VITAKO-LEITFADEN

# Musterverfahrens-beschreibung

## Teil der Leitlinie zum ersetzenden Scannen in Kommunen

Vitako-Projektgruppe ersetzendes Scannen
März 2017

VITAKO
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V.

VITAKO
Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e.V.

## Inhalt

VITAKO
Bundes-Arbeitsgemeinschaft der
Kommunalen IT-Dienstleister e.V.

## Vorbemerkung

Die hier vorliegende Musterverfahrensbeschreibung für kommunale Verwaltungen ist auf der Basis der TR RESISCAN entstanden. Dabei geben die Größe der Verwaltung, das Aufgabenspektrum und nicht zuletzt die IT-Ausstattung einen bestimmten Handlungsspielraum vor, der hier Berücksichtigung findet. Die Zielsetzung der TR RESISCAN, Papierdokumente (Posteingänge und Aktenbestände) mit Erhaltung der Beweiskraft zu scannen, bleibt bestehen. Denn ein wirtschaftlicher Vorteil ergibt sich nicht nur aus der Digitalisierung der Dokumente und damit der Prozesse sondern insbesondere auch durch die Vernichtung der Papierbelege (Raumkapazität, Verfügbarkeit, etc.). Basis für das beweiswerterhaltende Scannen ist neben einer Verfahrensbeschreibung auch die Durchführung einer Schutzbedarfsanalyse für die zu scannenden Dokumente.

Diese Verfahrensbeschreibung befasst sich mit der ordnungsgemäßen Digitalisierung von Dokumenten mit dem Ziel der Aufrechterhaltung der Beweiskraft des Digitalisats im Vergleich zum Papieroriginal. Sie benennt sicherheitsrelevante Maßnahmen, die beim (rechtskonformen) ersetzenden Scannen zu gewährleisten sind. Betrachtet werden nur die von der Behörde selbst durchgeführten Scanprozesse. Bei der Beauftragung externer Dienstleister müssen besondere Rahmenbedingungen beachtet werden, auf die an dieser Stelle nicht eingegangen wird.

Ziel dieser Musterverfahrensbeschreibung ist es, den Scanprozess einfach umsetzen zu können. Die elektronische Akte soll vollständig sein und ein medienbruchfreies Arbeiten ermöglichen.

Mit Hilfe dieser Musterverfahrenbeschreibung kann Schritt für Schritt der örtlich eingesetzte Scanprozess dokumentiert werden. Gliederung und Text sind so angelegt, dass entweder Textpassagen ergänzt werden oder auf die Erstellung notwendiger Dokumente aufmerksam gemacht werden kann. Um ein praktikables und handhabbares Gesamtwerk zu erhalten, wird grundsätzlich empfohlen, mit themenbezogenen Dokumenten als Anlage zu arbeiten. So können bei Veränderungen einzelne Anlagen erneuert werden, ohne das Gesamtwerk verändern zu müssen.

Die individuell modifizierte Musterverfahrensbeschreibung mit den jeweils erforderlichen Anlagen ergibt dann die für Ihre Kommune geltende Verfahrensbeschreibung im Sinne der TR-Resiscan.

# 1 Einleitung

Das vorliegende Dokument ist die Verfahrensbeschreibung für das ersetzende Scannen bei [Organisation] gemäß BSI-TR03138 (TR-RESISCAN).

Nur [die Leitung der Organisation] ist berechtigt Ausführungen und Änderungen der Verfahrensbeschreibung zu genehmigen. Sie wurde von [der Leitung der Organisation] am [Datum] von [Name] freigegeben, trägt die Versionsbezeichnung [Versionsbezeichnung] und gilt ab [Datum] bis zu einer Überarbeitung.

Diese Verfahrensbeschreibung dokumentiert die Maßnahmen und Verfahrensschritte, die für behördeninterne Scanprozesse inkl. der Vernichtung der originären Papierbelege in der [Organisation] gelten.

Die beschriebenen Maßnahmen und Verfahren sind von allen beteiligten Personen zu befolgen. Jeder an einem Prozess-Schritt Beteiligte ist unterwiesen und autorisiert.

