AOK Baden-Württemberg
Die Gesundheitskasse.

Dieses Muster dient lediglich zur Ansicht und muss nicht eingereicht werden.

<Installation und Betrieb von Applikation> / Muster – muss nicht eingereicht werden.

Sicherheitskonzept

Muster

Datum	29.01.2015
Version	<0.0.0>
Dokumenteneigner	AOK Baden-Württemberg
Klassifizierung	C_C Vertraulich

INHALTSVERZEICHNIS

1. DokumentenInformation-/Freigabehistorie 4

1.1 Dokumentenhistorie 4

1.2 Dokumentenfreigabe 4

1.3 Verteilerliste 4

1.4 Ablageort des Dokuments 4

1.5 Vorlagenhistorie 4

2. Einleitung 5

2.1 Geltungsbereich 5

3. Generelle Beschreibung des Verfahrens/Applikation 6

3.1 Überblick zum Verfahren 6

3.2 Assets 6

3.3 Beschreibung Produktionsumgebung / Testumgebung 6

4. Angaben zum Datenschutz 8

4.1 Datenschutzfolgeabschätzung (DSFA) 8

4.2 Klassifizierung der Informationen 8

4.3 Auswertung von personenbezogenen Daten 9

5. Risikoanalyse 10

5.1 Besondere Sicherheitsanforderungen 10

5.2 Ergebnisse der Risikoanalyse 10

5.3 Fachliche Risikobewertung 10

5.4 Mapping der Vorgabedokumente 11

6. Kommunikationsbeziehungen / Schnittstellen 12

7. Rollen und Berechtigungskonzept 14

7.1 Rollen 14

7.2 Prozess zur Benutzer- und Berechtigungsvergabe 14

8. Umsetzung der Hard- und Softwaresicherheit 16

8.1 Sichere Betriebsumgebung 16

8.2 Schutz von Schnittstellen 16

8.3 Durchgeführte Härtungsmaßnahmen 16

8.4 Durchführung von Penetrationstests und Systemprüfungen 17

8.5 Einsatz von Malwarescanner 17

8.6 <weitere Maßnahme aus der Risikoanalyse> 17

9. Softwarepflege/-wartung 18

Muster

10. Monitoring bzw. Überwachung 19

11. Datenhaltung 20

11.1 Protokollierung 20

11.2 Kontrolle der Logfiles 20

11.3 Datenspeicherung/ Datenaufbewahrung / Datenlöschung / Archivierung 20

12. Eingesetzte Verschlüsselungsverfahren inkl. Schlüsselverwaltung 22

13. Verfügbarkeit & Backup 24

13.1 Allgemeine Maßnahmen zur Sicherstellung der Verfügbarkeit 24

13.2 Datensicherungs- bzw. Backupkonzept 24

Muster

Wahrung der Vertraulichkeit

Dieses vorliegende Sicherheitskonzept enthält vertrauliche Informationen zu Abläufen und Verfahren bei der ITSCare und stellt geistiges Eigentum des ITSCare dar. Die Weitergabe oder Offenlegung der Inhalte ist ohne schriftliche Zustimmung der ITSCare nicht zulässig.

1. DOKUMENTENINFORMATION-/FREIGABEHISTORIE

1.1 Dokumentenhistorie

Version	Status	Datum	geändert von	Art der Änderung / Bemerkung
0.0.1	Entwurf	Klicken oder tippen Sie, um ein Datum einzugeben.		Initiale Erstellung

1.2 Dokumentenfreigabe

Funktion	Name/Instanz	Datum
<Funktion der Führungskraft>	<Name der Führungskraft>	Klicken oder tippen Sie, um ein Datum einzugeben.

1.3 Verteilerliste

Funktion	Name	Datum
IT-Sicherheit		Klicken oder tippen Sie, um ein Datum einzugeben.
Datenschutzmanagement		Klicken oder tippen Sie, um ein Datum einzugeben.
Informationssicherheit		Klicken oder tippen Sie, um ein Datum einzugeben.

1.4 Ablageort des Dokuments

Dokument	Ablageort	Datum
Sicherheitskonzept		
Risikoanalyse		

1.5 Vorlagenhistorie

Version	Status	Datum	geändert von	Art der Änderung / Bemerkung

Muster

2. EINLEITUNG

Neben den IT-Sicherheitsrichtlinien, welche allgemeine Vorgaben der Informationssicherheit dokumentieren, sind Sicherheitskonzepte (Siko) notwendig. Diese dokumentieren die Umsetzung der Sicherheitsstrategie und die Maßnahmen, um die Sicherheitsziele in einem bestimmten Bereich zu erreichen.

<Bitte die Einleitung bezogen auf das Projekt formulieren und den Text ersetzen.>

2.1 Geltungsbereich

<Der Geltungsbereich soll Ausschlüsse und Abgrenzungen definieren. Für Sicherheitskonzepte als Anwendungsbetreiber umfasst dies insbesondere die Abgrenzung zum Mandanten, zu anderen Services auf gleicher Ebene und zu darunterliegenden Services wie etwa dem Plattformbetrieb.>

<Sofern auf Anforderung eines Mandanten abweichende Maßnahmen und Abläufe umgesetzt werden, sollte nachfolgende Formulierung aufgenommen werden und die Dokumente in die Dokumentenliste (Abschnitt 1.4) aufgenommen werden:>

Dieses Dokument gilt für den Betrieb für die:
☐ AOK Baden-Württemberg
☐ AOK Hessen
☐ AOK Rheinland-Pfalz/Saarland
☐ AOKs-im bundesweiten Gesamtverbund
☐ ITSCare

Das Dokument gilt für den Standardbetrieb der ITSCare. Kundenspezifische Abweichungen sind im mandantenspezifischen Anhang A beschrieben.

