**Reifegradmodell 1.3 (Word-Version)**

Einordnung des Dokuments:

Dieses Dokument wurde von einem Gesundheitsamt bereitgestellt. Das vorliegende Dokument wurde vom EvalDiGe-Konsortium überarbeitet und ist somit an die aktuelle Version angepasst. Es bietet eine schnelle Übersicht über die Dimensionen, deren Subdimensionen und deren Kriterien. Für den Fall, dass z. B. einzelne Subdimensionen im Rahmen gemeinsamer Treffen besprochen werden, können die betreffenden Seiten schnell herauskopiert und an die betreffenden Personen weitergeleitet werden, so dass der Gesprächsgegenstand klar umrissen werden kann.

**Achtung:** Nutzen Sie diese Version bitte nicht zur tatsächlichen Einordnung in das Reifegradmodell

**Inhaltsverzeichnis**

[Digitalisierungsstrategie 3](#_Toc120625909)

[Definition, Kommunikation und Umsetzung 3](#_Toc120625910)

[Verantwortlichkeiten 4](#_Toc120625911)

[Digitalisierungsbudget 4](#_Toc120625912)

[Mitarbeitende 5](#_Toc120625913)

[Sensibilisierung 5](#_Toc120625914)

[Partizipation 5](#_Toc120625915)

[Schulungen 6](#_Toc120625916)

[Prozessdigitalisierung 8](#_Toc120625917)

[Dokumentation 8](#_Toc120625918)

[IT-Unterstützung 8](#_Toc120625919)

[Übergreifende Prozesse 9](#_Toc120625920)

[Evaluation 9](#_Toc120625921)

[IT-Bereitstellung 11](#_Toc120625922)

[IT-Arbeitsplatz 11](#_Toc120625923)

[Organisation der IT-Beschaffung 12](#_Toc120625924)

[Bezug von IT-Infrastruktur 12](#_Toc120625925)

[Anwendung IT-Service Prozesse 14](#_Toc120625926)

[IT-Sicherheit 15](#_Toc120625927)

[IT-Sicherheitsmanagement 15](#_Toc120625928)

[Umgang mit IT-Sicherheitsrisiken und Angriffen 16](#_Toc120625929)

[Identitäts- und Zugangsmanagement 18](#_Toc120625930)

[Bürger\*innenzentrierung 20](#_Toc120625931)

[Interaktion 20](#_Toc120625932)

[Präferenzen 20](#_Toc120625933)

[Zusammenarbeit 21](#_Toc120625934)

[Zusammenarbeit innerhalb des Gesundheitsamtes 21](#_Toc120625935)

[Zusammenarbeit zwischen Gesundheitsämtern untereinander und mit Landesstellen 21](#_Toc120625936)

[Zusammenarbeit mit externen Stakeholder\*innen 22](#_Toc120625937)

[Software, Daten und Interoperabilität 23](#_Toc120625938)

[Fachanwendungen 23](#_Toc120625939)

[Technische Interoperabilität 23](#_Toc120625940)

[Datenanalyse, Berichterstattung 24](#_Toc120625941)

[Anforderungen und Dokumentation 24](#_Toc120625942)

[Datenschutz 25](#_Toc120625943)

# Digitalisierungsstrategie

## Definition, Kommunikation und Umsetzung

1. Eine Digitalisierungsstrategie liegt für das Gesundheitsamt vor oder ist mindestens in Planung.
2. Der Ist- und Zielzustand der digitalen Reife des Gesundheitsamtes ist beschrieben oder die Beschreibung ist mindestens geplant.
3. Die Vorgaben des Bundes und Landes hinsichtlich der Digitalisierung sind in der Digitalisierungsstrategie des Gesundheitsamtes konkretisiert.
4. Einzelne Digitalisierungsmaßnamen im Gesundheitsamt sind definiert.
5. Organisationseinheiten des Gesundheitsamtes bzw. konkrete Aufgaben mit Digitalisierungspotenzial sind bekannt.
6. In der Digitalisierungsstrategie wird der Ist- sowie der Zielzustand der digitalen Reife des Gesundheitsamtes konkretisiert. Diese Zustände können mithilfe des Reifegradmodells ermittelt werden.
7. Die Digitalisierungsstrategie wird schriftlich festgehalten und steht allen Mitarbeitenden zur Verfügung.
8. Die Digitalisierungsstrategie wird mindestens einmal im Jahr hinsichtlich des Erreichens gesetzter Ziele evaluiert.
9. Einzelne Organisationseinheiten leiten aus der Digitalisierungsstrategie kurz-, mittel- und langfristige Digitalisierungsmaßnahmen ab.
10. Entscheidungen in Bezug auf die Digitalisierung werden im Einklang mit der Digitalisierungsstrategie getroffen.
11. Aus der Digitalisierungsstrategie werden für alle relevanten Organisationseinheiten konkrete Maßnahmen abgeleitet (z. B. wird eine Prioritätenliste mit konkreten Maßnahmen erstellt).
12. Die Digitalisierungsstrategie wird mindestens zweimal im Jahr in organisationseinheitsübergreifenden Treffen hinsichtlich des Erreichens gesetzter Ziele evaluiert und entsprechend angepasst.
13. Digitalisierungsmaßnahmen werden entsprechend der Priorisierung im Gesundheitsamt umgesetzt.
14. Der Status der Umsetzung von Digitalisierungsmaßnahmen wird mindestens einmal im Quartal evaluiert und Maßnahmen werden entsprechend nachgesteuert.
15. Eine Unterstützung anderer Gesundheitsämter in Bezug auf deren Digitalisierungsstrategie und zu konkreten Digitalisierungsmaßnahmen besteht (z. B. werden andere Gesundheitsämter angeleitet). Gegebenenfalls werden übergreifende Digitalisierungsmaßnahmen initiiert.
16. Das Gesundheitsamt tauscht sich mit anderen Gesundheitsämtern über den angestrebten Zielzustand der digitalen Reife sowie geplante Digitalisierungsmaßnahmen aus.

## Verantwortlichkeiten

1. Erste Verantwortlichkeiten in Bezug auf Digitalisierung sind für das Gesundheitsamt festgelegt.
2. Für einzelne Digitalisierungsmaßnahmen ist mindestens eine Ansprechperson definiert, welche die Maßnahme(n) gemäß der Digitalisierungsstrategie vorantreibt. Die Ansprechperson muss nicht im Gesundheitsamt beschäftigt sein.
3. Digitalisierungsmaßnahmen werden durchgeführt, zum Teil durch einzelne engagierte Mitarbeitende.
4. Es gibt eine\*n Digitalisierungsverantwortliche\*n (diese\*r kann auch extern verortet sein).
5. Mindestens eine Person vermittelt zwischen Organisationseinheiten, EDV-Team und Softwareanbieter\*innen.
6. Digitalisierungsverantwortliche haben Kompetenzen im Fachgebiet (z. B. Systemadministration, Wirtschaftsinformatik, Informatik).
7. Digitalisierungsverantwortliche sind über die Gesundheitsämter bzw. Städte/Kommunen hinweg vernetzt und tauschen sich mindestens zweimal jährlich aus.
8. Digitalisierungsverantwortliche sind im regelmäßigen Austausch mit anderen Gesundheitsämtern und Stakeholder\*innen bzgl. des Vorgehens und des aktuellen Wissens zur Digitalisierung.

## Digitalisierungsbudget

1. Für die Umsetzung von Digitalisierungsmaßnahmen ist mindestens geplant, ein erforderliches Budget und Personal pro Maßnahme zu definieren.
2. Es wird pro Digitalisierungsmaßnahme ein Digitalisierungsbudget definiert, das für die entsprechende Umsetzung erforderlich ist.
3. Die Priorisierung der Digitalisierungsmaßnahmen erfolgt anhand der Kritikalität sowie des verfügbaren Digitalisierungsbudgets.
4. Die für das Budget zuständige Person steht in engem Austausch mit Verantwortlichen der übergeordneten Behörde und beantragt das für Digitalisierungsmaßnahmen erforderliche Budget (pro Jahr).
5. Das Digitalisierungsbudget wird regelmäßig angepasst, wenn Digitalisierungsmaßnahmen fortgeschritten oder umgesetzt sind.
6. Das Gesundheitsamt tauscht sich mit anderen Gesundheitsämtern über geplante Digitalisierungsmaßnahmen und dafür geplante Digitalisierungsbudgets aus.
7. Das Gesundheitsamt unterstützt Gesundheitsämter mit geringerer digitaler Reife bei der Festlegung eines Digitalisierungsbudgets für Digitalisierungsmaßnahmen.