# 2 Ersetzendes Scannen

## 2.1 Organisatorisches Umfeld

[Beschreibung des organisatorischen Umfelds]

Hinweis:

Die Struktur der Organisation muss definiert und dokumentiert sein, beispielsweise in einem Gliederungsplan, auf den an dieser Stelle als mitgeltendes Dokument verwiesen wird. Soweit dies bei der Größe der Organisation sinnvoll ist, erfolgt eine kurze Beschreibung der Organisationseinheiten, in denen das ersetzende Scannen relevant ist. Tabellen, Grafiken und Organigramme können die Darstellung vereinfachen. Zum leichteren Verständnis können umfangreiche Erläuterungen als ‚mitgeltende Unterlagen' gesammelt in den Anhang übernommen werden.

Beispiel:

Name und Anschrift der Institution.

Die Behörde gliedert sich gemäß Gliederungsplan lt. mitgeltender Unterlage. Der Betrieb der Behörde erfolgt an mehreren Standorten innerhalb des Gemeinde-/Stadt-/Kreisgebietes.

Das ersetzende Scannen findet an den nachfolgend beschriebenen Orten mit folgenden Scanszenarien statt (Der Nachweis erfolgt in Form einer Tabelle als

Anlage):

- Amt, Fachbereich, Straße, PLZ und Ort,
- Scanszenario (Scannen am Arbeitsplatz, im Amt oder Fachbereich, in einer zentralen Posteingangsstelle),
- Ort der Ablage der Originaldokumente bis hin zur Vernichtung,
- Häufigkeit der Digitalisierung (täglich, wöchentlich, bei Bedarf).

## 2.2 Rechtliche Rahmenbedingungen

Für das ersetzende Scannen bei [Organisation] gelten die einschlägigen rechtlichen und organisatorischen Rahmenbedingungen.

## 2.3 Verarbeitete Dokumente

Digitalisiert werden originär in Papierform vorliegende bzw. eingehende Dokumente, die eine Belegfunktion erfüllen und deshalb einer Dokumentations- und Aufbewahrungspflicht unterliegen. (Vgl. hierzu ausführlich Kap 4.1)

Dies umfasst beispielhaft folgende Belegarten

- Eingangsrechnungen
- Posteingänge
- sonstige Papierdokumente (u.a. papierne Bestandsakten)

## 2.4 Nicht zu vernichtende Dokumente

Explizit von der Vernichtung ausgeschlossen sind Dokumente, denen aufgrund ihrer Beweiskraft, öffentlichen Glaubens oder gesetzlicher Bestimmung im Original besondere Bedeutung zukommt, wie z.B. [Urkunden, Testate unter Siegelverwendung, Eröffnungsbilanzen und Abschlüsse, Wertpapiere, Zollpapiere mit fluoreszierendem Original-Stempel, …], auch wenn sie verarbeitet werden.

Bei einer Durchsicht vor der Vernichtung werden sie ausgesondert und geordnet archiviert. Für diese Dokumente erfolgt eine papierbasierte Aufbewahrung des Originaldokuments nach den entsprechenden Regelungen. (Vgl. hierzu ausführlich Kap 4.1)

## 2.5 Der Scanprozess

Der Prozess für das ersetzende Scannen umfasst folgende Schritte:

- Eingang des Dokuments

- Dokumentenvorbereitung der Papieroriginale
- Scannen der Papieroriginale
- Nachverarbeitung der Digitalisate
- Integritätssicherung der Digitalisate
- Aufbewahrung der Digitalisate
- Vernichtung der Papieroriginale

### 2.5.1 Eingang des Dokumentes

Der Scanprozess beginnt mit dem Eingang des Papierdokumentes an den in der Anlage genannten Orten.

### 2.5.2 Dokumentenvorbereitung

#### *2.5.2.1 Vorsortierung mit Prüfung*

Bei der Sichtung der zu öffnenden Posteingänge bzw. der vorgelegten Dokumente erfolgt eine Prüfung auf Vollständigkeit und Unversehrtheit der Eingangspost. Liegen Zweifel vor, wird das Verfahren bzgl. der betroffenen Dokumente beendet und von einer weiteren Bearbeitung vorläufig abgesehen. Es erfolgt eine Rücksprache mit der zuständigen Stelle und bei Bedarf dem Absender des Dokuments.

#### *2.5.2.2 Identifikation der zu scannenden Belege (rechtliche bzw. faktische Prüfung)*

Die geöffnete Eingangspost wird hinsichtlich des Belegcharakters der einzelnen Dokumente vom zuständigen Personal geprüft. Dabei werden alle zu erfassenden Dokumente für die anschließende Digitalisierung identifiziert.