Muster

3. GENERELLE BESCHREIBUNG DES VERFAHRENS/APPLIKATION

3.1 Überblick zum Verfahren

<Dieser Abschnitt soll einem Dritten den Verfahrensablauf nachvollziehbar darstellen. Dazu ist es notwendig darzustellen, welche Anwendung betrieben wird und wer oder was in welcher Form mit der Anwendung interagiert. Zur Interaktion gehören manuelle Handlungen des Anwenders, aber auch automatisierte Abrufe oder Übermittlungen von oder zu anderen Verfahren. Weiterhin müssen die Anwendungsart und der Anwendungszugriff nachvollziehbar sein. Handelt es sich beispielsweise um eine Webanwendung, auf die der Anwender per Standardbrowser zugreift oder wird dazu eine zusätzliche Komponente auf dem Client benötigt (bspw. SAP GUI)? Der weitere technische Aufbau ist Bestandteil von Kapitel 3.3.

Gibt es regelmäßige, anlassbezogene oder anforderungsbezogene Tätigkeiten der ITSCare in der Anwendung? Werden beispielsweise regelmäßig Daten in die Anwendung importiert oder gepflegt? - Wie sieht die Schnittstelle zum Mandanten aus? Sind Abrufe, Erweiterungen oder Pflegeaufträge abgestimmt (bspw. Pflege von Adresslisten, Bereitstellung einzelner Geräte, ..)? Werden diese per AMSys oder Warenkorb beauftragt?

Reguläre systemadministrative Aufgaben wie etwa die Aktualisierung, u.a. die Installation sicherheitsrelevanter Updates, der Anwendung, die Auswertung von Logfiles oder Datensicherung sind grundsätzlich nicht Bestandteil dieses Abschnitts, sondern Maßnahmen für einen sicheren Betrieb des Verfahrens.>

3.2 Assets

Zum Betrieb des Verfahrens werden folgende Komponenten benötigt:

Asset	Kategorie	supportet durch
<APPDB123>	<Oracle Datenbank>	<ITSCare>
<ZZ999WS0001>	<Windows Webplattform>	<ITSCare>
<zentrales AD>	<Active Directory >	<T-Systems>

Tabelle 1: Assets

<Es sind nur die unmittelbar benötigten Assets anzugeben. Das exemplarisch eine Webplattform auch eine Netzwerkinfrastruktur mit Firewall benötigt ist impliziert und nicht Bestandteil der Assetliste.>

3.3 Beschreibung Produktionsumgebung / Testumgebung

- ☐ Die Anwendung oder ein Teil davon wird auf Systemen in den Rechenzentren der ITSCare betrieben.
- ☐ Die Anwendung oder ein Teil davon wird auf Systemen außerhalb der Rechenzentren der ITSCare, bspw. in Technikräumen der AOK oder bei externen Dienstleistern, betrieben.
  - <externer Betriebsort 1>
- ☐ Eine Teilkomponente der Anwendung wird auf Clients betrieben, die durch die ITSCare gemangt werden.
- ☐ Die Anwendung ist eine reine Clients-Anwendung und wird auf Clients betrieben, die durch die ITSCare gemangt werden.

Muster

☐ Es ist ein Fernwartungszugang für Supportunterstützung durch <Angabe> eingerichtet.

<In diesem Abschnitt ist der technische Aufbau der Produktionsumgebung zu beschreiben. Aus welchen konkreten Komponenten besteht die Anwendung? Ist die Anwendung um irgendwelche Module oder Plug-Ins erweitert worden? Wie werden die Komponenten installiert? Gibt es beispielsweise eine zentrale Serverkomponente, die manuell installiert wird, und eine Clientkomponente, die über die zentrale Softwareverteilung zugewiesen wird? Würde die Komponente auf jedem Client installiert oder auf Anforderung?

Sofern eine Testumgebung vorhanden ist, wäre diese hier zu beschreiben. Sofern die Umgebung ähnlich zur Produktionsumgebung ist, reicht eine Darstellung der Unterschiede aus.

- Aus welchen Komponenten besteht die Produktionsumgebung?
- Welche Module oder Erweiterungen sind ggf. in die Anwendung integriert, um das Verfahren abzubilden?
- Grundsätzliche Beschreibung der Produktionsumgebung (sinnvolle schematischer Überblick)
- Wie unterscheidet sich die Testumgebung von der Produktionsumgebung?
- Welche Arten von Tests werden in der Testumgebung durchgeführt?
- Werden Tests mit anonymisierten, pseudonymisierten oder Echtdaten vollzogen?
- Wie werden die Tests vollzogen?
- Wie sehen die Transporte zwischen den verschiedenen Umgebungen aus? Welche Daten werden wohin übertragen?

Wie erfolgt die Installation der Anwendung? Wird die Anwendung manuell installiert, aus den Systemquellen des Betriebssystems (bspw. bei Linux-Systemen)? Besteht die Anwendung aus mehreren Komponenten? Unterscheiden sich hierbei die Installationsarten?

Muster

4. ANGABEN ZUM DATENSCHUTZ

4.1 Datenschutzfolgeabschätzung (DSFA)

Bei der in Art. 35 DS-GVO geregelten Datenschutzfolgenabschätzung handelt es sich um die Pflicht des Verantwortlichen, vor Beginn einer geplanten Datenverarbeitung eine Abschätzung der Folgen der Verarbeitungstätigkeit vorzunehmen und zu dokumentieren.

Wer Verantwortlicher im Sinne dieses Gesetzes ist, wird in Art 4. Nr. 7 DS-GVO definiert. Danach ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

Grundsätzlich ist die vom Verantwortlichen durchzuführende Datenschutz-Folgenabschätzung immer dann vorzunehmen, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Darüber hinaus ist sie zwingend durchzuführen, wenn eines der in Art. 35 EU-DSGVO in Abs. 3 bestimmten Regelbeispiele vorliegt.

Für die Bewertung und ggf. Erstellung einer Datenschutzfolgenabschätzung ist zuständig:

☐ ITSCare ☐ AOKs

4.2 Klassifizierung der Informationen

Die Schutzbedürftigkeit und somit auch die notwendigen Maßnahmen leiten sich im Wesentlichen aus den verarbeiteten Daten ab. Im Rahmen des Verfahrens werden folgende Datenarten verarbeitet:

☐ Kundendaten, bspw. Sozialdaten oder Daten der AOK Mitarbeiter
☐ Personenbezogene Daten der ITSCare[1]
☐ besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, bspw. Gesundheitsdaten, biometrische Daten usw.
☐ Technische Daten
☐ Interne Daten, bspw. Dokumente der ITSCare, die keine anderweitige Kennzeichnung haben
☐ Vertrauliche Daten ohne Personenbezug, bspw. Sicherheitskonzepte, Schwachstellenberichte
☐ Geschäftsgeheimnisse

[1] Personenbezogene Daten des Kunden sind als Kundendaten zu werten.

4.3 Auswertung von personenbezogenen Daten

☐ Im Rahmen dieses Verfahrens werden regelmäßig folgende Auswertungen erstellt und dem angegebenen Empfänger zur Verfügung gestellt:

Report	Zweckbeschreibung	Ausgewertete Datenkategorie	Verknüpfung mit anderen Verfahren	Empfänger
<Name>	<Kurzbeschreibung>	<Kategorie>	☐ nein ☐ ja, <Verfahren>	☐ AOKs ☐ ITSCare

Tabelle 2: Auswertung personenbezogener Daten

☐ Im Rahmen des Verfahrens haben Anwender Zugriff auf vordefinierte Standardreports der Anwendung.

☐ Im Rahmen dieses Verfahrens können die Anwender innerhalb der Anwendung freie Abfragen durchführen.

Muster

5. RISIKOANALYSE

5.1 Besondere Sicherheitsanforderungen

<Sicherheitsanforderungen, die sich entweder aus dem Tailoring ergeben haben oder sich aus gemeinsamen Kundenanforderungen ergeben und über die Richtlinien der ITSCare hinausgehen, sind hier anzuführen. Hier wäre auch anzugeben, wenn für das Verfahren die Einhaltung besondere Standards, beispielsweise gematik Steckbriefe, relevant sind. Individuelle Sicherheitsanforderungen eines Mandanten wären Bestandteil der mandantenspezifischen Ergänzung.>

☐ Es wurden keine besonderen Sicherheitsanforderungen definiert.
☐ Für das Verfahren sind folgende Standards einzuhalten: <Aufzählung der Standards>
☐ Es wurden nachfolgende besonderen Risiken und Anforderungen definiert:

Risiko	Schutzziel(e)	Anforderung
<zusätzlich identifiziertes Risiko>	☐ Vertraulichkeit ☐ Integrität ☐ Verfügbarkeit ☐ Authentizität ☐ Belastbarkeit	<Anforderung>

5.2 Tabelle 3: Besondere SicherheitsanforderungenErgebnisse der Risikoanalyse

<Summary zur Risikoanalyse, insb. Angabe auf welcher Basis (bspw. Bausteine des IT-Grundschutzkompendiums, Tailoring) die Risiken identifiziert wurden, den wesentlichen Risiken. Können durch die getroffenen Maßnahmen nicht alle Risiken auf ein angemessenes Niveau reduziert werden, sollte das ebenso beschrieben sein wie Maßnahmen, die noch zu implementieren sind. Die Risikoanalyse ist auch im Abschnitt 1.4 zu benennen.>

Die Risikoanalyse vom Klicken oder tippen Sie, um ein Datum einzugeben. in der Version <Versionsnummer> ist als Anlage beigefügt.

5.3 Fachliche Risikobewertung

<Die Ergebnisse einer fachliche Risikobewertung, die direkt von den betroffenen Fachbereichen der jeweiligen AOK durchgeführt werden soll, sind hier anzuführen. Hierbei ist hervorzuheben, dass die identifizierten Risiken aus der durch die ITScare durchgeführte Risikoanalyse erneut durch die Fachbereich betrachtet und bewertet werden sollen, um somit auch eine fachliche Risikobewertung zu erhalten>

<HINWEIS: Die fachliche Risikoanalyse kann durch die unterhalb dargestellte Übersicht, die sich im Anhang befindliche Tabelle oder ein externes Dokument erfasst werden.>

☐ Es wurden keine gesonderten fachlichen Risiken definiert.

Muster

☐ Für das Verfahren sind folgende Standards einzuhalten: <Aufzählung der Standards>

☐ Es wurden nachfolgende fachliche Risiken und Anforderungen definiert:

Risiko	Schutzziel(e)	Anforderung
<zusätzlich identifiziertes Risiko>	☐ Vertraulichkeit ☐ Integrität ☐ Verfügbarkeit ☐ Authentizität ☐ Belastbarkeit	<Anforderung>

Tabelle 4: Fachliche Risikobewertung

Die fachliche Risikoanalyse vom Klicken oder tippen Sie, um ein Datum einzugeben. in der Version <Versionsnummer> ist als Anlage beigefügt.

5.4 Mapping der Vorgabedokumente

Die in der Risikoanalyse angeführten einzelnen Maßnahmen werden in diesem Dokument im Kapitelverweis einzeln beschrieben. Bei der Umsetzung der Maßnahme wurden das\die angegebenen Vorgabedokument(e) berücksichtigt.

Maßnahme	relevante Vorgabedokument(e) für die Umsetzung der Maßnahme	Kapitel	Vorgabe vollständig umgesetzt
Berechtigungskonzept	2.9 Policy für Benutzerrechte	7	Wählen Sie ein Element aus.
Kontrolle der Logfiles	5.31 Guideline für Traffic- und Logfileanalyse	11.2	Wählen Sie ein Element aus.
Anwendungshärtung	5.36 Guideline für Integration, Zertifizierung und Produktivsetzung von Applikationen	8.1	Wählen Sie ein Element aus.
Penetrationstest	2.12 Policy für Penetrationstests, 5.36 Guideline für Integration, Zertifizierung und Produktivsetzung von Applikationen	8.4	Wählen Sie ein Element aus.
Systemprüfung	5.36 Guideline für Integration, Zertifizierung und Produktivsetzung von Applikationen	8.4	Wählen Sie ein Element aus.
Malwarescanner	5.4 Policy zum Schutz vor Schadsoftware	8.5	Wählen Sie ein Element aus.

Tabelle 5: Mapping der Vorgabedokumente und Maßnahmen

<Ist die Maßnahme bereits in einem anderen Sicherheitskonzept beschrieben, kann im referenzierten Kapitel auf das andere Dokument verwiesen werden. Zur besseren Nachvollziehbarkeit in der Tabelle sollten darin keine Verweise auf andere Dokumente enthalten sein. Die notwendigen Maßnahmen müssen innerhalb des Dokuments prüfbar und nachvollziehbar in den referenzierten Kapiteln beschrieben sein.>

Muster

6. KOMMUNIKATIONSBEZIEHUNGEN / SCHNITTSTELLEN

Unter welchen Voraussetzungen kann welche Komponente oder welcher Nutzer wie mit anderen Komponenten oder Nutzern kommunizieren?

<Sind in dieses Verfahren Komponenten mit weiteren Schnittstellen integriert (bspw. USB-Schnittstelle, NFC), so sind die Komponenten mit den verfügbaren Schnittstellen anzugeben, idealerweise als Schaubild mit lesbaren Angaben.>

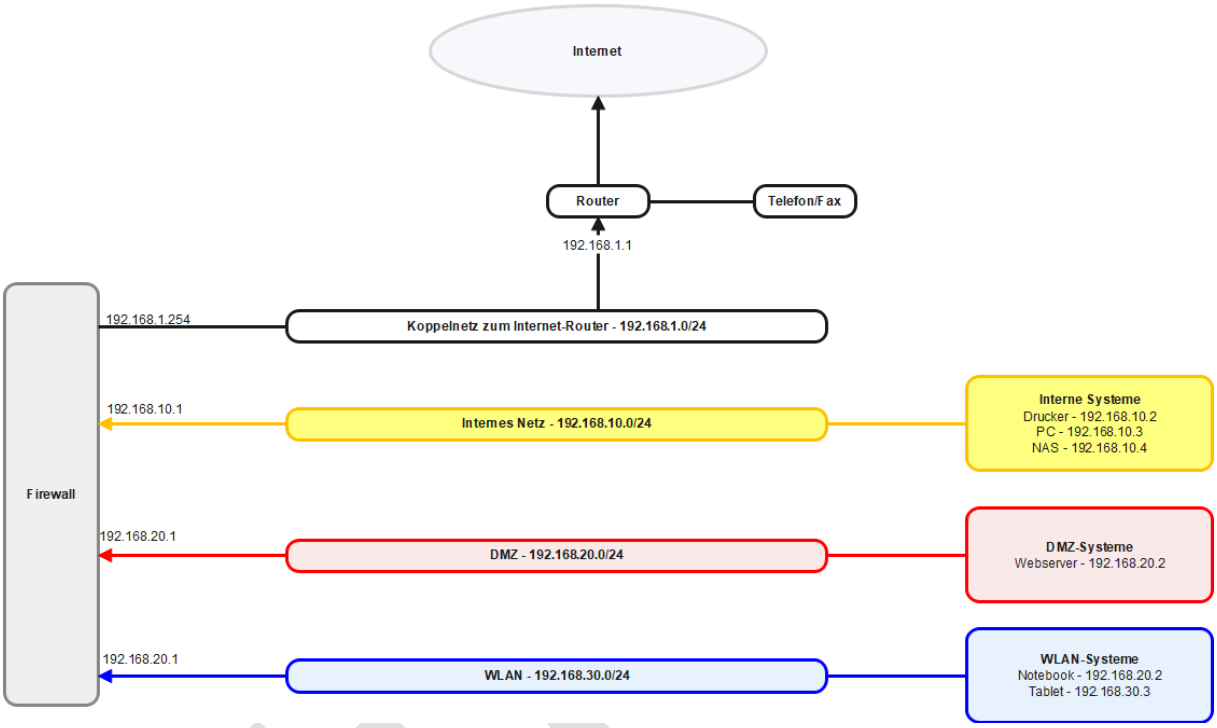


Abbildung 1: Netzwerkdiagramm (Beispiel)

<Das Beispiel ist durch ein konkretes Netzwerkdiagramm zu ersetzen. Folgende Informationen müssen, soweit relevant, in dem Netzwerkdiagramm erkennbar sein:

- *Clients (je Typ symbolisch 1x)*
- *Firewalls (inkl. Name der FW)*
- *Web Application Firewall (WAF)*
- *Internet*
- *Proxy (für ausgehende Verbindungen)*
- *Applikationshost(s)*
- *Datenbank*
- *Filestorage*
- *weitere beteiligte Systeme (AD, Exchange, ...)>*

Für das Verfahren sind folgende Kommunikationsbeziehungen notwendig:

Quellsystem(e)	Zielsystem(e)	Zielport(s)	Protokoll	Beschreibung
<ZZ001AS9999>	<ZZ002DB12345>	<9999/TCP>	<HTTP>	

Tabelle 6: Kommunikationsmatrix

Muster

7. ROLLEN UND BERECHTIGUNGSKONZEPT

7.1 Rollen

Rollen für Betreiber der Anwendung

Rolle	Nutzergruppe der Rolle	Kurzbeschreibung und wesentliche Funktionen der Rolle

Tabelle 7: Anwendungsrollen des Betreibers

Rollen für Nutzer der Anwendung

Rolle	Kurzbeschreibung und wesentliche Funktionen der Rolle

Tabelle 8: Anwendungsrollen des Nutzers

Technische/Maschinelle Benutzer

Benutzername	Verantwortlicher	Kurzbeschreibung und wesentliche Funktionen des Benutzers

Tabelle 9: Technische Rollen

<Sofern die Rollen als zentral gemanagte Gruppen (AD-Gruppen) eingerichtet werden, sollte entweder das Bildungsschema für den Gruppenname inkl. OU angegeben werden oder tabellarisch aufgelistet werden.

7.2 Prozess zur Benutzer- und Berechtigungsvergabe

☐ Die Benutzer und Berechtigungen der Anwendungsnutzer werden durch IdM gemanagt.
☐ Die Benutzer und Berechtigungen des Betriebs werden durch IdM gemanagt.

<Sofern Betreiber- oder Nutzerrollen nicht oder nicht vollständig durch IdM gemangt werden, ist zu beschreiben, wie die jeweilige Rolle beantragt und zugewiesen wird. Es ist anzugeben, wer die Rolle jeweils beantragen kann und wer diese genehmigen muss. Gibt es Abgrenzungen, welches IdM zuständig ist?

Werden die Berechtigungen direkt oder indirekt (via IdM) per AD Gruppenmitgliedschaften zugewiesen sollte klar werden, wie AD Gruppen in systemlokale Berechtigungen übersetzt werden. Werden die AD Gruppen beispielsweise direkt verwendet und berechtigt oder findet eine Zuordnung von AD-Gruppe zu systemlokaler Gruppe statt? Aus welcher Domäne kommen welche Rollen? Aus der jeweiligen Kundendomäne, aus der ITSCare-Domäne?

Lassen sich Rollen manuell anpassen oder sind technisch nur die vorkonfigurierten Rollen nutzbar? Wer ist für mögliche Rollenanpassungen zuständig? Wer darf Rollenanpassungen anfordern? Wer ordnet den Benutzerkonten die jeweilige Rolle zu? Hier ist insbesondere die notwendige Funktionstrennung zwischen Benutzer- und Rollenadministration darzustellen. Gibt es technische Sperren, die eine Vergabe beider Adminrollen verhindern?

Muster

Gerade bei einem lokalen Usermanagement ist wichtig, dass auch Konten ausgeschiedener oder organisatorisch anderweitig zugeordnete Mitarbeiter gesperrt und gelöscht werden. Wie sieht hier das Verfahren aus? Bei einem ActiveDirectory integrierten Usermanagement kommt es vor, dass die Benutzer in den lokalen Userstore der Anwendung bei der erstmaligen Anmeldung übertragen, bei einem Ausscheiden oder Versetzung das Benutzerkonto nicht vollständig gelöscht wird. Wie sieht hierzu der Ablauf aus? Sofern hierzu irgendwelche Reports erstellt werden, sind diese in Kapitel 4 anzugeben.

Wie erfolgt die Trennung zwischen einem administrativen und einem fachlichen Benutzerkonto? Gibt es Vorgaben, welche Rollen und Berechtigungen einer Kontenart nicht zugewiesen werden dürfen? Was ist mit Mitarbeitern, die sowohl fachlich als auch administrativ tätig sind? Haben diese zwei Benutzerkonten?>

Die Benutzerauthentifizierung erfolgt mittels

Rolle	**Authentifizierungsverfahren**	
<Rolle A> <Rolle B>	☐ Single-Sign On (SSO) ☐ Benutzername und Kennwort	☐ Multifaktor-Authentifizierung (MFA) ☐ <Sonstiges Verfahren>
<Rolle C>	☐ Single-Sign On (SSO) ☐ Benutzername und Kennwort	☐ Multifaktor-Authentifizierung ☐ <Sonstiges Verfahren>

Tabelle 10: Benutzerauthentifizierung

<Zur Authentifizierung sind folgende Punkte relevant: Worüber erfolgt das SSO? Welche Faktoren sind bei der MFA zulässig? Beispielsweise Passwort und PIN? Lässt sich ein Passwortwechsel technisch erzwingen? Werden Komplexitätsvorgaben technisch umgesetzt?

- ☐ Passwörter von lokal verwalteten Benutzerkonten werden als Hashwert gespeichert. Das Hashverfahren ist in Kapitel 12 beschrieben.
- ☐ Das Dienstkonto der Anwendung ist als gemanagtes Dienstkonto eingerichtet. Das Passwort wird automatisiert gemanagt.
- ☐ Passwörter von technischen/maschinellen Benutzern werden verschlüsselt gespeichert. Das Verschlüsselungsverfahren ist in Kapitel 12 beschrieben.
- ☐ Passwörter von technischen/maschinellen Benutzern werden im Klartext gespeichert.

<Sofern die Passwörter von technischen bzw. maschinellen Benutzern im Klartext gespeichert werden, ist die Maßnahme zum Schutz der Passwörter hier zu beschreiben. Sind die Leserechte auf die entsprechende Konfigurationsdatei möglicherweise auf den Anwendungsuser beschränkt? Oder hat ausschließlich der Datenbankuser der Anwendung Leserechte auf die entsprechende Tabelle?

Wird zu Fernwartungszwecke eine Remotezugang benötigt ist das Antrags- und Kontrollverfahren Bestandteil dieses Kapitels.>

Muster

8. UMSETZUNG DER HARD- UND SOFTWARESICHERHEIT

< In diesem Kapitel wird beschrieben, wie die Anforderungen der Vorgabedokumente aus dem Mapping konkret umgesetzt werden.

8.1 Sichere Betriebsumgebung

Die im Rechenzentrum der ITSCare betriebenen Anwendungsteile unterliegen den übergreifend festgelegten und etablierten Maßnahmen des sicheren Rechenzentrumsbetriebs. Dazu gehören insbesondere die Maßnahmen zur Zutrittskontrolle, Brandschutz, Klimatisierung und Energieversorgung.

<Sofern zusätzliche Maßnahmen getroffenen wurden, bitte hier beschreiben. Sofern Anwendungsteile in anderen Umgebungen, insbesondere an anderen Standorten, betrieben werden, sollten die Maßnahmen hier ebenfalls beschrieben werden.>

8.2 Schutz von Schnittstellen

☐Eingehende Netzwerkkommunikation wird auf allen verfahrensrelevanten Systemen durch eine hostbasierte Firewall geschützt.

<Die Schutzmechanismen der weiteren Schnittstellen aus Kapitel 6 sind anzugeben. Schutzmechanismen können sowohl mechanisch (bspw. durch ein USB-Port Schloss), als auch logisch (bspw. durch systemseitige Deaktivierung oder Installation durch eine Schutzsoftware) geschützt werden.>

8.3 Durchgeführte Härtungsmaßnahmen

Härtungsmaßnahmen dienen der Absicherung von Hard- oder Softwarekomponenten. Beispielsweise das Deaktivieren und ungenutzten Diensten, das nicht-Installieren oder Entfernen nicht benötigter Komponenten, das Abschalten oder Absichern von Ports, Aktivierung von Sicherheitsfunktionen usw.[2]

Folgende Härtungsstandards wurden angewandt:

- ☐ CIS Benchmarks[3]:
  - <Benchmark, Version und Level angeben>
- ☐ DISA Security Technical Implementation Guides (STIGs)[4]
  - <Guideline, Version, Revision>
- ☐ Hersteller Guidelines:
  - <Guideline und Version>
- ☐ weitere Härtungsstandards:
  - <Guideline und Version>

[2] u.a. NIST SP 800-152, S.82f (Version: October 2015).

[3] https://www.cisecurity.org/cis-benchmarks/

[4] https://public.cyber.mil/stigs/

Folgende individuellen Härtungsmaßnahmen wurden umgesetzt:

- <individuelle Härtungsmaßnahme>

8.4 Durchführung von Penetrationstests und Systemprüfungen

<Penetrationstests und Systemprüfungen sind gemäß den Richtlinien der ITSCare vor Produktivsetzung durchzuführen. Die Ergebnisse sind im Sicherheitskonzept und der Risikoanalyse zu berücksichtigen.>

☐ Die Konfiguration bzw. die Härtungsmaßnahmen der installierten Anwendung wurde vor Produktivsetzung durch einen unabhängigen Dritten überprüft.
☐ Die installierte Anwendung wurde vor Produktivsetzung einem Penetrationstest unterzogen.
☐ Der Penetrationstest wird anlassbezogen, mindestens bei jedem Releaseupdate, wiederholt.

8.5 Einsatz von Malwarescanner

Auf der Plattform ist folgender Malwarescanner installiert
☐ McAfee Endpoint Security
☐ TrendMicro OfficeScan
☐ <weiteres Produkt>

Der Malwarescanner ist
☐ in die zentrale Management-Plattform der ITSCare integriert
☐ lokal konfiguriert und unterliegt nicht dem zentralen Management

☐ Für das Verfahren sind folgende Scanausschlüsse notwendig

Verzeichnis\Datei	Verzeichnis- bzw. Dateibeschreibung	Ausschluss für Scanart	Ausschluss rekursiv
<Pfadangabe>	<Beschreibung>	☐ Dateizugriff ☐ Regelscan	Wählen Sie ein Element aus.

Tabelle 11: Scanausschlüsse

☐ Der Virenscanner erfordert für dieses Verfahren folgende besondere Konfiguration:

<besondere Konfiguration einfügen

8.6 <weitere Maßnahme aus der Risikoanalyse>

<Beschreibung der Maßnahmenumsetzung. Dieses Kapitel ist für jede weitere Maßnahme zu wiederholen.>

