allen Beschäftigten bekannt gemacht werden.

1 Ordnungsmäßigkeit des Einsatzes von Informationstechnik

Ordnungsmäßigkeit des Einsatzes von Informationstechnik (Betrieb von Hard- und Software) umfasst die Einhaltung der einschlägigen gesetzlichen, verwaltungsinternen und vertraglichen Regelungen (IT-Compliance). Insbesondere sind die in der Anlage 1 aufgeführten Rechtsnormen sowie sonstige Regelungen einzuhalten. Abhängig vom Aufgabenbereich können sich zusätzliche Anforderungen aus fachrechtlichen Regelungen ergeben

(z. B. §§ 80-84 SGB X bei der Verarbeitung von Sozialdaten, §§ 84, 88, 90, 91 Landesbeamtengesetz M-V bei der Verarbeitung personenbezogener Daten der Beamten).

Wichtige Regelungen wie z. B. die Festlegung von IT-Landesstandards (§ 15 Abs. 1 E-Government-Gesetz Mecklenburg-Vorpommern, EGovG M-V) und eine IT-Richtlinie (§ 15 Abs. 2 EGovG M-V) sind bisher vom zuständigen Ministerium für Energie, Infrastruktur und Digitalisierung (Energieministerium) nicht erlassen worden. Sobald diese Regelungen erlassen wurden, sind sie ergänzend zu Anlage 1 zu beachten.

2 Dokumentationsanforderungen

2.1 Dokumentationsumfang

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. Diese sollen einen rechtmäßigen Vollzug beim Einsatz von Informationstechnik sicherstellen.

Einrichtungen der Landesverwaltung verarbeiten i. d. R. personenbezogene Daten auf elektronische Weise und haben daher die aufgrund des Datenschutzrechts vorgeschriebenen Dokumentationen zu erstellen.

Im Unterschied zum Datenschutz, der die Perspektive des Betroffenen einnimmt, dient das Informationssicherheitsmanagement in erster Linie dazu, die Vertraulichkeit (insbesondere auch Wahrung von Amts- und Dienstgeheimnissen), Verfügbarkeit und Integrität der organisationseigenen Informationen und Daten sicherzustellen. Staatskanzlei und Ressorts haben gem. IS-Leitlinie M-V ein Mindestsicherheitsniveau auf der Basis des IT-Grundschutzes des Bundesamtes für die Sicherheit in der Informationstechnik (BSI)[1] zu gewährleisten. Einrichtungen der Landesverwaltung haben die nach diesen Regelungen vorgesehenen Dokumentationen zu erstellen.

Werden IT-Verfahren für Anordnungen, Zahlungen, Geldverwaltung und Abrechnung oder Buchführung, Belegung der Buchung, Abschlüsse und Rechnungslegung betrieben, sind die gem. VV Nr. 6 zu §§ 70 bis 80 LHO vorgeschriebenen Dokumentationen zu erstellen.

[1] Beim IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) handelt es sich um eine Sammlung von Standards (z. B. 200-1, 200-2, 200-3) und Katalogen (IT-Grundschutzkompendium), die pauschalisierte Vorgehensweisen zum Schutz der eingesetzten Informationstechnik beschreiben. In einem weiteren Sinn zählen hierzu auch Technische Richtlinien, wie z. B. die TR-RESICAN und sonstige Empfehlungen wie z. B. die Analyse der Telemetriekomponente in Windows 10 mit Konfigurations- und Protokollierungsempfehlungen, soweit diese Dokumente darauf gerichtet sind, die Schutzwerte Vertraulichkeit, Verfügbarkeit und Integrität zu gewährleisten.

Unabhängig von diesen konkreten Vorgaben erfordert allgemein auch die Regelgebundenheit des Verwaltungshandelns den Erlass organisatorischer Regelungen, die sicherstellen, dass die öffentliche Verwaltung gesetzmäßig handelt (Rechtsstaatsprinzip Art. 20 Abs. 3 GG, Compliance[2]).

Die durch den Verfahrensbetreiber zu erstellenden Dokumentationen, deren (Rechts-)Grundlagen und die inhaltlichen Anforderungen an diese Dokumentation sind in der Anlage 2 dargestellt. IT-verfahrensspezifische Regelungen müssen - soweit sie notwendig sind - für jedes einzelne IT-Verfahren erstellt werden. Für zentral genutzte Infrastrukturen und Dienste sowie allgemein gültige organisatorische Regelungen sind übergreifende Dokumentationen zu erstellen.

2.2 Grundsätze der Dokumentation

Aufgrund seiner Prüfungserfahrungen und den Vorgaben aus dem BSI-Grundschutz und dem Standarddatenschutzmodell Baustein 42 hat der Landesrechnungshof Grundsätze für die Dokumentation entwickelt.

2.2.1 Grundsatz der Vollständigkeit und Aktualität

Die Dokumentation ist vollständig und aktuell, wenn alle Verarbeitungsprozesse mit allen rechtlichen Forderungen und allen Daten, Systemen und Prozessen so erfasst sind, dass der Produktivbetrieb einer Organisation hinreichend genau und den tatsächlichen Gegebenheiten entsprechend beschrieben ist und alle Maßnahmen entsprechend dem festgestellten Schutzbedarf mit ihrem Erfüllungsgrad dargestellt sind.

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

Sofern auf Zertifikate des Dienstleisters verwiesen wird (z. B. ISO 27001 Zertifizierung auf Basis von IT-Grundschutz) ist durch den Verfahrensbetreiber zu prüfen, inwieweit der betrachtete Informationsverbund vom Zertifikat abgedeckt ist, Auflagen aus dem Zertifizierungsverfahren erfüllt wurden und die Maßnahmen geeignet und ausreichend sind, die Schutzziele des Verfahrensbetreibers zu gewährleisten.

---

[2] Compliance umfasst alle Ansatzpunkte und Instrumentarien, die die zuverlässige Befolgung von Gesetzen und Regeln durch Organisationen und ihre Mitarbeiter systematisch und nachhaltig gewährleisten sollen (Vgl. Faust, Thomas: Compliance-Management in öffentlichen Verwaltungen, in: Innovative Verwaltung, 10/2013, S. 28.). Hierzu zählt auch die Schaffung von Regelwerken (Verhaltenskodizes).