Besondere Regelungen (Negativliste für z.B. Werbung, Kataloge etc.) werden als mitgeltende Unterlagen dieser Verfahrensbeschreibung hinzugefügt.

| |
|---|
| Hinweis:<br>Besondere Regelungen können sich auf einzelne Organisationseinheiten oder die gesamte Verwaltung (z.B. Postzustellungsurkunden) beziehen. |

Sofern Dokumente wegen ihrer Belegfunktion bereits digitalisiert wurden und in ihrer originalen Papierversion nach der Digitalisierung noch weitere Informationen (z.B. Notizen/Vermerke) auf diesen angebracht werden, die ebenfalls Be-

legcharakter haben, so werden diese Dokumente nochmals digitalisiert und als weitere Version des ursprünglichen Originalbelegs aufbewahrt. Der Zusammenhang zwischen den verschiedenen Versionen des Belegs wird durch die Versionierungsfunktion des eingesetzten DMS gewährleistet.

Haben die zuständigen Beschäftigten Zweifel am Belegcharakter eines Dokuments, so holen sie bei der zuständigen Stelle eine entsprechende Auskunft ein.

#### *2.5.2.3 Vorbereitung der zu digitalisierenden Dokumente (technische Prüfung)*

Alle für eine Digitalisierung identifizierten Belege werden durch das zuständige Personal daraufhin geprüft, ob eine Digitalisierung des Dokuments technisch möglich ist und ein originalgetreues Abbild erzeugt werden kann.

Das zuständige Personal prüft, ob für einen erfolgreichen Scanvorgang vorherige Maßnahmen am Dokument erforderlich sind. Als solche kommen beispielhaft in Frage:

- Lösen von Klammerungen
- Sorgfältiges Sortieren, um die Reihenfolge zu gewährleisten
- Ordnungsgemäße Trennung der Dokumente
- Aufbereiten von Dokumenten mit Notiz- und/oder Klebezetteln in eine Form, die dem Digitalisierungsgerät zugeführt werden kann

### 2.5.3 Scannen

Der Digitalisierungsvorgang beginnt mit der Zuführung der Dokumente durch das zuständige Personal in das Digitalisierungsgerät.

Der Digitalisierungsvorgang endet mit der Ausgabe des digitalen Mediums im eingesetzten Dokumentenmanagementsystem. Eine detaillierte Darstellung des Digitalisierungsvorgangs kann der Anlage [Dokumentenname] entnommen werden.

Vor der Digitalisierung ist zu prüfen, ob alle erforderlichen Hard- und Softwarekomponenten betriebsbereit sind und die vorgegebenen Grundeinstellungen am Digitalisierungsgerät eingestellt sind.

Die Einstellungen für die zu verwendenden Digitalisierungsgeräte sind in der Anlage [Dokumentenname] festgelegt. Je nach Ausprägung des jeweiligen Scanprozesses kann es gegebenenfalls für das gleiche Gerät dokumentenabhängig mehrere Scanprofile geben.

Es wird sichergestellt, dass keine unzulässigen Kompressionsverfahren eingesetzt werden (vgl. TR-RESISCAN). Unzulässig sind insbesondere Bildkompressionsverfahren auf Basis von “Pattern Matching & Substitution” oder “SoftPattern

Matching", wie sie beispielsweise beim JBIG2 Format gemäß ISO/IEC 14492 genutzt werden."

Der Zugriff auf das Digitalisat wird durch das in der Anlage beigefügte Rollen- und Berechtigungskonzept geregelt.

Liegen Papieroriginale in Spezialformaten vor, so erfolgt eine Weiterleitung an eine mit entsprechender Technik ausgestattete und für ersetzendes Scannen autorisierte Scanstelle.

### 2.5.4 Nachverarbeitung

Das zuständige Personal überprüft stichprobenartig, unmittelbar im Anschluss an den Digitalisierungsvorgang, die Vollständigkeit und Lesbarkeit des Digitalisats und nimmt gegebenenfalls Korrekturen vor. Je höher die festgestellte Fehlerquote ausfällt, desto häufiger werden Stichproben durchgeführt.

Durch technische und organisatorische Maßnahmen ist eine nachträgliche Veränderung des Digitalisats ausgeschlossen.

