System Assessment Bericht

bezogen auf elektronische Daten und elektronische Unterschriften;

Final Rule, 21 CFR Part 11

System: MagIC Net 1.1

1 Verfahren und Kontrollen für geschlossene Systeme

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.1	11.10 (a)	Validierung{ XE "Validierung" \t "1.1" \f "n" }{ XE "Validierung" }, IQ{ XE "IQ" \t "1.1" \f "n" }{ XE "IQ" }, OQ{ XE "OQ" \t "1.1" \f "n" }{ XE "OQ" }	Ist das System validiert?	**B**			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. Metrohm bietet diesbezüglich eine Reihe von Validierungs-Services an: Konformitätszertifikate, vorbereitete Unterlagen für IQ und OQ, Durchführung der IQ und OQ beim Betreiber,... Im System sind Standardmethoden für die Systemvalidierung gespeichert.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.2	11.10 (a)	Audit Trail{ XE "Audit Trail" \t "1.2" \f "n" }{ XE "Audit Trail" }, Änderung{ XE "Änderung" \t "1.2" \f "n" }{ XE "Änderung" }	Kann das System ungültige oder geänderte Aufzeichnungen erkennen?	**X**			Alle Bedienereingaben 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. Der Report kann im Reportgenerator so definiert werden, dass geänderte Ergebnisdaten (Resultate) angezeigt werden. 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. 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. 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.
1.3	11.10 (b)	Report{ XE "Report" \t "1.3" \f "n" }{ XE "Report" }, Ausdruck{ XE "Ausdruck" \t "1.3" \f "n" }{ XE "Ausdruck" }, elektronische Aufzeichnung{ XE "elektronische Aufzeichnung" \t "1.3" \f "n" }{ XE "elektronische Aufzeichnung" }	Kann das System genaue und vollständige Papierausdrucke der elektronischen Aufzeichnungen erstellen?	**X**			Für Bestimmungen (Ergebnisdaten) können konfigurierbare Reports gedruckt werden. Das Ändern der Report-Konfiguration kann für Routineanwender gesperrt werden. 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. Jeder Ausdruck ist mit einem Zeitstempel mit Angabe der Differenz zu UTC versehen.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.4	11.10 (b)	Report{ XE "Report" \t "1.4" \f "n" }{ XE "Report" }, elektronische Aufzeichnung{ XE "elektronische Aufzeichnung" \t "1.4" \f "n" }{ XE "elektronische Aufzeichnung" }, FDA{ XE "FDA" \t "1.4" \f "n" }{ XE "FDA" }	Kann das System genaue und vollständige Kopien der Aufzeichnungen in elektronischer Form zur Kontrolle, Überprüfung und Vervielfältigung durch die FDA erstellen?	**X**			Alle Daten können als verschlüsseltes XML-File abgespeichert werden. Unverschlüsselt können die Daten im XML- und AIA-Format ausgegeben werden. 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.
1.5	11.10 (c)	elektronische Aufzeichnung{ XE "elektronische Aufzeichnung" \t "1.5" \f "n" }{ XE "elektronische Aufzeichnung" }, Aufbewahrungszeit{ XE "Aufbewahrungszeit" \t "1.5" \f "n" }{ XE "Aufbewahrungszeit" }, Archivierung{ XE "Archivierung" \t "1.5" \f "n" }{ XE "Archivierung" }	Sind die Aufzeichnungen während der ganzen Aufbewahrungszeit ohne weiteres wiederauffindbar?	**B**			Für die Aufbewahrung/Archivierung ist ausschliesslich der Betreiber verantwortlich. *MagIC Net* lässt sich als Local-Server oder Client-Version installieren. Das System kann Daten in der *MagIC Net*-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. Die im MagIC Net 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 *MagIC Net*-Software jederzeit gelesen werden. Das Verfahren, wie Daten archiviert werden und welche Daten das sind, muss der Betreiber festlegen.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.6	11.10 (d)	Login{ XE "Login" \t "1.6" \f "n" }{ XE "Login" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "1.6" \f "n" }{ XE "Zugriffsschutz" }, Berechtigung{ XE "Berechtigung" \t "1.6" \f "n" }{ XE "Berechtigung" } Benutzer{ XE "Benutzer" \t "1.6" \f "n" }{ XE "Benutzer" }, Administrator{ XE "Administrator" \t "1.6" \f "n" }{ XE "Administrator" }	Ist der Systemzugriff auf berechtigte Personen beschränkt?	**X**			Die Software besitzt ein Login mit einer unbegrenzten Anzahl Profilen (Zugriffsrechten/ Personengruppen). Die Zugriffsrechte für die einzelnen Benutzergruppen können von Administratoren frei definiert werden. Das System besitzt eine interne Passwortverwaltung. Folgende Parameter können eingestellt werden: • 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) Alternativ kann die Passwortverwaltung durch Windows erfolgen. Die für das System verantwortlichen Personen (Administratoren) müssen sicherstellen, dass nur berechtigte Personen eine Zugangsberechtigung erhalten. Alle Änderungen an den Zugriffsrechten, Anmeldungen, Abmeldunugen und Accountsperre werden im Audit Trail aufgezeichnet.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.7	11.10 (e)	Audit Trail{ XE "Audit Trail" \t "1.7" \f "n" }{ XE "Audit Trail" }, elektronische Aufzeichnung{ XE "elektronische Aufzeichnung" \t "1.7" \f "n" }{ XE "elektronische Aufzeichnung" }, Bedienereingaben{ XE "Bedienereingaben" \t "1.7" \f "n" }{ XE "Bedienereingaben" }	Besteht ein sicherer, rechnergenerierter, zeitgestempelter Audit Trail, der Datum und Zeit der Bedienereingaben und Aktionen protokolliert, welche elektronische Aufzeichnungen erstellen, ändern oder löschen?	**X**			Im Audit trail werden alle relevanten Bedienereingaben und Aktionen mit Datum, Uhrzeit mit Differenz zu UTC und Anwender dokumentiert. Zu allen Methoden und Bestimmungen werden Historien geführt; alle Versionen bleiben verfügbar.
