Verwaltungsvorschrift des Ministeriums für Inneres, Digitalisierung und Migration über IT-Standards des Landes (VwV IT-Standards)

Vom 26.11.2018 - Az.: 5-0272.1/34 –

INHALTSÜBERSICHT

1 Ziele, Rechtsgrundlage und Geltungsbereich

2 Begriffsbestimmungen

3 Übergreifende Architekturvorgaben

4 Vorgaben zur Geschäftsarchitektur

5 Vorgaben zur Anwendungsarchitektur

6 Vorgaben zur System- und Sicherheitsarchitektur

7 Technische Spezifikationen

8 Nutzung vorgegebener Entwicklungslinien

9 Standards zum Management von IT-Projekten

10 Übergangs- und Schlussvorschriften

1 Ziele, Rechtsgrundlage und Geltungsbereich

1.1 Ziel der vorliegenden Verwaltungsvorschrift ist es, die Entwicklung der IT-Gesamtarchitektur der Landesverwaltung mithilfe allgemeiner Entscheidungshilfen sowie konkreter Vorgaben zu steuern. Architekturrelevante Fragestellungen sollen innerhalb der Landesverwaltung nach einheitlichen Kriterien transparent und nachvollziehbar beantwortet werden. Hierzu ist es notwendig, über Fragen des Technologieeinsatzes hinaus, ressortübergreifend einheitliche Steuerungsmechanismen für die Beauftragung und Umsetzung von IT-Vorhaben

festzulegen. Nur so lassen sich vorhabenbezogene Architekturentscheidungen abstimmen sowie deren Einhaltung überwachen.

1.2 Diese Verwaltungsvorschrift gilt für alle Vorhaben der Landesverwaltung, die eine Neuentwicklung von Anwendungssystemen, ein Redesign bestehender Systeme oder die Beschaffung und Integration neuer IT-Systeme vorsehen. Sie ist bei der Umsetzung von IT-Vorhaben der Landesverwaltung von allen beteiligten Rollen (Projektleitung, Systemarchitekturverantwortliche etc.) verpflichtend anzuwenden. Begründete Ausnahmen bilden bundesrechtliche oder europarechtliche Vorgaben oder Vorgaben im Rahmen einer Kooperation mit Bund, Ländern, Kommunen oder Regionalverbänden. Auf Verfahren, die in länderübergreifenden Verbünden definiert werden, ist diese Verwaltungsvorschrift nicht anwendbar.

1.3 Rechtsgrundlage für die Verwaltungsvorschrift ist § 21 Nummer 1 des E-Government-Gesetzes Baden-Württemberg (EGovG BW) in Verbindung mit § 24 Absatz 2 Variante 2 EGovG BW. Diese Verwaltungsvorschrift gilt mit Ausnahme des Rechnungshofs und der Steuerverwaltung für alle Dienststellen und Einrichtungen der unmittelbaren Landesverwaltung, einschließlich der Gerichte sowie für die rechtlich selbstständigen Einrichtungen nach § 2 Absatz 2 Nummer 4 bis 7 des Errichtungsgesetzes BITBW (BITBWG). Für Landesbetriebe finden die Nummern 9.1 bis 9.5 keine Anwendung, soweit Haushaltsmittel für diese nicht vom informationstechnischen Gesamtbudget erfasst sind.

1.4 Eine Detaillierung und Begründung der Vorgaben dieser Verwaltungsvorschrift befindet sich in dem Dokument „IT-Architekturrichtlinie und IT-Standards des Landes Baden-Württemberg“. Eine webbasierte zielgruppenspezifische Fassung wird aufgebaut.

2 Begriffsbestimmungen

2.1 Eine **Anwendungssoftware** stellt den softwaretechnischen Teil zur Unterstützung einer fachlichen Aufgabe innerhalb eines Anwendungssystems dar. Bei einer Anwendungssoftware handelt es sich um den fachlichen Programmcode und somit um eine Fachanwendung. Zusammen mit der Basissoftware bildet es das Softwaresystem.

2.2 Ein **Anwendungssystem** umfasst die software- und hardwaretechnischen Komponenten zur Unterstützung eines bestimmten Aufgabengebiets und setzt

sich somit aus einem Softwaresystem und einem Hardwaresystem zusammen. Im Unterschied zum Informationssystem bildet ein Anwendungssystem nicht notwendigerweise die Vollständigkeit der Interaktion des Benutzers mit dem Hard- und Softwaresystem ab. Bei einem Anwendungssystem handelt es sich um den informationstechnischen Teil eines Fachverfahrens.

2.3 Die **Anwendungsarchitektur** beschreibt die grundlegende Organisation eines Anwendungssystems, bestehend aus Komponenten und ihren Beziehungen.