# Mitarbeitende

## Sensibilisierung

1. Mitarbeitende kennen einzelne Digitalisierungsmaßnahmen (z. B. sind laufende Maßnahmen zur Umstellung auf papierlose Prozesse bekannt).
2. Mitarbeitende werden sensibilisiert für die Bedeutung und Ziele der Digitalisierung, den Datenschutz und die Möglichkeiten der digitalen Zusammenarbeit (z. B. über E-Mail oder Intranet).
3. Die Personalentwicklung umfasst regelmäßige Schulungen, in denen folgende Themen behandelt werden: Digitalisierung, insbesondere die Sensibilisierung der Mitarbeitenden für die Bedeutung und Ziele der Digitalisierung, den Datenschutz sowie die Möglichkeiten der digitalen Zusammenarbeit (z. B. über E-Mail oder Intranet).
4. Die Sensibilisierung der Mitarbeitenden im Hinblick auf die Digitalisierung erfolgt aufgabenbezogen.
5. Die Sensibilisierung der Mitarbeitenden wird kontinuierlich durchgeführt, d. h. neue Aspekte für die Sensibilisierung werden identifiziert und in entsprechenden Maßnahmen (z. B. Workshops) vermittelt.

## Partizipation

1. Einzelne Mitarbeitende sind bei der Definition der Digitalisierungsstrategie und der Umsetzung der Digitalisierungsmaßnahmen eingebunden.
2. Partizipationsmöglichkeiten für Mitarbeitende sind mindestens in Planung.
3. Mitarbeitende kennen Verantwortliche von Digitalisierungsmaßnahmen und bringen sich mindestens reaktiv ein (z. B. melden Mitarbeitende sich mit Feedback zu Digitalisierungsmaßnahmen).
4. Der Dialog zwischen Verantwortlichen von Digitalisierungsmaßnahmen und Mitbestimmungsgremien (z. B. Personalrat, Schwerbehindertenvertretung) zum Thema Inklusion (z. B. hinsichtlich vielfältiger Hintergründe und Altersgruppen) bei Digitalisierungsmaßnahmen erfolgt mindestens anlassbezogen, aber in der Regel noch unregelmäßig.
5. Alle betroffenen Mitarbeitenden werden frühzeitig über relevante Digitalisierungsmaßnahmen informiert und können im Rahmen von Arbeitsgruppen oder Pilotprojekten partizipieren (z. B. bei Anforderungserhebungen oder Tests).
6. Bei der Involvierung ausgewählter Mitarbeitenden in Digitalisierungsmaßnahmen wird auf Inklusion geachtet (z. B. hinsichtlich vielfältiger Hintergründe und Altersgruppen).
7. Alle betroffenen Mitarbeitenden werden aktiv in relevante Digitalisierungsmaßnahmen einbezogen (z. B. bei der Definition der Strategie, der Entwicklung neuer Prozesse, Softwarefunktionen und/oder der Auswahl und Implementierung von Software/Hardware).
8. Regelmäßige Workshops zur Digitalisierung des Gesundheitsamtes werden durchgeführt (z. B. Vorstellen aktueller Digitalisierungsmaßnahmen und -projekte oder Identifikation neuer Digitalisierungsmaßnahmen).
9. Es gibt Mitarbeitende im Team, die den Funktionsumfang der Fachanwendungen kennen, Nutzeranfragen beantworten und Anforderungen an Software-Dienstleister\*innen vermitteln können.
10. Ein Dialog zwischen Digitalisierungsverantwortlichen und Mitbestimmungsgremien (z. B. Personalrat, Schwerbehindertenvertretung) erfolgt mindestens einmal jährlich.
11. Neu eingestellten Mitarbeitenden werden die für ihren Aufgabenbereich relevanten Digitalisierungsmaßnahmen vorgestellt.
12. Die Mitarbeitenden kennen den/die Digitalisierungsverantwortliche\*n, bei dem/der sie z. B. proaktiv ihre Ideen hinsichtlich neuer Digitalisierungsmaßnahmen einbringen können.
13. Mitarbeitende sind interessiert, Fachanwendungen weiterzuentwickeln und vermerken Feedback, welches durch die verantwortliche Person an der Schnittstelle an die Dienstleister\*innen/Hersteller\*innen weitergeleitet wird.
14. Ein Dialog zwischen Digitalisierungsverantwortlichen und Mitbestimmungsgremien (z. B. Personalrat, Schwerbehindertenvertretung) erfolgt mindestens zweimal jährlich.
15. Bei Systemen und Prozessen wird auf eine starke Nutzerzentriertheit gesetzt, zudem wird die Nutzerzentriertheit kontinuierlich analysiert und verbessert (z. B. wird Wert auf Gebrauchstauglichkeit und maximal sinnvolle Digitalisierung gelegt).
16. Das Gesundheitsamt (ggf. durch die Kommune unterstützt) tauscht sich mit anderen Gesundheitsämtern über Bundeslandgrenzen hinweg zu Partizipationsmöglichkeiten von Mitarbeitenden bei der Digitalisierung aus.
17. Das Gesundheitsamt unterstützt andere Gesundheitsämter mit geringerer digitaler Reife (z. B. durch das Anbieten von übergreifenden Workshops oder Beratungsangeboten zu konkreten Digitalisierungsmaßnahmen).

## Schulungen

1. Es existieren einzelne Schulungen zu Kommunikation und Zusammenarbeit, Office-Anwendungen (z. B. Word, Outlook), Fachanwendungen, IT-Sicherheit und zum Datenschutz.
2. Fähigkeiten werden im Umgang mit Office-Anwendungen oder Fachanwendungen mindestens selbständig erworben.
3. Es existieren in regelmäßigen Abständen verpflichtende Schulungen für alle Mitarbeitenden im Gesundheitsamt zu Kommunikation und Zusammenarbeit, Office-Anwendungen (z. B. Word, Outlook, Excel), Fachanwendungen, IT-Sicherheit und Datenschutz.
4. Mitarbeitende können Office- und Fachanwendungen für ihre Aufgaben einsetzen.
5. Verantwortliche der Organisationseinheiten des Gesundheitsamtes ermitteln regelmäßig den Schulungsbedarf ihrer Mitarbeitenden. Das Schulungsangebot wird entsprechend regelmäßig angepasst.
6. Ein Schulungskonzept für alle Mitarbeitenden ist erstellt. Dieses enthält eine Übersicht an (verpflichtenden und empfohlenen) Schulungsangeboten für unterschiedliche Mitarbeitenden-Rollen, eine Priorisierung der Schulungen und eine Ansprechperson für Schulungen.
7. Im Krisenfall können Mitarbeitende schnell für neue Aufgaben geschult werden (z. B. ist der Umgang mit Fachanwendungen gut dokumentiert und aufbereitet).
8. Das erstellte Schulungskonzept ist allen Mitarbeitenden zugänglich und wird ihnen aktiv kommuniziert.
9. Schulungsangebote werden im Schulungskonzept zielgruppenspezifisch und für unterschiedliche Fähigkeitslevel zusammengestellt (z. B. Fachanwendungen, Grundlagen der Prozessorientierung) und mindestens zweimal im Jahr angeboten.
10. Die Schulungsangebote werden so geplant und organisiert, dass sie in den Arbeitsalltag integriert werden können.
11. Bei der Einstellung neuer Mitarbeitenden wird die digitale Kompetenz der Personen beachtet.
12. Die Mitarbeitenden bekommen gemäß ihren Aufgaben relevante Schulungsangebote vorgeschlagen.
13. Es gibt aufgabenspezifische Schulungen, die kontinuierlich und terminunabhängig abgerufen werden können (z. B. als Präsentation, Video).
14. Es werden Rahmenbedingungen für eine digitale Weiterbildungskultur geschaffen (z. B. durch Zugang zu einer Plattform mit unterschiedlichen Schulungsangeboten, selbstbestimmte Teilnahme an Schulungen oder Freiräume für Mitarbeitende für Schulungen).
15. Schulungen werden bedarfsorientiert mindestens zweimal im Jahr zur Auffrischung angeboten.
16. Schulungen werden durch das Gesundheitsamt evaluiert und je nach Ergebnis wiederholt, verbessert oder verworfen.
17. Mitarbeitende geben ihr Wissen aus den Schulungen an andere Mitarbeitende im Gesundheitsamt in einem strukturierten Austauschformat weiter (z. B. durch regelmäßige Termine, Workshops, schriftliche Dokumentationen).
18. Mindestens einzelne Mitarbeitende erhalten Schulungen zu IT-gestützter Dokumentation von Prozessen mittels Prozessmodellierungssprache und Tools zur Prozessmodellierung.
19. Es existiert ein Weiterbildungskonzept für die/den individuelle\*n Mitarbeitenden, das spezifiziert, wie deren/dessen Fähigkeiten kontinuierlich und individuell weiterentwickelt und aufgefrischt werden können.
20. Die Mitarbeitenden können nicht nur an Schulungen aus einem vorgegebenen Schulungskatalog teilnehmen, sondern es werden ihnen auch selbständig ausgesuchte Schulungen (z. B. von externen Plattformen) finanziert.
21. Erfahrungen zu Schulungen werden mit anderen Gesundheitsämtern ausgetauscht. Das Schulungsangebot wird mindestens zweimal im Jahr angepasst.

# Prozessdigitalisierung

## Dokumentation

1. Es gibt ein Konzept, wie fachspezifische Prozesse einheitlich nach einer schriftlichen Vorgabe dokumentiert werden (z. B. durch ein selbst definiertes Flowchart).
2. Es wird ein Abstraktionslevel für die Prozessdokumentation festgelegt, z. B. auf Basis von Verantwortlichkeiten, Input, Output, konkreten Aktivitäten.
3. Es sind einheitliche Dokumentationsrichtlinien (z. B. Modellierungssprache, evtl. auch ohne standardisierte Syntax/Semantik wie z. B. flowchartähnliche Sprachen) und Inhalte der Dokumentation (z. B. Aufgaben, Rollen, Ressourcen, Schnittstellen, Integration von IT) festgelegt.
4. Mindestens einzelne Prozesse sind IT-gestützt entsprechend der Dokumentationsrichtlinie dokumentiert und kommuniziert.
5. Die Mehrheit der standardisierten Prozesse ist IT-gestützt entsprechend der Dokumentationsrichtlinie dokumentiert und kommuniziert.
6. Bei neu hinzukommenden Fachanwendungen werden Prozesse weiterentwickelt, d. h. Verbesserungs- und Veränderungspotenzial wird identifiziert, umgesetzt und dokumentiert.
7. Für Prozesse, die digitalisiert werden sollen, werden Soll-Prozesse definiert und dokumentiert.
8. Ein Austausch mit anderen Gesundheitsämtern bzgl. der Prozessdokumentation findet statt.
9. In Krisenzeiten werden abhängig der Bedarfe, Prozesse neu definiert und dokumentiert.
10. Die wesentlichen Prozesse sind anhand einer standardisierten Modellierungssprache modelliert (z. B. BPMN).
11. Die Mehrheit der standardisierten Prozesse wird durch die IT-Unterstützung automatisch dokumentiert.

## IT-Unterstützung

1. Das Gesundheitsamt definiert Bewertungs- und Beurteilungskriterien für Prozesse, die das Digitalisierungspotenzial von (Teil-)Prozessen abbilden (z. B. Prozesse mit klaren Ablaufregeln, Prozesse mit hoher Ablaufhäufigkeit, niedrigem Ermessensspielraum sowie datenintensive Prozesse).
2. Prozesse werden analysiert, um deren Digitalisierungspotenzial zu bewerten und um darauf basierend eine Entscheidung zu treffen, welche Prozesse digitalisiert werden können.
3. Für Prozesse mit hohem Digitalisierungspotenzial werden geeignete IT-Systeme identifiziert und in die Prozesse integriert (z. B. um Prozesse zu beschleunigen und deren Transparenz zu erhöhen).
4. Mit der Integration der IT-Systeme in die Prozesse werden die Prozessabläufe entsprechend der Funktionalität der IT-Systeme angepasst bzw. die IT-Systeme entsprechend der Prozessabläufe genutzt.
5. Die Dokumentation standardisierter Prozesse wird weitestgehend automatisch durch die IT-Systeme unterstützt.
6. Schnittstellen zwischen den wichtigsten Fachanwendungen werden durch IT-Systeme unterstützt, sodass Daten z. B. nicht an unterschiedlichen Stellen doppelt zu pflegen sind.
7. Einzelne Prozesse sind durch IT-Systeme vollautomatisiert (z. B. Corona-Infektion: Meldung bis Quarantäne-Entlassung).

## Übergreifende Prozesse

1. Es gibt ein Konzept, wie Prozesse über Organisationseinheiten des Gesundheitsamtes hinweg definiert werden.
2. Es existiert eine Prozessdokumentation über mindestens erste Organisationseinheiten hinweg.
3. Mitarbeitende kennen die Prozesse, die direkt mit ihren eigenen Aufgaben in Verbindung stehen.
4. Mitarbeitende kennen die Abhängigkeiten und Schnittstellen von vor- und nachgelagerten Prozessen/Aufgaben.
5. Es existiert eine Prozessdokumentation über alle Organisationseinheiten hinweg.
6. Mitarbeitende kennen die Abhängigkeiten und Schnittstellen von vor- und nachgelagerten Prozessen/Aufgaben und wissen, welcher Input und Output an der Schnittstelle geliefert werden muss.
7. Prozesse sind an ersten Schnittstellen gut aufeinander abgestimmt, sodass Medienbrüche minimiert werden und der Output als Input weiterverwendet werden kann.
8. Die wesentlichen Prozesse sind an allen relevanten Schnittstellen gut aufeinander abgestimmt, sodass Medienbrüche minimiert werden und der Output als Input weiterverwendet werden kann.
9. Zur kontinuierlichen Verbesserung von Prozessen mit gemeinsamen Schnittstellen finden regelmäßig prozessübergreifende Abstimmungen statt.

## Evaluation

1. Eine Evaluation der Prozesse ist mindestens in Planung.
2. Eine Evaluation wesentlicher Prozesse in Hinsicht auf Gütekriterien (z. B. Effektivität oder Effizienz) findet mindestens unstrukturiert statt (z. B. erfolgt die Evaluation rein mündlich und wird nicht zentral gesammelt).
3. Eine Evaluation wesentlicher Prozesse in Hinsicht auf Gütekriterien (z. B. Effektivität, Effizienz) findet strukturiert mit Softwareunterstützung statt (z. B. wird die Evaluation schriftlich in einer vorgegebenen Maske in z. B. Excel zentral gesammelt).
4. Aus der Evaluation werden spezifische Prozessverbesserungsmaßnahmen abgeleitet (z. B. Vereinheitlichung von Prozessen, Reduktion unnötiger Schnittstellen).
5. Das Gesundheitsamt evaluiert kontinuierlich, ob die Prozessdokumentation mit der tatsächlichen Ausführung der Prozesse übereinstimmt. Die Prozessdokumentation wird entsprechend angepasst.
6. Eine Evaluation wesentlicher Prozesse in Hinsicht auf Gütekriterien (z. B. Effektivität, Effizienz) findet strukturiert mit Softwareunterstützung unter Einsatz vordefinierter Kennzahlen (z. B. Prozessdurchlaufzeit, Zufriedenheit der Kunden) statt. Die Evaluation erfolgt mindestens einmal jährlich.
7. Eine Evaluation von Erfolg/Misserfolg der abgeleiteten Prozessverbesserungsmaßnahmen findet statt.
8. Die Prozessdokumentation wird zweimal jährlich geprüft und bei Bedarf angepasst (z. B. auf Vollständigkeit, Übersichtlichkeit, Verständlichkeit und Struktur).
9. Eine Evaluation erster Prozesse erfolgt automatisiert hinsichtlich ausgewählter Kennzahlen.

# IT-Bereitstellung

## IT-Arbeitsplatz

* + 1. Die notwendige Hardware ist für alle Mitarbeitenden je nach Bedarf an jedem Arbeitsplatz zugänglich (z. B. Computer, Drucker, Scanner, Telefon).
    2. Eine Internetverbindung (LAN oder WLAN) ist an jedem Arbeitsplatz gewährleistet.
    3. Betriebssysteme befinden sich auf dem neuesten Stand und Systemupdates sind installiert, sofern den Anforderungen des Gesundheitsamtes entsprochen wird.
    4. Mindestens einzelne Außendienstmitarbeitende haben Zugang zu mobilen geschäftlichen Endgeräten (z. B. Laptops, Mobiltelefone).