Bei der nachbereitenden Qualitätssicherung sind die Anforderung von Originalbelegen bzw. ein erneutes Scannen technisch und/oder organisatorisch geregelt.

Hinweis:

Der Prozess für die Anforderungen von Originalbelegen bzw. ein erneutes Scannen kann hier oder in einer Anlage genauer beschrieben werden.

### 2.5.5 Integritätssicherung

Die Integrität und Verkehrsfähigkeit der Digitalisate im Vergleich zum Papieroriginal wird durch Anwendung technischer und organisatorischer Maßnahmen abgesichert und gewährleistet:

Hinweis:

Mögliche Anlagen können sein:

- Dokumentation Scan-Software
- Dokumentation DMS-System Anlage Dokumentation Scan-Software
- Anlage Dokumentation DMS-System mit Langzeitspeicher
  falls im Einsatz: Anlage Dokumentation von Zeitstempel- bzw. Signaturkomponenten

### 2.5.6 Aufbewahrung

Für digitalisierte Dokumente gelten die gleichen Regelungen wie für Papierdokumente.

### 2.5.7 Vernichtung des Originals

Die Vernichtung der digitalisierten Papierbelege erfolgt in einem zeitlich festgelegten Turnus für alle Papierbelege, deren Vorhaltefrist abgelaufen ist. Die Vorhaltefrist ist der Zeitraum, in dem ein erneuter Digitalisierungsvorgang angestoßen werden kann. Die für die Aufbewahrung des Papiers zuständige Stelle autorisiert und initiiert die Vernichtung nach festgelegten Vorgaben (Datenschutz). In keinem Falle erfolgt eine Vernichtung vor dem Durchlaufen aller in der vorliegenden Verfahrensbeschreibung dargestellten Schritte.

Bei der Vernichtung werden datenschutzrechtliche Aspekte berücksichtigt. Müssen Originale vor allem aus rechtlichen Gründen als Papierbeleg aufbewahrt werden, erfolgt die Ablage in Papierrumpfakten (Hybridakte).

## 2.6 Das Scansystem

Das Scansystem umfasst die nachfolgend aufgeführten Hardware- und Softwarekomponenten zur Digitalisierung, Integritätssicherung und Aufbewahrung.

Eine Pflege der für die Digitalisierung eingesetzten Hard- und Software obliegt der zuständigen Organisationseinheit. Die Dokumentation der eingesetzten Komponenten erfolgt eigenverantwortlich durch diese Organisationseinheit.

### 2.6.1 Digitalisierung

Die für die Digitalisierung eingesetzten Geräte sind in die IT-Infrastruktur integriert und unterliegen deren Regelungen (IT-Sicherheit). Die Einhaltung dieser Vorgaben wird durch die zuständige(n) Organisationseinheit(en) sichergestellt. Gleiches gilt für die eingesetzte Scansoftware. Ein Nachweis über die zum Digitalisierungszeitpunkt eingesetzte Hard- und Software wird fortlaufend als Anlage [Dokumentenname] dokumentiert.

| |
|---|
| Hinweis:<br><br>Es muss jederzeit erkennbar sein, welche Hard- und Software zu welchem Zeitpunkt im Einsatz war. |

### 2.6.2 Integritätssicherung

Die Integrität des Digitalisats wird durch Anwendung der folgenden technischen und organisatorischen Maßnahmen abgesichert:

- [Darstellung eingesetzter Schutzsoftware oder anderer technischer Maßnahmen]
- sowie die organisatorischen Maßnahmen nach Ziffer 3.1.

Die Integrität der Scansoftware wird eigenverantwortlich durch die Organisationseinheit gewährleistet, die für den Betrieb und die Pflege dieser Komponenten zuständig ist.

### 2.6.3 Aufbewahrung

Nach dem Scanprozess wird das Digitalisat an ein für die langfristige Aufbewahrung geeignetes DMS übergeben.

Die für das DMS verwendeten Komponenten unterliegen der eigenverantwortlichen Aufsicht und Pflege der für das DMS zuständigen Organisationseinheit(en), wobei die Einhaltung der gesetzlich empfohlenen und geforderten Rahmenbedingungen für den Betrieb von Geräten, Software und Netzen der Datenverarbeitung, als eingehalten vorausgesetzt werden.

### 2.6.4 Umgebung

Die Software für die Digitalisierung, Integritätssicherung und Aufbewahrung der digitalisierten Belege wird einer geeigneten Systemumgebung betrieben. Die für die Systemumgebung verwendeten Komponenten unterliegen der eigenverantwortlichen Aufsicht und Pflege der für die Systemumgebung zuständigen Organisationseinheit(en), wobei die gesetzlich empfohlenen und geforderten Rahmenbedingungen für den Betrieb von Geräten, Software und Netzen der Datenverarbeitung, eingehalten werden. Eigenerklärungen zur Konformität sind hinreichend.

# 3 Maßnahmen

Anlage P der TR-RESISCAN definiert Anforderungen, die vom betrachteten Scansystem erfüllt werden sollen. Hierzu wird sowohl die Verfahrensbeschreibung als auch das implementierte Scansystem mit den praktizierten Prozessen betrachtet. Im Einzelnen sind folgende Kategorien relevant:

- Grundlegende Anforderungen mit Strukturanalyse, Schutzbedarfsanalyse und Verfahrensbeschreibung
- Organisatorische Maßnahmen
- Personelle Maßnahmen
- Technische Maßnahmen
- Sicherheitsmaßnahmen bei der Dokumentenvorbereitung
- Sicherheitsmaßnahmen beim Scannen
- Sicherheitsmaßnahmen bei der Nachbearbeitung
- Sicherheitsmaßnahmen bei der Integritätssicherung

Hinweis:

Der Umfang und die Tiefe der Bearbeitung der Themen hängen von dem jeweiligen Scanszenario bzw. vom Schutzbedarf der Dokumente ab und liegen in der Verantwortung der jeweiligen Behörde.

## 3.1 Organisatorische Maßnahmen

### 3.1.1 Verantwortlichkeiten und Regelungen

Die Dokumentenvorbereitung, der Digitalisierungsvorgang, die Nachverarbeitung, die Integritätssicherung, die geeignete Aufbewahrung der Dokumente und die Freigabe zur Vernichtung der Dokumente werden von den in der Anlage [Dokumentenname] genannten Personen oder Funktionen durchgeführt.

### 3.1.2 Regelungen für Wartungs- und Reparaturarbeiten

Die Wartung und die Reparatur der für den Scanvorgang eingesetzten IT-Systeme und Anwendungen werden von der für den Bereich Wartung bestimmten Organisationseinheit eigenverantwortlich durchgeführt.

Externes Personal zur Lösung von Hardware- und Softwareproblemen oder Dienstleister für das DMS System erhalten im Rahmen der Sicherheitsleitlinien nur Zugang zu den entsprechenden Systemen, wenn dies unter Begleitung der zuständigen und verantwortlichen Organisationseinheit stattfindet.

Änderungen an den Systemen, die sich auf diese Verfahrensbeschreibung auswirken können, werden dokumentiert.

### 3.1.3 Lesbarmachung

Es wird sichergestellt, dass die digitalisierten Daten bei Lesbarmachung mit den ursprünglichen papiergebundenen Unterlagen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen. Sie sind während der Dauer der Aufbewahrungsfrist verfügbar und können jederzeit innerhalb angemessener Frist lesbar gemacht werden.

Bei einer Änderung der digitalisierungs- und/oder archivierungsrelevanten Hardware und/oder Software wird neben der Dokumentation der Systemänderung sichergestellt, dass die Lesbarkeit der digitalisierten Dokumente gewährleistet bleibt.

### 3.1.4 Aufrechterhaltung der Informationssicherheit

Für die Informationssicherheit im Scanprozess ist [Name, Vorname oder Funktion in der Organisation] verantwortlich.

In angemessenen zeitlichen Abständen erfolgt eine Überprüfung der Wirksamkeit und Vollständigkeit der für die Informationssicherheit beim ersetzenden Scannen vorgesehenen Maßnahmen.

Die Ergebnisse dieser Überprüfung werden dokumentiert. Sofern Sicherheitslücken oder andere Probleme gefunden werden, werden entsprechende Korrekturmaßnahmen durchgeführt.

Für die Korrekturmaßnahmen wird ein Zeitplan mit verantwortlichen Mitarbeitern definiert. Detaillierte Festlegungen finden sich im jeweiligen Protokoll.

### 3.1.5 Anforderungen beim Outsourcing des Scanprozesses

Die organisatorischen und technischen Schnittstellen zwischen Auftraggeber und Auftragnehmer (Übertragungswege, Datenablageorte, beteiligte Akteure, Rückfallverfahren etc.) sind folgendermaßen gegeben:

- [...]

Der Auftragnehmer wird zur Einhaltung der vom Auftraggeber definierten Sicherheitsmaßnahmen verpflichtet. Dies umfasst insbesondere

- [...]

Die Analyse der durch die Aufgabenteilung zusätzlich entstehenden Risiken hat zu folgendem Ergebnis geführt:

- [...]

Zusätzlich zur regelmäßigen Auditierung werden unangemeldete Stichprobenprüfungen durchgeführt. Verantwortlich für die Durchführung und Auswertung dieser Stichprobenprüfung ist

- [Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation]

Darüber hinaus existieren folgende vertragliche Regelungen:

- [...]

## 3.2 Personelle Maßnahmen

### 3.2.1 Grundlegende Anforderungen

An die in den Scanprozess eingebundenen Beschäftigten werden die folgenden grundlegenden Anforderungen gestellt:

- Kenntnisse vom Aufbau der Organisation
- Umgang mit den relevanten IT-Systemen, DMS-Komponenten und dem IT-Netzwerk

### 3.2.2 Verpflichtung der Beschäftigten

Die im Rahmen der fachlichen Schutzbedarfsanalyse identifizierten Rahmenbedingungen werden den in den Scanprozess involvierten Beschäftigten zur Kenntnis gebracht. Die Beschäftigten werden auf die Einhaltung der einschlägigen Gesetze, Vorschriften, Regelungen und der Verfahrensbeschreibung verpflichtet.

Diese Verpflichtung wird von der für die Beschäftigten zuständigen Organisationseinheit umgesetzt.

### 3.2.3 Maßnahmen zur Qualifizierung und Sensibilisierung

#### *3.2.3.1 Einweisung zur ordnungsgemäßen Bedienung des Scansystems*

Die Beschäftigten, die den Scanvorgang durchführen, werden durch Personal der festgelegten Organisationseinheit hinsichtlich der eingesetzten Geräte, Anwendungen und sonstigen Abläufe eingewiesen. Dies umfasst insbesondere

- die grundsätzlichen Abläufe im Scanprozess einschließlich der Dokumentenvorbereitung, dem Scannen, der Indexierung, der zulässigen Nachbearbeitung und der Integritätssicherung,
- die geeignete Konfiguration und Nutzung des Scanners und der Scan-Workstation,
- Anforderungen hinsichtlich der Qualitätssicherung,
- die Konfiguration und Nutzung der Systeme zur Integritätssicherung und
- das Verhalten im Fehlerfall.

Hierfür werden die in der Anlage [Dokumentenname] aufgeführten Dokumente genutzt.

#### *3.2.3.2 Einweisung zu Sicherheitsmaßnahmen im Scanprozess*

Zuständige Beschäftigte, die den Scanvorgang durchführen oder verantworten, werden durch Personal der zuständigen Organisationseinheit in geeigneter Weise hinsichtlich der dabei umzusetzenden sowie der implementierten Sicherheitsmaßnahmen eingewiesen. Dies umfasst insbesondere:

- die Sensibilisierung der Beschäftigten für Informationssicherheit,
- personenbezogene Sicherheitsmaßnahmen im Scanprozess,
- systembezogene Sicherheitsmaßnahmen im Scansystem,
- Verhalten bei Auftreten von Schadsoftware,
- Bedeutung der Datensicherung und deren Durchführung,
- Umgang mit personenbezogenen und anderen sensiblen Daten und
- Einweisung in Notfallmaßnahmen.

Hierfür werden die in der Anlage [Dokumentenname] aufgeführten Dokumente genutzt.

#### *3.2.3.3 Schulung des Wartungs- und Administrationspersonals*

Personal, das IT-Systeme und Anwendungen für den Scanprozess wartet und administriert, wird hinsichtlich der hierfür notwendigen Kenntnisse durch die zuständige Organisationseinheit geschult.

Hierfür werden die in der Anlage [Dokumentenname] aufgeführten Dokumente genutzt.

#### *3.2.3.4 Sensibilisierung der Beschäftigten in Bezug auf Informationssicherheit*

Alle am Scanprozess beteiligten Beschäftigten werden zur Einhaltung der Regelungen zur Informationssicherheit sensibilisiert. Die beteiligten Mitarbeiter ver-

pflichten sich mit Ihrer Unterschrift zur Einhaltung dieser Verfahrensbeschreibung.

## 3.3 Technische Maßnahmen

### 3.3.1 Grundlegende Sicherheitsmaßnahmen für IT-Systeme

Die in den Scanprozess involvierten IT-Systeme werden gemäß der Anlage [Dokumentenname] betrieben.

### 3.3.2 Zulässige Kommunikationsverbindungen

Da die für das Scannen eingesetzten IT-Systeme über ein Netzwerk verbunden sind, werden in diesem Netzwerk sowie auf den IT-Systemen selbst die zulässigen Kommunikationsverbindungen durch entsprechende Maßnahmen geschützt. Die für den Bereich Kommunikationsverbindungen verantwortliche Organisationseinheit dokumentiert eigenverantwortlich die angewendeten Maßnahmen. Bei einer neu geschaffenen Infrastruktur, die sich von bisher verwendeten Schutzkomponenten unterscheidet, bestätigt die Organisationseinheit die Wirksamkeit des Schutzes der verwendeten Schutzkomponenten. Ist eine Netzinfrastruktur bereits vorhanden, die schutzkonform bereits eingesetzt wird, so ist deren Wirksamkeit als gegeben anzunehmen.

### 3.3.3 Schutz vor Schadprogrammen

Die für den Bereich Schutz vor Schadprogrammen zuständige Organisationseinheit dokumentiert eigenverantwortlich die angewendeten Maßnahmen. Nur für den Fall der Abweichung von den bisher angewendeten Schutzmaßnahmen, bestätigt die Organisationseinheit die Wirksamkeit der getroffenen Maßnahmen. Ansonsten wird der Schutz als gegeben angesehen.

# 4 Anlagen

Neben den vorstehend aufgeführten Regelungen gelten folgende Dokumente:

- [...]

Beispiele:

- Anwenderhandbücher
- weitere Arbeits- und Organisationsanweisungen
- Berechtigungskonzept
- Bericht über Prüfung des Archivsystems
- Freigaberichtlinien
- IT-Sicherheitskonzept
- Organigramme
- Vereinbarung/Vertrag zwischen X und Y

VITAKO
Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V.

Diese Musterverfahrensbeschreibung für das ersetzende Scannen in Kommunen wurde im Jahr 2016 von einer Reihe kommunaler Akteure erarbeitet, die sich unter dem Dach von Vitako in einer Projektgruppe ersetzendes Scannen zusammen gefunden haben. Wir bedanken uns herzlich bei allen Akteuren für das große Engagement.

An diesem Dokument mitgewirkt haben

| **Kommunen** | |
|---|---|
| Gemeinde Neu Wulmstorf | Katja Kockmann |
| Kreis Paderborn | Sabrina Koch |
| Landkreis Breisgau-Hochschwarzwald | Andreas Gippert und Thomas Östreich |
| Landkreis Ludwigslust-Parchim | Andreas Schreiber |
| Landkreis Schwäbisch-Hall | Robert Schneider |
| Landkreis Schwarzwald-Baar-Kreis | Sigrid Faden |
| Landkreis Weilheim-Schongau | Stephan Grosser |
| Stadt Erlangen | Claudia Kauffmann |
| Stadt Freiburg | Burkhard Hermann |
| Stadt Hagen | Marco Hasken |
| Stadt Köln | Lutz Hensel |
| Stadt Nürnberg | Susanne Schieck |
| Stadt Olpe | Georg Schnüttgen |
| Stadt Paderborn | Daniel Prior |
| Stadt Witten | Thomas Heucken |
| Städteregion Aachen | Manuela Henn |
| **Kommunale IT-Dienstleister** | |
| Citkomm | Volker Rombach |
| Dataport | Marit Heidrich |
| KDVZ Rhein-Erft-Rur Frechen | Falk Trauttmansdorff |
| KIVBF | Stefan Rotter |
| KRZ Minden-Ravensberg/Lippe | Frank Lehnert |
| Lecos GmbH | Katrin Gottschling |
| **Weitere Institutionen** | |
| BSI | Astrid Schumacher |
| Deutscher Landkreistag | Heino Sauerbrey |
| Vitako | Tina Siegfried |