

System Assessment Bericht
bezogen auf elektronische Daten und elektronische Unterschriften;
Final Rule, 21 CFR Part 11

System: MagIC Net 1.0

1 Verfahren und Kontrollen für geschlossene Systeme

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.1	11.10 (a)	Validierung, IQ, OQ	Ist das System validiert?	B			<p>Für die Validierung des Systems ist ausschliesslich der Betreiber verantwortlich. Die Verantwortung des Lieferanten liegt in der Bereitstellung validierfähiger Systeme. Dabei hilft das Metrohm-interne Qualitätswesen, welches jederzeit auditiert werden kann.</p> <p>Metrohm bietet diesbezüglich eine Reihe von Validierungsservices an: Konformitätszertifikate, vorbereitete Unterlagen für IQ und OQ, Durchführung der IQ und OQ beim Betreiber,...</p> <p>Im System sind Standardmethoden für die Systemvalidierung gespeichert.</p>

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.2	11.10 (a)	Audit Trail, Änderung	Kann das System ungültige oder geänderte Aufzeichnungen erkennen?	X			<p>Alle Bedieneingaben werden in einem automatisch generierten Audit Trail mit Datum, Uhrzeit mit Differenz zu UTC (Coordinated Universal Time) und Anwender dokumentiert. Diese Zeit ist die Client-Zeit, deshalb muss der Administrator dafür Sorge tragen, dass die Zeit am Rechner korrekt ist.</p> <p>Der Report kann im Reportgenerator so definiert werden, dass geänderte Ergebnisdaten (Resultate) angezeigt werden.</p> <p>Bei Methodenänderung werden alle früheren Versionen in der Datenbank gespeichert und es muss ein Kommentar eingegeben werden. Für Methoden ist eine Versionskontrolle implementiert. Das heisst, die geänderten Daten einer Methode führen zu einem neuen Eintrag (Version) in der Datenbank.</p> <p>Beim Ändern von Ergebnisdaten (Nachrechnen) werden alle früheren Versionen in der Datenbank gespeichert und es muss ein Kommentar eingegeben werden. Für Bestimmungen ist eine Versionskontrolle implementiert. Das heisst, die geänderten Daten führen zu einem neuen Eintrag in der Datenbank.</p> <p>Ungültige Resultate können dadurch erkannt werden, dass Grenzwerte definiert werden. Im System kann festgelegt werden, ob bei Überschreiten der Grenzen eine Meldung auf dem Bildschirm oder dem Report erscheint oder per e-mail gesendet wird. Zusätzlich kann definiert werden, ob die Bestimmung abgebrochen werden soll.</p>
1.3	11.10 (b)	Report, Ausdruck, elektronische Aufzeichnung	Kann das System genaue und vollständige Papierausdrucke der elektronischen Aufzeichnungen erstellen?	X			<p>Für Bestimmungen (Ergebnisdaten) können konfigurierbare Reports gedruckt werden. Das Ändern der Report-Konfiguration kann für Routineanwender gesperrt werden.</p> <p>Der automatische Ausdruck am Ende einer Analyse kann im Methodenablauf definiert werden. Damit kann erreicht werden, dass der Betreiber des Systems mit Sicherheit vor dem Ändern, Überschreiben oder Löschen einer Bestimmung die Daten nachvollziehen kann.</p> <p>Jeder Ausdruck ist mit einem Zeitstempel mit Angabe der Differenz zu UTC versehen.</p>