1. Eine angemessene Ausstattung für Videokonferenzen und Telekonferenzen ist vorhanden. Das bedeutet, dass alle Mitarbeitenden bei Bedarf Zugriff auf jeweils ein Mikrofon und eine Webcam haben.
2. Eine stabile und leistungsstarke Internetverbindung (LAN oder WLAN) ist an jedem Arbeitsplatz gewährleistet.
3. Mobiles Arbeiten wird ausgewählten Mitarbeitenden durch den Einsatz von mobilen Endgeräten wie z. B. Laptops ermöglicht.
4. Digitale Faxe sind, soweit erforderlich, vorhanden.
5. Ergonomisches und effizientes Arbeiten ist auf Wunsch der Mitarbeitenden möglich (z. B. höhenverstellbare Bildschirme, zweiter Bildschirm, ergonomische Maus).
6. Kompatibilität zwischen den Arbeitsplätzen im Homeoffice und im Außendienst ist teilweise gegeben (z. B. durch Laptop oder Mobiltelefone mit Datenvolumen, sodass Daten zwischen unterschiedlichen Endgeräten übertragen werden können).
7. Im Gesundheitsamt sind Präsentationsmöglichkeiten vorhanden (z. B. Beamer oder Multifunktionsboard).
8. Mobiles Arbeiten (z. B. Homeoffice) wird allen Mitarbeitenden durch Bereitstellung geeigneter Hardware unter Beachtung von IT-Sicherheit und Datenschutz dauerhaft ermöglicht (z. B. durch die Bereitstellung von Laptops oder Tablets).
9. Die ortsunabhängige Zusammenarbeit der Mitarbeitenden wird durch Softwarelösungen für eine digitale Dokumentenablage unterstützt (z. B. File-Sharing).
10. Die ortsunabhängige Zusammenarbeit der Mitarbeitenden wird durch Softwarelösungen für eine digitale Kommunikation unterstützt (z. B. Chatfunktion, Forum etc.).
11. Die Kompatibilität zwischen den Arbeitsplätzen vor Ort, im Homeoffice und im Außendienst ist medienbruchfrei gegeben (z. B. können Fachanwendungen auch auf mobilen Endgeräten außerhalb des Gesundheitsamtes genutzt werden).
12. Einzelne Außendienstmitarbeitende haben je nach Bedarf Zugang zu mobilen geschäftlichen Endgeräten (z. B. Laptops, Tablets, Smartphones), welche mit den entsprechenden Fachanwendungen kompatibel sind.
13. Ausgewiesene Flächen für kollaboratives Arbeiten mit remote Zusammenarbeitsmöglichkeiten inkl. Konferenzsysteme sind vorhanden (z. B. digitales Whiteboard und Multifunktionsboard).
14. Die ortsunabhängige Zusammenarbeit der Mitarbeitenden wird durch Softwarelösungen unterstützt, die das gleichzeitige Bearbeiten von Dokumenten ermöglicht.
15. Alle Außendienstmitarbeitenden haben je nach Bedarf Zugang zu mobilen geschäftlichen Endgeräten (z. B. Laptops, Tablets, Smartphones), welche mit den entsprechenden Fachanwendungen kompatibel sind.
16. Ausgewiesene Flächen für kollaboratives Arbeiten mit remote Zusammenarbeitsmöglichkeiten inkl. Konferenzsysteme sind in ausreichender Anzahl verfügbar (z. B. digitales Whiteboard und Multifunktionsboard).
17. Die ortsunabhängige Zusammenarbeit der Mitarbeitenden wird durch integrative Softwarelösungen für die digitale Kommunikation und Dokumentenablage unterstützt, sodass Mitarbeitende nicht zwischen verschiedenen Softwarelösungen wechseln müssen.
18. Die Zusammenarbeit im Gesundheitsamt wird durch eine intuitiv bedienbare und kontinuierlich betreute Wissens- und Kollaborationsplattform unterstützt.

## Organisation der IT-Beschaffung

1. Es existieren mindestens einzelne Leitlinien für die Beschaffung der IT-Ausstattung.
   * 1. Die Beschaffung der IT-Ausstattung erfolgt zentral und bedarfsorientiert. Sie berücksichtigt Lieferstau/-engpässe.
        1. Die Verwaltung verfügt über ein IT-Ausstattungskonzept.
        2. Die Beschaffung und Verwaltung der IT-Ausstattung erfolgen zentral, bedarfsorientiert und über eine dafür definierte Stelle (z. B. über die IT-Abteilung).
        3. Die Beschaffung der IT-Ausstattung wird evaluiert, sodass Optimierungspotenziale erkannt werden können.
2. Der Bedarf an neuer Hardware für sicheres stationäres Arbeiten wird regelmäßig ermittelt und entsprechend vorausschauend aktualisiert oder ergänzt.
3. Mitarbeitende werden in den Prozess der IT-Beschaffung eingebunden (z. B. können Mitarbeitende IT-Artikel aus einer Auswahl wählen).
4. Der Bedarf an neuer Hardware für sicheres mobiles Arbeiten wird regelmäßig ermittelt und entsprechend vorausschauend aktualisiert oder ergänzt.
5. Qualifiziertes Fachpersonal wie z. B. Arbeitsmediziner\*innen unterstützen bei der Auswahl ergonomischer IT-Hardware.

## Bezug von IT-Infrastruktur

1. Die Definition einer IT-verantwortlichen Person ist mindestens in Planung oder schon erfolgt.
2. Die IT-verantwortliche Person definiert die IT-Sourcing-Strategie für die Infrastrukturkomponenten.
3. Für das Gesundheitsamt stehen die wesentlichen Infrastruktur-Basiskomponenten zur Nutzung zur Verfügung (Netzwerkzugang am Arbeitsplatz, Server und Speicher).
4. Das Gesundheitsamt nutzt mindestens ein Stand-Alone-Rechenzentrum (ohne Redundanz für einen möglichen Ausfall). Das Rechenzentrum kann auch von der darüberliegenden Behörde zur Verfügung gestellt werden und gemeinsam genutzt werden.
5. Die IT-verantwortliche Person ist den Mitarbeitenden bekannt.
6. Es erfolgt eine strukturierte Abstimmung zwischen der IT-verantwortlichen Person, den Organisationseinheites des Gesundheitsamtes und externen IT-Verantwortlichen oder IT-Dienstleister\*innen.
7. Die IT-Infrastruktur unterstützt alle Fachanwendungen.
8. Das Gesundheitsamt (evtl. inkl. dazugehörender Behörde) verfügt über einen Cold- oder sogar Hot-Standby. Das Rechenzentrum kann auch von der darüberliegenden Behörde zur Verfügung gestellt werden und gemeinsam genutzt werden.
9. Ein Konzept für die Evaluation der Leistungsfähigkeit der IT-Infrastruktur wird von einer IT-verantwortlichen Person gemeinsam mit den Organisationseinheiten definiert, ist aber ggf. noch nicht umgesetzt.
10. Ein enger Austausch zwischen der IT-verantwortlichen Person und den Organisationseinheiten ist etabliert, sodass die IT-Infrastruktur entlang der Anforderungen der Organisationseinheit gemeinsam weiterentwickelt wird.
11. Die IT-Infrastruktur wird ganzheitlich über alle Organisationseinheiten hinweg geplant und umgesetzt (z. B. durch eine standortübergreifende IT-Infrastruktur inkl. WLAN bei dezentralen Gesundheitsämtern mit mehreren Standorten).
12. Die IT-Infrastruktur ist modular aufgebaut, sodass einzelne Komponenten flexibel ausgetauscht und erweitert werden können.
13. Das Gesundheitsamt (evtl. inkl. dazugehörender Behörde) verfügt über einen Hot Standby als Notfallschutz. Das Rechenzentrum kann auch von der darüberliegenden Behörde zur Verfügung gestellt werden und gemeinsam genutzt werden.
14. Die IT-Infrastruktur wird nach Kennzahlen der Leistungsfähigkeit durch die IT-verantwortliche Person evaluiert und entsprechend angepasst.
15. Die IT-Infrastruktur (z. B. Server, Speicher, Rechenkapazität) kann in Krisenzeiten schnell erweitert werden, um die Mitarbeitenden in ihren Aufgaben bestmöglich zu unterstützen.
16. Die IT-Infrastrukturkomponenten orientieren sich am aktuellen Stand der Technik und sind für das gesamte Gesundheitsamt konsolidiert.
17. Eine Virtualisierungsstrategie für die IT-Infrastruktur ist definiert. Für die IT-Infrastrukturkomponenten ist spezifiziert, ob und wann diese virtualisiert werden.
18. Anzahl und Größe lokaler und virtueller Komponenten wird im Hinblick auf die Anforderungen der Organisationseinheiten kontinuierlich evaluiert und angepasst.
19. Virtuelle Server und Speicher ermöglichen die ortsunabhängige Arbeitsfähigkeit (z. B. Software ist verfügbar, zentrale Datenablage, Datenaustausch mit anderen Organisationen).
20. Speicher für große Datenmengen werden bereitgehalten.
21. Ein Cloudkonzept mit Anforderungen an die IT-Sicherheit und Datenschutz ist nach Bedarf ausgearbeitet und wird genutzt.
22. Die IT-Infrastruktur wird vom IT-Sicherheitsverantwortlichen proaktiv und kontinuierlich unter Bezug der aktuellsten Technik weiterentwickelt.
23. Die IT-Infrastruktur ermöglicht die bestmögliche Zusammenarbeit mit anderen Organisationen (z. B. wird sie auf Länderebene und, wo sinnvoll, länderübergreifend geplant und umgesetzt).