2.4 Eine **Anwendungslandschaft** ist die Gesamtheit aller Anwendungssysteme innerhalb einer Organisation.

2.5 Als elektronische **Archivierung** wird die datenbankgestützte, langzeitige, sichere und unveränderbare Aufbewahrung reproduzierbarer Informationsobjekte verstanden. Gemäß Landesarchivgesetz (LArchG) wird mit diesem Begriff der Transfer von archivwürdigen Informationen und Daten als Archivgut an das Landesarchiv bezeichnet. Archivgut sind Informationen, die zur Erfüllung der Aufgaben der Behörden nicht mehr erforderlich sind und die wegen ihres historischen oder rechtlichen Werts auf Dauer zu erhalten sind.

2.6 **Basissoftware** ist der Teil eines Softwaresystems, der fachlich unabhängigen Programmcode beinhaltet.

2.7 Ein **Basissystem** ist ein Hard- und Softwaresystem, das nicht-fachspezifische Funktionen ressortübergreifend zur Verfügung stellt.

2.8 Das **Business Continuity Management** ist eine Managementmethode, die anhand eines Lebenszyklus-Modells die Fortführung der Geschäftstätigkeit unter Krisenbedingungen oder zumindest unvorhersehbar erschwerten Bedingungen absichert. Dabei handelt es sich um eine Sammlung von Maßnahmen und Prozessen, die den Fortbestand der Geschäftstätigkeit einer Organisation im Störungsfall sicherstellen und das mit der Störung verbundene Schadenspotenzial minimiert.

2.9 Ein **Dienst** stellt eine technische, eigenständige Einheit dar, die logisch zusammenhängende Funktionalitäten bündelt und diese über eine wohldefinierte Schnittstelle zur Verfügung stellt. Darüber hinaus sind in einem entsprechenden Servicevertrag (Service Contract) für die Nutzung relevante Richtlinien und Rahmenparameter hinterlegt (zum Beispiel bezüglich Performanz, Verfügbar-

keit etc.) Ein Dienst wird mittels eines entsprechenden Anwendungs- oder Basissystems implementiert (je nachdem ob die dort gebündelten Funktionalitäten fachspezifisch oder fachunabhängig sind).

2.10 Eine **Domäne** bezeichnet im Sinne dieser Verwaltungsvorschrift ein Fachgebiet.

2.11 Ein **Fachverfahren** ist ein fachspezifisches Verfahren, das in der Regel durch ein Anwendungssystem unterstützt wird.

2.12 Die **Geschäftsarchitektur** beschreibt das Zusammenwirken von Geschäftsobjekten und Geschäftsprozessen zum Erreichen der Geschäftsziele.

2.13 Ein **Grundverfahren** ist ein Fachverfahren, das innerhalb mehrerer Fachgebiete verwendet werden kann.

2.14 Ein **Informationssystem** ist ein aus Hard- und Softwarekomponenten bestehendes Anwendungssystem, das für ein fachliches Aufgabengebiet die Vollständigkeit der Mensch-Technik-Interaktion zur Lösung der betrieblichen Aufgaben abbildet. Bei einem Informationssystem handelt es sich um die technische Umsetzung eines Fachverfahrens.

2.15 Die **IT-Architektur** ist neben der Geschäftsarchitektur der Teil der Unternehmensarchitektur, der die fachliche Struktur der Anwendungslandschaft einschließlich der zugrundeliegenden software- und hardwaretechnischen Komponenten beschreibt.

2.16 Eine **Langzeitspeicherung** bezeichnet die Aufbewahrung von Informationen über die Lebensdauer von Hard- und Software hinaus, jedoch mit einer definierten Aufbewahrungsfrist. Sie ist ein Teilaspekt einer Archivierung.

2.17 Ein **Softwaresystem** setzt sich aus Anwendungssoftware und zugeordneter Basissoftware zusammen.

2.18 Eine **Stored Procedure** bezeichnet eine programmierte Abfolge fachlicher Funktionen innerhalb eines Datenbankmanagementsystems.

2.19 Aufgabe der **Unternehmensarchitektur** ist es, den Einsatz der Informationstechnologie optimal auf die Aufgaben und Ziele aller Fach- und Querschnitts-

domänen auszurichten. Sie bildet eine ganzheitliche Sicht auf die Geschäftsarchitektur und die zugrunde liegende IT-Architektur.

2.20 Für **IT-Projekte, den laufenden IT-Betrieb** und **IT-Vorhaben** gelten die Nummern 2.4, 2.5 und 2.6 VwV IT-Organisation vom 7. Juni 2016 (GABl. 2016, 518) in ihrer jeweils geltenden Fassung.

3 Übergreifende Architekturvorgaben

3.1 Frühzeitige und vollständige Berücksichtigung der rechtlichen Rahmenbedingungen

Rechtliche Rahmenbedingungen sind bereits bei der Planung von Anwendungssystemen zu berücksichtigen.

3.2 Verwendung von Standards und einheitlichen Methoden

Für die Entwicklung und den Betrieb von IT-Systemen sind standardisierte Vorgehensmodelle sowie einheitliche Architekturen, Middleware-Komponenten und Software-Bibliotheken zu verwenden, die wiederrum standardisierte Schnittstellen bereitstellen. Auf die Einhaltung gängiger Best-Practices ist zu achten.