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.4	11.10 (b)	Report, elektronische Aufzeichnung, FDA	Kann das System genaue und vollständige Kopien der Aufzeichnungen in elektronischer Form zur Kontrolle, Überprüfung und Vervielfältigung durch die FDA erstellen?	X			<p>Alle Daten können als verschlüsseltes XML-File abgespeichert werden. Unverschlüsselt können die Daten im XML- und AIA-Format ausgegeben werden.</p> <p>Der automatische Datenexport am Ende einer Analyse kann im Methodenablauf definiert werden. Damit kann erreicht werden, dass der Betreiber des Systems mit Sicherheit vor dem Ändern, Überschreiben oder Löschen einer Bestimmung die Daten nachvollziehen kann.</p>
1.5	11.10 (c)	elektronische Aufzeichnung, Aufbewahrungszeit, Archivierung	Sind die Aufzeichnungen während der ganzen Aufbewahrungszeit ohne weiteres wiederauffindbar?	B			<p>Für die Aufbewahrung/Archivierung ist ausschliesslich der Betreiber verantwortlich.</p> <p><i>MagIC Net</i> lässt sich als Local-Server oder Client-Version installieren. Das System kann Daten in der <i>MagIC Net</i>-Datenbank speichern und in verschiedenen Formaten exportieren (Konfigurationsdaten, Methoden, Bestimmungen). Die exportierten Daten können mit betreibereigenen Archivierungssystemen auf dem PC, auf einem Netzlaufwerk oder mittels Papier dauerhaft abgelegt werden. Die Datenbank besitzt eine automatische Backup-Funktion.</p> <p>Die im <i>MagIC Net</i> eigenen Format exportierten Daten auf den Datenträgern werden verschlüsselt und mit einer Checksumme versehen. Sie sind so vor ungewollter und unsachgemäßer Änderung geschützt. Änderungen werden vom System erkannt. Der Inhalt kann mit der <i>MagIC Net</i>-Software jederzeit gelesen werden.</p> <p>Das Verfahren, wie Daten archiviert werden und welche Daten das sind, muss der Betreiber festlegen.</p>

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.6	11.10 (d)	Login, Zugriffsschutz, Berechtigung Benutzer, Administrator	Ist der Systemzugriff auf berechtigte Personen beschränkt?	X			<p>Die Software besitzt ein Login mit einer unbegrenzten Anzahl Profilen (Zugriffsrechten/ Personengruppen). Die Zugriffsrechte für die einzelnen Benutzergruppen können von Administratoren frei definiert werden.</p> <p>Das System besitzt eine interne Passwortverwaltung. Folgende Parameter können eingestellt werden:</p> <ul style="list-style-type: none"> • Maximale Anzahl Fehlversuche bevor ein Account gesperrt wird • Benachrichtigung wenn ein Account gesperrt wird • Eindeutiges Passwort erforderlich • Sonderzeichen erforderlich • Minimale Passwortlänge • Gültigkeitsdauer • Dauer bis zur automatischen Abmeldung • Erneute Anmeldung nur durch gleichen Benutzer (optional) <p>Alternativ kann die Passwortverwaltung durch Windows erfolgen.</p> <p>Die für das System verantwortlichen Personen (Administratoren) müssen sicherstellen, dass nur berechtigte Personen eine Zugangsberechtigung erhalten.</p> <p>Alle Änderungen an den Zugriffsrechten, Anmeldungen, Abmeldungen und Accountsperrungen werden im Audit Trail aufgezeichnet.</p>
1.7	11.10 (e)	Audit Trail, elektronische Aufzeichnung, Bedieneingaben	Besteht ein sicherer, rechnergenerierter, zeitgestempelter Audit Trail, der Datum und Zeit der Bedieneingaben und Aktionen protokolliert, welche elektronische Aufzeichnungen erstellen, ändern oder löschen?	X			<p>Im Audit trail werden alle relevanten Bedieneingaben und Aktionen mit Datum, Uhrzeit mit Differenz zu UTC und Anwender dokumentiert.</p> <p>Zu allen Methoden und Bestimmungen werden Historien geführt; alle Versionen bleiben verfügbar.</p>