1.8	11.10 (e)	elektronische Aufzeichnung{ XE "elektronische Aufzeichnung" \t "1.8" \f "n" }{ XE "elektronische Aufzeichnung" }, Überschreiben von Daten{ XE "Überschreiben von Daten" \t "1.8" \f "n" }{ XE "Überschreiben von Daten" }, Änderung{ XE "Änderung" \t "1.8" \f "n" }{ XE "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{ XE "Audit Trail" \t "1.9" \f "n" }{ XE "Audit Trail" }, Aufbewahrungszeit{ XE "Aufbewahrungszeit" \t "1.9" \f "n" }{ XE "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 archivert werden. Für die Aufbewahrung der archivierten Audit Trails und die Sicherstellung der Datenintegrität ist ausschliesslich der Betreiber verantwortlich.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.10	11.10 (e)	Audit Trail{ XE "Audit Trail" \t "1.10" \f "n" }{ XE "Audit Trail" }, FDA{ XE "FDA" \t "1.10" \f "n" }{ XE "FDA" }, Einsichtnahme{ XE "Einsichtnahme" \t "1.10" \f "n" }{ XE "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{ XE "Sequenzialisierung" \t "1.11" \f "n" }{ XE "Sequenzialisierung" }, Ablauf{ XE "Ablauf" \t "1.11" \f "n" }{ XE "Ablauf" }, Plausibilitätsprüfung{ XE "Plausibilitätsprüfung" \t "1.11" \f "n" }{ XE "Plausibilitätsprüfung" }, Geräte{ XE "Geräte" \t "1.11" \f "n" }{ XE "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.
1.12	11.10 (g)	Login{ XE "Login" \t "1.12" \f "n" }{ XE "Login" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "1.12" \f "n" }{ XE "Zugriffsschutz" }, Berechtigung{ XE "Berechtigung" \t "1.12" \f "n" }{ XE "Berechtigung" }, Benutzer{ XE "Benutzer" \t "1.12" \f "n" }{ XE "Benutzer" }, Administrator{ XE "Administrator" \t "1.12" \f "n" }{ XE "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.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.13	11.10 (h)	Waage{ XE "Waage" \t "1.13" \f "n" }{ XE "Waage" }, Anschluss{ XE "Anschluss" \t "1.13" \f "n" }{ XE "Anschluss" }, Endgerät{ XE "Endgerät" \t "1.13" \f "n" }{ XE "Endgerät" }, Eingabedaten{ XE "Eingabedaten" \t "1.13" \f "n" }{ XE "Eingabedaten" }, Geräte{ XE "Geräte" \t "1.13" \f "n" }{ XE "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{ XE "Schulung" \t "1.14" \f "n" }{ XE "Schulung" }, Support{ XE "Support" \t "1.14" \f "n" }{ XE "Support" }, Benutzer{ XE "Benutzer" \t "1.14" \f "n" }{ XE "Benutzer" }, Administrator{ XE "Administrator" \t "1.14" \f "n" }{ XE "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 Anwendungsbereiche an. Individuelle Trainings können gesondert vereinbart werden. Entwickler und Service-Personal der Metrohm werden regelmässig weitergebildet.
1.15	11.10 (j)	Policy{ XE "Policy" \t "1.15" \f "n" }{ XE "Policy" }, Verantwortung{ XE "Verantwortung" \t "1.15" \f "n" }{ XE "Verantwortung" }, elektronische Unterschrift{ XE "elektronische Unterschrift" \t "1.15" \f "n" }{ XE "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.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
1.16	11.10 (k)	Dokumentation{ XE "Dokumentation" \t "1.16" \f "n" }{ XE "Dokumentation" }, Verteilung Dokumentation{ XE "Verteilung Dokumentation" \t "1.16" \f "n" }{ XE "Verteilung Dokumentation" }, Zugriff auf Dokumentation{ XE "Zugriff auf Dokumentation" \t "1.16" \f "n" }{ XE "Zugriff auf Dokumentation" }, Systemdokumentation{ XE "Systemdokumentation" \t "1.16" \f "n" }{ XE "Systemdokumentation" }, Logbuch{ XE "Logbuch" \t "1.16" \f "n" }{ XE "Logbuch" }, Gebrauchsanleitungen{ XE "Gebrauchsanleitungen" \t "1.16" \f "n" }{ XE "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{ XE "SOP" }{ XE "SOP" \t "1.17" \f "n" }, Dokumentation{ XE "Dokumentation" \t "1.17" \f "n" }{ XE "Dokumentation" }, Gebrauchsanleitungen, { XE "Gebrauchsanleitungen" \t "1.17" \f "n" }{ XE "Gebrauchsanleitungen" }Systemdokumentation{ XE "Systemdokumentation" \t "1.17" \f "n" }{ XE "Systemdokumentation" }, Audit Trail{ XE "Audit Trail" \t "1.17" \f "n" }{ XE "Audit Trail" }, Logbuch{ XE "Logbuch" \t "1.17" \f "n" }{ XE "Logbuch" }	Besteht ein formeller Änderungskontrollablauf für die Systemdokumentation, der einen Audit Trail der Änderungen mit Zeitablauf festhält?	**B**			Die von Metrohm gelieferte Dokumentation unterliegt den Metrohm internen Richtlinien zur Dokumentenlenkung (klare Systemzuordnung und Versionierung der Dokumentation). Für Änderungskontrolle und Audit Trail zur betreibereigenen Dokumentation ist der Betreiber verantwortlich. Der Betreiber muss ein Logbuch führen und die Änderungen am System vermerken. Vorlagen für diese Dokumente werden von Metrohm zur Verfügung gestellt.