Muster

9. SOFTWAREPFLEGE/-WARTUNG

Die Überprüfung auf Updates erfolgt

- ☐ manuelle turnusmäßige Überprüfung der Herstellerinformationen durch <Rolle>, der Turnus beträgt <Intervall>.
  - ☐ Die Überprüfung wird im <Ticketsystem> dokumentiert.
  - ☐ Die Umsetzung der organisatorischen Maßnahme wird durch <Rolle> kontrolliert.
- ☐ automatisiert durch Überprüfung durch die Anwendung, der konfigurierte Turnus für die Überprüfung beträgt <Intervall>, verfügbare Updates werden
  - ☐ per E-Mail an die Funktionsmailbox <FMB> gesendet
  - ☐ durch Benachrichtigung innerhalb der Anwendung. Die Anwendung wird durch <Rolle> alle <Intervall> manuell auf Aktualisierungshinweise geprüft.
- ☐ durch aktive Benachrichtigung des Herstellers <Name> per E-Mail an die Funktionsmailbox <FMB>
- ☐ <Beschreibung>

Die im Rahmen dieses Verfahrens eingesetzten Softwarekomponenten werden wie folgt gepflegt:

- ☐ Die eingesetzten Softwarekomponenten aktualisieren sich selbstständig im Hintergrund.
- ☐ Die eingesetzten Softwarekomponenten werden manuell durch <Rolle\CC\Team> aktualisiert.

<Sofern für die Durchführung des Updates ein besonderes Tool notwendig ist, sollte dies bereits in Kapitel 3.3 genannt, als Asset (Kapitel 3.2) aufgeführt sein und im Berechtigungskonzept (Kapitell 7) berücksichtigt sein. Wird die Anwendung durch einen Dienstleister gewartet oder durch die AOK gepflegt, so ist das hier anzuführen. Wird dafür ein Fernwartungszugang genutzt, sollte auf die Maßnahme in diesem Dokument referenziert werden.>

<Hier ist anzugeben, ob und ggf. welche Aktualisierungen zunächst im Testsystem durchgeführt werden. Sofern aus Betriebssicht technischen Tests durchgeführt werden, sind die konkreten Testfälle zu benennen. Sind neben den technischen Tests auch weitere interne Tests durchzuführen, sollten diese ebenfalls aufgeführt werden. Ggf. hat der Kunde auch die Durchführung von fachlichen Tests beauftragt? In jedem Fall ist anzugeben, wo und wie das Testergebnis dokumentiert wird. Führt der Kunde eigene Tests durch? Muss der Kunde eine Freigabe erteilen? Werden die Aktualisierungen über das interne Change-Management gesteuert?>

Muster

10. MONITORING BZW. ÜBERWACHUNG

Um Störungen und Auffälligkeiten rechtzeitig erkennen und behandeln zu können sind Systeme und Anwendungen dauerhaft zu überwachen. Die Überwachung sollte dabei so eingerichtet sein, dass Störungen und Ausfälle zeitnah entdeckt werden können.

Im Rahmen dieses Verfahrens werden die Komponenten wir folgt überwacht:

- ☐ Serversysteme werden auf Ebene des Betriebssystems mittels HP Onboard Administrator überwacht und bei Überschreiten von Schwellwerten alarmiert.
- ☐ Sicherheitsrelevante Ereignisse werden auf Ebene des Betriebssystems gemäß dem Betriebsstandard durch das SIEM der ITSCare korreliert, durch das Security Operation Center vorbewertet und per Ticket alarmiert.
- ☐ Sicherheitsrelevante Ereignisse werden auf Ebene der Anwendung durch das SIEM der ITSCare korreliert, durch das Security Operation Center vorbewertet und per Ticket alarmiert.
- ☐ Die Verfügbarkeit der Anwendung wird durch das zentrale Monitoring beim Leitstand überwacht bei Überschreiten der Schwellwerte per <Methode> alarmiert.

<Sofern die Überwachung nur für bestimmte Komponenten gilt oder anderweitig überwacht werden ist das zu konkretisieren.>

Folgende Parameter werden für das Verfahren überwacht:

Überwachter Parameter	Überwachungsintervall	Alarmierung an
<Fehlermeldungen im Anwendungslog>	<alle x Minuten>	<Rolle\Funktionspostfach>
<Erreichbarkeit des Frontends>	<alle y Minuten>	<Rolle\Funktionspostfach>
<Gerätebestand im Lager>	<z.B. wöchentlich>	<Rolle\Funktionspostfach>

Tabelle 12: Überwachte Parameter

Muster

11. DATENHALTUNG

11.1 Protokollierung

Protokolle dienen dazu, betriebs- und sicherheitsrelevante Ereignisse bei der Nutzung eines Systems nachvollziehbar aufzuzeichnen. Die Aufzeichnungen dienen u.a. dazu, Ressourcenengpässe frühzeitig zu entdecken, Hard- und Softwareprobleme aufzuzeigen sowie Sicherheitsprobleme und Angriffe nachverfolgen zu können. Im Rahmen dieses Verfahrens werden folgende Ereignisse protokolliert

<Aufzählung protokollierter Ereignisse, bspw. Authentifizierungsversuche, Änderungen an Benutzerkonten. Berechtigungsänderungen, Passwortänderungen, Konfigurationsänderungen, Änderungen von Inhaltsdaten, Datenlöschungen, Anwendungsfehler, …>

<Sofern für einzelne Benutzer oder Rollen eine vollständige Protokollierung erfolgt, ist das hier anzugeben.>

11.2 Kontrolle der Logfiles

☐ Die Logfiles der Anwendung sind in das zentrale Event-Management eingebunden und werden automatisiert auf Fehlermeldungen überprüft.
☐ Die Logfiles der Anwendung sind in das SIEM integriert und werden durch das eingesetzte Security Operation Center auf sicherheitsrelevante Ereignisse überprüft.
☐ Die Logfiles der Anwendung werden regelmäßig manuell gesichtet und auf Fehlermeldungen und sicherheitsrelevante Ereignisse überprüft.
  ☐ Die durchgeführte Überprüfung wird im Ticketsystem dokumentiert.
  ☐ Die durchgeführte Überprüfung und Dokumentation werden vom Vorgesetzten überwacht.

11.3 Datenspeicherung/ Datenaufbewahrung / Datenlöschung / Archivierung

Die Speicherung der Inhaltsdaten ergibt sich aus der Architekturbeschreibung gemäß Kapitel 3.3.

☐ Es wurden keine fachlichen Lösch- oder Archivierungsfristen benannt. Inhaltsdaten werden nicht durch den Betrieb archiviert oder gelöscht.

<Falls fachliche Lösch- und Archivierungsfristen genannt wurden sind diese entsprechenden Verfahren hier zu beschreiben.>

< Dieser Abschnitt ist bezogen auf technische Daten bzw. technische Protokolle. >

Protokollart	Löschfrist	Archivierungsfrist

Tabelle 13: Protokolle

Muster

<Werden aus dem Verfahren heraus Reports erstellt, sind die entsprechenden Lösch- und Archivierungsfristen ebenfalls anzugeben.>

Muster

12. EINGESETZTE VERSCHLÜSSELUNGSVERFAHREN INKL. SCHLÜSSELVERWALTUNG

Es werden im Rahmen des Verfahrens folgende Transportverschlüsselungen konfiguriert:

System / Schnittstelle	TLS-Version(en)	Cipher Suites
<Schnittstelle>	☐ TLS 1.3 ☐ TLS 1.2 ☐ TLS 1.1 ☐ <sonstige>	☐ AES-256-SHA256 ☐ AES-128-SHA256 ☐ AES256-GCM-SHA384 ☐ AES128-GCM-SHA256 ☐ ECDHE-RSA-AES-256-SHA384 ☐ ECDHE-RSA-AES128-SHA256 ☐ ECDHE-RSA-AES256-GCM-SHA384 ☐ ECDHE-RSA-AES128-GCM-SHA256 ☐ DHE-RSA-AES-256-SHA256 ☐ DHE-RSA-AES-128-SHA256 ☐ DHE-RSA-AES256-GCM-SHA384 ☐ DHE-RSA-AES128-GCM-SHA256 ☐ <weitere Cipher Suite>

Tabelle 14: Transportverschlüsselung

Es werden im Rahmen des Verfahrens folgende Zertifikate eingesetzt:

Zertifikat	System\Schnitt-stelle(n)	Cipher Suites
<Zertifikatsname>	<Schnittstelle>	☐ PKI der ITSCare ☐ PKI von <Anbieter> ☐ ohne PKI / selbst signiert

Tabelle 15: Zertifikate

Für die Verschlüsselung der Daten kommen folgende Verfahren zum Einsatz

Daten/-kategorie	Algorithmus	Verfahrensart
<Datenkategeorie>	☐ AES-256 ☐ AES-192 ☐ AES-128 ☐ <sonstige>	☐ Passwort ☐ Passphrase ☐ Zertifikat

Tabelle 16: Inhaltsverschlüsselung

Für die Bildung von Hashwerten kommen folgende Funktionen zum Einsatz

Daten/-kategorie	Algorithmus	SALT-Länge
<Datenkategeorie>	☐ SHA-256 ☐ SHA-512/256 ☐ SHA 384 ☐ SHA3-256 ☐ SHA3-384 ☐ SHA3-512 ☐ <sonstige>	<Anzahl> Zeichen

Tabelle 17: Hashwertalgorithmen

<Bitte hier beschreiben, wie Zertifikate verwaltet werden.

Muster

Wird beispielsweise ein Certificate Signing Request (CSR) erstellt und dann aus der PKI der ITSCare ein Zertifikat abgerufen?

Wie erfolgt der Wechsel der Zertifikate?

Wie erfolgt die Überwachung des Zertifikatablaufs?

Wer hat Zugriff auf das Schlüsselmaterial?

Wird das Zertifikat in die Anwendung hochgeladen oder im Dateisystem abgelegt und in die Konfiguration eingebunden?>

Muster

13. VERFÜGBARKEIT & BACKUP

13.1 Allgemeine Maßnahmen zur Sicherstellung der Verfügbarkeit

- Welche Maßnahmen sind implementiert?
- Werden die Maßnahmen regelmäßig getestet?
- Datenspiegelung
- Redundanzen
- Werden die allgemeinen Maßnahmen regelmäßig durchgeführt? Falls ja, in welchen Intervallen?
- Durchführung von K-Falltests?
- Sind mit den Dienstleistern SLAs vereinbart, auf die verwiesen werden kann?

13.2 Datensicherungs- bzw. Backupkonzept

Die Sicherung erfolgt

☐ automatisiert durch die zentral bereitgestellte Backup-Infrastruktur gemäß dem Standard der ITSCare.

☐ abweichend vom Standardverfahren

<Bei einem abweichenden Verfahren ist zu beschreiben, welche Daten gesichert werden, wohin die Datensicherung erfolgt, wer die Sicherung durchführt, und wie häufig die Sicherung erfolgt.>

<Es ist zu beschreiben, ob einzelne Daten wiederhergestellt werden können (bspw. einer Datensatz oder eine einzelne Datei), und/oder eine Zeitpunktbezogene Sicherung wiederhergestellt werden kann. In welchem Intervall wird die Sicherung überprüft? Werden im Rahmen der Überprüfung auch Wiederherstellungstests durchgeführt? Gibt es weitere anlassbezogene Tests, beispielsweise im Rahmen eines Releasewechsels?>

Folgende Daten werden nicht gesichert

Datenkategorie	Begründung

Tabelle 18: Sicherungsausschlüsse

Muster