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.8	11.10 (e)	elektronische Aufzeichnung, Überschreiben von Daten, Änderung	Wenn elektronische Aufzeichnungen geändert werden, bleiben früher aufgezeichnete Informationen im System noch verfügbar (d.h. werden diese durch die Änderung nicht überschrieben)?	X			Ja, wenn Methoden oder Bestimmungen verändert und gespeichert werden, wird automatisch eine neue Version erstellt. Die Vorgängerversion bleibt erhalten und ist einsehbar. Änderungen in der Konfiguration werden mit altem und neuem Wert im Audit Trail protokolliert.
1.9	11.10 (e)	Audit Trail, Aufbewahrungszeit	Bleibt der Audit Trail einer elektronischen Aufzeichnung während der ganzen Aufbewahrungszeit der Aufzeichnung wiederauffindbar?	X			So lange der Audit Trail nicht gelöscht wird, bleibt er bestehen. Der Speicherplatz ist hier der beschränkende Faktor. Der Audit Trail kann nur gelöscht werden, wenn er archiviert wurde. Der Audit Trail kann auch gemeinsam mit der Konfigurationsdatenbank archiviert werden. Für die Aufbewahrung der archivierten Audit Trails und die Sicherstellung der Datenintegrität ist ausschliesslich der Betreiber verantwortlich.
1.10	11.10 (e)	Audit Trail, FDA, Einsichtnahme	Ist der Audit Trail zur Überprüfung und Vervielfältigung durch die FDA verfügbar?	X			Der Audit trail kann als Textdatei exportiert werden und ist so in elektronischer Form und auf Papier verfügbar. Ausserdem kann ein geschützter Audit Trail in Form einer pdf-Datei erzeugt werden.
1.11	11.10 (f)	Sequenzialisierung, Ablauf, Plausibilitätsprüfung, Geräte	Wenn der Ablauf der Systemschritte oder Ereignisse wichtig ist, wird dieser durch das System erzwungen (z.B. wie es in einem Steuerungssystem der Fall wäre)?	X			Im System werden Plausibilitätsprüfungen schon beim Start der Bestimmung durchgeführt, so wird zum Beispiel überprüft, ob alle benötigten Geräte vorhanden und betriebsbereit sind. Der Ablauf der Bestimmung ist in der Methode programmiert und muss strikt eingehalten werden. Die Methode wird bei der Erstellung und vor dem Start auf Konsistenz geprüft. Falls Inkonsistenzen auftreten wird der Benutzer gewarnt. Das Einhalten des Ablaufs wird durch die Verwendung der Probenzuordnungstabelle oder der automatischen Probedatenabfrage unterstützt. Es sind immer nur die Funktionen zugänglich, die ausgeführt werden können.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.12	11.10 (g)	Login, Zugriffsschutz, Berechtigung, Benutzer, Administrator	Stellt das System sicher, dass nur berechtigte Personen das System benutzen, Aufzeichnungen elektronisch visieren, auf die Funktion, die Rechnersystemeingabe- oder Ausgabeeinheit zugreifen, eine Aufzeichnung ändern oder andere Funktionen ausführen können?	X			Durch die Loginfunktion kann der Benutzer identifiziert werden. (Die für das System verantwortlichen Personen (Administratoren) müssen sicherstellen, dass nur berechtigte Personen eine Zugangsberechtigung erhalten.) Die Administratorfunktion kann von Benutzerrollen klar getrennt werden, siehe auch 11.10 (d), Nr. 1.6. Methoden und Bestimmungen können unterschrieben und somit elektronisch freigegeben werden. Es sind zwei Unterschriftsebenen eingerichtet. Das System fordert, dass Prüfer und Freigebender nicht die selbe Person ist. Dazu müssen die entsprechenden Berechtigungen vergeben werden.
1.13	11.10 (h)	Waage, Anschluss, Endgerät, Eingabedaten, Geräte	Kontrolliert das System die Gültigkeit der angeschlossenen Geräte?	X			Während der IQ werden alle angeschlossenen Geräte in die Geräteliste eingetragen und später geprüft. Metrohm-Geräte werden automatisch erkannt, auf Gültigkeit geprüft und in die Geräteliste eingetragen. Die Validierung der angeschlossenen Geräte erfolgt im Rahmen der Systemvalidierung (siehe auch 11.10 (a), Nr. 1.1).
1.14	11.10 (i)	Schulung, Support, Benutzer, Administrator	Gibt es dokumentierte Schulungen, einschliesslich Ausbildung am Arbeitsplatz (trainig on the job), für Systembenutzer, Entwickler, IT-Supportpersonal?	B			Für die Schulung ist der Betreiber verantwortlich. Metrohm bietet Standard-Schulungen für alle Anwendungsgebiete an. Individuelle Trainings können gesondert vereinbart werden. Entwickler und Service-Personal der Metrohm werden regelmässig weitergebildet.
1.15	11.10 (j)	Policy, Verantwortung, elektronische Unterschrift	Bestehen schriftliche Grundsätze (Policy), welche die Zuständigkeit und volle Verantwortung von Personen für Handlungen vorschreiben, die mit ihren elektronischen Unterschriften unternommen wurden?	B			Der Betreiber muss im Falle der Nutzung der elektronischen Unterschrift eine Policy haben, die die Gleichheit der handschriftlichen und der elektronischen Unterschrift klarstellt.
1.16	11.10 (k)	Dokumentation, Verteilung Dokumentation, Zugriff auf Dokumentation, Systemdokumentation, Logbuch, Gebrauchsanleitungen	Wird die Verteilung, der Zugriff auf sowie die Benutzung der Systembedienungs- und Wartungsdokumentation kontrolliert?	B			Das System besitzt eine umfangreiche Online-Hilfe, die den Benutzer und das Wartungspersonal unterstützt. Die Verteilung der papierbasierten Dokumentation liegt beim Betreiber.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.17	11.10 (k)	SOP, Dokumentation, Gebrauchsanleitungen, Systemdokumentation, Audit Trail, Logbuch	Besteht ein formeller Änderungskontrollablauf für die Systemdokumentation, der einen Audit Trail der Änderungen mit Zeitablauf festhält?	B			<p>Die von Metrohm gelieferte Dokumentation unterliegt den Metrohm internen Richtlinien zur Dokumentenlenkung (klare Systemzuordnung und Versionierung der Dokumentation).</p> <p>Für Änderungskontrolle und Audit Trail zur betreibereigenen Dokumentation ist der Betreiber verantwortlich.</p> <p>Der Betreiber muss ein Logbuch führen und die Änderungen am System vermerken. Vorlagen für diese Dokumente werden von Metrohm zur Verfügung gestellt.</p>