2 Zusätzliche Verfahren und Kontrollen für offene Systeme

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
2.1	11.30	Daten{ XE "Daten" \t "2.1" \f "n" }{ XE "Daten" }, Verschlüsselung{ XE "Verschlüsselung" \t "2.1" \f "n" }{ XE "Verschlüsselung" }, Datenübertragung{ XE "Datenübertragung" \t "2.1" \f "n" }{ XE "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. 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.
2.2	11.30	elektronische Unterschrift{ XE "elektronische Unterschrift" \t "2.2" \f "n" }{ XE "elektronische Unterschrift" }	Werden digitale Unterschriften verwendet?	**X**			

3 Unterschriebene elektronische Daten

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
3.1	11.50	elektronische Unterschrift{ XE "elektronische Unterschrift" \t "3.1" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "3.2" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "3.3" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "4.1" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "4.2" \f "n" }{ XE "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 Anmeldename nicht einer anderen Person zugeordnet wird. Ein Reaktivierung bleibt davon unberührt.
4.3	11.100 (a)	elektronische Unterschrift{ XE "elektronische Unterschrift" \t "4.3" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "4.4" \f "n" }{ XE "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)

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
5.1	11.200 (a) (1)(i)	elektronische Unterschrift{ XE "elektronische Unterschrift" \t "5.1" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "5.2" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "5.3" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "5.4" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "5.5" \f "n" }{ XE "elektronische Unterschrift" }, el. Unterschrift fälschen{ XE "el. Unterschrift fälschen" \t "5.5" \f "n" }{ XE "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{ XE "elektronische Unterschrift" \t "6.1" \f "n" }{ XE "elektronische Unterschrift" }, biometrische el. Unterschrift{ XE "biometrische el. Unterschrift" \t "6.1" \f "n" }{ XE "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{ XE "Identifikationscode" \t "7.1" \f "n" }{ XE "Identifikationscode" }, Eindeutigkeit{ XE "Eindeutigkeit" \t "7.1" \f "n" }{ XE "Eindeutigkeit" }, Passwort{ XE "Passwort" \t "7.1" \f "n" }{ XE "Passwort" }, Identifikation{ XE "Identifikation" \t "7.1" \f "n" }{ XE "Identifikation" }, Login{ XE "Login" \t "7.1" \f "n" }{ XE "Login" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.1" \f "n" }{ XE "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**			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! 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. Generell wird empfohlen, organisationsweit Richtlinien festzulegen, in denen die Erstellung von Anwenderkonten und die Verwendung von Passwörtern (Länge, Gültigkeitsdauer,...) festgelegt wird.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.2	11.300 (b)	Identifikationscode{ XE "Identifikationscode" \t "7.2" \f "n" }{ XE "Identifikationscode" }, Passwort{ XE "Passwort" \t "7.2" \f "n" }{ XE "Passwort" }, Gültigkeit{ XE "Gültigkeit" \t "7.2" \f "n" }{ XE "Gültigkeit" }, Identifikation{ XE "Identifikation" \t "7.2" \f "n" }{ XE "Identifikation" }, Login{ XE "Login" \t "7.2" \f "n" }{ XE "Login" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.2" \f "n" }{ XE "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{ XE "Passwort" \t "7.3" \f "n" }{ XE "Passwort" }, Gültigkei{ XE "Gültigkeit" \t "7.3" \f "n" }t{ XE "Gültigkeit" }, Verfall Passwort{ XE "Verfall Passwort" \t "7.3" \f "n" }{ XE "Verfall Passwort" }, Identifikation{ XE "Identifikation" \t "7.3" \f "n" }{ XE "Identifikation" }, Login{ XE "Login" \t "7.3" \f "n" }{ XE "Login" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.3" \f "n" }{ XE "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 Passworthistorie, somit ist eine Wiederverwendung von Passwörtern nicht möglich.