*Vorbemerkung:  
Dieses Dokument enthält diejenigen Festlegungen bezüglich des Scan-Verfahrens, die einen technischen Anteil haben. Bei der Ausfüllung der entsprechenden Teile der Verfahrensdokumentation wird regelmäßig die Unterstützung durch den Systembetreuer des Büros erforderlich sein. Dem dafür beschäftigten Mitarbeitenden oder externen Unternehmen kann dieses Dokument ausgehändigt werden, um die für die Dokumentation erforderlichen Informationen zu liefern, die Maßnahmen umzusetzen und die Umsetzung zu bestätigen.  
Hier sind auch Abschnitte der Verfahrensdokumentation aufgenommen, die organisatorische Maßnahmen enthalten. Die Beteiligung des Systembetreuers wird sich dann in der Regel auf die technischen Maßnahmen beschränken.*

1. **Eingesetzte Scan-Hardware und -Software / Hardware und Software zur Integritätssicherung**

|  |  |  |
| --- | --- | --- |
| **Abschnitt** | **Maßnahme** | **Status** |
| **2.6.1**  Scan-Hardware | *Scangerät: [Angabe des Herstellers und Typenbezeichnung, Software-Version]*  *Server: [Angabe zum Betriebssystem des Servers]*  *Client: [Angabe zum Betriebssystem des Clients]* |  |
| **2.6.1**  Scan-Software | *XNP (Basisanwendung der Bundesnotarkammer) mit dem Modul „Urkundenverzeichnis“ wird zur Qualitätssicherung, zur Nachbearbeitung (soweit zulässig) und zur Integritätssicherung durch Signatur genutzt.*  *Über die auf der Scan-Hardware integrierte Software hinaus wird keine Scan-Software eingesetzt.*  *[alternativ:] Angabe der eingesetzten Scan-Software mit Produktbezeichnung, Hersteller, Version; (das ist nur relevant, falls ein (Arbeitsplatz-)Scanner eingesetzt wird, der nicht ohne externe Software bereits PDF-Dateien erzeugen und auf einer Netzwerkablage speichern kann)* |  |
| **2.6.2**  Mechanismen zur Integritätssicherung | *Die Integrität der Zwischenprodukte wird organisatorisch durch Ablage auf einem Datenträger gewährleistet, auf den ausschließlich die am Scanprozess beteiligten Mitarbeitenden Zugriff erhalten. Es werden verschlüsselte Netzwerkverbindungen genutzt. [Dies sichert gegen physischen Zugriff auf die Verbindungen.]*  *[empfohlen, aber nicht zwingend erforderlich:] Der verwendete Datenträger ist verschlüsselt. (Dadurch besteht ein zusätzlicher Schutz gegen Angreifer, die physischen Zugriff auf den Datenträger erlangen.)*  *Der Zugriff auf alle Teile des Scan-Systems ist über die Benutzerverwaltung auf berechtigte Mitarbeitende begrenzt. [Wenn am Scanner selbst keine Authentisierung umgesetzt ist, muss sichergestellt sein, dass nur berechtigte Mitarbeitende physisch auf den Scanner zugreifen können.]* |  |
| **2.6.2**  Hardware zum Anbringen der elektronischen Signatur | *N-Karte / Signaturkarte der Zertifizierungsstelle der Bundesnotarkammer*  *Kartenlesegerät der Sicherheitsklasse 3 [Angabe des Herstellers und Typenbezeichnung]* |  |
| **2.6.2**  Software zur Integritätssicherung | *Zum Signieren wird XNP (Basisanwendung der Bundesnotarkammer) mit dem Modul „Urkundenverzeichnis“ genutzt.* |  |

1. **Einstellungen am Scangerät**

|  |  |  |
| --- | --- | --- |
| **Abschnitt** | **Maßnahme** | **Status** |
| **2.5.2**  Grundeinstellungen | |  |  | | --- | --- | | **Zielformat** | PDF/A-1b | | **Auflösung** | 300 dpi / Grundrisse und Lagepläne werden mit einer Auflösung von  600 dpi gescannt, sofern nicht offensichtlich 300 dpi genügen. | | **Scannen in Farbe** | Farb-Scan | | **Kontrast** | […] | | **Helligkeit** | […] | | **Einzug** | automatisch  manuell  einseitig  beidseitig (Duplex) | | **Weitere Einstellungen** | […] | |  |
| **2.5.2**  Auswahl eines geeigneten Bildkompressionsverfahrens | *Eingesetztes Bildkompressionsverfahren: JPEG, hohe Qualität*  *[alternativ:] Eingesetztes Bildkompressionsverfahren: TIFF, hohe Qualität* |  |
| **2.5.2**  Zwischenablage und Benennung | |  |  | | --- | --- | | Ablage/Verzeichnis | […]  *Beispiel: L:\Ablage\Scandateien* | | Benennung | *(Jahrgang)−(fortlaufende Nummer im Urkundenverzeichnis – xy-stellig mit führenden Nullen)-(Nummer des Dokuments – xy-stellig mit führender Null).pdf*  *[Für Sozietäten:] (Notarkürzel)-(Jahrgang)−(fortlaufende Nummer im Urkundenverzeichnis – xy-stellig mit führenden Nullen)-(Nummer des Dokuments – xy-stellig mit führender Null).pdf* | |  |

1. **Absicherung des Scan-Systems**

|  |  |  |
| --- | --- | --- |
| **Abschnitt** | **Maßnahme** | **Status** |
| **2.5.3**  Ausschluss eines unautorisierten manuellen Zugriffs auf das Scanprodukt | *Der Zugang zum Arbeitsplatz ist für unbefugte Personen nicht unbeaufsichtigt möglich. Eine Authentisierung am Arbeitsplatz durch Log-in am Computer ist erforderlich. Zugriff auf die verwendete Dateiablage haben nur Mitarbeitende, die am Scanprozess beteiligt sind.*  *[empfohlen, aber nicht zwingend:] Der Computer wird nur von Mitarbeitenden benutzt, die am Scanprozess beteiligt sind.*  *[empfohlen, aber nicht zwingend erforderlich:] Das Scanprodukt wird auf einer verschlüsselten Festplatte abgelegt. Dadurch besteht ein zusätzlicher Schutz gegen Angreifer, die physischen Zugriff auf den Datenträger erlangen.* |  |
| **2.5.6**  Ausschluss eines unautorisierten manuellen Zugriffs auf die elektronischen Dokumente | *Der Zugang zum Arbeitsplatz ist für unbefugte Personen nicht ohne Begleitung von Mitarbeitenden möglich. Eine Authentisierung am Arbeitsplatz durch Log-in ist bei allen Computern erforderlich, von denen aus ein Zugriff auf die elektronischen Dokumente erfolgen kann.*  *[empfohlen, nicht zwingend:] Der Computer wird nur von Mitarbeitenden benutzt, die am Scanprozess beteiligt sind.* |  |
| **3.1.1**  Ausschließliche Nutzung der Komponenten durch die zuständigen Mitarbeiterinnen / Mitarbeiter | *Alle eingesetzten Komponenten sind durch einen wirksamen Zugriffsschutz gesichert, sodass sie nur von am Scanprozess beteiligten Mitarbeitenden verwendet werden können.*  *Die eingesetzten Clients und Server verfügen über eine eingerichtete Nutzerkontensteuerung. Nur die für den Umgang mit Urkunden berechtigten und am Scanprozess beteiligten Mitarbeitenden verfügen über ein Nutzerkonto für diese Systeme.*  *Die für das Scannen verwendeten Komponenten befinden sich in einem geschützten Arbeitsbereich. Der Zugang zu diesem Bereich ist für dritte Personen nur in ständiger Begleitung durch einen Mitarbeitenden möglich.* |  |
| **3.1.7**  Verfahren im Hinblick auf sicherheitsrelevante Updates | *Antiviren-Software führt Updates der Virensignaturen automatisiert durch.*  *Alle vier Wochen werden durch einen externen Administrator (Systembetreuer) das System, Firmware der Geräte und die installierte Software auf Updates geprüft. Falls stabile Update-Versionen vorhanden sind, werden diese installiert.*  *[alternativ:] Die / der in Anlage 1 dafür angegebene zuständige Mitarbeitende informiert sich regelmäßig über Updates für Software, Firmware etc. und veranlasst gegebenenfalls ein Update. Einmal monatlich, und zwar immer am zweiten Arbeitstag des Monats, prüft die/der Mitarbeitende die Hard- und Software auf relevante Updates prüft und führt diese gegebenenfalls durch.* |  |
| **3.1.8**  Abnahme- und Freigabeverfahren bei Änderung von Hard- und Software-Komponenten | * *Es wird eine Sicherung der Konfiguration vor einer Änderung durchgeführt (gegebenenfalls auch als Ausdruck auf Papier).* * *Neben der geänderten Einstellung sind die grundsätzlichen, nicht von der Änderung betroffenen, Einstellungen aus der vorhergehenden Konfiguration zu übernehmen (z. B. Farb-Scan).* * *Es wird insbesondere sichergestellt, dass als Ausgabe-Format PDF/A-1b konfiguriert ist.* * *Scanprofile sind aus der vorhergehenden Konfiguration zu übernehmen.* * *Schutzmechanismen sind grundsätzlich zu übernehmen. Wie bei der initialen Verwendung müssen z. B. Standard-Passwörter geändert werden und die Zugänge für Mitarbeitende wiederhergestellt bzw. erstellt werden.*   *Beim Austausch bzw. Änderung (auch durch Updates) einer Komponente, die für den Scanprozess eingesetzt wird, wird ein Testlauf mit einem Testdokument durchgeführt. Das Testdokument enthält neben einfachen Textzeilen auch Bilder in unterschiedlichen Farben. Der Scanvorgang wird vollständig durchgeführt, in XNP wird das Dokument jedoch nur im Modul „Dokumente“ geöffnet und nicht im Modul „Urkundenverzeichnis“. Sofern bei der bildlichen und inhaltlichen Überprüfung Abweichungen festgestellt werden, ist unter Berücksichtigung der festgelegten Grundeinstellungen (siehe Abschnitt 2.5.2) eine Kalibrierung des Systems vorzunehmen.*  *Das Ergebnis des Freigabeverfahrens wird dokumentiert.* |  |
| **3.3**  Alternative organisatorische und zusätzliche technische Maßnahmen | *Beispiel:*  *Die eingesetzte Scan-Hardware wird (entgegen der Empfehlung) über einen Firewire-Anschluss angebunden. Der Raum, in dem die Scan-Hardware aufgestellt ist, ist nur den Mitarbeiterinnen und Mitarbeitern zugänglich, die für den Scanprozess zuständig sind. Vor der Benutzung der Scan-Hardware wird der Firewire-Anschluss auf offensichtliche Veränderungen überprüft.* |  |
| **3.3.2**  Schutz der Kommunikationsverbindungen vor Zugriffen von außerhalb | *Folgende in den Notarbüros übliche Konfiguration entspricht den Anforderungen:*   * *Zwischen dem internen Netz und dem Internet regeln ein Router / eine Firewall den Datenverkehr.* * *Alle netzwerkfähigen IT-Systeme, mit welchen auf das Elektronische Urkundenarchiv oder grundsätzlich auf XNP zugegriffen wird, sind entweder über die Registerbox oder über die Notarnetzbox mit dem Notarnetz verbunden.*   *[alternativ:] Alle am Scanprozess beteiligten Komponenten und Netzwerke sind mit dem gesamten Büronetzwerk durch eine Firewall geschützt. Netzwerkverbindungen können nur innerhalb dieses abgeschlossenen Netzwerks aufgebaut werden. Für die Übertragung von elektronischen Dokumenten an das Elektronische Urkundenarchiv besteht eine Verbindung mit dem Notarnetz.*  *[ggf. ergänzend, falls Service-Schnittstelle vorhanden:] Die Scan-Hardware verfügt über eine Service-Schnittstelle, die über das Internet Daten vom Gerätehersteller abruft. Durch eine Firewall wird sichergestellt, dass nur diese Verbindung zum Gerätehersteller außerhalb des internen Netzwerks möglich ist.* |  |
| **3.3.3**  Eingesetztes Viren-Schutzprogramm | *Angabe des eingesetzten Produkts […], Version […]* |  |
| **3.3.3**  Aktualisierung von Viren-Schutzprogrammen und Signaturen | *Die Aktualisierung erfolgt automatisch.*  *[alternativ:] Die Aktualisierung wird von der zuständigen Mitarbeiterin / vom zuständigen Mitarbeiter […] regelmäßig alle […] Tage durchgeführt.* |  |
| **3.3.3**  Eingesetztes Datensicherungsverfahren | *[Beispiel, keine besondere Empfehlung; vielfältige andere Gestaltungen möglich:]*  *Die Vollsicherung erfolgt einmal täglich über USB-Festplatten im Rotationsprinzip. Die nicht angeschlossenen USB-Festplatten werden räumlich getrennt aufbewahrt (Keller).*  *Es erfolgen eine wöchentliche Vollsicherung sowie tägliche inkrementelle Datensicherungen.* |  |
| **3.3.4**  Maßnahmen zur Gewährleistung der angemessenen Verfügbarkeit | *Es wird zertifizierte Marken-Hardware (Festplatten) verwendet.*  *Es werden interne und externe Back-ups angefertigt (die Hinterlegung erfolgt an unterschiedlichen Orten).* |  |
| **3.5.2**  Zugang zum Scansystem | *Der Zutritt zum Büro ist nur mit Schlüsseln möglich; die Schlüssel der Mitarbeitenden werden von der Notarin / dem Notar verwaltet.*  *Personen, die nicht im Notarbüro beschäftigt sind, werden im Büro außerhalb des Wartebereichs und der sanitären Anlagen ständig von Mitarbeitenden begleitet.*  *Der Zugriff auf alle Teile des Scansystems ist über die Benutzerverwaltung auf berechtigte Mitarbeitende begrenzt.*  *[Nicht zwingend, aber empfohlen:] Das Scangerät kann nur bedient werden, wenn sich ein Mitarbeitender authentifiziert hat. [Wenn am Scangerät selbst keine Authentifizierung oder andere Zugriffskontrolle umgesetzt ist, muss sichergestellt sein, dass ausschließlich die in Anlage 1 genannten Mitarbeitenden, physisch auf das Scangerät zugreifen können.] Ein Mitarbeitender ist während des ganzen Scanvorgangs anwesend.* |  |
| **3.5.2**  Zugriff auf die Administration des Scangeräts | *Der Administrationsbereich des Scangeräts ist durch ein geeignetes Passwort geschützt. Dieses ist nur der Notarin / dem Notar und der Bürovorsteherin / dem Bürovorsteher bekannt und unterscheidet sich von den Zugangsdaten der Mitarbeiterinnen und Mitarbeiter, die das Scansystem bedienen.*  *Die Fern-Administrationsschnittstelle wurde so konfiguriert, dass der Zugriff nur für den zuständigen Support-Dienstleister (über die IP-Adresse des Dienstleisters) möglich ist.*  *[alternativ:] Die Fern-Administrationsschnittstelle wurde deaktiviert.* |  |
| **3.5.10**  Maßnahmen und Konfiguration zur Zugriffsbeschränkung | *Grundsätzlich existieren verschlüsselte oder direkte Verbindungen zwischen den IT-Systemen:*   * *Das Scangerät ist über eine direkte LAN-Verbindung mit dem Server verbunden.* * *Der Rechner erhält das Scanprodukt über eine verschlüsselte Verbindung zur Weiterverarbeitung.*   *Der Zugriff auf die Datenablage (Server) ist nur über eine Authentifizierung möglich.* |  |

1. **Sonstige Maßnahmen**

|  |  |  |
| --- | --- | --- |
| **Abschnitt** | **Maßnahme** | **Status** |
| **3.5.9**  Maßnahmen bei Außerbetriebnahme von Scangeräten | *Die Daten werden von allen Datenträgern durch sicheres, nicht-rekonstruierbares Löschen entfernt. Auf den außer Betrieb zu nehmenden Komponenten werden alle Einstellungen, Passwörter und Benutzerkonten gelöscht oder zurückgesetzt.* |  |
| **3.5.11**  Protokollierung von Änderungen | *Die Notarin / der Notar oder die zuständige Mitarbeiterin / der zuständige Mitarbeiter führt ein elektronisches Protokoll [oder: Protokoll in Papierform] hinsichtlich der Änderung von kritischen Konfigurationsparametern sowie der Änderung von Authentisierungs- und Berechtigungsinformationen.* ***Gegebenenfalls unterstützt der Scanner die automatische Protokollierung der genannten Punkte.*** |  |
| **3.5.11**  Information, wer das Scansystem, wann und in welcher Weise genutzt hat | *Das Gerät wird ausschließlich von nach § 26 BNotO verpflichteten Mitarbeitenden, die in Anlage 1 aufgenommen sind, zum Einscannen von Urkunden und für die Unterstützung der sonstigen notariellen Amtstätigkeit verwendet. [Wenn dies gegeben ist, ist es nur empfohlen, nicht aber zwingend vorgegeben, eine der anderen Maßnahmen umzusetzen.]*  *[empfohlen, aber nicht zwingend:] In der Nebenakte zur Urkunde wird (auf einem Laufblatt) vermerkt, wann und von wem (Kürzel) die Urkunde gescannt wurde.*  *[alternativ, nicht zwingend:] Die zuständige Mitarbeiterin / Der zuständige Mitarbeiter führt ein Protokoll (z. B. Excel-Liste) mit der Information, wer das Scansystem, wann und in welcher Weise genutzt hat.*  *[alternativ, nicht zwingend:]* ***Das Scangerät bietet die Möglichkeit, automatisiert Protokolldateien über die Authentisierung und Verwendung anzulegen.***  […] |  |
| **3.5.11**  Fehlgeschlagene Authentisierungsvorgänge / Sonstige Fehler | *Auffälligkeiten und Fehler bei der Authentisierung werden sogleich der Notarin / dem Notar / der Bürovorsteherin / dem Bürovorsteher mitgeteilt, um das weitere Vorgehen zu klären.*  *[Weiteres Beispiel:]* ***Das Scangerät bietet die Möglichkeit, automatisiert Protokolldateien über fehlgeschlagene Authentisierungsvorgänge und sonstige Fehler anzulegen.*** |  |
| **3.5.11**  Schutz gemäß den datenschutzrechtlichen Bestimmungen | ***Eine automatisierte Protokollierung von personenbezogenen Daten findet nicht statt.*** *Für die jegliche sonstige Protokollierung werden nur die Kürzel der Mitarbeitenden verwendet. Die Protokolldaten sind nur befugten Mitarbeitenden zugänglich.*  *[alternativ:] Für jegliche Protokollierung werden nur die Kürzel der Mitarbeitenden verwendet. Die Protokolldaten sind nur befugten Mitarbeitenden zugänglich.*  *Protokolldaten werden nach 30 Tagen vernichtet bzw. gelöscht, soweit sie nicht Bestandteil von Aufzeichnungen mit längerer Aufbewahrungsfrist sind (z.B. Nebenakte).*  ***[ggf.] Die automatisiert erfassten Protokolldaten werden nach 30 Tagen gelöscht.***  […] |  |
| **4.3.3**  Maßnahmen für das zuverlässige Löschen von Zwischenergebnissen | *Die Löschung von Zwischenergebnissen durch einen berechtigten Mitarbeitenden erfolgt am Ende jeder Arbeitswoche. Die Sicherheit der Scan-Räumlichkeiten durch die Anwesenheit von berechtigen Mitarbeitenden ist gewährleistet.*  *[alternativ:]* ***Vor dem Verlassen der Scan-Räumlichkeiten sind die Zwischenergebnisse auf dem Scangerät manuell zu löschen (z. B. durch eine spezielle Funktion).***  *[alternativ:]* ***Eine Löschung von Zwischenergebnissen erfolgt am Ende eines jeden Arbeitstages.***  **[…]** |  |
| **4.4.2**  Fehlertolerante Protokolle | *Es werden fehlertolerante Übertragungsprotokolle verwendet, bei denen nicht unbemerkt eine Übertragung fehlschlagen kann (z. B. SFTP/SMB/HTTPS).* |  |