2 Zusätzliche Verfahren und Kontrollen für offene Systeme

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
2.1	11.30	Daten, Verschlüsselung, Datenübertragung	Können Methoden oder Bestimmungen sicher von einem System zum Nächsten übertragen werden? Sind Daten auf dem Weg vom Absender zum Empfänger verschlüsselt?	X			Das System wurde zum Betrieb als geschlossenes System designed. Die Daten werden als Datei gespeichert, verschlüsselt und mit Prüfsumme versehen abgelegt. Die Daten sind somit vor unerlaubter Veränderung geschützt. Im Falle einer Änderung werden die Daten unbrauchbar. Auch wenn defekte Daten auf ein anderes System übertragen werden, wird dies erkannt.
2.2	11.30	elektronische Unterschrift	Werden digitale Unterschriften verwendet?	X			Methoden und Bestimmungen können unterschrieben und somit elektronisch freigegeben werden. Es sind zwei Unterschriftsebenen eingerichtet. Das System fordert, dass Prüfer und Freigebender nicht dieselbe Person ist. Digitale Unterschriften werden derzeit nicht unterstützt.

3 Unterschriebene elektronische Daten

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
3.1	11.50	elektronische Unterschrift	Enthalten unterschriebene elektronische Aufzeichnungen die folgenden verwandten Informationen? - vollständiger Name des Unterzeichners - Datum und Zeit der Unterschrift - Bedeutung der Unterschrift (wie Genehmigung, Überprüfung, Verantwortung)	X			Bei Methoden und Bestimmungen enthalten alle Unterschriften den vollständigen Namen des Unterschreibenden, das Datum und die Uhrzeit zum Zeitpunkt der Unterschrift, und die Begründung (aus Auswahlliste) für die Unterschrift. Zusätzlich kann zu einer Unterschrift ein Kommentar eingegeben werden, der zusammen mit der elektronischen Unterschrift abgespeichert wird. Benutzerdaten und Audit Trail sind keine unterschriftspflichtigen Daten und werden somit nicht unterschrieben.
3.2	11.50	elektronische Unterschrift	Erscheint die oben erwähnte Information in angezeigten und gedruckten Kopien der elektronischen Aufzeichnung?	X			Bei der Anzeige im Display und auf Ausdrucken werden die kompletten Unterschriftsdaten ausgegeben. Unterschriftslisten sind als vordefinierte Reportbausteine verfügbar.
3.3	11.70	elektronische Unterschrift	Besteht eine Verbindung zwischen den Unterschriften und den entsprechenden elektronischen Aufzeichnungen, um sicherzustellen, dass sie nicht mit gewöhnlichen Mitteln zu Fälschungszwecken ausgeschnitten, kopiert oder sonst übertragen werden können?	X			Die Unterschrift ist untrennbar mit der Methode oder der Bestimmung verbunden. Fälschungen sind hierbei nicht möglich. In die Unterschrift werden die Benutzerinformationen komplett übernommen. Diese sind bei der Darstellung der Unterschrift dann immer Klartext lesbar!

4 Elektronische Unterschriften (allgemein)

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
4.1	11.100 (a)	elektronische Unterschrift	Sind elektronische Unterschriften eindeutig einer Person zugeordnet?	X			Ja durch eindeutige Beziehung zwischen Benutzername und Person im System. Die Software stellt sicher, dass jeder Benutzername nur einmal vergeben werden kann. Betrieblich ist sicherzustellen, dass (vor allem bei Mehrfachinstallationen) keine Mehrfachverwendung von Anmeldenamen stattfindet.
4.2	11.100 (a)	elektronische Unterschrift	Werden elektronische Unterschriften je durch andere Personen wiederverwendet oder anderen Personen zugeteilt?	B			Ein verwendeter Benutzername ist einer Person zugeordnet. Es ist betrieblich sicherzustellen, dass dieser Anmelde-name nicht einer anderen Person zugeordnet wird. Ein Reaktivierung bleibt davon unberührt.
4.3	11.100 (a)	elektronische Unterschrift	Erlaubt das System die Übertragung der Berechtigung von elektronischen Unterschriften (Stellvertreterregelung)?	B			Die Zuordnung von Stellvertretern ist durch den Administrator durchzuführen. Betriebliche Regelung ist hier notwendig.
4.4	11.100 (b)	elektronische Unterschrift	Wird die Identität einer Person vor der Zuteilung einer elektronischen Unterschrift überprüft?	B			Es ist durch den Ablauf des Berechtigungsantrags organisatorisch zu lösen, dass die beantragende Person die korrekte Person ist.

5 Elektronische Unterschriften (nicht-biometrisch)

Ifd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
5.1	11.200 (a)(1)(i)	elektronische Unterschrift	Besteht die Unterschrift aus mindestens zwei Elementen, wie Identifikationscode (z.B. Benutzername) und Passwort oder Identifikationskarte und Passwort?	X			Ja, Benutzername und Passwort.
5.2	11.200 (a)(1)(ii)	elektronische Unterschrift	Wird das Passwort bei jeder Unterschrift verlangt, wenn mehrere Unterschriften im Laufe einer durchgehenden Sitzung angebracht werden? (Hinweis: beide Elemente müssen bei der ersten Unterschrift einer Sitzung angegeben werden)	X			Zu jeder Unterschrift muss der Benutzername und das Passwort eingegeben werden.
5.3	11.200 (a)(1)(iii)	elektronische Unterschrift	Werden immer beide Elemente der elektronischen Unterschrift verlangt, wenn Unterschriften nicht während einer durchgehenden Arbeitssitzung angebracht werden?	X			Zu jeder Unterschrift muss der Benutzername und das Passwort eingegeben werden.
5.4	11.200 (a)(2)	elektronische Unterschrift	Werden nichtbiometrische Unterschriften ausschliesslich durch ihre tatsächlichen Eigentümer verwendet?	B			Der Betreiber muss sicherstellen, dass jeder Anwender nur seine eigene Unterschrift verwendet.
5.5	11.200 (a)(3)	elektronische Unterschrift, el. Unterschrift fälschen	Benötigt ein Versuch, eine elektronische Unterschrift zu fälschen, das Zusammenwirken von mindestens zwei Personen?	X			Ja.