## Anwendung IT-Service Prozesse

1. Die IT-Service-Prozesse nach ITIL Standard (z. B. Support, Incident-Management, Change-Management, Beschaffungsprozesse) sind der IT-verantwortlichen Person bekannt.
2. Eine Absicherung für Systemausfälle und ad hoc Probleme ist vorhanden (z. B. können Mitarbeitende zur Not auf manuelle Prozesse zurückgreifen und sind auf entsprechende Krisensituationen vorbereitet).
3. Die Prozesse für den Service-Delivery und Support werden definiert und kommuniziert.
4. Für Mitarbeitende bestehen strukturierte Kanäle für die Anfrage von IT-Services (z. B. Hotline, Ticket-Tool).
5. Die IT-Service-Management-Prozesse für Service-Delivery und Support sind etabliert. Zuständige Verantwortlichkeiten sind definiert.
6. Es bestehen sinnvolle Service Level Agreements, die eingehalten werden.
7. Ein IT-Service-Management für eine nachhaltige Ursachenforschung und die Beseitigung von Störungen ist etabliert.
8. Die Qualität des IT-Service-Managements wird anhand von Kriterien (z. B. Verfügbarkeit, Dauer der Störung) gemessen und entsprechend angepasst.
9. IT-Service-Management-Prozesse werden nach geltendem ISO Standard und nach dem Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik zertifiziert.
10. Das IT-Service-Management wird kontinuierlich weiterentwickelt und auf die Bedarfe des Gesundheitsamtes angepasst.

# IT-Sicherheit

## IT-Sicherheitsmanagement

1. Es existieren mindestens erste Ideen hinsichtlich eines IT-Sicherheitskonzepts oder ein IT-Sicherheitskonzept wurde bereits entworfen.
2. Die Rolle eines/einer für das Gesundheitsamt verantwortlichen IT-(Sicherheits)beauftragten ist definiert.
3. Alle relevanten Mitarbeitenden werden in den IT-Sicherheitsprozess integriert.
4. Eine Inventarliste aller physischen Geräte sowie der genutzten Systeme und Anwendungen ist vorhanden.
5. Sicherheitsmaßnahmen sind systematisch in einem IT-Sicherheitskonzept dokumentiert.
6. Der IT-Sicherheitsprozess und die Rolle der/des IT-(Sicherheits)beauftragten werden allen Mitarbeitenden bekannt gemacht.
7. Eine Inventarliste aller physischen Geräte sowie der genutzten Systeme und Anwendungen ist vorhanden und wird nach einem festgelegten Prozess anlassbezogen sowie periodisch gepflegt.
8. Ein zentrales IT-Sicherheitskonzept inkl. Risikomanagement ist vorhanden.
9. Zuständigkeiten und eine geeignete Organisationsstruktur für die IT-Sicherheit sind festgelegt.
10. Das IT-Sicherheitskonzept inkl. IT-Sicherheitsprozesse wird dokumentiert und regelmäßig auf Wirksamkeit und Angemessenheit überprüft.
11. Es existieren definierte Reporting-Mechanismen z. B. in Form von Management-Berichten, welche die wesentlichen relevanten Informationen über den IT-Sicherheitsprozess enthalten, insbesondere über Probleme, Erfolge und Verbesserungsmöglichkeiten.
12. Maßnahmen aus dem IT-Sicherheitskonzept werden in der Praxis vollständig umgesetzt und deren Umsetzung wird regelmäßig kontrolliert.
13. Bei Arbeitsspitzen bzgl. der IT-Sicherheit werden, wenn möglich, zusätzliche interne oder externe Mitarbeitende eingesetzt.
14. Das IT-Sicherheitskonzept wird regelmäßig überprüft und an die Anforderungen des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik angepasst.
15. Die IT-(Sicherheits)beauftragten tauschen sich regelmäßig und bedarfsorientiert zu Themen der IT-Sicherheit im Gesundheitsamt aus und versuchen IT-Sicherheitsrisiken gemeinsam zu reduzieren.

## Umgang mit IT-Sicherheitsrisiken und Angriffen

1. E-Mail-Filter, sichere Browser und Sicherheitsupdates für Hard- und Software werden regelmäßig genutzt.
2. Die Amtsleitung wird ausreichend durch den/die IT-(Sicherheits)beauftragte\*n sensibilisiert und leitet entsprechende Maßnahmen ein (z. B. unterstützt sie/er bei der Durchführung von Schulungsprogrammen zur IT-Sicherheit)
3. Die für die IT-Sicherheit verantwortlichen Personen kennen den CERT-Bund des Bundesamtes für Sicherheit in der Informationstechnik bzw. vergleichbare Landesdienste. (Mouseover Diese Dienste enthalten mindestens die Meldungen des CERT-Bund). Die vorhandenen IT-Systeme werden mindestens einmal pro Halbjahr auf Grundlage der Meldungen des CERT-Bund oder der entsprechenden Meldungen vergleichbarer Landesdienste mit der Risikostufe 4-5 überprüft.
4. Es existieren Sicherheitsrichtlinien für die Detektion von sicherheitsrelevanten Ereignissen.
5. Es sind Meldewege für sicherheitsrelevante Ereignisse definiert.
6. Systemfunktionen zur Detektion von sicherheitsrelevanten Vorfällen auf eingesetzten IT-Systemen sind aktiviert und werden genutzt (z. B. Virenscanner).
7. Vorgaben für den Umgang mit einigen Sicherheitsvorfällen sowie Ansprechpartner\*innen sind festgelegt und den Mitarbeitenden bekannt gemacht.
8. Auf Warn- oder Vorfallsmeldungen wird reagiert bzw. werden diese an die zuständigen Stellen gemeldet.
9. Mindestens einzelne Mitarbeitende haben die Fähigkeit, bei dem Einspielen von Sicherheitsupdates und Softwareupdates unterstützen zu können.
10. Alle Mitarbeitenden und externen Nutzer\*innen werden in den sicheren Umgang mit IT-Komponenten einmalig eingewiesen und sensibilisiert, soweit dies für ihre Arbeitszusammenhänge relevant ist.
11. Die vorhandenen IT-Systeme werden mindestens zweimal jährlich umfassend anhand der CERT-Bund-Meldungen des Bundesamtes für Sicherheit in der Informationstechnik oder der entsprechenden Meldungen vergleichbarer Landesdienste überprüft.
12. Betroffene Mitarbeitende werden ad hoc mit Warnmeldungen über IT-Sicherheitsvorfälle informiert, sodass Daten mit den systemseitigen Tools „sicher“ gelöscht werden können.
13. Die Sicherheitsrichtlinien für die Detektion von sicherheitsrelevanten Vorfällen werden regelmäßig überprüft und sind allen im Bereich IT-Sicherheit zuständigen Mitarbeitenden bekannt.
14. Meldewege für sicherheitsrelevante Ereignisse werden regelmäßig geprüft, erprobt und aktualisiert.
15. Zusätzliche Schadcodescanner auf zentralen IT-Systemen werden bedarfsgerecht installiert und genutzt.
16. Die IT-Sicherheitsrichtlinien und Ansprechpartner\*innen zur Behandlung von Sicherheitsvorfällen sind allen Mitarbeitenden bekannt. Die Kontaktinformationen sind immer aktuell und leicht zugänglich.
17. Vorfälle werden zentral erfasst und die Behebung nachverfolgt bis zu deren Erledigung.
18. Eine zentrale Administration zur Isolierung von betroffenen Geräten und Systemen ist vorhanden. Diese reagiert unverzüglich, mindestens innerhalb desselben Tages.
19. Es existiert eine definierte Stelle, die beim Einspielen von Sicherheitsupdates und Softwareupdates unterstützt.
20. Verbindliche, verständliche und aktuelle Richtlinien zur Nutzung der jeweiligen IT-Systeme stehen allen Mitarbeitenden kontinuierlich zur Verfügung (z. B. über Aushänge, das Intranet oder Impulsvorträge).
21. Die vorhandenen IT-Systeme werden mindestens einmal im Monat anhand der CERT-Bund-Meldungen mit der Risikostufe 4-5 des Bundesamtes für Sicherheit in der Informationstechnik oder der entsprechenden Meldungen vergleichbarer Landesdienste überprüft.
22. IT-Sicherheit wird verpflichtend im Rahmen der Einführung von Geräten, Systemen und Anwendungen und bei Neueinstellungen von Mitarbeitenden mit den entsprechenden Akteur\*innen erörtert.
23. Eine zentrale Protokollierungsinfrastruktur für die Auswertung und Überwachung sicherheitsrelevanter Ereignisse wird genutzt.
24. Für schutzbedürftige Netzsegmente werden zusätzliche Detektionssysteme auf Basis des Netzplans eingesetzt und zentral verwaltet (z. B. Schadcodedetektionssysteme oder zusätzliche netzbasierte Angriffserkennungssysteme).
25. Vorhandenen Detektionssysteme und getroffenen Maßnahmen werden in regelmäßigen Audits auf ihre Aktualität und Wirksamkeit hin überprüft.
26. Eine Vorgehensweise zur Behandlung und Bewertung von Sicherheitsvorfällen ist etabliert, bekannt und wird regelmäßig überprüft (z. B. durch ein Sicherheitsvorfallteam).
27. Die Dokumentation und Nachbereitung der Behebung von Sicherheitsvorfällen erfolgen standardisiert.
28. Die IT-Sicherheit wird proaktiv im Vorfeld von Vorhaben zur Einführung von Geräten, Systemen und Anwendungen mit den Akteur\*innen erörtert (z. B. mit Sicherheitsbeauftragten, Datenschutzbeauftragten, Hausleitung, Personalrat).
29. Die Lernerfolge im Bereich IT-Sicherheit werden zielgruppenbezogen quantitativ und qualitativ gemessen und ausgewertet, um festzustellen, inwieweit die in den Sensibilisierungs- und Schulungsprogrammen zur IT-Sicherheit beschriebenen Ziele erreicht sind (z. B. Anzahl von IT-Sicherheitsvorfällen).
30. Die vorhandenen IT-Systeme werden mindestens einmal im Monat umfassend anhand der CERT-Bund-Meldungen des Bundesamtes für Sicherheit in der Informationstechnik oder der entsprechenden Meldungen vergleichbarer Landesdienste überprüft.
31. Ein Schwachstellenscanner ist im Einsatz und die Auswertung der Erkenntnisse ist in die Sicherheitsprozesse integriert.
32. Die Auswertung der Protokollierungsdaten erfolgt durch spezialisiertes Personal.
33. Der Einsatz von zusätzlichen Detektionssystemen erfolgt nach Schutzbedarfsanforderungen.
34. Prioritäten für die Behandlung von Sicherheitsvorfällen werden vorab festgelegt und regelmäßig aktualisiert.
35. Meldewege für entsprechende Sicherheitsvorfälle erfolgen schnell, einfach und über vertrauenswürdige Kanäle.
36. Ein Expertenteam für die Behandlung und eine dedizierte Stelle zur Meldung von Sicherheitsvorfällen sind eingerichtet.
37. Die IT-Sicherheit wird mindestens einmal pro Quartal mit weiteren relevanten Stakeholder\*innen erörtert (z. B. Hausleitung, Personalrat, Schwerbehindertenvertretung).
38. Die Ergebnisse der Erfolgskontrollmessung fließen in die Verbesserung des Sensibilisierungs- und Schulungsangebots zur IT-Sicherheit in geeigneter Weise ein.
39. Es findet ein regelmäßiger Austausch zwischen IT-(Sicherheits)beauftragten und den anderen für die IT-Sicherheit relevanten Ansprechpartner\*innen (z. B. Datenschutz, Gesundheits- und Arbeitsschutz, Brandschutz) über die Effizienz der Aus- und Weiterbildung statt.
40. Die vorhandenen IT-Systeme werden täglich vollständig gegen die CERT-Bund-Meldungen des Bundesamtes für Sicherheit in der Informationstechnik oder den entsprechenden Meldungen aus vergleichbaren Landesdiensten geprüft.
41. Ein Schwachstellenmanagement ist etabliert und erfolgt kontinuierlich im Rahmen der Sicherheitsprozesse.
42. Ein Austausch mit anderen Behörden oder den zuständigen Landesbehörden oder dem Bundesamt für Sicherheit in der Informationstechnik findet regelmäßig statt.
43. Eine zentrale Detektion und Echtzeitüberprüfung von IT-Ereignismeldungen findet statt.
44. Die Meldung von IT-sicherheitsrelevanten Ereignissen erfolgt durch die eingesetzten Detektionssysteme automatisiert und eine Reaktion erfolgt mit geeigneten Schutzmaßnahmen.
45. IT-Systeme und -Lösungen inkl. Cloud-Lösungen entsprechen der höchsten Sicherheitsstufe und werden kontinuierlich evaluiert und hinsichtlich neuer Anforderungen angepasst.
46. Eine dedizierte Stelle zur Meldung von Sicherheitsvorfällen ist auch außerhalb der normalen Arbeitszeiten verfügbar.
47. Es existiert ein Managementsystem zur Behandlung von IT-Sicherheitsvorfällen, welches regelmäßig auf Wirksamkeit und Aktualität hin überprüft wird.
48. Bestehende Prozesse werden durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen (auch in anderen Gesundheitsämtern) kontinuierlich weiterentwickelt.

## Identitäts- und Zugangsmanagement

1. Die Vergabe von Zutrittsberechtigungen, Zugangsberechtigungen und Zugriffsrechten ist für bestimmte IT-Systeme und Mitarbeitende geregelt.
2. Der Passwortgebrauch ist verbindlich geregelt.
3. Ein Identitäts- und Berechtigungskonzept ist in schriftlicher Form vorhanden.
4. Neben Passwörtern wird der Einsatz zusätzlicher Authentisierungsmerkmale bzw. -verfahren bei schutzbedürftigen Ressourcen evaluiert.
5. Das Identitäts- und Berechtigungskonzept wird in der Praxis vollständig umgesetzt.
6. Es gelten genau definierte Zugriffsregeln für einzelne Benutzende oder Benutzendengruppen auf die Daten eines IT-Systems.
7. Mehr-Faktor-Authentisierung, z. B. mit kryptografischen Zertifikaten, digitalen Signaturen, Chipkarten oder Token, wird genutzt.
8. Aktionen, bei denen das Vier-Augen-Prinzip anzuwenden ist, werden evaluiert (z. B. bei administrativen Tätigkeiten in besonders kritischen IT-Systemen).
9. Die Wirksamkeit der Benutzertrennung am IT-System bzw. an der Anwendung wird fortlaufend kontrolliert und entsprechend angepasst.
10. Die Authentisierungsmechanismen werden bedarfsgerecht gemäß dem Schutzbedarf ausgewählt und kontinuierlich evaluiert.
11. Eine Notfallvorsorge ist etabliert, damit das Gesundheitsamt bei einem ausgefallenen Identitäts- und/oder Berechtigungsmanagement-System weiterhin arbeitsfähig ist.
    * 1. Das Identitäts- und Zugangsmanagement wird regelmäßig an die technischen Voraussetzungen der IT-Systeme angepasst.

# Bürger\*innenzentrierung

## Interaktion

* + 1. Die Kommunikation mit Bürger\*innen erfolgt auch digital (z. B. E-Mail oder Kontaktformulare).
    2. Eine Online-Verfügbarkeit und Web-Präsenz von Informationen über Politik, Dienstleistungen und Ansprechpersonen ist vorhanden.

1. Mindestens eine digitale One-Way Kommunikation vom Gesundheitsamt an Bürger\*innen besteht für passende Angelegenheiten (z. B. durch die Verfügbarkeit von downloadbaren Formularen).
2. FAQs zu den häufigsten Fragen der Bürger\*innen aus den Organisationseinheiten sind online verfügbar (z. B. zu Quarantäneregelungen oder Einreisebestimmungen).
3. Die digitale Two-Way Kommunikation wird ermöglicht (z. B. durch die Möglichkeit für Bürger\*innen Dokumente hochzuladen, E-Mails, Online-Chatroom und Online-Terminvergabe).
4. Den Bürger\*innen wird eine medienbruchfreie Kommunikation ermöglicht. Der Online-Auftritt ist auf Bürger\*innen ausgerichtet und erlaubt eine regelhafte Kommunikation (z. B. Ansprechpersonen sind leicht zu finden und auch über mehrere alternativen Wege zu erreichen).
5. Einfache bzw. grundlegende Beratungsleistungen werden digital vom Gesundheitsamt angeboten (z. B. als Videomaterial oder Videokonferenz).
6. Es wird eine Mischung aus Online- und Offline-Diensten angeboten (z. B. Beratungsangebote über Videokonferenz und in Person).
7. Beratungsgespräche und Angebote zur Gesundheitsförderung bzw. -prävention werden, wenn passend, ergänzend zu Präsenzangeboten auch komplett digital angeboten (z. B. Aufklärungsgespräche zum Thema Prävention, Schwangerenkonfliktberatung, Tumorberatung, Sexualberatung, Risikokommunikation oder Krisenkommunikation).
   * 1. Die individuellen Präferenzen von Bürger\*innen werden in der Interaktion und Kommunikation berücksichtigt (z. B. Adaption der Ansprache entsprechend analoger/digitaler Vorerfahrung und Rückmeldungen der Bürger\*innen, insbesondere auch entsprechend der individuellen Präferenzen bezüglich der digitalen Kanäle).

## Präferenzen

* + 1. Die online verfügbaren Informationen werden regelmäßig durch das Gesundheitsamt aktualisiert.
    2. Ein alternativer Kanal für "nicht-digitale Bürger\*innen" erlaubt eine ausreichende Kommunikation mit dem Gesundheitsamt.
    3. Gesetzliche Vorgaben hinsichtlich der Barrierefreiheit sind umgesetzt.
    4. Proaktive Push-Benachrichtigungen und/oder E-Mail-Benachrichtigungen werden an Bürger\*innen versendet (z. B. Terminerinnerungen oder Fristenerinnerungen).
    5. Das Gesundheitsamt stellt Bürger\*innen die gängigen Onlineanwendungen bereit, mit denen die Bürger\*innen Transaktionen, Authentifizierungen und Verifizierungen ggf. unter Nutzung digitaler Signaturen online erledigt können.
    6. Geschäftsprozesse und IT-Systeme werden von den Bürger\*innenbedürfnissen gesteuert.

# Zusammenarbeit

## Zusammenarbeit innerhalb des Gesundheitsamtes

* + 1. Mindestens eine erste IT-gestützte organisationseinheitenübergreifende Kommunikation findet statt (z. B. per E-Mail).
    2. Das Gesundheitsamt verfügt über eigene gesundheitsamtsspezifische E-Mail-Adresse (z. B. GA@LandkreisX.de).
    3. Es existiert mindestens die Planung einer ersten IT-gestützten Zusammenarbeit über erste Organisationseinheiten eines Gesundheitsamtes hinweg, bei denen eine Zusammenarbeit sinnvoll ist (z. B. Psychosozialer Dienst und Kinder- und Jugendgesundheitsdienst).
    4. Die Mitarbeitenden nutzen gemeinsame digitale Kalender für die Terminplanung.
    5. Es existiert ein digitaler Schichtplan.
    6. Es existiert eine IT-gestützte Zusammenarbeit über mindestens erste Organisationseinheiten hinweg, überall da, wo die Zusammenarbeit sinnvoll ist (z. B. Psychosozialer Dienst und Kinder- und Jugendgesundheitsdienst). Dies geschieht über definierte Schnittstellen für den Datenaustausch, sodass Inkonsistenzen für diese Organisationseinheiten vermieden werden.
    7. Es werden die Empfehlungen eingehalten zu technischen und semantischen Standards, Profilen und Leitfäden der Interoperabilitätsfestlegungen (u. a. die der Gematik).
    8. Das Gesundheitsamt verfügt über ein internes Netzwerk für den internen Datenaustausch.
    9. Es existiert eine IT-gestützte Zusammenarbeit über alle Organisationseinheiten hinweg, für die eine Zusammenarbeit sinnvoll ist (z. B. Psychosozialer Dienst und Kinder- und Jugendgesundheitsdienst). Dies geschieht über definierte Schnittstellen für den Datenaustausch, sodass Inkonsistenzen für diese Organisationseinheiten vermieden werden.
    10. Eine Zusammenarbeit über alle Ebenen hinweg ist realisiert durch die Nutzung einer intuitiv bedienbaren und kontinuierlich betreuten Wissens- und Kollaborationsplattform.
    11. Die Zusammenarbeit basiert standardmäßig auf digitalen standardisierten Prozessen ohne Medienbrüche. Diese Prozesse werden auf Basis neuer Technologien/Standards ständig aktualisiert und weiterentwickelt.
    12. Die Kommunikationsinfrastruktur arbeitet auf Basis aktueller und gemeinsam definierter bzw. zentral normierter Datenaustauschstandards (z. B. mittels HL7).

## Zusammenarbeit zwischen Gesundheitsämtern untereinander und mit Landesstellen

* + 1. Das Gesundheitsamt tauscht sich mit anderen Gesundheitsämtern und Landesstellen aus (z. B. über E-Mail).
    2. Das Gesundheitsamt tauscht sich regelmäßig mit Nachbar-Gesundheitsämtern sowie mit relevanten Landesstellen über IT-gestützte Kanäle aus (z. B. über Videokonferenzen).
    3. Es existiert eine digitale Kommunikation mit Gesundheitsämtern anderer Bundesländer bei Bedarf (z. B. Information über einen Quarantänefall eines Urlaubers).
    4. Mitarbeiter\*innen des Gesundheitsamtes nehmen an übergreifenden Arbeitsgruppen innerhalb des Bundeslandes teil. Dabei nutzen sie digitale Medien (z. B. Videokonferenzen).
    5. Das Gesundheitsamt tauscht sich regelmäßig mit anderen Gesundheitsämtern und mit Landestellen aus. Dieser Austausch geschieht ohne Medienbrüche über digitale Kanäle (z. B. über Videokonferenzen).
    6. Es werden die Empfehlungen eingehalten zu technischen und semantischen Standards, Profilen und Leitfäden der Interoperabilitätsfestlegungen (u. a. die der Gematik).
    7. Das Gesundheitsamt tauscht sich regelmäßig mit anderen Gesundheitsämtern und mit Landestellen aus. Dieser Austausch geschieht ohne Medienbrüche über permanent zur Verfügung stehende digitale Kanäle (z. B. über gemeinsam genutzte Fachanwendungen/Software).
    8. Das Gesundheitsamt tauscht sich mit anderen Gesundheitsämtern zum Vorgehen und Wissen über die Digitalisierung aus (z. B. gemeinsames Nutzerboard zum Austausch für Anforderungen von Fachanwendungen).
    9. Eine Zusammenarbeit über alle Ebenen hinweg ist realisiert durch die Nutzung einer intuitiv bedienbaren und kontinuierlich betreuten Wissens- und Kollaborationsplattform.
    10. Die Zusammenarbeit basiert standardmäßig auf digitalen standardisierten Prozessen ohne Medienbrüche. Diese Prozesse werden auf Basis neuer Technologien/Standards ständig aktualisiert und weiterentwickelt.
    11. Die Kommunikationsinfrastruktur arbeitet auf Basis aktueller und gemeinsam definierter bzw. zentral normierter Datenaustauschstandards (z. B. mittels HL7).

## Zusammenarbeit mit externen Stakeholder\*innen

* + 1. Die digitale Zusammenarbeit mit externen Stakeholder\*innen (z. B. RKI, Krankenhäuser oder Arztpraxen, Gerichte) ist mindestens in Planung oder bereits in der Umsetzung (z. B. über E-Mail).
    2. Kanäle für IT-gestützte Kommunikation/Zusammenarbeit mit ersten externen Stakeholder\*innen (insb. Labore, RKI) können z. B. über Videokonferenzen realisiert werden.
    3. Kanäle für IT-gestützte Kommunikation/Zusammenarbeit mit weiteren externen Stakeholder\*innen (insb. Krankenhäuser, Reha, Hausärzt\*innen, Altenheime) können ad hoc über gemeinsam genutzte Fachanwendungen erstellt werden oder sind über Videokonferenzen möglich.
    4. Es werden die Empfehlungen eingehalten zu technischen und semantischen Standards, Profilen und Leitfäden der Interoperabilitätsfestlegungen (u. a. die der Gematik).
    5. Kanäle für IT-gestützte Kommunikation/Zusammenarbeit mit allen relevanten externen Stakeholder\*innen (Gerichte, Polizei, Forschungspartner\*innen) stehen permanent zur Verfügung, sodass Medienbrüche, inkonsistente Arbeit und Doppeleingaben vermieden werden können (z. B. durch gemeinsam definierte Austauschformate).
    6. Eine Zusammenarbeit über alle Ebenen hinweg ist realisiert durch die Nutzung einer intuitiv bedienbaren und kontinuierlich betreuten Wissens- und Kollaborationsplattform.
    7. Die Zusammenarbeit basiert standardmäßig auf digitalen standardisierten Prozessen ohne Medienbrüche. Diese Prozesse werden auf Basis neuer Technologien/Standards ständig aktualisiert und weiterentwickelt.
    8. Die Kommunikationsinfrastruktur arbeitet auf Basis aktueller und gemeinsam definierter bzw. zentral normierter Datenaustauschstandards (z. B. mittels HL7).

# Software, Daten und Interoperabilität

## Fachanwendungen

* + 1. Fachanwendungen/Software und Geschäftsprozesse werden gemeinsam betrachtet.
    2. Geschäftsprozesse werden durch Fachanwendungen unterstützt.
    3. Fachanwendungen erlauben das gleichzeitige Arbeiten mehrerer Mitarbeitenden auf einer Datenbank, sodass Workarounds unnötig sind.
    4. Fachanwendungen werden bereits (auch teilweise) entlang der Geschäftsprozesse genutzt und akzeptiert.
    5. Bundesweit zentral bereitgestellte Fachanwendungen werden genutzt.
    6. Fachanwendungen decken definierte Best-Practices ab und sind entlang der Geschäftsprozesse ineinander integriert.
    7. Neue, potenzialreiche Software kann ausprobiert und getestet werden (z. B. im Rahmen von Pilotnutzungen).
    8. Fachanwendungen sind resilient in Krisensituationen. Sie sind performant mit hohen Zugriffen, parallelen Nutzenden und erlauben eine Versionsspeicherung.
    9. Eine erste eAkten-konforme Verarbeitung durch Software / Fachanwendungen erfolgt.
    10. Die Fachanwendungen/Software erlauben eine Anbindung von webbasierten Anwendungen (z. B. Symptomtagebuch) und sind ggf. auf einer zentralen Plattform integriert.
    11. Alle Geschäftsprozesse werden durch Fachanwendungen / Software unterstützt.
    12. Geschäftsprozesse und Fachanwendungen werden integriert betrachtet und gemeinsam fortlaufend optimiert. Neue Funktionalitäten/Best Practices werden kontinuierlich integriert.
    13. Modulare Möglichkeiten zur Erstellung neuer digitaler Lösungen sind vorhanden (z. B. für den Einsatz von Chatbots).
    14. Rechtskonformes eAkten-System ist vorhanden.

## Technische Interoperabilität

* + 1. Erste Implementierung von Schnittstellen erfolgt zwischen Fachanwendungen.
    2. Fachanwendungen verfügen bereits über grundsätzliche Schnittstellen zueinander, die aber noch nicht vollständig genutzt werden.
    3. Daten werden in einem gemeinsamen Datenbestand gehalten.
    4. Duplikate werden bereinigt, ggf. manuell bzw. teilautomatisiert.
    5. Der Datentransfer erfolgt mittels standardisierter Schnittstellen mindestens (teil-) automatisiert.
    6. Möglichkeiten für einen institutionsübergreifendenden Datenaustausch sind vorhanden (z. B. beim Infektionsschutz).
    7. Vorhandene Schnittstellen sind, wenn notwendig, bidirektional.
    8. Schnittstellen für den Austausch von Daten zwischen allen wichtigen Stakeholder\*innen werden kontinuierlich an aktuellen Standards angepasst.
    9. Es existieren Gateways/Plattformen als Lösung noch fehlender Schnittstellen (sofern noch Schnittstellen fehlen).

## Datenanalyse, Berichterstattung

* + 1. Grundlegende Datenanalyse-Lösungen sind vorhanden.
    2. Es erfolgt eine Sammlung und Integration von Kennzahlen.
    3. Bestehende Systeme werden durch Schnittstellen in den Meldewegen berücksichtigt.
    4. Eine manuelle oder automatisierte Erstellung von internen Berichten anhand interner Daten erfolgt.
    5. Individualisierte Berichte und Datenabfragen werden generiert.
    6. Analytische Bevölkerungsdaten, einschließlich Big Data, werden in den Betrieb einbezogen.
    7. Es erfolgt eine (teil-)automatisierte Produktion von täglichen Metriken.
    8. Reportings/Daten werden zur Prognose und Entscheidungsunterstützung genutzt.
    9. Meldungen können auch automatisiert versendet werden.
    10. Reportings/Daten werden für die Public Health Forschung bereitgestellt.
    11. Ein vollständiges Datenqualitätsmanagement inkl. Datawarehouse mit einer Business Intelligence-Lösung ist umgesetzt.
    12. Es existiert ein Alarmmanagement auf Basis von Echtzeitdaten.
    13. Die Datenanalyse wird permanent betrieben und optimiert.

## Anforderungen und Dokumentation

* + 1. Die technische Dokumentation von Fachanwendungen ist in Planung oder wird bereits umgesetzt.
    2. Die Anforderungen an Daten sind anhand unterschiedlicher Akteur\*innen definiert.
    3. Es gibt informelle oder formelle Prozesse, um Funktionen und neue Ideen für die Weiterentwicklung von Fachanwendungen zu melden.
    4. Die technische Dokumentation von Fachanwendungen ist umgesetzt.
    5. Fachanwendungen werden systematisch ausgewählt (1. Schwachstellen aus Prozesslandkarte identifiziert; 2. Fachkonzept mit Anforderungen abgeleitet, 3. Auswahl geeigneter Fachanwendungen).
    6. Es besteht ein Lebenszyklus-Konzept für Fachanwendungen / Software.
    7. Updates und Upgrades werden strukturiert geplant und durchgeführt.
    8. Datenqualitäts-Kennzahlen sind definiert und werden regelmäßig ausgewertet.
    9. Es gibt einen definierten Priorisierungsprozess für die Umsetzung von Funktionen.
    10. Anforderungen an User Interfaces und User Experience sind vorhanden und ermöglichen eine hohe Nutzerfreundlichkeit der Anwendungen.
    11. Der Dialog mit Softwarehersteller\*innen wird kontinuierlich verbessert.
    12. Fachanwendungen werden kontinuierlich hinsichtlich Performance, Barrierefreiheit und Datenschutz bewertet und verbessert.
    13. Die Funktionen von Software/Fachanwendungen werden basierend auf neuen technischen Möglichkeiten kontinuierlich ergänzt (z. B. Bilderkennung, Schrifterkennung, Prozessautomatisierung).
    14. Eine schnelle Systemeinrichtung bei der Neuausstattung von Mitarbeitenden ist garantiert.

## Datenschutz

* + 1. Das IT-Datenschutzkonzept bemisst Datenschutz- und IT-Sicherheitsprozesse und beschreibt das Datenschutzniveau.
    2. Fachanwendungen berücksichtigen gesetzliche Vorgaben (z. B. Aufbewahrungsfristen, Anforderungen an die Sicherheit).
    3. Das IT-Datenschutzkonzept umfasst einen Maßnahmenkatalog mit technischen und organisatorischen Maßnahmen.
    4. Die/der Datenschutzbeauftragte\*r wird bei den nötigen Aktionen, die schutzbedürftige Daten umfassen, einbezogen.
    5. Prozesse, die den Datenschutz betreffen, werden laufend anhand der aktuellen gesetzlichen Regelungen aktualisiert.
    6. Es gibt regelmäßig Maßnahmen, die den Mitarbeitenden die Aspekte des Datenschutzes bewusst machen.
    7. Es sind Konzepte zum Schutz von Daten vorhanden (z. B. Pseudonymisierung und Anonymisierung).
    8. Es erfolgt ein Austausch mit anderen Gesundheitsämtern sowie Landesstellen und Bundesbehörden über die Regelungen zum Datenschutz und deren Umsetzung.