3.3 Gewährleistung der Informationssicherheit, des Datenschutzes, des Geheimschutzes und der Informationsfreiheit

Die geltenden Vorgaben zur Informationssicherheit, insbesondere der VwV Informationssicherheit und zum Datenschutz sowie die Regelungen zum Geheimschutz sind frühzeitig bei der Planung und Konzeption wie auch bei Ausschreibungen anzuwenden sowie nach dem jeweils aktuellen Stand der Technik während des Designs (zum Beispiel „Security by Design“ Prinzipien), der Umsetzung und dem Betrieb einzuhalten und deren Anwendung zu dokumentieren. Dabei muss insbesondere der Schutz der Integrität, Verfügbarkeit und Vertraulichkeit der verarbeitenden Daten und Informationen entsprechend dem zuvor fachlich festgelegten Schutzbedarf gewährleistet sein.

Weiterhin sind für das Anwendungssystem beziehungsweise die darin verarbeiteten oder erzeugten Daten die gegebenenfalls geltenden Vorgaben zur Informationsfreiheit zu beachten (zum Beispiel Landesinformationsfreiheitsgesetz).

3.4 Berücksichtigung von Referenzarchitekturen

Bei der Konzeption und Entwicklung von Anwendungssystemen sind die für die Landesverwaltung festgelegten Referenzarchitekturen vorrangig zu berücksichtigen. Sofern keine für das zukünftige Anwendungssystem geeignete Referenzarchitektur vorliegt, sind nach dem jeweils aktuellen Stand der Technik für diese Klasse der Anwendungssysteme entsprechende Architektur- und Entwurfsmuster zu nutzen.

3.5 Sicherstellung von Benutzerfreundlichkeit und Barrierefreiheit

Anforderungen an die Ergonomie von Informationssystemen, insbesondere der Norm DIN EN ISO 9241, sind bereits in der Planung zu berücksichtigen. Mediale Angebote der Landesverwaltung sind entsprechend der Maßgaben des Landes-Behindertengleichstellungsgesetzes vom 17. Dezember 2014 (GBl. S. 819) in der jeweils geltenden Fassung, barrierefrei zu gestalten.

3.6 Vermeidung von Herstellerabhängigkeiten

Der Technologieeinsatz in der Landesverwaltung ist so zu konzipieren und umzusetzen, dass Abhängigkeiten zu Herstellfirmen minimiert werden. Soweit möglich sollen daher bei Entwicklung und Betrieb offene Standards oder Branchenstandards eingesetzt werden und enge Kopplungen an proprietäre Systeme vermieden werden. Hierzu zählen neben (umfangreichen) Anwendungssystemen bspw. herstellerspezifische Erweiterungen von Application Servern, Datenbankmanagementsysteme (insbesondere Stored Procedures), proprietäre Softwarebibliotheken etc. Bei Individualentwicklungen durch externe dienstleistende Personen oder Unternehmen ist darauf hinzuwirken, dass der zugehörige Quelltext der Landesverwaltung möglichst unter einer von der OSI anerkannten OpenSource-Lizenz für die weitere Entwicklung und Nutzung zur Verfügung steht. Soweit der Einsatz herstellerspezifischer Funktionen erforderlich ist, sollten diese soweit möglich so gekapselt werden, dass ein späterer Austausch erleichtert wird. Darüber hinaus ist für Anwendungen grundsätzlich sicherzustellen, dass ein Wechsel des angebotsstellenden Unternehmens mit vertretbarem Aufwand möglich ist.

3.7 Gewährleistung der Interoperabilität von Anwendungen und Diensten

Anwendungen und Dienste sind derart zu konzipieren, dass ihre Kommunikation mit anderen Systemen über standardisierte Protokolle und Beschreibungssprachen erfolgen kann. Die Interoperabilität wird durch den Einsatz geeigneter Austauschformate und Serviceschnittstellen hergestellt. Es sollten jeweils anerkannte Internet-Standards verwendet werden.

3.8 Sicherstellung von loser Kopplung / Modularität

Synchrone Kopplungen zwischen Anwendungssystemen sind auf ein notwendiges Minimum zu reduzieren. Asynchrone technische Verfahren, die eine zeitliche Entkopplung erlauben, sind synchronen technischen Verfahren vorzuziehen. Dies ist bereits in der technischen Konzeption der Fachverfahren zu berücksichtigen. Insbesondere eine enge Kopplung von Anwendungssystemen über einen Direktzugriff auf eine gemeinsame Datenbank ist nicht erlaubt. Stattdessen sind entsprechende Aufrufe über eine separate Zugriffsschicht abzubilden.

3.9 Gewährleistung einer nachhaltigen Informationstechnik

Für den gesamten Lebenszyklus von IT-Systemen ist eine umweltschonende und nachhaltige Nutzung zu berücksichtigen. Dies schließt die Beschaffung energieeffizienter IT-Geräte, den ressourcenschonenden Betrieb sowie die umweltverträgliche Aussonderung ein.

3.10 Reduzierung der Komplexität auf ein notwendiges Maß

Die Komplexität von Anwendungssystemen selbst, als auch die Komplexität bzgl. ihrer Interaktion mit anderen Systemen ist so gering wie möglich zu halten. So sind Anwendungssysteme derart zu konzipieren und umzusetzen, dass sie auch für andere Entwickelnde verständlich und wartbar sind. Dies schließt sowohl die Dokumentation des Quelltextes als auch die Art und Weise der Programmierung ein (zum Beispiel Verschachtelungstiefe, eindeutige Schnittstellen, Typsicherheit, Kapselung, Fassadenzugriff). Abhängigkeiten zu entfernten Systemen sind soweit wie möglich gering zu halten.

3.11 Qualitätssicherung und automatisierte Tests

Zur Unterstützung der Qualitätssicherung sind automatisierte Tests wie Modul- und Regressionstests mit ausreichender Testabdeckung zu verwenden. Die

Tests sollten auch die Einhaltung der Regelungen zur Code-Komplexität sowie von üblichen Best Practices überprüfen.

3.12 Verwendung von Standardbibliotheken

Soweit möglich, sind etablierte Standardbibliotheken und -Komponenten in einer aktuellen Version, die alle Sicherheitsmaßnahmen und Fehlerbehebungen einschließt, zu verwenden. Änderungen oder Ergänzungen an unter Open-Source-Lizenz stehenden Bibliotheken sind zu vermeiden.

3.13 Sicherstellung der Wirtschaftlichkeit von Architekturen und korrespondierenden Vorhaben

Architekturentscheidungen erfolgen auf der Grundlage einer transparenten Wirtschaftlichkeitsbetrachtung, die den fachlichen Nutzen der Lösung, den Lebenszyklus des IT-Systems und dessen Rolle innerhalb der gesamten Anwendungslandschaft der Landesverwaltung berücksichtigt. Sie sind immer im Gesamtkontext der Landes-IT zu treffen.

IT-Systeme sind im jeweiligen fachlichen Anwendungsbereich darüber hinaus derart zu dimensionieren, dass funktionale und nicht-funktionale Anforderungen einerseits nicht übererfüllt werden, andererseits sie jedoch eine spätere Skalierung erlauben.

3.14 Vorgehensmodelle zur Umsetzung von Anwendungssystemen

Für die Umsetzung von Anwendungssystemen muss ein zum Projektmanagement passendes Vorgehensmodell zur Softwareentwicklung eingesetzt werden. Hierbei ist für zugehörige Wartungsaufgaben (unter Wartungsaufgaben wird neben den Kategorien „Korrigierende Wartung“, „Anpassungswartung“, „Perfektionierende Wartung“, „Unterstützung und Betreuung“ auch die Kategorie „Funktionserweiterung“ verstanden) der Softwarelebenszyklus zu beachten, d. h. die für ein Anwendungssystem relevanten IT-Prozesse und die über eine initiale Bereitstellung hinaus gegebenenfalls notwendigen Softwareentwicklungsarbeiten (Fehlerbereinigung, Weiterentwicklung etc.).

3.15 Architekturmanagementprozess

Die ressortübergreifende Definition und Umsetzung der Architekturvorgaben, Referenzarchitekturen und technischen Spezifikationen sowie die Sicherstellung deren Einhaltung erfolgt innerhalb eines Architekturmanagementprozesses durch ein Architekturboard, das sich im monatlichen Turnus aus den Domänenarchitekturverantwortlichen des Landes zusammensetzt. Nähere Bestimmungen zum genauen Verfahren finden sich in Anlage 1 zu dieser Verwaltungsvorschrift.

4 Vorgaben zur Geschäftsarchitektur

4.1 Dokumentation von Verwaltungsprozessen

Zur Dokumentation von Verwaltungsprozessen sind landeseinheitliche Modellierungssprachen und geeignete grafische Notationen zu verwenden. Eine Auflistung dieser findet sich in Anlage 1 zu dieser Verwaltungsvorschrift.

Dokumentationsbedarf besteht insbesondere

- für verwaltungsübergreifende Geschäftsprozesse
- für Prozesse, die personenbezogene Daten verarbeiten,
- für Verfahren, die eine systemtechnische Workflowsteuerung beinhalten,
- sowie für Verfahren, für die aktuell oder zukünftig eine Prozessmodellierung stattfindet oder stattfinden soll.

Bei der Modellierung ist auf einen geeigneten und allgemein verständlichen Detaillierungsgrad zu achten.

4.2 Vorgaben zum Informationsaustausch (fachlich / semantisch)

Für Verfahren, die Daten für andere Verfahren zur Verfügung stellen, ist eine semantische Beschreibung der Austauschdaten anzufertigen.

5 Vorgaben zur Anwendungsarchitektur

5.1 Nutzung von Anwendungen und Diensten

Die ressortübergreifende Nutzung von Grundverfahren der Landesverwaltung einschließlich der zugrunde liegenden Anwendungssysteme sowie von Anwendungen beziehungsweise Diensten für Querschnittsfunktionen ist zu prüfen. Eine verbindliche Nutzung setzt ein transparentes Freigabeverfahren sowie die Benennung einer für das Verfahren beziehungsweise Produkt verantwortlichen Person voraus. Nähere Bestimmungen zu den zu beachtenden Entwicklungslinien finden sich in Anlage 1 zu dieser Verwaltungsvorschrift.

5.2 Dokumentation der Anwendungsarchitektur

Für jedes Anwendungssystem ist während der Konzeptionsphase eine Dokumentation der Anwendungsarchitektur zu erstellen. Diese enthält mindestens eine Darstellung der

- entwickelten beziehungsweise verwendeten Komponenten und Module einschließlich ihrer Funktion und Verteilung auf spezifische Netzwerksegmente (DMZ etc.),

- bereitgestellten Schnittstellen und allen Schnittstellenaufrufen zu entfernten Komponenten,

- genutzten (Querschnitts-)Dienste,

- begründeten Abweichungen und Besonderheiten,

- implementierten Maßnahmen und Mechanismen zur Gewährleistung von Datenschutz und Informationssicherheit oder entsprechende Verweise auf das Sicherheitskonzept

- für das Systemverständnis und für eine Erweiterung relevanten Randbedingungen und übergreifenden Architekturaspekte.

Diese Dokumentation ist während des gesamten Lebenszyklus der Anwendung zu pflegen und bereitzustellen.

5.3 Dokumentation der anwendungsübergreifenden Schnittstellen und zugehörigen Dienste

Anwendungsübergreifend bereitgestellte Dienste und Schnittstellen sind hinsichtlich ihres Leistungsumfangs, ihrer Leistungsqualität sowie den für deren Nutzung relevanten Rahmenbedingungen geeignet zu dokumentieren. Hierzu sind folgende Angaben in Anlehnung an IEC 62304 erforderlich:

- Name und Zweck der Schnittstellenfunktion beziehungsweise des Dienstes,

- Name, Bedeutung und Wertebereiche von Übergabe- und Rückgabeparametern

- Verhalten des Dienstes bei Nutzung der zugehörigen Schnittstellenfunktionen (zum Beispiel hinsichtlich Fehlertoleranz, Performanz, Sicherheit, Robustheit, Zuverlässigkeit etc.)

5.4 Nutzung vorgegebener Entwicklungslinien

Neue Entwicklungsvorhaben der Landesverwaltung, die mit eigenem Fachpersonal durchgeführt werden, sind mittels der vorgegebenen Entwicklungslinien des Landes umzusetzen. Dies gilt ebenso für Entwicklungsvorhaben, die durch Dritte durchgeführt werden und mit entsprechenden Nutzungsrechten des Landes am Quellcode eine Weiterentwicklung ermöglichen. Abweichungen von den vorgegebenen Entwicklungslinien erfordern die Zustimmung der für die IT-Landesarchitektur beauftragten Person. Eine Auflistung der entsprechenden Entwicklungslinien einschließlich der damit verbundenen Entwicklungsstandards befindet sich in Anlage 1 zu dieser Verwaltungsvorschrift.

5.5 Vorgaben zu grafischen Benutzungsschnittstellen

Benutzungsschnittstellen dienen ausschließlich dem Informationsaustausch zwischen Anwendung und System und sind Client-seitig grundsätzlich plattformunabhängig zu konzipieren und umzusetzen. Entsprechend der Zuständigkeitstrennung (Separation of Concerns) sind grafische Benutzungsschnittstellen frei von fachlicher Logik zu implementieren.

5.6 Nutzung von Middleware-Plattformen

Beim Einsatz einer Middleware-Plattform ist die Verwendung der in Anlage 1 zu dieser Verwaltungsvorschrift vorgegebenen und dem jeweiligen Einsatzzweck

entsprechenden Technologie vorzusehen. Der Begriff „Middleware-Plattformen“ bezieht sich im Rahmen dieser Verwaltungsvorschrift insbesondere auf Application Server, Technologien zur Anwendungsintegration (Enterprise Application Integration - EAI) wie Bus-Systeme und Prozess-Engines (Enterprise Service Bus - ESB), Technologien zur asynchronen Kommunikation (Message Oriented Middleware - MOM) und Technologien zur verteilten Kommunikation (Object Request Broker - ORB).

5.7 Berücksichtigung von Virtualisierung und Automatisierung

Methoden zur Virtualisierung von Umgebungen im Sinne einer wirtschaftlichen Betreibbarkeit von Anwendungen sowie Maßnahmen zur Automatisierung des Entwicklungs- und Bereitstellungsprozesses sind bereits in der Konzeptionsphase zu berücksichtigen.

5.8 Berücksichtigung betriebsrelevanter nicht-funktionaler Anforderungen

Betriebsrelevante nicht-funktionale Anforderungen sind bereits während der Konzeptions- und Designphase einer Anwendung mit dem Betriebsdienstleistenden Unternehmen abzustimmen. Hierzu zählen insbesondere Anforderungen an Systemressourcen (u. a. Hardware, virtuelle Maschinen, Peripherie), Skalierbarkeits- und Sicherheitsaspekte etc.

5.9 Festlegungen zu Austauschformaten (technisch / konkret)

Zum Datenaustausch mit Basis- beziehungsweise Anwendungssystemen sind einheitliche beziehungsweise standardisierte Datei- und Datenaustauschformate zu nutzen (siehe Nummer 7.4). Sofern vorhanden, sind darüber hinaus keine proprietären, sondern offene Austauschformate und Standards einzusetzen. Als Leitlinie für solche Austauschformate gilt, dass deren Spezifikation vollständig publiziert wurde und die Publikation entweder kostenfrei oder gegen ein angemessenes Entgelt erhältlich ist sowie dass die Verwendung der Spezifikation für Herstellende und Nutzende der Software-Systeme uneingeschränkt und kostenfrei möglich ist. Herstellerspezifische Erweiterungen bestehender Standards sind, soweit möglich, zu vermeiden.

5.10 Verwendung des Unicode-Standards

Der Standard „Lateinische Zeichen in Unicode“ (String.Latin) ist in der Landesverwaltung zu verwenden. Dieser Standard wird im Auftrag des IT-Planungsrats entwickelt. Die Unicode-Zeichen sind mit UTF-8 zu kodieren. Die Nutzung von Zeichensätzen, die keine vollständige Abbildung von String.Latin erlauben, ist ausgeschlossen. Für IT-Lösungen, die zusätzliche Zeichen erfordern, ist im Einzelfall auch über UTF-8 hinaus der Einsatz einer Erweiterung des Zeichenumfangs zulässig.

6 Vorgaben zur System- und Sicherheitsarchitektur

6.1 Verwendung der Hardware- und Softwarestandards für technische Infrastruktur

Die Standards für Systemarchitekturen und für die technische Infrastruktur sind einzuhalten (siehe Nummer 7.6). In begründeten Fällen kann bei Spezialhardware hiervon abgewichen werden. Solche Abweichungen sind nur nach Zustimmung durch die IT-Landesarchitektin beziehungsweise den IT-Landesarchitekten zulässig.

6.2 Verwendung energieeffizienter und ressourcenschonender Technologien

Bei den eingesetzten IT-Systemen ist über den gesamten Lebenszyklus hinweg – Beschaffung, Nutzung und Weiterverwertung – auf Energieeffizienz und Ressourcenschonung zu achten. Die Regelungen der VwV-Beschaffung sind bei Ausschreibungen zu beachten.

6.3 Vorgaben für das Monitoring (System- und Anwendungs-Monitoring)

Serversysteme sind mit einem einheitlichen Systemmonitoring auszustatten, welches Kennzahlen einzelner Komponenten (zum Beispiel CPU, Speicher, Disk, Netz) zur Laufzeit erfasst und bereitstellt. Darauf aufbauend ist bereits beim Design von Anwendungen und Diensten die Bereitstellung von Kennzahlen zur Laufzeit im Sinne einer Überprüfung und Gewährleistung vorgegebener nicht-funktionaler Anforderungen zu berücksichtigen. Dies beinhaltet ein fachliches Monitoring, das Kennzahlen für die wesentlichen Funktionen des Anwendungssystems beziehungsweise Dienstes in Relation zu den vorhandenen Systemkennzahlen enthält. Für jede Anwendung, die innerhalb der Landesverwaltung entwickelt wird, muss ein angemessenes Monitoringkonzept unter Berücksichtigung der Anforderungen des Betriebs erstellt werden. Für eine Analyse des Verhaltens der Anwendung (fachliches Monitoring) sind verschiedene Log-

ging-Level umzusetzen und zu dokumentieren, die eine Fehlerbehebung im laufenden Betrieb vereinfachen. Das Umsetzungskonzept sollte standardisierte Schnittstellen und sichere Übertragungswege verwenden, so dass Log-Daten durch standardisierte Werkzeuge verarbeitet werden können.

6.4 Vorgaben zur Netzwerkarchitektur

Die Netzwerkarchitektur ist so zu planen und umzusetzen, dass der Schutz von Informationen in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen nach dem jeweils aktuellen Stand der Technik sichergestellt ist. Hierbei sind auch netzwerktechnische Schutzmaßnahmen erforderlich, die den Schutzbedarf innerhalb des Landesverwaltungsnetzes berücksichtigen. Die Sicherheit von übertragener Information, sowohl innerhalb des Landesverwaltungsnetzes als auch mit jeglicher externen Stelle, ist durch geeignete Maßnahmen zu gewährleisten. Bis zu den Außengrenzen der Verwaltungssysteme sind technische Maßnahmen zu ergreifen. Darüber hinaus ist die Sicherheit übertragener Information mittels geeigneter Verträge beziehungsweise Bindungen bei den beteiligten externen Stellen einzufordern.

Zwischen den Subnetzen sind die Kommunikationsprotokolle festzulegen, die zur Kommunikation benutzt werden können und auf den Firewall-Systemen freizuschalten sind. Die damit verbundenen Risiken, sind von den Verantwortlichen der beteiligten Subnetze zu tragen.

Die Domäne *.bwl.de ist die Domäne des Landesverwaltungsnetzes (LVN). Das bedeutet, dass E-Mails mit der Absenderdomäne *.bwl.de nicht aus anderen Netzen in das Landesverwaltungsnetz gesendet werden dürfen und somit verworfen werden. Web-Server mit der Domäne *.bwl.de dürfen nur innerhalb des Landesverwaltungsnetzes verwendet werden. Mailserver sind unter Beachtung der geltenden Vorgaben zur Informationssicherheit zu konfigurieren. Methoden wie die serverseitige Prüfung des Vorliegens einer Sende-Autorisierung für eine Domäne müssen genutzt werden.

An das LVN angeschlossene lokale Netze der Dienststellen dürfen nicht über einen zusätzlichen eigenen Anschluss mit dem Internet verbunden werden. Der zentrale Internet-Zugang der BITBW ist zu nutzen.

6.5 Vorgaben zum Datenschutz

Bei der Konzeption, Umsetzung und dem Betrieb ist nach dem Prinzip „Privacy by Design – Privacy by Default“ zu verfahren, das heißt der Schutz und die Sicherheit personenbezogener Daten muss Standardvorgabe und oberstes Designprinzip sein. Hierfür sind die Vorgaben aus der Datenschutzgrundverordnung (DSGVO) und der Richtlinie (EU) 2016/680 (JI-Richtlinie) umzusetzen. Insbesondere die in Artikel 5 und 25 der Datenschutzgrundverordnung (DSGVO) dargelegten Grundsätze sind nachweisbar einzuhalten. Bereits in der Designphase sollte der oder die Landesbeauftragte für den Datenschutz und die Informationsfreiheit beratend zugezogen werden.

Gemäß Kapitel III der DSGVO sind die Betroffenenrechte und entsprechende Anforderungen (zum Beispiel proaktive Benachrichtigungen gemäß Artikel 13 und Artikel 14 DSGVO, das Auskunftsrecht gemäß Artikel 15 DSGVO sowie Berichtigungs- und Widerspruchsrecht etc.) bei Konzeption, Umsetzung und Betrieb von Anwendungssystemen zu berücksichtigen und gegebenenfalls in Form eines Auftragsverarbeitungsvertrags zu regeln.

Um der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO gerecht zu werden, sind zuständige Datenschutzbeauftragte möglichst frühzeitig einzubinden.

Die Anforderungen an die Sicherheit der Verarbeitung aus Art. 32 DSGVO sind einzuhalten. Es sind technische und organisatorische Maßnahmen nach dem Stand der Technik zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Sensible personenbezogene Daten sind grundsätzlich verschlüsselt zu speichern, so dass auch die Systemadministration ohne weiteres keinen Zugriff auf die Klartext-Daten hat. Datenträger sind grundsätzlich zu verschlüsseln, so dass auch im Falle eines Diebstahls die Vertraulichkeit gewährleistet bleibt.

Für die Kommunikation per E-Mail insbesondere mit Bürgerinnen und Bürgern ist eine Form der gesicherten Kommunikation nach Internet-Standards anzubieten.

Gemäß den Architekturvorgaben zur Gewährleistung der Informationssicherheit, des Datenschutzes, des Geheimschutzes und der Informationsfreiheit sind alle geltenden rechtlichen Anforderungen zu erfüllen. Die hier aufgeführten Aspekte können nicht umfassend alle Bereiche des Datenschutzes abdecken. Anwendungsspezifische Datenschutzbetrachtungen auf Grundlage des jeweils

geltenden Rechts und im Sinne des spezifischen Zweckes der Anwendung sind daher unerlässlich.

6.6 Vorgaben zur Nutzung von extern gehosteten Diensten und Plattformen

Der Einsatz von Diensten und Plattformen, wie zum Beispiel Cloud-Diensten, die außerhalb der Landesverwaltung gehostet werden, erfordert die Zustimmung der für die IT-Landesarchitektur zuständigen Person unter etwaiger Einbeziehung der oder des Informationssicherheitsbeauftragten der Landesverwaltung.

7 Technische Spezifikationen

Nachfolgende Festlegungen und Spezifikationen sind einzuhalten.

7.1 Festlegungen zur Kopplung von Anwendungssystemen

Anwendungssysteme beziehungsweise Basissysteme werden mit Hilfe standardisierter und universell einsetzbarer Kommunikationsprotokolle miteinander gekoppelt. Der Einsatz programmiersprachenspezifischer Protokolle wie zum Beispiel RMI ist nicht zulässig (eine Ausnahme bildet der systemspezifische Remote Function Call (RFC) im SAP-Umfeld). Für die synchrone Kommunikation können folgende Protokolle verwendet werden:

- HTTPs
- RFC
- SOAP über HTTPs
- REST über HTTPs

Die Kommunikation von Anwendungssystemen muss gemäß den jeweils geltenden rechtlichen und notwendigen sicherheitstechnischen Anforderungen abgesichert werden. Dabei ist eine Transportverschlüsselung nach BSI TR-02102-2 zu verwenden.

7.2 Grundausstattung des einheitlichen BK-Arbeitsplatzes

Die Definition des einheitlichen BK-Arbeitsplatzes in seiner Grundausstattung orientiert sich am Pflichtenheft für die Einführung eines Standardarbeitsplatzes für die Landesverwaltung. In dieses Dokument wurden die Ziele und Anforderungen der Ressorts sowie der BITBW an die Grundausstattung aufgenommen und einschließlich der technischen Umsetzung dokumentiert.

7.3 Web-Browser

Standardbrowser innerhalb der Landesverwaltung ist Microsoft Edge. Unter Beachtung der geltenden Vorgaben zur Informationssicherheit ist die Bereitstellung eines alternativen Browsers (Mozilla Firefox oder Google Chrome) für die korrekte Darstellung von webbasierten Inhalten erforderlich. Für sämtliche webbasierten Anwendungen der Landesverwaltung ist sicherzustellen, dass diese unter Verwendung von Microsoft Edge beziehungsweise des Microsoft Internet Explorers korrekt dargestellt und mit vollständigem Funktionsumfang genutzt werden können. Dies betrifft sowohl Eigenentwicklungen der Landesverwaltung als auch Software von Drittanbietern.

Es ist darauf hinzuwirken, dass Anwendungen der Landesverwaltung, die über das Internet für Dritte zugänglich sind, mittels marktüblicher Browser ohne Einschränkungen genutzt werden können.

7.4 Standardisierte Austauschformate

Als Datenaustauschformate für die behördenübergreifende Kommunikation sind bevorzugt zertifizierte XöV-Standards zu verwenden. Eine Übersicht und weiterführende Informationen zu den XöV-Standards finden sich u. a. unter www.xrepository.de (herausgegeben von der für die XöV-Standards verantwortlichen Koordinierungsstelle für IT-Standards – KoSIT).

7.5 IT-Standards für Geoinformationen, Geo-Daten, Geoanwendungen und -diensten

Vorgaben zu Geoinformationen, Geo-Daten und Austauschformaten, Geoanwendungen und -diensten finden sich in Anlage 1 zu dieser Verwaltungsvorschrift.

7.6 Hardware- und Softwarestandards für Server und Clients

Grundlage der auf die funktionalen und nicht-funktionalen Anforderungen der Ressorts ausgerichteten Hardware- und Softwarestandards für Server und Clients ist das zur Erbringung der entsprechenden Leistungen gemäß BITBW IT-Servicekatalog definierte und mit der Stelle für IT-Koordination im Innenministerium abgestimmte Hardware- & Software Portfolio.

7.7 Netzstandards

Es gelten die Vorgaben der „LAN-Konzeption der Landesverwaltung Baden-Württemberg einschließlich Hochschulbereich“ (http://lvn-id-neu.bwl.de/IuK/leitfaeden/Leitfaden_Dokumente/) in der jeweils gültigen Fassung.

8 Nutzung vorgegebener Entwicklungslinien

Soweit vorhanden, sind für landeseigene Entwicklungsvorhaben, die nicht innerhalb länderübergreifender Kooperationen stattfinden, standardisierte Entwicklungslinien zu nutzen. Näheres zu den Entwicklungslinien findet sich Anlage 1 zu dieser Verwaltungsvorschrift.

9 Standards zum Management von IT-Projekten

Die Vorgaben zur Bewertung von IT-Vorhaben und IT-Projekten sowie für deren Planung, Beantragung und Durchführung gemäß Anlage 1 zu dieser Verwaltungsvorschrift sind einzuhalten.

10 Übergangs- und Schlussvorschriften

10.1 Auf am 01.01.2019 bereits produktive Systeme ist diese Verwaltungsvorschrift nicht anwendbar, es sei denn, die Systeme erfahren wesentliche Änderungen. Ob eine wesentliche Änderung vorliegt, entscheidet die IT-Landesarchitektin oder der IT-Landesarchitekt unter Berücksichtigung von Wirtschaftlichkeitsaspekten im Benehmen mit dem Architekturboard sowie der oder dem Vorhabenverantwortlichen und der jeweiligen Systemarchitektin oder dem jeweiligen Systemarchitekten.

10.2 Diese Verwaltungsvorschrift tritt am 01.01.2019 in Kraft. Sie tritt am 31.12.2025 außer Kraft.