2.2.2 Grundsatz der Transparenz und Übersichtlichkeit

Die Gesamtdokumentation soll übersichtlich strukturiert sein. Der Bestand an Dokumenten sollte übersichtlich dargestellt sein. Der Kontext, in dem die jeweiligen Dokumente stehen und die Beziehungen der Dokumente untereinander sollten erkennbar sein. Es sollte eine Rahmendokumentation mit Übersicht und Beschreibung des Aufbaus der Dokumentation sowie der Aufbewahrungs- bzw. Speicherorte erstellt werden. Die vorhandenen Dokumente können in einem Dokumentenmodell dargestellt werden. In 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.

2.2.3 Grundsatz der Revisionsfestigkeit

Dokumentationen müssen revisionssicher sein. Der Stand der Dokumentation muss nachgewiesen sein. Nur berechtigte Personen dürfen Änderungen an den Dokumenten vornehmen können. Die Änderungen sind zu dokumentieren. Es sollten Versionierungsregeln erlassen werden.

Die Dokumentation muss in einer angemessenen Zeit 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.

2.2.4 Grundsatz der Angemessenheit und Wirtschaftlichkeit

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

Erstellung und Fortschreibung der Dokumentation sollten durch den Einsatz von IT-Verfahren unterstützt werden. Für die Modellierung des Informationsverbundes und der technischen und organisatorischen Maßnahmen sowie die Dokumentation des Umsetzungsgrades sollte die Basiskomponente verinice.pro eingesetzt werden.

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

3 Auftragsverarbeitung und Outsourcing

Ministerien und Behörden der Landesverwaltung nehmen aufgrund des DVZ-Gesetzes i. d. R. die DVZ M-V GmbH für allgemeine und anwenderbezogene Dienstleistungen in Anspruch. Die DVZ M-V GmbH ist Auftragsverarbeiter i. S. v. Art. 4 Nr. 8 DS-GVO und Outsourcing-Dienstleister i. S. d. IT-Grundschutzkompendiums Baustein OPS.2.1.

Das Ministerium bzw. die Behörde hat ein Sicherheitskonzept für das Outsourcing zu erstellen, in dem die Sicherheitsanforderungen an die DVZ M-V GmbH definiert werden. Die DVZ M-V GmbH hat ebenfalls ein Sicherheitskonzept vorzulegen. Beide sind aufeinander abzustimmen und in einem Gesamtsicherheitskonzept zusammenzufügen. Das Ministerium bzw. die Behörde oder unabhängige Dritte sollten das Gesamtsicherheitskonzept regelmäßig auf seine Wirksamkeit überprüfen.[3]

Die DVZ M-V GmbH ist vertraglich auf die Umsetzung der durch den Verfahrensbetreiber im Sicherheitskonzept entsprechend des Schutzbedarfes festgelegten Maßnahmen sowie des BSI-Grundschutzes zu verpflichten. Die Rechte und Pflichten der Vertragsparteien sowie Rollen und Mitwirkungspflichten zur Erstellung, Prüfung und Änderung des Sicherheitskonzepts sollten schriftlich geregelt sein[4].

[3] Vgl. IT-Grundschutzkompendium, OPS.2.1.A6.

[4] Vgl. ebd., OPS.2.1.A4.

Bei erhöhtem Schutzbedarf bei den Schutzwerten Vertraulichkeit und/oder Integrität sollte mit dem Dienstleister vertraglich vereinbart werden, dass die Vertrauenswürdigkeit des eingesetzten Personals in geeigneter Weise überprüft wird. Dazu sollten gemeinsam Kriterien festgelegt werden.

Die Regelungen zur Auftragsverarbeitung und zum Outsourcing sollten als eigenständige Anlagen zu einem EVB-IT-Vertrag geregelt werden.

4 Planung und Vollzug des IT-Haushalts

Bei Ersatz- und Neubeschaffungen von Hard- und Software sind gem. Nr. 3.12.2 des 1. Bewirtschaftungserlasses 2019 die definierten Standards des IT-Strukturrahmens als Bestandteil der künftigen IT-Richtlinie anzuwenden. Bis zum Inkrafttreten der IT-Richtlinie sind alle Neu- und Ersatzbeschaffungen von Hard- und Software für die Bürokommunikation mit einem Gesamtwert über 10.000 Euro beim Energieministerium, Referat für ressortübergreifende IT-Angelegenheiten vor der Auftragserteilung anzuzeigen. Das Energieministerium gibt eine Einschätzung ab, ob das Beschaffungsvorhaben der in der IT-Richtlinie geplanten Standardsetzung entspricht.

Bei der Haushaltsaufstellung 2020/2021 prüft das Energieministerium gem. Nr. 1.3 IT-Ergänzungserlass[5] bei allen erstmalig beantragten und bisher nicht veranschlagten Einzelmaßnahmen zu IT-Projekten u. a. auch die Einhaltung vorgegebener Standards.

Die IT-Richtlinie gem. § 15 Abs. 2 EGovG M-V ist noch immer nicht in Kraft gesetzt. Damit ist nach den Bewirtschaftungserlassen die Beschaffung von Hard- und Software nur eingeschränkt möglich. Ohne eine Definition der funktionalen Anforderungen an Hard- und Software in den IT-Landesstandards kann nicht sichergestellt werden, dass die beschaffte Hard- und Software zukünftig diesen Anforderungen genügt. Würde Hard- und Software beschafft, die den Standards nicht genügt und daher möglicherweise zukünftig nicht mehr für die geplante Nutzungsdauer eingesetzt werden kann, verstieße dies gegen den Grundsatz der Wirtschaftlichkeit. Größere Ersatz- und Neubeschaffungen sollten daher erst vorgenommen werden, wenn das Energieministerium die IT-Landesstandards festgelegt hat.

Softwareprodukte müssen den Anforderungen aus dem Datenschutzrecht und dem Informationssicherheitsmanagement entsprechen. Vor der Beschaffung ist daher zu prüfen, ob ein bestimmtes Produkt unbedenklich eingesetzt werden kann. Dies gilt insbesondere, wenn Schwachstellen wie z. B. die umfangreiche und intransparente Übermittlung von Da-

[5] Festlegungen zur Aufstellung des Haushaltsplan-Entwurfs 2020/2021 für den Bereich der IT-Ausgaben (IT-Ergänzungserlass): https://cms-lotse.cn.mv-regierung.de/zentrales-it-management/.

ten bei Windows 10 und MS-Office 2016, bekannt sind. 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 gegen den Grundsatz der Wirtschaftlichkeit.

5 Besonderheiten beim Einsatz von Verfahren nach VV Nr. 6 zu §§ 70 bis 80 LHO

Beim Betrieb von IT-Verfahren für Anordnungen, Zahlungen, Geldverwaltung und Abrechnung sowie Buchführung, Belegung der Buchungen, Abschlüsse und Rechnungslegung sind VV Nr. 6 zu §§ 70 bis 80 LHO, die Grundsätze ordnungsmäßiger Buchführung bei Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen (GoBIT-HKR - Anlage 6) und die Verfahrensrichtlinie zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen im Land Mecklenburg-Vorpommern zu beachten. Dies gilt auch für Arbeitsschritte in einem abgesetzten Verfahren (Vorverfahren), wenn die Ergebnisse elektronisch in das zentrale automatisierte HKR-Verfahren übergeben werden. Voraussetzung für die Sicherheit dieser Verfahren ist die vollumfängliche Umsetzung des IT-Grundschutzes des BSI.

Der Betrieb dieser Verfahren bedarf der Einwilligung des Finanzministeriums im Einvernehmen mit dem Landesrechnungshof. Stellt der Landesrechnungshof im Rahmen seiner Prüfung erhebliche Verstöße fest, die nicht innerhalb einer kurzen Frist beseitigt werden, kann er sein Einvernehmen zur Einwilligung überprüfen und dem Finanzministerium empfehlen, seine Einwilligung zurückzuziehen.

gez. Dr. Johannsen gez. Arenskrieger

gez. Fuhrmann gez. Scheeren

Anlagen:

Anzuwendende Rechtsvorschriften und Prüfungsmaßstäbe

Dokumentationsanforderungen beim Einsatz von IT und elektronischer Datenverarbeitung

Anlage 1: Anzuwendende Rechtsvorschriften und Prüfungsmaßstäbe

Beim Einsatz von IT in der elektronischen Datenverarbeitung sind neben fachrechtlichen Anforderungen insbesondere die folgenden Rechtsgrundlagen zu beachten:

- EU-Datenschutz-Grundverordnung (DS-GVO)[1] seit 25. Mai 2018,
- Datenschutzgesetz für das Land Mecklenburg-Vorpommern (Landesdatenschutzgesetz – DSG M-V) n. F., vom 22. Mai 2018[2], in Kraft getreten am 25. Mai 2018
- Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (E-Government-Gesetz Mecklenburg-Vorpommern – EGovG M-V)[3],
- § 3a Landesverwaltungsverfahrensgesetz VwVfG M-V und nach geplanter Änderung des VwVfG M-V: §§ 24 Abs. 1 S. 3, 35a, 41 Abs. 2a,
- eIDAS-Verordnung[4] und Vertrauensdienstegesetz[5],
- Gesetz über die Rechtsstellung des Datenverarbeitungszentrums Mecklenburg-Vorpommern (Datenverarbeitungszentrumsgesetz – DVZG M-V)[6].

Für den Betrieb von Verfahren nach VV Nr. 6 zu §§ 70 bis 80 LHO[7]:

- VV Nr. 6 zu §§ 70 bis 80 LHO a. F. bis zum 18. Juli 2016 i. V. m. Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD),
- VV Nr. 6 zu §§ 70 bis 80 LHO neue Fassung gültig ab 19. Juli 2016[8],
- Grundsätze ordnungsgemäßer Buchführung bei Einsatz von IT-Verfahren im Haushalts-, Kassen und Rechnungswesen – Anlage 6 zu VV Nr. 6 zu §§ 70 bis 80 LHO (GoBIT-HKR) ab 19. Juli 2018[9],

---

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 (Datenschutz-Grundverordnung, DS-GVO), ABl. L 119 vom 4. Mai 2016, S. 1-88. Die DS-GVO ist am 25. Mai 2016 in Kraft getreten und gilt nach einer zweijährigen Übergangsfrist ab dem 25. Mai 2018 unmittelbar in der gesamten Europäischen Union.

2 Datenschutzgesetz für das Land Mecklenburg-Vorpommern (Landesdatenschutzgesetz - DSG M-V), vom 22. Mai 2018, neu gefasst durch das Gesetz zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften im Zuständigkeitsbereich des Innenministerium Mecklenburg-Vorpommern an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, GVoBl. M-V S. 193.

3 Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern (E-Government-Gesetz Mecklenburg-Vorpommern - EGovG M-V) vom 25. April 2016, GVOBl. M-V 2016 S. 198, zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Mai 2018 (GVOBl. M-V S. 192).

4 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. 73-114.

5 Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), geändert durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745).

6 Gesetz über die Rechtsstellung des Datenverarbeitungszentrums Mecklenburg-Vorpommern (Datenverarbeitungszentrumsgesetz - DVZG M-V) vom 1. November 2000, GVOBl. M-V S. 522, zuletzt geändert durch Art. 22 des Gesetzes vom 19. Dezember 2005, GVOBl. M-V S. 640.

7 Für zum Zeitpunkt der Änderung der VV zu §§ 70 bis 80 LHO in Betrieb befindliche Verfahren nach VV Nr. 6 zu §§ 70 bis 80 LHO sind die Vorgaben der folgenden Regelungen spätestens dann zu erfüllen, wenn eine maschinelle Schnittstelle zum HKR- oder Zahlungsverkehrsverfahren des Landes eingerichtet oder das IT-Verfahren wesentlich verändert werden (Nr. 8.2 VerfRi-IT-HKR).

8 Zehnte Änderung der Verwaltungsvorschriften zur Landeshaushaltsordnung Mecklenburg-Vorpommern vom 30. Juni 2016, AmtsBl. M-V S. 797.

9 Ebd.

- Verfahrensrichtlinie zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen im Land Mecklenburg-Vorpommern (VerfRi-IT-HKR)[10].

Weitere Maßstäbe für die Prüfung der Ordnungsmäßigkeit sind:

- Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V)[11],
- Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern (ISM)[12],
- Standards des Bundesamtes für die Sicherheit in der Informationstechnik (BSI):
  - 200-1 Managementsysteme für Informationssicherheit,
  - 200-2 IT-Grundschutzmethodik,
  - 200-3 Risikomanagement und
  - 100-4 Notfallmanagement
  - bzw. bis einschließlich 2017 deren Vorgänger (BSI-Standards 100-1, 100-2, 100-3),
- BSI Grundschutzkataloge bis 31. Januar 2018,
- BSI Grundschutz-Kompendium, 1. Edition, ab 01. Februar 2018,
- Technische Richtlinien des BSI wie z. B. die TR-RESISCAN beim ersetzenden Scannen
- Sonstige Empfehlungen des BSI zur IT-Sicherheit, insbesondere die Analyse der Telemetriekomponente in Windows 10 (Konfigurations- und Protokollierungsempfehlungen),
- Grundsatzpapier zum Informationssicherheitsmanagement der Rechnungshöfe des Bundes und der Länder[13],
- Rundschreiben Nr. 2/2016 des LRH M-V: Informationssicherheitsmanagement vom 11. Januar 2016[14],
- Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (IuK-Mindestanforderungen 2016)[15],

---

10 https://www.regierung-mv.de/Landesregierung/fm/Haushalt/Haushaltsplan/Haushaltsrecht/

11 Ministerium für Inneres und Sport *[jetzt Inneres und Europa]* Mecklenburg-Vorpommern: Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern, IS-Leitlinie M-V, vom 12. Mai 2014:
https://cms-lotse.cn.mv-regierung.de/zentrales-it-management/it-sicherheit/, zuletzt aufgerufen am 28. Juni 2018.

12 Ministerium für Inneres und Sport *[jetzt Inneres und Europa]* Mecklenburg-Vorpommern: Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern (ISM M-V), 12. Mai 2014.
https://cms-lotse.cn.mv-regierung.de/zentrales-it-management/it-sicherheit/, zuletzt aufgerufen am 18. Juni 2018.

13 Quelle: https://www.bundesrechnungshof.de/de/veroeffentlichungen/weitere/informationssicherheitsmanagement-grundsatzpapier-der-rechnungshoefe-des-bundes-und-der-laender-1.

14 http://www.lrh-mv.de/Veröffentlichungen/Rundschreiben/.

15 Quelle: https://www.bundesrechnungshof.de/de/veroeffentlichungen/weitere/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informations-und-kommunikationstechnik/view.

- Rundschreiben Nr. 1/2017 des LRH M-V vom 25. Januar 2017[16],
- Standarddatenschutzmodell der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und die Bausteine des Maßnahmenkatalogs[17].

[16] http://www.lrh-mv.de/Veröffentlichungen/Rundschreiben/.
[17] Das Standarddatenschutzmodell und die Bausteine befinden sich in der Erprobungsphase. https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

Anlage 2: Dokumentationsanforderungen beim Einsatz von IT und elektronischer Datenverarbeitung

Dokument	Grundlage	Beschreibung/ Anforderungen
I Übergreifende Regelungen		
I a Basisregeln		
Hausordnung, Geschäftsordnung/-anweisung, Brandschutzordnung, Geschäftsverteilungsplan, Organigramm	Art. 5 Absatz 2 DS-GVO: Rechenschaftspflicht Art. 24 Absatz 1 DS-GVO: Nachweis DSGVO-konformer Datenverarbeitung	• übergreifende organisatorische Maßnahmen des Datenschutzes festlegen, soweit nicht eigenständig geregelt
	SDM M 42.09	• Organigramm und GVP
	Art. 24 Abs. 1 DS-GVO SDM M42.14	• Dokumentation der Datenschutzorganisation
	IT-Grundschutzkompendium ORP.1.A1 MUSS, R 1	• Verantwortlichkeiten und Befugnisse für sicherheitsrelevante Aufgaben festlegen • verbindliche Regelungen zur Informationssicherheit für verschiedene betriebliche Aspekte übergreifend festlegen • regeln, welche Informationen mit wem ausgetauscht werden und wie diese dabei zu schützen sind
	IT-Grundschutzkompendium ORP1.A2 MUSS, R 1	• für alle Informationen, Geschäftsprozesse, Anwendungen und IT-Komponenten Verantwortliche festlegen
	IT-Grundschutzkompendium ORP.1.A6 SOLL, R 1	• regeln, dass an unbeaufsichtigten Arbeitsplätzen sensible Informationen und IT-Systeme nicht frei zugänglich sein dürfen
Übersicht über vorhandene Dokumentation, Regelungen zur Erstellung, Änderung und Aufbewahrung von Dokumentationen	SDM M42.03 bis M42.08 BSI 200-2 Abschnitt 5.2.3 Anforderungen an die Dokumentationen	• Aufbau sowie Gliederung der Dokumentation zum Datenschutz darstellen • Aufbewahrungsorte- und -medien festlegen • Namenskonvention festlegen • Mindestangaben zur Beschreibung der Dokumente (Metadaten) festlegen • Regelung zu Vertraulichkeitsgrad und Zugriffsrechten treffen • Aktualisierungs- und Fortschreibungsregeln festlegen
I b Geschäftsprozessdarstellungen		
Prozesslandkarte	Voraussetzung für Geschäftsprozessdarstellung *Voraussetzung für Qualitätsmanagement*	• Hauptprozesse in ihrer Wirkung als Managementprozesse, Wertschöpfungsprozesse und Supportprozesse grafisch beschreiben
Prozessdarstellungen	IT-Grundschutzkompendium	• Sicherheitsprozess ISMS.1.A13, SOLL, R 1 • Prozess zur Beseitigung von Restinformationen CON.6.A7, SOLL, R 1 • Änderungsmanagement, OPS.1.1.3.A4, SOLL, R 1 • Konfigurationsmanagement, ISMS.1.M9, MUSS

Dokument	Grundlage	Beschreibung/ Anforderungen
		• Identitäts- und Berechtigungsmanagement, ORP.4.A15, SOLL, R 1; ORP.5.A4, SOLL, R 3 • Compliancemanagement, ORP.5.A1, MUSS, R 3 • Prozesse zur Behandlung von Sicherheitsvorfällen, DER.2.1.A7, SOLL • Prozesse zur Meldung, Eskalation und Alarmierung bei Notfällen, BSI 100-4 Nr. 7.1.1
	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 M42.34	• Implementierung und Dokumentation der Prozesse, welche die Aktualität, Vollständigkeit, Eindeutigkeit, Verständlichkeit und Verfügbarkeit der Dokumentationen im Rahmen des SDM gewährleisten
	Nr. 5.1.1 VerfRi-IT-HKR	• Prozess für die Verwaltungen von Berechtigungen (Einrichten, Verändern, Entzug gem. Ordnungsmäßigkeitskonzept) • zu jedem Zeitpunkt muss festgestellt werden können, welche Person zu welchem Zeitpunkt mit welcher Berechtigung ausgestattet gewesen sind
I c Anforderungen der DS-GVO		
Datenschutzleitlinie bzw. -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 Eg. 39 DS-GVO, SDM M42.23	• 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 • darstellen, wie Betroffenenrechte umgesetzt werden sollen
Verzeichnis der Verarbeitungstätigkeiten	Art. 30 DS-GVO SDM M42.22	• Angaben zum Verantwortlichen und zum Datenschutzbeauftragten • fortlaufende Darstellung der Beschreibung der jeweiligen Verarbeitungstätigkeit
Rahmen-Datenschutzkonzept	SDM M42.13	• übergreifende Schutzmaßnahmen darstellen • Verantwortliche und Ansprechpartner benennen
Protokollierungskonzept	SDM 42.33	• regeln, welche Protokolle genutzt und was pro-

Dokument	Grundlage	Beschreibung/ Anforderungen
		tokolliert werden soll • Aufbewahrungsorte, Aufbewahrungsfristen und Zugriffsregelungen festlegen
Darstellung der IT-Infrastruktur	SDM M42.02	• Darstellung aller in die Verarbeitung personenbezogener Daten involvierter Systeme
I d Anforderungen aus dem IT-Grundschutzkompendium des BSI		
Baustein ISM Informationssicherheitsmanagement		
Sicherheitsleitlinie	ISMS.1.A3 MUSS, R 1	• Stellenwert der Informationssicherheit, die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie sowie die Organisationsstruktur für Informationssicherheit beschreiben
	ISMS.1.M3	• 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 Sicherheitsstategie benennen • Leitaussagen zur Erfolgskontrolle treffen • Organisationsstruktur zur Umsetzung des Sicherheitsprozesses beschreiben
Basis- bzw. Rahmensicherheitskonzept (zentrale Infrastruktur und Dienste)	ISMS1.A7 MUSS, R 1	• alle Sicherheitsmaßnahmen systematisch im Sicherheitskonzept dokumentieren
	ISMS.1.M7	• 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 Benutzer, angelegte Benutzergruppen und Rechteprofile dokumentieren
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 (Pass-	ORP.4.A8, MUSS, R 1	• Passwortgebrauch verbindlich vorschreiben • Anforderungen zu Länge und Komplexität so-

Dokument	Grundlage	Beschreibung/ Anforderungen
wortrichtlinie)	ORP.4.A11, SOLL, R 1	wie 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 Benutzer und vergebene Rechte dokumentieren • regeln, dass Benutzer nur auf IT-Systeme und Dienste zugreifen können, wenn sie vorher angemessen identifiziert und authentisiert wurden • Standard-Rechteprofile vorgeben, die den Funktionen und Aufgaben der Mitarbeiter entsprechen • schriftliche Zugriffsregelungen für jedes IT-System und jede IT-Anwendung
Sensibilisierungs- und Schulungsprogramm 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 könne
Richtlinien zum Umgang mit IT- und IoT-Komponenten	ORP.3.A3, MUSS, R 1	• verbindliche, verständliche, aktuelle und verfügbare Richtlinien • in den sicheren Umgang mit den jeweiligen Komponenten einweisen
Darstellung der IT-Infrastruktur	ORP.1.A7, SOLL, R 1	• Darstellung aller Objekte des ITM: Hardware, Netzwerk, Betriebssysteme, Anwendungen, Datenspeicherung, Datenausgabe • dient der Ermittlung der Schutzobjekte im Rahmen von Bedrohungs- und Risikoanalysen
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)
Baustein CON Konzepte und Vorgehensweisen		
Datensicherungskonzept	CON.3.A4 Minimaldatensicherungskonzept MUSS, R 1, CON.3.A6 Datensicherungskonzept SOLL, R 1	• Einflussfaktoren der Datensicherung darstellen, insbes. rechtliche Anforderungen • 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) • 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

Dokument	Grundlage	Beschreibung/ Anforderungen
Baustein OPS Betrieb		
Archivierungskonzept	OPS1.2.2.A2, MUSS, R 3	• technische, rechtliche und organisatorische Einflussfaktoren ermitteln und dokumentieren • Ziele der Archivierung benennen • 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, insbes. auch Abgrenzung zwischen Fach- und Systemadministration vornehmen
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
Schulungsplan IT-Administratoren	OPS.1.1.2.A10, SOLL, R 1	• geeignete Fort- und Weiterbildungsmaßnahmen entsprechend dem aktuellen Stand der Technik und erwarteten technischen Entwicklungen festlegen
Regelungen für Wartungs- und Reparaturarbeiten	OPS.1.1.2.A12, SOLL, R 1	• Regelungen für Wartungs- und Reparaturarbeiten (Sicherheitsaspekte, Verantwortlichkeiten) festlegen
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 regeln
Outsourcing-Strategie	OPS.2.1.A5, SOLL, R 2	• wirtschaftliche, rechtliche, technische, organisatorische und sicherheitsrelevante Rahmenbedingungen definieren • Ziele, Chancen und Risiken des Outsourcing beschreiben • Geschäftsprozesse, Aufgaben oder Anwendungen, die für Outsourcing in Frage kommen festlegen • notwendige Fähigkeiten, Kompetenzen und Ressourcen eines Outsourcing-Dienstleisters definieren • notwendige eigene Fähigkeiten, Kompetenzen und Ressourcen definieren, die vorgehalten werden müssen
Betriebskonzept Outsourcing	OPS.2.1.A11, SOLL, R 2	• Sicherheitsaspekte festlegen • Prüfung der Sicherheitskonzepte der Outsourcing-Partner auf Konsistenz und Aktualität sowie Kontrollen der Sicherheitsmaßnahmen festlegen • Durchführung regelmäßiger Übungen und Tests zur Aufrechterhaltung des Sicherheitsniveaus