6 Elektronische Unterschriften (biometrisch)

lfd. Nr.	Ref.		Frage	Ja	Nein	zum Teil	Bemerkungen
6.1	11.200 (b)	elektronische Unterschrift, biometrische el. Unterschrift	Ist es erwiesen, dass biometrische elektronische Unterschriften ausschliesslich durch ihren tatsächlichen Eigentümer verwendet werden können?	N/A			Biometrische Unterschriften werden nicht unterstützt.

7 Kontrolle von Identifikationscode und Passwort

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.1	11.300 (a)	Identifikationscode, Eindeutigkeit, Passwort, Identifikation, Login, Zugriffsschutz	Bestehen Kontrollen, um die Einmaligkeit jeder Kombination von Identifikationscode und Passwort sicherzustellen, so dass keine Person die gleiche Kombination von Identifikationscode und Passwort haben kann?	X/ B			<p>Das System stellt sicher, dass jeder Identifikationscode (Anwendername) nur einmal innerhalb des Systems verwendet wird, so kann auch eine Kombination von Identifikationscode und Passwort nur einmal vorkommen. Namensänderungen müssen vom Betreiber organisatorisch verwaltet werden!</p> <p>Das System kann als Client-Server-System betrieben werden. Dadurch ist sichergestellt, dass die Identifikationscodes in allen Clients identisch sind. Es wird empfohlen, unternehmensweit eindeutige systemübergreifende Identifikationscodes (z.B. Personalnummer oder Namenskürzel) zu verwenden.</p> <p>Generell wird empfohlen, organisationsweit Richtlinien festzulegen, in denen die Erstellung von Anwenderkonten und die Verwendung von Passwörtern (Länge, Gültigkeitsdauer,...) festgelegt wird.</p>
7.2	11.300 (b)	Identifikationscode, Passwort, Gültigkeit, Identifikation, Login, Zugriffsschutz	Sind Verfahren vorgeschrieben, um sicherzustellen, dass die Gültigkeit der Identifikationscodes periodisch überprüft wird?	B			Für die Überprüfung der Identifikationscodes ist der Betreiber verantwortlich.
7.3	11.300 (b)	Passwort, Gültigkeit, Verfall Passwort, Identifikation, Login, Zugriffsschutz	Unterstehen Passwörter dem periodischen Verfall, damit sie regelmässig geändert werden müssen?	X			Die Gültigkeitsdauer für das Passwort kann vom Administrator festgelegt werden. Werte zwischen 30 und 90 Tagen sind gebräuchlich. Eine lange Gültigkeitsdauer stellt ein Sicherheitsrisiko dar. Eine zu kurze Gültigkeitsdauer bedeutet, dass sich Anwender häufig ein neues Passwort merken müssen und dieses eventuell aufschreiben. Das System speichert die Passworhistorie, somit ist eine Wiederverwendung von Passwörtern nicht möglich.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.4	11.300 (b)	Identifikationscode, Passwort, Gültigkeit, Sperrung Zugangsbe- rechtigung, Identifikation, Login, Zugriffsschutz	Besteht ein Verfahren für den Rückruf oder die Sperrung von Identifikationscodes und Passwör- tern, wenn eine Person austritt oder den Arbeits- platz wechselt?	B			Das Verfahren muss vom Betreiber festgelegt werden. Der entsprechende Benutzer kann im System vom Administrator entfernt werden, bleibt jedoch im System in der Gruppe „ent- fernte Anwender“ ohne jegliche Zugriffsrechte gespeichert.
7.5	11.300 (c)	Identifikationscode, Passwort, Gültigkeit, Sperrung Zugangsbe- rechtigung, Identifikation, Login, Zugriffsschutz, Verlust ID-Karte	Besteht ein Verfahren zur elektronischen Sperrung eines Identifikationscodes oder Passwortes, wenn es möglicherweise unsicher oder verloren gegang- en ist?	B			Das Verfahren muss vom Betreiber festgelegt werden. Der entsprechende Benutzer kann im System vom Administrator entfernt werden, bleibt jedoch im System in der Gruppe „ent- fernte Anwender“ ohne jegliche Zugriffsrechte gespeichert.
7.6	11.300 (d)	Missbrauch, Login, Zugriffsschutz	Besteht ein Verfahren zur Erkennung von Miss- brauchsversuchen und Benachrichtigung der Si- cherheitsstelle?	X			Nach n-maligen Fehlversuchen (Anzahl kann vom Administra- tor definiert werden) wird eine Meldung, dass die maximale Anzahl erfolgloser Login-Versuche erreicht wurde, ausgege- ben und der Benutzer gesperrt. Eine entsprechende Mitteil- ung kann per E-mail an das Management verschickt werden.
7.7	11.300 (d)	Missbrauch, Login, Zugriffsschutz	Besteht ein Verfahren zur Meldung an das Mana- gement von wiederholten oder schwerwiegenden Missbrauchsversuchen?	B			Ein Verfahren zur Meldung an das Management muss vom Betreiber festgelegt werden. Nach n-maligen Fehlversuchen wird eine Meldung, dass die maximale Anzahl erfolgloser Login-Versuche erreicht wurde, ausgegeben und der Benutzer gesperrt. Eine entsprechende Mitteilung kann per E-mail an das Management verschickt werden.
7.8	11.300 (c)	Verlust ID-Karte, ID- Karte, Missbrauch, Zugriffsschutz	Besteht ein Verlustbearbeitungsverfahren, falls ein Gegenstand zur Identifikation (z.B. ID-Karte) verlo- ren geht oder gestohlen wird?	N/A			Eine Hardware zur Identifikation ist nicht vorgesehen.
7.9	11.300 (c)	Verlust ID-Karte, elektro- nische Sperrung ID- Karte, ID-Karte, Miss- brauch, Zugriffsschutz	Besteht ein Verfahren zur elektronischen Sperrung eines solchen Gegenstandes, falls er verloren, gestohlen oder möglicherweise unsicher ist?	N/A			Eine Hardware zur Identifikation ist nicht vorgesehen.
7.10	11.300 (c)	ID-Karte, Zugriffsschutz	Bestehen Kontrollen über die Ausgabe von tempo- rären und festen Ersatzgeräten?	N/A			Eine Hardware zur Identifikation ist nicht vorgesehen.
7.11	11.300 (e)	Überprüfung ID-Karte, ID-Karte, Zugriffsschutz	Werden Identifikationsmarken und Karten am An- fang und danach periodisch überprüft?	N/A			Eine Hardware zur Identifikation ist nicht vorgesehen.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.12	11.300 (e)	Änderung ID-Karte, ID-Karte, Missbrauch, Zugriffsschutz	Beinhaltet diese Prüfung auch eine Kontrolle, dass keine unerlaubten Änderungen vorgenommen wurden?	N/A			Eine Hardware zur Identifikation ist nicht vorgesehen.

B = Die Verantwortung liegt beim Betreiber.

N/A = Trifft auf das System nicht zu (not applicable)

8 Indices

Verweise auf die Seitenzahl:

A

Ablauf	5
Administrator	4, 5, 6
Änderung	2, 4
Änderung ID-Karte	14
Anschluss	5
Archivierung	3
Audit Trail	2, 4, 6
Aufbewahrungszeit	3, 4
Ausdruck	3

B

Bedienereingaben	4
Benutzer	4, 5, 6
Berechtigung	4, 5
biometrische el. Unterschrift	11

D

Daten	7
Datenübertragung	7
Dokumentation	6

E

Eindeutigkeit	12
Eingabedaten	5
Einsichtnahme	4
el. Unterschrift fälschen	10
elektronische Aufzeichnung	3, 4
elektronische Sperrung ID-Karte	13
elektronische Unterschrift	6, 7, 8, 9, 10, 11
Endgerät	5

F

FDA	3, 4
-----------	------

G

Gebrauchsanleitungen	6
Geräte	5
Gültigkeit	12, 13

I

Identifikation	12, 13
Identifikationscode	12, 13
ID-Karte	13, 14
IQ	2

L

Logbuch	6
Login	4, 5, 12, 13

M

Missbrauch	13, 14
------------------	--------

O

OQ	2
----------	---

P

Passwort	12, 13
Plausibilitätsprüfung	5
Policy	6

R

Report	3
--------------	---

S

Schulung	6
Sequenzialisierung	5
SOP	6
Sperrung Zugangsberechtigung	13
Support	6
Systemdokumentation	6

Ü

Überprüfung ID-Karte	14
Überschreiben von Daten	4

V

Validierung	2
Verantwortung	6
Verfall Passwort	12
Verlust ID-Karte	13
Verschlüsselung	7
Verteilung Dokumentation	6

W

Waage	5
-------------	---

Z

Zugriff auf Dokumentation	6
Zugriffsschutz	4, 5, 12, 13, 14

Verweise auf die laufende Nummer des Tabelleneintrags:**A**

Ablauf	1.11
Administrator	1.14 1.12 1.6
Änderung	1.8 1.2
Änderung ID-Karte	7.12
Anschluss	1.13
Archivierung	1.5
Audit Trail	1.17 1.10 1.9 1.7 1.2
Aufbewahrungszeit	1.9 1.5
Ausdruck	1.3

B

Bedienereingaben	1.7
Benutzer	1.14 1.12 1.6
Berechtigung	1.12 1.6
biometrische el. Unterschrift	6.1

D

Daten	2.1
Datenübertragung	2.1
Dokumentation	1.17 1.16

E

Eindeutigkeit	7.1
Eingabedaten	1.13
Einsichtnahme	1.10
el. Unterschrift fälschen	5.5
elektronische Aufzeichnung	1.8 1.7 1.5 1.4 1.3
elektronische Sperrung ID-Karte	7.9
elektronische Unterschrift	6.1 5.5 5.4 5.3 5.2 5.1
.....	4.4 4.3 4.2 4.1 3.3 3.2 3.1 2.2 1.15

Endgerät	1.13
----------------	------

F

FDA	1.10 1.4
-----------	----------

G

Gebrauchsanleitungen	1.17 1.16
Geräte	1.13 1.11
Gültigkeit	7.5 7.4 7.3 7.2

I

Identifikation	7.5 7.4 7.3 7.2 7.1
Identifikationscode	7.5 7.4 7.2 7.1
ID-Karte	7.12 7.11 7.10 7.9 7.8
IQ	1.1

L

Logbuch	1.17 1.16
Login	7.7 7.6 7.5 7.4 7.3 7.2 7.1 1.12 1.6

M

Missbrauch	7.12 7.9 7.8 7.7 7.6
------------------	----------------------

O

OQ	1.1
----------	-----

P

Passwort	7.5 7.4 7.3 7.2 7.1
Plausibilitätsprüfung	1.11
Policy	1.15

R

Report	1.4 1.3
--------------	---------

S

Schulung	1.14
Sequenzialisierung	1.11
SOP	1.17
Sperrung Zugangsberechtigung	7.5 7.4
Support	1.14
Systemdokumentation	1.17 1.16

Ü

Überprüfung ID-Karte	7.11
Überschreiben von Daten	1.8

V

Validierung	1.1
Verantwortung	1.15
Verfall Passwort	7.3
Verlust ID-Karte	7.9 7.8 7.5
Verschlüsselung	2.1
Verteilung Dokumentation	1.16

W

Waage	1.13
-------------	------

Z

Zugriff auf Dokumentation	1.16
Zugriffsschutz	7.12 7.11 7.10 7.9 7.8 7.7 7.6 7.5
.....	7.4 7.3 7.2 7.1 1.12 1.6