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.4	11.300 (b)	Identifikationscode{ XE "Identifikationscode" \t "7.4" \f "n" }{ XE "Identifikationscode" }, Passwort{ XE "Passwort" \t "7.4" \f "n" }{ XE "Passwort" }, Gültigkeit{ XE "Gültigkeit" \t "7.4" \f "n" }{ XE "Gültigkeit" }, Sperrung Zugangsberechtigung{ XE "Sperrung Zugangsberechtigung" \t "7.4" \f "n" }{ XE "Sperrung Zugangsberechtigung" }, Identifikation{ XE "Identifikation" \t "7.4" \f "n" }{ XE "Identifikation" }, Login{ XE "Login" \t "7.4" \f "n" }{ XE "Login" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.4" \f "n" }{ XE "Zugriffsschutz" }	Besteht ein Verfahren für den Rückruf oder die Sperrung von Identifikationscodes und Passwörtern, wenn eine Person austritt oder den Arbeitsplatz 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 „entfernte Anwender“ ohne jegliche Zugriffsrechte gespeichert.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.5	11.300 (c)	Identifikationscode{ XE "Identifikationscode" \t "7.5" \f "n" }{ XE "Identifikationscode" }, Passwort{ XE "Passwort" \t "7.5" \f "n" }{ XE "Passwort" }, Gültigkeit{ XE "Gültigkeit" \t "7.5" \f "n" }{ XE "Gültigkeit" }, Sperrung Zugangsberechtigung{ XE "Sperrung Zugangsberechtigung" \t "7.5" \f "n" }{ XE "Sperrung Zugangsberechtigung" }, Identifikation{ XE "Identifikation" \t "7.5" \f "n" }{ XE "Identifikation" }, Login{ XE "Login" \t "7.5" \f "n" }{ XE "Login" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.5" \f "n" }{ XE "Zugriffsschutz" }, Verlust ID-Karte{ XE "Verlust ID-Karte" \t "7.5" \f "n" }{ XE "Verlust ID-Karte" }	Besteht ein Verfahren zur elektronischen Sperrung eines Identifikationscodes oder Passwortes, wenn es möglicherweise unsicher oder verloren gegangen 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 „entfernte Anwender“ ohne jegliche Zugriffsrechte gespeichert.
7.6	11.300 (d)	Missbrauch{ XE "Missbrauch" \t "7.6" \f "n" }{ XE "Missbrauch" }, Login{ XE "Login" \t "7.6" \f "n" }{ XE "Login" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.6" \f "n" }{ XE "Zugriffsschutz" }	Besteht ein Verfahren zur Erkennung von Missbrauchsversuchen und Benachrichtigung der Sicherheitsstelle?	**X**			Nach n-maligen Fehlversuchen (Anzahl kann vom Administrator definiert werden) 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.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.7	11.300 (d)	Missbrauch{ XE "Missbrauch" \t "7.7" \f "n" }{ XE "Missbrauch" }, Login{ XE "Login" \t "7.7" \f "n" }{ XE "Login" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.7" \f "n" }{ XE "Zugriffsschutz" }	Besteht ein Verfahren zur Meldung an das Management 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{ XE "Verlust ID-Karte" \t "7.8" \f "n" }{ XE "Verlust ID-Karte" }, ID-Karte{ XE "ID-Karte" \t "7.8" \f "n" }{ XE "ID-Karte" }, Missbrauch{ XE "Missbrauch" \t "7.8" \f "n" }{ XE "Missbrauch" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.8" \f "n" }{ XE "Zugriffsschutz" }	Besteht ein Verlustbearbeitungsverfahren, falls ein Gegenstand zur Identifikation (z.B. ID-Karte) verloren geht oder gestohlen wird?	**N/A**			Eine Hardware zur Identifikation ist nicht vorgesehen.

