Bundesamt
für Sicherheit in der
Informationstechnik

BSI Technische Richtlinie 03138 Ersetzendes Scannen

Bezeichnung:	Ersetzendes Scannen (RESISCAN) Anwendungshinweis V – Exemplarische Verfahrensanweisung
Kürzel:	BSI TR-03138-V
Version:	1.2.1
Datum:	24.06.2020

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: resiscan@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Hinweis: Das vorliegende Dokument enthält Textbausteine für eine exemplarische Verfahrensanweisung und zielt darauf ab, die Einführung und/oder Durchführung eines ordnungsgemäßen Scanprozesses gemäß der BSI Richtlinie „Ersetzendes Scannen (RESISCAN)“ [BSI-TR03138] zu unterstützen. Sie stellt eine Hilfestellung bei der anwendungsbezogenen Umsetzung der durchzuführenden Maßnahmen entsprechend dem im konkreten Anwendungsbereich ermittelten Schutzbedarf dar. Um die Umsetzung zu erleichtern, ist das Dokument wie ein Template mit Platzhaltern für die jeweilige Institution/Organisation erstellt worden. Abweichungen sind möglich, jedoch wird empfohlen, insbesondere auf Vollständigkeit der Maßnahmen und zu treffenden Regelungen zu achten.

Das vorliegende Dokument ist die Verfahrensweisung für das ersetzende Scannen bei [Organisation] gemäß [BSI-TR03138].

Nur die Leitung der Organisation ist berechtigt Ausführungen und Änderungen der Verfahrensanweisung zu genehmigen, namentlich [Leiter der Organisation].

Diese Verfahrensanweisung wurde von der Leitung der Organisation am [Datum] von [Name] freigegeben, trägt die Versionsbezeichnung [Versionsbezeichnung] und gilt ab [Datum] bis zu einer Überarbeitung.

Hinweis: Absatz streichen, sofern nicht anwendbar.

Die vorliegende Verfahrensanweisung ersetzt die bis dahin geltende Verfahrensanweisung [vorherige Versionsbezeichnung].

Diese Verfahrensanweisung dokumentiert die Maßnahmen und Verfahrensschritte, die für den Scanprozess inkl. der Vernichtung der originären Papierbelege in der [Organisation] gelten.

Die beschriebenen Maßnahmen und Verfahren sind von allen beteiligten Personen, die an den einzelnen Prozess-Schritten beteiligt sind sowie für diese unterwiesen und autorisiert wurden, zu befolgen.

Diese Verfahrensanweisung ist beschränkt auf eine ordnungsmäßige Digitalisierung von Dokumenten mit dem Ziel der Aufrechterhaltung der Beweiskraft des Digitalisats im Vergleich zum Papieroriginal, unter Berücksichtigung der geltenden Ordnungsmäßigkeitsanforderungen. Sonstige im Vergleich zu Papierbelegen analogen Verfahren bleiben unangetastet und gelten weiterhin gemäß der in der [Organisation] getroffenen Regelungen.

2 Überblick

2.1 Organisatorisches Umfeld

Hinweis: Entsprechende Beschreibung der Organisation samt Branchenbesonderheiten einfügen.

[Kurze Beschreibung der Organisation: Name, Sitz, Rechtsform, Branche, Geschäftszweck.]

[Kurze Erläuterung von Branchenbesonderheiten der Organisation bzgl. der Verarbeitung und Aufbewahrung von Dokumenten.]

[Soweit dies bei bei der Größe der Organisation sinnvoll ist, erfolgt eine kurze Beschreibung der für das ersetzende Scannen relevanten Organisationseinheiten.]

In der Institution fallen zu digitalisierende Dokumente in folgenden Organisationseinheiten und Prozess-Schritten an:

- [Organisationseinheit:] [Prozess-Schritt, z. B. Bearbeitung der Eingangspost]
- [...]

Die Digitalisierung findet an nachfolgend beschriebenen Orten statt:

- [ggf. Adresse, Raum].
- [...]

Die Ablage der Originaldokumente bis hin zur Vernichtung erfolgt an folgenden Orten:

- [ggf. Adresse, Raum].

Die Digitalisierung erfolgt [fallweise/in [täglichen/wöchentlichen/monatlichen] Digitalisierungsläufen].

2.2 Rechtliche Rahmenbedingungen

Für das ersetzende Scannen bei [Organisation] sind die folgenden rechtlichen Rahmenbedingungen zu berücksichtigen:

- [... siehe auch [BSI-TR03138-R]]

2.3 Verarbeitete Dokumente

Digitalisiert werden originär in Papierform vorliegende bzw. eingehende Dokumente, die eine Belegfunktion erfüllen und deshalb einer Dokumentations- und Aufbewahrungspflicht unterliegen.

Dies umfasst insbesondere

- [...]

2.4 Nicht verarbeitete Dokumente

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

Diese werden explizit von der [Erfassung und] Vernichtung ausgenommen. Dafür werden sie [im Rahmen der Dokumentenvorbereitung/bei einer Durchsicht vor der Vernichtung] ausgesondert und geordnet archiviert. Für diese Dokumente erfolgt eine papierbasierte Aufbewahrung des Originaldokuments nach den entsprechenden Regelungen [der Organisation]. In Zweifelsfällen holt der für die Zuordnung der Dokumente zum Scannen zuständige Mitarbeiter[1] Auskunft bei der zuständigen Führungskraft ein.

2.5 Der Scanprozess

Der Prozess für das ersetzende Scannen bei [Organisation] umfasst folgende Schritte:

- Eingang des Dokumentes
- Dokumentenvorbereitung
- Scannen
- Nachverarbeitung
- Integritätssicherung

Hinweis: Hinsichtlich der Aufbewahrung (siehe auch Abschnitt 2.6.3) ist zu entscheiden, ob im Rahmen der vorliegenden Verfahrensanweisung die komplette Aufbewahrung während des gesamten Aufbewahrungszeitraumes der Unterlagen oder nur die Aufbewahrung der Unterlagen bis zur Übergabe an ein zur langfristigen Aufbewahrung geeignetes System erfasst wird.

- Aufbewahrung [bis zur Übergabe an Langzeitspeicher]
- Vernichtung des Originals

2.5.1 Eingang des Dokumentes

Der Scanprozess beginnt mit dem Eingang des papiergebundenen Dokumentes [an Ort].

2.5.2 Dokumentenvorbereitung

2.5.2.1 Vorsortierung mit Prüfung auf Echtheit

Der Posteingang wird unter Beachtung der Vollständigkeit (kein Verlust von eingegangenen Sendungen, keine ungeprüfte Vernichtung) vom zuständigen Mitarbeiter geöffnet, gesichtet und nach den organisationsinternen Vorgaben [mit einem Posteingangsstempel versehen,] vorsortiert und [an Ort] abgelegt.

Bei der Sichtung erfolgt eine Prüfung auf Echtheit und Unversehrtheit der Eingangspost. Liegen Zweifel vor (z. B. fehlender Stempel auf Original; fehlende Unterschriften; fehlende Form; Beschädigungen, z. B. Risse; fehlende Seiten, z. B. erkennbar an durchbrochener fortlaufender Nummerierung), wird das Verfahren bzgl. der betroffenen Dokumente beendet und von einer weiteren Bearbeitung vorläufig abgesehen. Es erfolgt eine Rücksprache mit der zuständigen Führungskraft und bei Bedarf dem Absender des Dokuments.

1 Im Rahmen der vorliegenden Verfahrensanweisung sind unter dem Begriff „Mitarbeiter“ sowohl weibliche als auch männliche Mitarbeiter umfasst.

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

Die geöffnete, [gestempelte] und vorsortierte Eingangspost wird hinsichtlich des Belegcharakters der einzelnen Dokumente vom zuständigen Mitarbeiter geprüft. Dabei werden alle gemäß Abschnitt 2.3 zu erfassenden Dokumente für die anschließende Digitalisierung identifiziert und an [Ort] abgelegt. Der dem Schutzbedarf angemessene Zugriffsschutz wird durch [...] gewährleistet.

Sofern in der Organisation die entsprechenden 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 Belegcharakter 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 [...] gewährleistet.

Hat der zuständige Mitarbeiter Zweifel am Belegcharakter eines Dokuments, so holt er bei der zuständigen Führungskraft eine entsprechende Auskunft ein.

2.5.2.3 Vorbereitung der zu digitalisierenden Dokumente (technische Prüfung)

Alle für eine Digitalisierung identifizierten Belege werden durch den zuständigen digitalisierenden Mitarbeiter daraufhin geprüft, ob eine Verarbeitung durch das Digitalisierungsgerät technisch möglich ist und ein originalgetreues Abbild erzeugt werden kann.

Es wird im Einzelnen geprüft, 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
- Ordnungsgemäßes Einlegen von Trennblättern
- Entfernen von Notiz- und Klebezetteln

2.5.3 Scannen

Der Beginn des Digitalisierungsvorgangs besteht im Auflegen auf das Digitalisierungsgerät bzw. im Einlegen in den Einzug durch den zuständigen Mitarbeiter.

Der Digitalisierungsvorgang endet mit der Ausgabe des digitalen Mediums und der Speicherung [auf dem Export-Datenpfad/...]. Darüber hinaus sind folgende Details zu berücksichtigen:

- [...]

Vor der Digitalisierung prüft der zuständige Mitarbeiter, ob alle erforderlichen Hard- und Softwarekomponenten betriebsbereit sind und die vorgegebenen Grundeinstellungen am Digitalisierungsgerät eingestellt sind.

Es wird sichergestellt, dass keine unzulässigen Kompressionsverfahren (siehe Anforderung A.SC.12 in [BSI TR-03138]) eingesetzt werden.

Die Grundeinstellungen für die Digitalisierung sind folgendermaßen definiert:

- [...]
- Zielformat: [PDF/TIFF/...]
- Auflösung: [X] dpi
- [Farbscan/Graustufenscan/Schwarz-Weiß-Scan] mit [Einstellung]
- Kontrast: [Einstellungen zu Kontrast]
- [Automatischer/manueller] und [einseitiger/beidseitiger] Einzug

- Durch [...] ist sichergestellt, dass keine unzulässigen Kompressionsverfahren[2] eingesetzt werden.
- [...]

Der Umgang mit Vorder-/Rückseite ist wie folgt geregelt:

- [Es wird immer Vor- und Rückseite gescannt]
- [Die Rückseite wird nur dann nicht gescannt, wenn sie leer ist]
- [...]

Die Zwischenablage und Benennung der erzeugten Scandateien ist wie folgt geregelt:

Ablageort/Verzeichnis: [...]

- Namenskonvention: [...]
- [...]

2.5.4 Nachverarbeitung

Nach dem Scanvorgang werden die Papieroriginale vollständig und in unveränderter Ordnung zum Zwecke der Kontrolle und der weiteren Behandlung in einer gegen unbefugten Zugriff geschützten Weise [an Ort] abgelegt.

Der zuständige Mitarbeiter stellt unmittelbar im Anschluss an die Digitalisierung sicher, dass jeder Papierbeleg genau einmal gescannt wurde (Vollständigkeit und Existenz der digitalisierten Kopie). Dies ist insbesondere bei mehrseitigen Originaldokumenten von Bedeutung, wobei auch auf die fortlaufende Nummerierung der Seiten geachtet wird. Fehlende digitale Dokumente werden erneut der Digitalisierung zugeführt, Mehrfachdigitalisierungen werden bis auf eine Kopie gelöscht oder entsprechend als Kopie gekennzeichnet und von einer doppelten Weiterverarbeitung ausgeschlossen.

Der zuständige Mitarbeiter überprüft zudem auf bildlich und inhaltlich korrekte Übertragung des Inhalts des papierbasierten zum digitalen Dokument, um einem Informationsverlust oder Informationsveränderungen vorzubeugen (Lesbarkeits- und Plausibilitätskontrolle).

Hierbei erfolgt eine [vollständige/stichprobenartige] Sichtkontrolle[, die mindestens x % der verarbeiteten Dokumente umfasst].

Fehlerhafte digitale Dokumente werden erneut der Digitalisierung zugeführt, Mehrfachdigitalisierungen werden bis auf eine Ausfertigung gelöscht oder entsprechend als Kopie gekennzeichnet und von einer doppelten Weiterverarbeitung ausgeschlossen.

Eine unautorisierte manuelle Veränderung des Scanproduktes ist ausgeschlossen, da [...].

Das Scanergebnis in Form des digitalisierten Belegs wird im Zuge der Nachverarbeitung um folgende Index- und Metadaten angereichert:

- [...]

2 Unzulässig wären insbesondere Bildkompressionsverfahren auf Basis von „Pattern Matching & Substitution“ oder „Soft Pattern Matching“, wie sie beispielsweise beim JBIG2 Format gemäß ISO/IEC 14492 genutzt werden.

2.5.5 Integritätssicherung

Die Integrität der digitalen Beleg-Kopie mit dem Beleg-Original wird durch Anwendung folgender technischer und organisatorischer Maßnahmen abgesichert:

- [...]

Die Verkehrsfähigkeit der digitalen Beleg-Kopien ist durch [...] gewährleistet.

2.5.6 Aufbewahrung [bis zur Übergabe an Langzeitspeicher]

Die digitalisierten Belege werden unter Verwendung der in Abschnitt 2.6 beschriebenen Systeme bis [zum Ende der Aufbewahrungszeit/zur Übergabe der Unterlagen an ein für die langfristige Aufbewahrung geeignetes System] (vgl. Abschnitt 2.2) aufbewahrt. Die Verfügbarkeit, Auffindbarkeit und Lesbarkeit wird durch folgende Maßnahmen sichergestellt:

- [...]
- Insbesondere erfolgt eine Löschung der digitalen Archivbestände nicht vor Ablauf der Aufbewahrungsfrist. Sie ist nach Prüfung der Aufbewahrungsfristen ausschließlich von den dafür zuständigen Mitarbeitern zu autorisieren und von zuständigen Mitarbeitern durchzuführen.

2.5.7 Vernichtung des Originals

Die Vernichtung der digitalisierten Papierbelege erfolgt in einem zeitlich festgelegten Turnus, und zwar [täglich/wöchentlich/monatlich/...] für alle Papierbelege mit einem Alter von mehr als [einem Tag/einer Woche/einem Monat]. Sie wird vom zuständigen Mitarbeiter autorisiert und vom zuständigen Mitarbeiter durchgeführt.

In keinem Falle erfolgt eine Vernichtung vor dem Durchlaufen aller in der vorliegenden Verfahrensdokumentation dargestellten Schritte inkl. mindestens eines durchgeführten Backup-Laufes.

Bei der Vernichtung werden datenschutzrechtliche Aspekte berücksichtigt, indem [alle Belege/alle Belege mit Personenbezug] vollständig nach den Empfehlungen des Datenschutzes je nach Vertraulichkeitsstufe geschreddert werden.

2.6 Das Scansystem

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

2.6.1 Digitalisierung

Für die Digitalisierung kommt folgende Hardware zum Einsatz:

- [...]

Weitere Angaben über die eingesetzte Hardware der Digitalisierung sind [...] zu entnehmen.

Für die Digitalisierung kommt folgende Software zum Einsatz:

- [...]

Weitere Angaben über die eingesetzte Software der Digitalisierung sind [...] zu entnehmen.

2.6.2 Integritätssicherung

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

- [...]

Für die Integritätssicherung der Scanprodukte kommt folgende Hardware zum Einsatz:

- [...]

Weitere Angaben über die eingesetzte Hardware zur Integritätssicherung sind [...] zu entnehmen.

Für die Integritätssicherung der Scanprodukte kommt folgende Software zum Einsatz:

- [...]

Weitere Angaben über die eingesetzte Software zur Integritätssicherung sind [...] zu entnehmen.

Für den Schutz der Integrität der in den Scanprozess involvierten Systeme sind die in Abschnitt 3.3.3 näher erläuterten Maßnahmen vorgesehen.

2.6.3 Aufbewahrung [bis zur Übergabe an Langzeitspeicher]

Für die Aufbewahrung der digitalisierten Belege [bis zur Übergabe an ein für die langfristige Aufbewahrung geeignetes System] kommt folgende Hardware zum Einsatz:

- [...]

Weitere Angaben über die für die Aufbewahrung der digitalisierten Belege eingesetzte Hardware sind [...] zu entnehmen.

Für die Aufbewahrung der digitalisierten Belege kommt folgende Software zum Einsatz:

- [...]

Weitere Angaben über die für die Aufbewahrung der digitalisierten Belege eingesetzte Software sind [...] zu entnehmen.

Details zum Speichermedium für die digitalisierten Belege sowie deren Ablage sind [...] zu entnehmen.

Hinweis: Sofern im Rahmen der vorliegenden Verfahrensdokumentation die zuverlässige, langfristige Aufbewahrung berücksichtigt wird, müssen beispielsweise auch entsprechende Festlegungen zu Backups getroffen werden.

Die gespeicherten Belege werden durch folgende Verfahren einem systematischen Backup- Prozess unterzogen, damit im Falle eines Ausfalls des Speichermediums jederzeit eine vollständige und verlustfreie Wiederherstellung der Daten im Archivsystem erreicht werden kann:

- [technische Verfahren der Absicherung, z. B. tägliche Spiegelung]
- [Backup-Verfahren; Turnus und Logik der Backups]

Sowohl bei Ersteinrichtung als auch turnusmäßig ([monatlich/halbjährlich/jährlich]) erfolgt ein Funktionsfähigkeitstest des Backup- und Wiederherstellungsverfahrens.

Sowohl bei Ersteinrichtung als auch turnusmäßig ([monatlich/halbjährlich/jährlich]) erfolgt ein stichprobenartiger Lesbarkeitstest von digitalisierten Belegen im Archivsystem.

[Durch folgende Maßnahmen/Aus folgenden Gründen] ist sichergestellt, dass die Zuverlässigkeit der Speicherung im Hinblick auf den Schutzbedarf der Datenobjekte angemessen ist:

- [...]

2.6.4 Umgebung

Die Software für die Digitalisierung, Integritätssicherung und Aufbewahrung der digitalisierten Belege läuft in folgender Systemumgebung:

- [...]

Weitere Angaben über die Umgebung der eingesetzten Software sind [...] zu entnehmen.

Für die eingesetzten Hard- und Software-Komponenten liegen folgende Softwarebescheinigungen oder Zertifikate vor, die auch Teil des Auswahlprozesses dieser Komponenten waren:

- [...]

Angaben über die notwendige Einsatzumgebung der eingesetzten Software sind [...] zu entnehmen.

3 Maßnahmen

3.1 Organisatorische Maßnahmen

3.1.1 Verantwortlichkeiten und Regelungen

Die nachfolgend aufgeführten Mitarbeiter sind zur Durchführung der einzelnen Verarbeitungsschritte eingewiesen und verantwortlich:

- [...]

3.1.1.1 Dokumentenvorbereitung

Die Dokumentenvorbereitung wird durchgeführt von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

3.1.1.2 Scannen

Der Digitalisierungsvorgang wird durchgeführt von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

3.1.1.3 Nachverarbeitung

Die Nachverarbeitung, die insbesondere die Vollständigkeits-/Lesbarkeits- und Plausibilitätskontrolle umfasst, wird durchgeführt von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

Hinweis: Sofern besonders schutzwürdige Dokumente verarbeitet werden und hierfür gesonderte Regelungen vorgesehen sind, sind die folgenden Passagen relevant.

Es ist nur folgenden Personen gestattet die Digitalisierung, Vollständigkeits-/Lesbarkeits- und Plausibilitätskontrolle sowie Nachverarbeitung und Aufbewahrung von Dokumenten mit Belegfunktion, die laut organisationsinterner Vorgaben als besonders schutzwürdig gelten, vorzunehmen:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

In diesen Fällen erfolgt die Ablage [auf einem gesonderten Export-Datenpfad welcher zur Sicherstellung dient/...], wobei der Zugang nur folgenden Personen gestattet ist:

- [...]

Hierbei ist der Zugriff durch folgende Maßnahmen geschützt:

- [...]

3.1.1.4 Integritätssicherung

Die Integritätssicherung wird durchgeführt von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation bzw. im System]

3.1.1.5 Geeignete Aufbewahrung [bis zur Übergabe an Langzeitspeicher]

Die Aufbewahrung der Dokumente [bis zur Übergabe an Langzeitspeicher] wird verantwortet von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

3.1.1.6 Vernichtung des Originals

Die Freigabe zur Vernichtung der Dokumente erfolgt durch

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

Die tatsächliche Vernichtung der originalen Dokumente erfolgt durch [Interne Stelle/Externen Dienstleister] und wird verantwortet von

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

Der externe Dienstleister ist von [Name] unter der Registrierungsnummer [...] zertifiziert.

Die Freigabe zur Löschung der digitalen Archivbestände erfolgt in keinem Fall vor Ablauf der Aufbewahrungsfrist und durch:

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

Die tatsächliche Löschung der digitalen Archivbestände erfolgt durch

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

3.1.2 Regelungen für Wartungs- und Reparaturarbeiten

Die Wartung und die Reparatur der für den Scanvorgang eingesetzten IT-Systeme und Anwendungen ist folgendermaßen geregelt:

Die Festlegung der Verantwortlichkeiten für die Beauftragung, Durchführung und ggf. Kontrolle von Wartungs- und Reparaturaufgaben obliegt [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation].

Regelungen zur Authentisierung und zum Nachweis der Autorisierung des Wartungspersonals werden von Mitarbeiter [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation] überwacht.

Die Dokumentation von sicherheitsrelevanten Veränderungen an den involvierten IT-Systemen und Anwendungen erfolgen durch Mitarbeiter [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation].

Die Dokumentation der erfolgreichen Durchführung der Maßnahmen zur Qualitätskontrolle und Freigabe vor der Wiederaufnahme des regulären Betriebs erfolgt durch Mitarbeiter [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation].

3.1.3 Abnahme- und Freigabe-Verfahren für Hardware und Software

Durch die ordnungsmäßige und ununterbrochene Nutzung der in Abschnitt 2.6 aufgeführten Hard- und Software wird insbesondere sichergestellt, dass die in Abschnitt 2.2 aufgeführten rechtlichen Rahmenbedingungen eingehalten werden.

Gleichzeitig wird sichergestellt, dass die digitalisierten Daten bei Lesbarmachung mit den ursprünglichen papiergebundenen Unterlagen bildlich und 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, gegebenenfalls Personalnummer 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 Audits werden regelmäßig alle [x Jahre/Monate] durchgeführt. [Beispielsweise wurde das letzte Audit von [Firma, Name] am [Datum] durchgeführt. Die fachliche Kompetenz und Unabhängigkeit für die qualifizierte Durchführung der Audits ist gewährleistet durch [...].

Die Ergebnisse dieser Überprüfung werden [schriftlich/elektronisch] 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 in [...].

3.1.5 Anforderungen beim Outsourcing des Scanprozesses

Hinweis: Sofern der Scanprozess komplett oder teilweise von spezialisierten Scandienstleistern durchgeführt wird, sind die in [BSI-TR03138] vorgesehenen Maßnahmen sowie die Anforderungen aus OPS 2.1 und OPS 3.1 des IT-Gundschutz-Kompendiums [BSI-GSK] zu berücksichtigen.

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 Mitarbeiter werden die folgenden grundlegenden Anforderungen gestellt:

- [...]

3.2.2 Verpflichtung der Mitarbeiter

Die im Rahmen der fachlichen Schutzbedarfsanalyse identifizierten und in Abschnitt 2.2 aufgeführten rechtlichen Rahmenbedingungen werden den in den Scanprozess involvierten Mitarbeitern zur Kenntnis gebracht. Die Mitarbeiter werden, sofern dies nicht bereits geschehen ist, auf die Einhaltung der einschlägigen Gesetze, Vorschriften, Regelungen und der Verfahrensanweisung verpflichtet.

Dies erfolgt durch Mitarbeiter [Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation].

3.2.3 Maßnahmen zur Qualifizierung und Sensibilisierung

3.2.3.1 Einweisung zur ordnungsgemäßen Bedienung des Scansystems

Die Mitarbeiter, die den Scanvorgang durchführen, werden vom verantwortlichen Mitarbeiter ([Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation]) 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 Abläufe und Anforderungen bei der Erstellung des Transfervermerks,
- die Konfiguration und Nutzung der Systeme zur Integritätssicherung und
- das Verhalten im Fehlerfall.

Hierfür werden die unter [...] abgelegten Schulungsunterlagen genutzt.

3.2.3.2 Einweisung zu Sicherheitsmaßnahmen im Scanprozess

Zuständige Mitarbeiter, die den Scanvorgang durchführen oder verantworten, werden von [Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation] in geeigneter Weise

hinsichtlich der dabei umzusetzenden sowie der implementierten Sicherheitsmaßnahmen eingewiesen. Dies umfasst insbesondere:

- die grundsätzliche Sensibilisierung der Mitarbeiter 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 unter [...] abgelegten Schulungsunterlagen genutzt.

3.2.3.3 Schulung des Wartungs- und Administrationspersonals

Zuständige Mitarbeiter für Wartungs- und Administrationsaufgaben für die in den Scanprozess involvierten IT-Systeme und Anwendungen werden hinsichtlich der hierfür notwendigen Kenntnisse über die eingesetzten IT-Komponenten geschult.

Dies erfolgt durch [Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation] [in regelmäßigen Abständen/zuletzt am ...] und umfasst insbesondere:

Selbstständigkeit bei alltäglichen Administrationsaufgaben,

- selbstständige Fehlererkennung und -behebung,
- regelmäßige selbsttätige Durchführung von Datensicherungen,
- Nachvollziehbarkeit von Eingriffen externen Wartungspersonals,
- das Erkennen und Beheben von Manipulationsversuchen oder unbefugten Zugriffen auf die Systeme.

Hierfür werden die unter [...] abgelegten Schulungsunterlagen genutzt.

3.2.3.4 Sensibilisierung der Mitarbeiter für Informationssicherheit

Zur Einweisung und Sensibilisierung der Mitarbeiter für die Informationssicherheit erfolgt für die in Abschnitt 3.1.1 genannten vorbereitenden, digitalisierenden, archivierenden, kontrollierenden, freigebenden und vernichtenden Mitarbeiter eine regelmäßige [jährliche/...] Unterweisung in den Digitalisierungs-, Archivierungs- und Vernichtungsprozess. Darüber wird ein Protokoll angefertigt und archiviert. Die beteiligten Mitarbeiter verpflichten sich in dieser Unterweisung explizit zur Einhaltung dieser Verfahrensdokumentation.

Bei einem Wechsel der personellen Zuständigkeit erfolgt eine Unterweisung in den Digitalisierungs-, Archivierungs- und Vernichtungsprozess sowie eine Schulung zur ordnungsmäßigen Bedienung des Digitalisierungs- und Archivierungssystems durch die zuständige Führungskraft. Der unterwiesene Mitarbeiter verpflichtet sich explizit zur Einhaltung dieser Verfahrensdokumentation.

3.3 Technische Maßnahmen

3.3.1 Grundlegende Sicherheitsmaßnahmen für IT-Systeme

Für die in den Scanprozess involvierte IT-Systeme werden die hierfür in den IT-Grundschutz-Katalogen [BSI-GSK] vorgesehenen Sicherheitsmaßnahmen umgesetzt. Die wirksame Umsetzung der Maßnahmen wurde geprüft durch [Name] am [Datum].

Gemäß des Sicherheitskonzeptes wurden hierbei insbesondere die folgenden IT-Grundschutz-Bausteine berücksichtigt:

- [...]

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. Dies umfasst insbesondere

- [...]

Der verantwortliche Mitarbeiter [Name] hat die Wirksamkeit der zum Schutz der IT-Infrastruktur vorgesehenen Sicherheitsmaßnahmen am [Datum] geprüft.

3.3.3 Schutz vor Schadprogrammen

Um einer Infektion durch Schadprogramme vorzubeugen werden die Anforderungen aus OPS 1.1.4 des [BSI-GSK] berücksichtigt. Dies umfasst insbesondere

- die Auswahl eines geeigneten Viren-Schutzprogramms, wie vom zuständigen Mitarbeiter [Name] am [Datum] festgelegt,
- die Meldung von Schadprogramm-Infektionen an den zuständigen Mitarbeiter ([Name]),
- die Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen (diese [erfolgt automatisch/wird vom zuständigen Mitarbeiter [Name] regelmäßig alle [...] angestoßen]),
- eine regelmäßige Datensicherung, die regelmäßig und [automatisch/vom zuständigen Mitarbeiter [Name]] alle [...] angestoßen wird.

4 Mitgeltende Unterlagen

Neben den vorstehend aufgeführten Regelungen gelten folgende Unterlagen:[...]

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

Literaturverzeichnis

[BSI-GSK] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Kompendium*, 2019

[BSI-TR03138] Bundesamt für Sicherheit in der Informationstechnik (BSI):*Ersetzendes Scannen (RESISCAN)*, Technische Richtlinie (TR) des BSI Nr. 03138

[BSI-TR03138-R] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Ersetzendes Scannen – Anwendungshinweis R: Unverbindliche rechtliche Hinweise*, BSI TR-03138-R, Version 1.2

[MVD-StB] *Muster-Verfahrensdokumentation zur Digitalisierung und elektronischen Aufbewahrung von Belegen inkl. Vernichtung der Papierbelege*, Gemeinsam erarbeitet durch die Bundessteuerberaterkammer (BstBK) und den Deutschen Steuerberaterverband e.V. (DStV)