Dokument	Grundlage	Beschreibung/ Anforderungen
		festlegen • Informationsfluss bei Sicherheitsvorfällen regeln
Regelungen für den Einsatz des Personals des Outsourcing-Dienstleiters	OPS.2.1.A8, SOLL, R 2	• längerfristig eingesetzte 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.)
Vereinbarung über Anbindung an Netze der Outsourcing-Partner	OPS.2.1.A9, 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
Vereinbarung über Datenaustausch zwischen Outsourcing-Partnern	OPS.2.1.A10, SOLL, R 2	• Sicherheitsmaßnahmen für regelmäßigen Datenaustausch mit festen Kommunikationspartnern festlegen • Datenformate und Vorgehensweise festlegen • Ansprechpartner für organisatorische und technische Probleme sowie sicherheitsrelevante Ereignisse benennen • Verfügbarkeiten und Reaktionszeiten vereinbaren • Zweckbindung der Datennutzung festlegen
Baustein OPS.2.2 Cloud-Nutzung		
Erstellung einer Cloud-Nutzungs-Strategie	OPS.2.2.A1, MUSS, R 2	• Cloud-Nutzungs-Strategie erstellen • Ziele, Chancen und Risiken definieren • rechtliche und organisatorische Rahmenbedingungen sowie technische Anforderungen untersuchen • Machbarkeisstudie für die Nutzung von Cloud-Diensten erstellen • festlegen des Bereitstellungsmodells für zukünftig vom Cloud-Diensteanbieter 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 technische und organisatorische Maßnahmen ändern • Roadmap zur Einführung von Cloud-Diensten planen
Erstellung einer 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

Dokument	Grundlage	Beschreibung/ Anforderungen
		• Definition der Sicherheitsanforderungen an den Cloud-Diensteanbieter • festgelegtes Schutzniveau für Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentieren • Berücksichtigung der länderspezifischen Anforderungen und gesetzlichen Bestimmungen bei Nutzung von internationalen Diensteanbietern
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
Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung	OPS.2.2.A7, SOLL, R 2	• Erstellung eines Sicherheitskonzepts für die Nutzung von Cloud-Diensten auf Basis der identifizierten Sicherheitsanforderungen aus OPS.2.2.A2
Sorgfältige Auswahl eines Cloud-Diensteanbieters	OPS.2.2.A8, SOLL, R 2	• Detailliertes Anforderungsprofil für einen Cloud-Diensteanbieter erstellen • Basis für das Profil ist die Service-Definition für den Cloud-Dienst (OPS.2.2.A3) • Leistungsbeschreibung und Lastenheft erstellen • Service-Beschreibungen des Cloud-Diensteanbieters sorfältig prüfen und hinterfragen
Vertragsgestaltung mit dem Cloud-Dienste-anbieter	OPS.2.2.A9, SOLL, R 2	• vertragliche Regelungen sollen in Art, Umfang und Detaillierungsgrad demSchutzbedarf 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 Sicherheitskonzept für die Cloud-Nutzung (OPS.2.2.A7) auf etwaige Anpassungsbedarfe
Erstellung eines Notfallkonzeptes für einen Cloud-Dienst	OPS.2.2.A11, SOLL, R 2	• Erstellung eines Notfallkonzepts
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
Geordnete Beendigung eines Cloud-Nutzungs-Ver-	OPS.2.2.A14, SOLL, R 2	• Vertrag mit dem Cloud-Diensteanbieter soll geordnete Auflösung des Dienstverhältnisses be-

Dokument	Grundlage	Beschreibung/ Anforderungen
hältnisses		inhalten
Anforderungen bei erhöhtem Schutzbedarf		
Durchführung eigener Datensicherungen	OPS.2.2.A16, SOLL, R 2, (IA)	• Anforderungen an Backupservice detailliert beschreiben
Einsatz von Verschlüs-selung bei Cloud-Nutzung	OPS.2.2.A17, SOLL, R 2, (IA)	• bei Verschlüsselung von Daten durch einen Cloud-Diensteanbieter 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 Benutzerservice, Wartungstermine, Fernwartung, Transport der IT-Geräte und Einführung von Standard-Telearbeitsrechnern, Hard- und Softwareprobleme 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
Baustein APP Anwendungen		
Sicherheitskonzept für den Einsatz von Verzeichnisdiensten SOLL	APP.2.1.A7, SOLL, R 2	• sämtliche sicherheitsbezogene Themenbereiche regeln • Zugriffsberechtigungen, Konfiguration und Konfigurationsänderungen regeln • Trennung administrativer Aufgaben für VD und Verwaltung der Daten festschreiben • Überwachungskonzept (APP.2.1.A.12)
Sicherheitsleitlinie für den Verzeichnisdienst MUSS	APP.2.1.A1, MUSS, R 2	• Regelungen für die Benutzer des Verzeichnisdienstes dokumentieren
Installations- und Konfigurationsanweisung Office-Produkte	APP.1.1.A7, SOLL, R 2	• erstellen und dokumentieren einer an den Bedarf der Institution angepassten Standardkonfiguration
Regelung der Software-Entwicklung mittels Office-Produkten durch Endbenutzer	APP.1.1.A10, SOLL, R 2	• Grundsatzentscheidung, ob Eigenentwicklung erwünscht sind • Verfahren und Verantwortlichkeiten festlegen, Dokumentation vorschreiben, Test und Frei-

Dokument	Grundlage	Beschreibung/ Anforderungen
		gabe regeln
I e Anforderungen beim Ersetzenden Scannen		
Verfahrensdokumentation einschließlich Verfahrensanweisung und Sicherheitskonzept beim ersetzenden Scannen	TR-RESISCAN Anforderung A.G.1 MUSS	• Art der verarbeiteten Dokumente festlegen • Umgang mit nicht verarbeitbaren Dokumenten regeln • Verantwortlichkeiten, Abläufe und Aufgaben im Scanprozess festlegen • Anforderungen an die in den Scan-Prozess involvierten Räume, IT-Systeme, Anwendungen und Sicherungsmittel entsprechend festgelegten Schutzbedarf 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	• festlegen, wer nach dem Berechtigungskonzept scannen darf • Scanzeitpunkt 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		
Notfallleitlinie	BSI 100-4 Nr. 4.4	• die Übernahme der Verantwortung durch die Institutionsleitung dokumentieren • Begriffe definieren, Stellenwert des Notfallmanagements 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 100-4, Nr. 5.5 SDM 42.20	• Kontinuitätsstrategien darstellen • Notfallszenarien und ihre Auswirkungen auf kritische Geschäftsprozess beschreiben • Wiederanlaufanforderungen für die Geschäftsprozesse festlegen • organisatorischen und konzeptuellen Aspekte sowie alle Maßnahmen und Tätigkeiten des

Dokument	Grundlage	Beschreibung/ Anforderungen
		Notfallmanagements, die nicht zur direkten Bewältigung eines Notfalls beitragen, beschreiben
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 100-4 Nr. 7.4	• benötigten Strukturen, Informationen sowie die erforderlichen Maßnahmen und Aktionen nach Eintritt eines Notfalles und zur Wiederaufnahme des Geschäfts zusammenfassen • Sofortmaßnahmeplan, Krisenstabsleitfaden, Krisenkommunikationsplan, Geschäftsfortführungspläne, Wiederanlaufpläne
II Bereichs-/Verfahrensspezifische Regelungen		
II a Vertragliche Regelungen		
Vertrag mit der DVZ M-V GmbH *(oder ggf. anderen Dienstleistern)*	§ 2 Abs. 1 DVZG M-V Bewirtschaftungserlass: Empfehlung EVB-IT Verträge zu nutzen	• Vertragsgegenstand beschreiben (Leistungsbeschreibung als Anlage zum Vertrag) • Vertragsbestandteile dokumentieren • Laufzeit und Kündigungsbedingungen sowie Pflichten nach Vertragsende regeln • Vergütung und Zahlungsbedingungen festlegen • Nutzungsrechte regeln • Haftungsregelungen treffen • zu beachtenden Regelungen zur IT-Sicherheit und ggf. zum Geheimschutz festlegen (Anlagen zum Vertrag) • schriftliche Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO zum Vertragsbestandteil machen (Anlage zum Vertrag)
Leistungsbeschreibung, Service-Level-Agreement (Anlage zum Vertrag)		• detaillierte Leistungsbeschreibung • Verantwortung Leistungserbringer • Verantwortung Leistungsempfänger • Verfügbarkeiten der Services • Reaktionszeiten
schriftliche Vereinbarung zur Auftragsverarbeitung (Anlage zum Vertrag)	Art. 28 Abs. 3 DS-GVO Vertragsbestandteil EVB-IT Vertrag SDM 42.24	• 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 Bstb. a) bis h) DS-GVO
schriftliche Regelung zur Informationssicherheit beim Outsourcing (Anlage zum Vertrag)	OPS.2.1.A4, SOLL, R 2	• Rechte und Pflichten der Vertragsparteien festlegen • 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 ab-	ISMS.1.A6 MUSS, R 1	• Aufgaben, Verantwortung und Kompetenzen im Sicherheitsmanagement durch Arbeitsanweis-

Dokument	Grundlage	Beschreibung/ Anforderungen
lauforganisatorische Regelungen)	ISMS.1.M.6 ISMS.1.M13	ungen und organisatorische Regelungen nachvollziehbar dokumentieren • Arbeitsabläufe, organisatorische Vorgaben und technische Sicherheitsmaßnahmen so dokumentieren, dass Sicherheitsvorfälle durch Unkenntnis oder Fehlhandlungen vermieden werden • sicherheitsrelevanten organisatorischen Maßnahmen festlegen, die erforderlich sind, um technische Sicherheitsdefizite zu kompensieren
	Rechtsstaatsgebot, Compliance: Sicherung rechtskonformer, einheitlicher und personenunabhängiger Aufgabenwahrnehmung Korruptionsprävention Risikomanagement Wirtschaftlichkeitsgebot § 7 LHO: Effizienz des Verwaltungshandelns	• detaillierte Weisungen des Arbeitgebers/ Dienstherrn an seine Arbeitnehmer/Beamte, wie eine bestimmte Arbeitsaufgabe an einem Arbeitsplatz zu verrichten ist (Ausführungsebene) • Verantwortlichkeiten festlegen (Durchführung, Entscheidung, Mitwirkung, Information) • Risiken darstellen und Kontrollen festlegen • als Dienstanweisung oder sonstige schriftliche Weisung erlassen • verbindlich, einheitlich, fachlich geprüft
Anleitungen für Mitarbeiter	ISMS.1.M13	• Merkblätter für den verantwortungsvollen Umgang mit internen Informationen, für die sichere Nutzung von IT-Systemen und Anwendungen sowie zum Verhalten bei Sicherheitsvorfällen • Handbücher und Anleitungen für die eingesetzten IT-Systeme und Anwendungen
Darstellung der durch das IT-Verfahren unterstützten Fachprozesse	Art. 5 Abs. 2 DSGVO Art. 24 Abs. 1 DS-GVO SDM M42.34	• Dokumentation der Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DS-GVO) in den Geschäftsprozessen, bei den personenbezogene Daten verarbeitet werden • Nachweis, das Verarbeitung gem. DS-GVO erfolgt • Darstellung aller in die Verarbeitung personenbezogener Daten involvierter Prozesse und deren funktionale Beschreibung
	ISMS.1.A9, MUSS R 1 ISMS.1.M9	• 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

Dokument	Grundlage	Beschreibung/ Anforderungen
II c Datenschutz		
Beschreibung des Verfahrens als Teil des Verzeichnisses der Verarbeitungstätigkeiten	Art. 30 DS-GVO	• Angaben gem. Art. 30 Abs. 1 Bstb. a bis g DS-GVO, insbesondere Angabe des Verantwortlichen, Verarbeitungszweck, Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten, Löschfristen und Beschreibung der technischen und organisatorischen Maßnahmen gem. Artikel 32 Abs. 1 DS-GVO
Dokumentation der verarbeiteten personenbezogenen Daten, Datenmodell	SDM M42.01	• detaillierte Beschreibung der Struktur und des Syntax der verarbeiteten Daten • Angabe wo Daten verarbeitet, ggf. gelöscht bzw. berichtigt werden
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 42.19	• 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 • festgelegten Sicherheitsmaßnahmen systematisch dokumentieren
vorhabenbezogenes Sicherheitskonzept Outsourcing	OPS.2.1.A6, SOLL, R 2	• individuelles Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben • zusammenführen mit Sicherheitskonzept des Outsourcing-Dienstleisters in einem Gesamtsicherheitskonzept
Rechte- und Rollenkonzept	SDM 42.21	• Zugriffsrechte auf der Basis eines Identitätsmanagements und sicherer Authentisierungsverfahren festlegen
Festlegung benötigter Sicherheitsfunktionen der Fachanwendung	CON.5.A1, MUSS, R 3	• notwendige Sicherheitsfunktionen bei der fachlichen Auswahl und der Integration in die IT-betrieblichen Infrastrukturen und Betriebsprozesse dokumentieren
Dokumentation der Anforderungen an die Anwendung	CON.5.A6, SOLL, R 3	• alle relevanten Anforderungen dokumentieren (Fachkonzept, Lastenheft)
Richtlinien, Arbeitsanweisungen, Handbücher zum Umgang mit der Anwendung	CON.5.A4, MUSS, R 3	• korrekte Nutzung und Administration der Anwendung einschließlich der Sicherheitsfunktionen beschreiben
Installationsanweisung Fachanwendung	CON.5.A3, MUSS, R 3	• benötigte Anwendungsmodule, Installationsreihenfolge und Konfiguration der Anwendungsmodule dokumentieren
Freigabeerklärung	OPS.1.1.6.A4, MUSS, R 1	• prüfen und bestätigen, ob Software gem. den Anforderungen getestet wurde und dabei recht-

Dokument	Grundlage	Beschreibung/ Anforderungen
		liche und organisatorische Vorgaben eingehalten wurden
	Nr. 5.9.3 VerfRi-IT-HKR	• IT-Verfahren fachlich und technisch prüfen und Gewährleistung der Datenintegrität bestätigen
II e Zusätzliche kasssenrechtliche Anforderungen		
Verfahrensdokumentation	Nr. 6.2 VV zu §§ 70 bis 80 LHO Nr. 7.4.1 VerfRi-IT-HKR	• 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 angemessener Zeit nachprüfbar ist • Dokumentation, wie elektronische Belege erfasst, empfangen, verarbeitet, ausgegeben und aufbewahrt werden (Nr. 4 GoBIT-HKR) • Prozessbeschreibung • Versionierung und Änderungshistorie
Ordnungsmäßigkeitskonzept	Nr. 6.4 VV zu §§ 70 bis 80 LHO	• Abgrenzung der Verantwortlichkeiten und Festlegung von Befugnissen (Berechtigungskonzept) • Vier-Augen-Prinzip • Anwendung vollautomatisierter Verfahrensabläufe (Dunkelverarbeitung) • zusätzliche Prüfverfahren oder Sicherheitsmaßnahmen
Prüfliste zur Einhaltung der kassenrechtlichen Vorschriften	Nr. 7.2 VerfRi-IT-HKR	• detaillierte Erklärung darüber, ob und inwieweit kassenrechtliche Vorschriften eingehalten werden
Dokumentation der Verantwortungsbereiche	Nr. 5.1.2 VerfRi-IT-HKR	• Dokumentation der Übertragung der im Ordnungsmäßigkeitskonzept festgelegten Verantwortungsbereiche und Zugriffsberechtigungen durch BfH
Bescheinigung der Verantwortungsbereiche	Nr. 5.1.3 VerfRi-IT-HKR	• schriftliche oder elektronische Dokumentation der ordnungsgemäßen Wahrnehmung der Verantwortungsbereiche gem. Ordnungsmäßigkeitskonzept
Antrag auf Einwilligung gem. VV Nr. 6 zu §§ 70-80 LHO	Nr. 8.3 VerfRi-IT-HKR	• Vordruck 8 (Anlage 4 VerfRi-IT-HKR)
Testbescheinigungen	Nr. 6.4 VerfRi-IT-	• Bescheinigung des LAF über den Batch-Input-Test • Bescheinigung des Finanzministeriums über den Test der Schnittstelle zwischen Fachverfahren und CBPay
Erhebungsbogen IT-Verfahren	Nr. 10.3 VerfRi-IT-HKR Anlage 5 VerfRi-IT-HKR	• jährliche Berichtspflicht bis zum 30.3 des Jahres
Nachweis der Änderung genehmigter IT-Verfahren	Nr. 7.3, 10.2 VerfRi-IT-HKR	• Änderungen beschreiben und mit der Änderung verbundene Risiken analysieren
Nachweis Programmidenti-	Nr. 5.10 VerfRi-IT-HKR	• kontrollieren, ob das eingesetzte IT-Verfahren

Dokument	Grundlage	Beschreibung/ Anforderungen
tät		dem dokumentierten und genehmigten Verfahren entspricht
Wartungsvertrag	Nr. 5.9.4 VerfRi-IT-HKR	• sicherstellen, dass Programmfehler oder Sicherheitslücken in angemessener Zeit beseitigt werden
II f Risikomanagement		
Risikobewertung	EG 76, Art. 24, 32 DS-GVO	• 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
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
Gefährdungsanalyse	Nr. 6.3 VV zu §§ 70 bis 80 LHO Nr. 7.4.2 VerfRi-IT-HKR	• Risiken, Sicherheitsmaßnahmen zur Risikoverringerung, verbleibende Eintrittswahrscheinlichkeit und potenzielle Schadenshöhe beschreiben • Verzicht auf weitergehende Schutzmaßnahmen erläutern

	übergreifend
	Datenschutz
	Informationssicherheitsmanagement
	Haushaltsrecht

Die dargestellten Anforderungen aus dem BSI Grundschutz (Informationssicherheitsmanagement) umfassen die Basis- und Standardanforderungen. Erhöhte Anforderungen können zusätzliche Dokumentationen erforderlich machen. Aufgeführte sind die Anforderungen aus den einzelnen Bausteinen (A). Zusätzlich sind Angaben zu den notwendigen Inhalten der Dokumente aus den Umsetzungshinweisen zum Baustein (M) aufgeführt, soweit vorhanden.

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.