lfd. Nr.	Ref.	Thema	Frage	Ja	Nein	zum Teil	Bemerkungen
7.9	11.300 (c)	Verlust ID-Karte{ XE "Verlust ID-Karte" \t "7.9" \f "n" }{ XE "Verlust ID-Karte" }, elektronische Sperrung ID-Karte{ XE "elektronische Sperrung ID-Karte" \t "7.9" \f "n" }{ XE "elektronische Sperrung ID-Karte" }, ID-Karte{ XE "ID-Karte" \t "7.9" \f "n" }{ XE "ID-Karte" }, Missbrauch{ XE "Missbrauch" \t "7.9" \f "n" }{ XE "Missbrauch" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.9" \f "n" }{ XE "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{ XE "ID-Karte" \t "7.10" \f "n" }{ XE "ID-Karte" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.10" \f "n" }{ XE "Zugriffsschutz" }	Bestehen Kontrollen über die Ausgabe von temporären und festen Ersatzgeräten?	**N/A**			Eine Hardware zur Identifikation ist nicht vorgesehen.
7.11	11.300 (e)	Überprüfung ID-Karte{ XE "Überprüfung ID-Karte" \t "7.11" \f "n" }{ XE "Überprüfung ID-Karte" }, ID-Karte{ XE "ID-Karte" \t "7.11" \f "n" }{ XE "ID-Karte" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.11" \f "n" }{ XE "Zugriffsschutz" }	Werden Identifikationsmarken und Karten am Anfang 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{ XE "Änderung ID-Karte" \t "7.12" \f "n" }{ XE "Änderung ID-Karte" }, ID-Karte{ XE "ID-Karte" \t "7.12" \f "n" }{ XE "ID-Karte" }, Missbrauch{ XE "Missbrauch" \t "7.12" \f "n" }{ XE "Missbrauch" }, Zugriffsschutz{ XE "Zugriffsschutz" \t "7.12" \f "n" }{ XE "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)

Ein physikalisches Audit wurde am 27.04.2006 auf Basis der Version MagIC Net 1.0 durchgeführt. Die aktuelle Software-Version beinhaltet gemäss Aussage der Geschäftsleitung der Metrohm keine 21 CFR Part 11 relevanten Änderungen. Aus diesem Grunde wurde auf ein überprüfendes physikalisches Audit zunächst verzichtet, dieses ist für Dezember 2008 vorgesehen.

8 Indices

Verweise auf die Seitenzahl:

Verweise auf die laufende Nummer des Tabelleneintrags: