	Leitfaden Computer in Prüflaboratorien	Nr.: **L 18**
Version/Datum 01 / 2003		Seite: 1 von 18
Erstellt: Fostel 10.12.2003	Geprüft: Beirat (95.Sitzung) 20.1.2004	Freigabe: Friers 20.1.2004

1 Zielsetzung

Dieses Dokument stellt einen Leitfaden hinsichtlich der Anwendung von Computern für Labors dar, welche ein Qualitätsmanagementsystem schon betreiben, oder beabsichtigen ein solches aufzubauen, das den Anforderungen der ÖVE/ÖNORM EN ISO/IEC 17025 (in Folge als ISO/IEC 17025 bezeichnet) entspricht. Die notwendigen Vorkehrungen bezüglich aller Tätigkeiten, an denen Computer oder mit Computern versehenen Einrichtungen beteiligt sind, werden dargelegt.
Dieser Leitfaden soll dazu beitragen, die Forderungen der ISO/IEC 17025 bezüglich der Verwendung von Computern transparenter und verständlicher zu gestalten. Ausdrücklich soll darauf verwiesen werden, dass das vorliegende Dokument als Leitfaden und keineswegs als Anforderungspapier zu verstehen ist. Leitfaden bedeutet das Aufzeigen von möglichen, aber nicht verbindlichen Interpretationen der Norm, weiters dürfen selbstverständlich keine über die Norm hinausgehenden Forderungen erhoben werden. Dieser Leitfaden soll Labors und Sachverständige unterstützen.
Entscheidend für die Beurteilung von Computern und Computersystemen im Labor ist eine aktuelle Risikoabschätzung vor Ort (siehe Fragenkatalog im Anhang).

*Bei Festlegung und Umsetzung sollte **der gesunde Menschenverstand** im Vordergrund stehen.*

2 Definitionen

1. **Computersysteme** umfassen Computer, automatische Mess- und Prüfsysteme, oder Einrichtungen, in denen Computer eingebaut sind.
   (Anmerkung: Computer und Computersysteme im Sinne dieses Leitfadens umfassen Hard- und Software.)
2. **Verifizierung**: Bestätigung der Erfüllung der Spezifikationen und die Dokumentation darüber.
   (Anmerkung: Oft sind die Einrichtungen im Labor schon längere Zeit in Betrieb, sodass das Labor meistens nicht mehr die Möglichkeit hat, den Lieferanten des Systems zu beauftragen, zusätzliche Informationen oder Hilfestellungen bei der Verifizierung des Systems zu geben. Für diese Fälle ist eine Vorgangsweise, die als retrospektive Verifizierung bezeichnet werden kann, anzuwenden. Retrospektive Verifizierung bedeutet, dass versucht wird, so gut wie möglich alle vorhergegangenen Operationen [wie Wartungen, Systemveränderungen, Updates udgl.] am System darzustellen. Dies umfasst zumindest den Zeitraum bis zur letzten qualitätssichernden Maßnahme, welche die ordnungsgemäße Funktion des Gesamtsystems sichergestellt hat.)
3. **Validierung:** Bestätigung der Erfüllung der Forderungen für einen bestimmten beabsichtigten Gebrauch oder Anwendung und die Aufzeichnungen darüber.
4. **Datenschutz:** bedeutet den Schutz aufgezeichneter Daten gegen unbefugten Zugriff und umfasst die Begriffe der Vertraulichkeit bzw. Zugangskontrolle
5. **Datensicherheit:** bedeutet den Schutz aufgezeichneter Daten gegen zufällige und unbeabsichtigte Veränderungen

6. **Datensicherung:** bedeuten alle Verfahren, die der Aufbewahrung und Rückverfolgung aufgezeichneter Daten dienen
7. **Elektronischer Prüfbericht:** Ein elektronischer Prüfbericht ist ein Dokument, das allen Anforderungen der ISO/IEC 17025 genügt. D.h. ein derartiger Bericht muss vollständig inkl. aller Beilagen (z.B. Photos, Diagrammen, Geräteausdrucken) vorliegen. Falls dies nicht möglich ist, kann kein elektronischer Bericht erstellt werden!
8. **Vorläufige Informationen:** Sind Ergebnisse oder Teilergebnisse von Prüfungen die zur Information an Kunden übermittelt werden, ohne allen formalen Anforderungen an Prüfberichte im Sinne der ISO/IEC 17025 entsprechen. Die zu erfüllenden Mindestkriterien sind im QM-System zu definieren.

3 Bezug zur ISO/IEC 17025

Die Norm ISO/IEC 17025 nimmt wiederholt ausdrücklich auf Computer, elektronische Daten udgl. Bezug.
Insbesonders zu beachten sind folgende Punkte der Norm:

- die Lenkung von Daten und Aufzeichnungen (Schutz und Sicherheit der Daten) (Pkt. 4.12.1.4 und 5.4.7.2)
- die Beschaffung von Ausrüstung (Pkt. 4.6)
- die Wartung, Instandhaltung, Kalibrierung, Validierung der Einrichtungen und Aufzeichnungen darüber (Pkt. 5.5.2, 5.5.5, 5.5.11 und 5.5.12), sowie
- die elektronische Übermittlung von Ergebnisberichten (Pkt 5.10.7)

4 Geltungsbereich

Die Anforderungen der ISO/IEC 17025 gelten im selben Ausmaß für alle Laboratorien, unabhängig davon, ob Computersysteme eingesetzt werden oder nicht.
Dieser Leitfaden gilt für alle akkreditierten Laboratorien, unabhängig von ihrer Größe oder ihrem technischen Tätigkeitsbereich.
Das einzige Kriterium für die Anwendung dieses Leitfadens sind die Tätigkeiten des Labors und die damit verbundenen Risiken. (siehe auch Anhang)
Weiters ist dieser Leitfaden für alle Systeme anwendbar, unabhängig davon, ob sie käuflich erworben oder selbst entwickelt wurden, das schließt auch alle Modifikationen, Anpassungen, Programmänderungen, unabhängig ob sie von Systemanbietern, unparteiischen Dritten oder Laborpersonal durchgeführt wurden, mit ein.
Ganz besonders wird die Verwendung von Programmen, bzw. Makros, die vom Benutzer selbst erstellt wurden, zu beachten sein.

5 Management und Organisation

Entscheidend für die Effizienz des Qualitätsmanagementsystem eines Labors ist, in wie weit sich die oberste Leitung tatsächlich mit dem QM-System auseinandersetzt.
Das lässt sich teilweise auch von den Formulierungen der Qualitätspolitik ablesen.
Die Qualitätspolitik hat alle Bereiche des Labors mit einzuschließen, selbstverständlich auch die Verwendung von Computern oder Computersystemen.
Das Labor muss über eine dokumentierte Geschäftspolitik und Verfahrensanweisungen zur Absicherung der Integrität des QM-Systems verfügen. Innerhalb dieses Systems ist glei-

ches auch für die vorhandenen Computersysteme zu verlangen. Es müssen dokumentierte Verfahrensanweisungen zur Absicherung der Integrität der Computersysteme und der vorhandenen Software, sowie aller Berichte, die vom System erzeugt, verwaltet oder aufbewahrt werden, vorliegen.
Das Labor hat eine Politik zu Sicherheit und Schutz von Daten zu formulieren, worin der zu erreichende Grad an Datensicherheit und -schutz dargelegt wird. Dabei sind die vorhandenen Risken bezüglich der Sensibilität der Daten und der technischen Gegebenheiten angemessen zu berücksichtigen.
Die Verfahren zur Sicherung der Integrität haben notwendigerweise insbesondere zu enthalten

- eine genaue Spezifikation des Systems
- Verfahren zur Beschaffung und Prüfung bei der Erstinbetriebnahme
- Installation von Software
- Regelungen für die Zugangskontrolle und Schutz vor unbefugten Zugriff
- Kontrolle von Veränderungen
- Schutz vor allen schädigenden Einflüssen, beispielsweise physikalische Einflüsse oder Computerviren.
- Maßnahmen bei unkontrollierten Systemzuständen
- Maßnahmen zur nachträglichen Verifizierung eines Systems, das schon längere Zeit im Einsatz ist
- Besondere Maßnahmen über die Verwendung transportabler Computer (z.B. Laptop), Geräte (z.B. Datenlogger, Messgeräte) und Speichermedien,
- Regelung der Verantwortlichkeiten

Das QM-System (einschließlich aller Verfahren) beinhaltet Festlegungen für die Erstinstallation, die Verifizierung, Wartung und die Reparatur von Computern und Computersystemen, das schließt auch Verfahren für Beschaffung (und Lieferantenbewertung) mit ein. Weiters gelten grundsätzlich die Regelungen der ISO/IEC 17025 Kapitel 5.5 Einrichtungen.

6 Anforderungen an Aufzeichnungen über Computer und -systeme

6.1 Büro-PC

6.1.1 Definition

Gerät, mit Standard Büro-Software (z.B.: Microsoft Office) zur Erstellung von Prüfberichten und für allgemeine Verwaltungstätigkeiten, auch für Berechnungen

6.1.2 Systembeschreibung

Die Systembeschreibung hat zumindest folgendes zu enthalten:

- Verwendungszweck
- Hersteller und Typenbezeichnung
- zusätzliche Komponenten (Angaben zu Komponenten, die der Datenarchivierung und der Kommunikation dienen.)
- Software (Betriebssystem und Applikationssoftware mit Versionsangabe)
- eindeutige Identifikation des Systems

6.2 Mess- und Auswerte - PC

6.2.1 Definition

Computer zur Steuerung von Messgeräten und zur Erfassung von Messdaten und deren Weiterverarbeitung

6.2.2 Systembeschreibung

Die Systembeschreibung hat zumindest folgendes zu enthalten:

- Verwendungszweck
- Hersteller und Typenbezeichnung
- zusätzliche Komponenten (Angaben zu Komponenten die zur Datenerfassung, -auswertung und Steuerung dienen)
- Software (Betriebssystem und Applikationssoftware mit Versionsangabe)
- eindeutige Identifikation des Systems

6.3 Netzwerk

6.3.1 Definition

Netzwerke stellen grundsätzlich Computer-Verbundsysteme dar, die auf Basis von LAN (Local Area Network) laborintern oder WAN (Wide Area Network) laborintern und/oder –extern, dem direkten oder indirekten Austausch von Daten dienen. Dies kann z.B. durch Kommunikation, Datentransfer oder gegenseitige Nutzung von Ressourcen (Drucker, Speicherplatz usw.) erfolgen.
Da die Topologien derartiger Systeme in Art und Aufbau sehr individuell konzipiert und strukturiert sind, ist eine allgemein gültige Definition nur sehr ungenügend möglich.
Es sei darauf hingewiesen, dass es aufgrund der Netzwerkstruktur, wie Größe und Ausdehnung (LAN/WAN), der Art der Vernetzung (z.B. W[wireless]LAN), der verwendeten Komponenten (Router, Switch usw.), der verwendeten Netzwerksoftware, um nur einige Einflussgrößen zu nennen, sowie im Besonderen der Art der Daten die sich am Netzwerk befinden, einer speziell auf das gegenständliche Netzwerk abgestimmte Risikobewertung (eines Risikomanagements) bedarf. (Siehe Fragenkatalog Risikoanalyse im Anhang)

6.3.2 Systembeschreibung

Die Systembeschreibung hat zumindest folgendes zu enthalten:

- Verwendungszweck
- Art und Struktur des Netzwerkes
- Hersteller und Typenbezeichnung der Netzwerkkomponenten
- zusätzliche Komponenten (z.B.: Zusätzlich Komponenten der Zugriffskontrolle)
- Software (Betriebssystem und Applikationssoftware mit Versionsangabe)
- eindeutige Identifikation des Systems

6.4 Laborinformations- und Datenmanagementsystem

6.4.1 Definition

Datenmanagement- und Datenverwaltungssysteme sind meist in Netzwerken arbeitende, softwaregestützte Systeme für die Erstellung, Bearbeitung, Verwaltung, Freigabe, Administrierung von Daten in vorgegebenen Arbeitsabläufen. Diese Abläufe können durch hierarchische Strukturen oder Arbeitsschemata (Workflows) vorgegeben sein.

Laborinformationssysteme (LIMS) können zusätzlich Elemente der Gerätesteuerung, sowie der Erfassung, Auswertung und Berechnung von Daten, sowie des Controllings und der Anonymisierung enthalten.

6.4.2 Systembeschreibung

Systembeschreibung des Netzwerkes gemäß Punkt 6.3.2

- Art des Workflows
- Software (Betriebssystem und Applikationssoftware mit Versionsangabe)

7 Beschaffung und Abnahme

Für die Beschaffung gelten die Anforderungen der ISO/IEC 17025 Punkt 4.6 bezüglich "Ausrüstung". Die Einhaltung der Spezifikationen ist vor dem Routineeinsatz zu verifizieren. Grundsätzlich ist jeder beschaffte Ausrüstungsgegenstand im Labor, soweit er die Qualität der Prüfungen und/oder Kalibrierungen beeinflusst, vor Abnahme auf seine Eignung zu prüfen (validieren). Das gilt selbstverständlich auch für Computer oder Computersysteme, auf den Dokumente und Daten erfasst, erstellt und verwaltet werden. Grundsätzlich können darunter insbesondere auch Überprüfungen im Rahmen einer Abnahme, z.B. Stichprobentest, Überprüfung der prüf- bzw. analysenrelevanten Systemfunktionalität etc., verstanden werden. Im Fall von Standardspezifikationen kann eine einfache Funktionsprüfung ausreichen.
Die Funktionsprüfung des Systems kann, wenn erforderlich durch die Anwendung von einem oder mehreren der folgenden Verfahren erfolgen. Der Einsatz von anderen relevanten Methoden ist möglich:

- durch Simulation von Vorgängen durch den Dateninput von theoretischen oder bereits vorhandenen Werten in die Computereinheit des Systems
- durch Durchführung von Messungen oder Prüfungen an einem oder mehreren Gegenständen mit bekanntem Ergebnis

Die Durchführung dieses Verfahren ist ausreichend aufzuzeichnen. Die Aufzeichnungen sollten zumindest enthalten:

- Daten und andere Ergebnisse aus der Verifizierung
- Identität der Person(en) welche die Verifizierung durchgeführt und deren Ergebnisse autorisiert hat
- das Datum der Verifizierung
- die gewählte Vorgangsweise für die Verifizierung

8 Verifizierung des Systems nach einer Systemänderung

Nach jeder Veränderung sind am System die relevanten Verifizierungsverfahren durchzuführen.
Eine Systemveränderung wurde vorgenommen, wenn eine der folgenden Tätigkeiten oder etwas Äquivalentes stattgefunden hat.

- Reparatur der Hardware des Systems
- Installation einer neuen Hardware
- eine neue Version der verwendeten Software wurde installiert
- neue Software wurde installiert

Wenn das Computersystem zur Messwerterfassung herangezogen wird, kann eine Rekalibrierung oder Revalidierung gegebenenfalls erforderlich sein.
Die Durchführung ist ausreichend aufzuzeichnen. (siehe Punkt 7).
Wenn bei der Reparatur bzw. Installation Komponenten getauscht oder eingesetzt werden, die keine Relevanz auf die Prüfverfahren haben (z.B. Tastatur, Maus, Bildschirm etc.) kann von einer wiederholten Verifizierung abgesehen werden. Eine Funktionsprüfung ist aber durchzuführen (ACHTUNG: neue Gerätetreiber).

8.1 Verfizierung nach unkontrollierten Systemzuständen

Nach unkontrollierten Systemzuständen, wie z.B. Programmabstürzen, Systemabstürzen („BLUESCREEN“) oder Virusinfektionen, sind relevante Verifizierungsverfahren, die die Datenintegrität, den Datenschutz und die Datensicherheit berücksichtigen, durchzuführen.

Wenn das Computersystem zur Messwerterfassung und/oder -auswertung herangezogen wird, kann eine Rekalibrierung oder Revalidierung gegebenenfalls erforderlich sein.
Dieses Verfahren ist angemessen aufzuzeichnen. (siehe Punkt 7)

9 Betreiben von Computern und Computersystemen

Grundsatz

Die folgenden Maßnahmen (Tätigkeiten und angemessene Dokumentation) haben auf die Art der Daten, sowie Umfang und Zweck deren Verwendung und den damit verbundenen Risiken, sowie auf den Stand der technischen Möglichkeiten und die bei der Realisierung erwachsenden Kosten Bedacht zu nehmen.

9.1 Auslagerung von Tätigkeiten an Dritte

Bei Tätigkeiten, die durch Dritte durchgeführt werden (z.B. Servicevertrag, Betreuung des Netzwerkes durch externe Stelle), sind entsprechende vertragliche Vereinbarungen zu treffen.

9.2 Datenschutz

In Abhängigkeit von Art und Nutzung der Daten und den damit verbunden Risiken sind Maßnahmen und Verfahren festzulegen und zu dokumentieren, welche für den Schutz der Integrität und Vertraulichkeit der Daten eingeführt und realisiert sind.

Darunter fallen z.B. folgende Maßnahmen und deren Aufzeichnung:

- Zutrittsrechte zu Eingabeplätzen
- Zugriffrechte auf Computer
- Zugriffrechte auf Datenmedien
- Zugriffsrechte auf Dateien, Verzeichnisse und Strukturen
- Regelungen zum Virenschutz
- Maßnahmen nach einem erkannten Virenbefall
- sonstige Maßnahmen (z.B. Firewall)

Bei allen Maßnahmen ist auf die Anforderungen des Datenschutzgesetztes (BGBl. I Nr. 165/1999 i.d.g.F) Bedacht zu nehmen.

9.3 Datensicherung und Archivierung

In Abhängigkeit von Art und Nutzung der Daten und den damit verbunden Risiken sind Maßnahmen und Verfahren festzulegen und zu dokumentieren, welche für die Verhinderung des Verlustes eingeführt und realisiert sind. Dies umfasst auch Verfahren, die für die Archivierung von Daten, einschließlich ihrer Lagerung und Aufbewahrungsdauer (siehe 9.8), zutreffend sind.

Darunter fallen z.B. folgende Maßnahmen und deren Aufzeichnung:

- Backup auf Datenträger
- Spiegelung von Datenträgern
- Kopien von Datenträgern

9.4 Wartung

Unter Wartung sind alle Maßnahmen (Regelungen, Verfahren und Pläne) zu verstehen, welche für die Pflege von Hardware und Software eingeführt und realisiert sind.

Beispiele:
Softwarepflege: Aktualisierung von Virensoftware und Firewalls, Pflege von Datenbeständen, Pflege von Zugriffberechtigungen, Pflege von Netzwerkstrukturen
Hardwarepflege: Reinigung von Bauteilen, Austausch von Verbrauchsmaterial (Druckerpatronen)

9.5 Aufstellung und Umgebung

Alle Teile des Computersystems einschließlich der elektronischen Speichermedien sollten in einer Umgebung betrieben und gelagert werden, welche die sichere Funktionsweise des Systems gewährleistet.
Ist dies nicht möglich, sind entsprechende Maßnahmen zu treffen, die die Funktionsweise, den Datenschutz und die Datensicherheit gewährleisten.

9.6 Schulung

Wie für alle anderen Ausrüstungsgegenstände, die im Labor verwendet werden, ist eine Einweisung der Mitarbeiter in die Nutzung der Hard- bzw. Software erforderlich.
Die Schulung kann intern oder extern erfolgen, hat auch, soweit erforderlich, die Aufrechterhaltung des notwendigen Wissens zu umfassen und ihre Durchführung ist aufzuzeichnen.

9.7 Lenkung von elektronischen Dokumenten

Dokumente, die in einem EDV-System bereitgehalten werden, müssen angemessen gegen Veränderung geschützt sein und allen betroffenen Mitarbeitern an den Stellen wo sie nötig sind zu Verfügung stehen.
Es muss ein dokumentiertes Verfahren vorliegen, in dem nachvollziehbar sichergestellt wird, dass die Dokumente von befugtem Personal genehmigt und bereitgestellt wurden. Diese Verfahren müssen sicherstellen, dass keine ungültigen Dokumente verwendet werden und die Rückverfolgbarkeit der Dokumentenhistorie gewährleistet ist. Ebenso muss das Verfahren Elemente enthalten, die die Information der betroffenen Personen über neue

und geänderte Dokumente sicherstellt. Änderungen in Dokumenten müssen für den Mitarbeiter erkennbar sein.
Eine unveränderbare Kopie der ungültigen Dokumente (inkl. ihrer Historie) ist entsprechend den Vorgaben für (technische) Aufzeichnungen zu archivieren.

9.8 Aufzeichnungen

Die Lenkung von Aufzeichnungen hat sich grundsätzlich an den Forderungen der ISO/IEC 17025 zu orientieren.
Aufzeichnungen müssen leserlich sein, leicht wieder auffindbar, datengesichert und datengeschützt über eine definierten Zeitraum aufbewahrt werden. Dies kann in geeigneter elektronischer Form oder in Papierform erfolgen.
Bei fehlerbedingten Änderungen von Aufzeichnungen muss sichergestellt werden, dass für jeden Fehler nachvollziehbar Korrekturen vorgenommen wurden.
Dies kann zum Beispiel:

- durch Anmerkung in der Aufzeichnung,
- Speicherung unter neuer nachvollziehbarer Dateikennung (Dateiname, Versionsnummer usw.),
- Protokollierung von Korrekturen oder
- gleichwertigen Maßnahmen erfolgen.

Ein reines Überschreiben von Daten in Aufzeichnungen ist nicht zulässig.

9.8.1 Technische Aufzeichnungen

Technische Aufzeichnungen im Sinne der ISO/IEC 17025, sind Aufzeichnung von ursprünglichen Beobachtungen und deren Ergebnisse, davon abgeleitete Daten und Daten, die es ermöglichen, Faktoren, die sich auf die Messunsicherheit auswirken, möglichst leicht erkennen zu können und um eine Wiederholung der Prüfung oder Kalibrierung unter Bedingungen zu ermöglichen die der, in der Aufzeichnung niedergelegten, möglichst nahe kommen.
Diese Aufzeichnungen müssen bei elektronischer Erstellung oder Erfassung zusätzlich folgende übliche Angaben enthalten:

- Identität des für diese Aufzeichnung verantwortlichen Personals,
- Zeitpunkt zu dem die Aufzeichnung erstellt wurde,
- Angaben zu den verwendeten Prüf-/Messmitteln, soweit erforderlich.

Wenn diese Aufzeichnungen zur Erstellung von Prüf- oder Kalibrierberichten herangezogen werden, so muss eine eindeutige Zuordenbarkeit vorhanden sein.
Eine unveränderbare Kopie von technischen Aufzeichnungen (inkl. der Berichte) muss entsprechend den Vorgaben der ISO/IEC 17025 archiviert und über einen Zeitraum von mindestens 10 Jahren aufbewahrt werden. Dies kann in geeigneter elektronischer Form oder in Papierform erfolgen.

9.8.2 Sonstige Aufzeichnungen

Sonstige Aufzeichnungen sind z.B. Protokolle, Auditberichte, Berichte über Managementbewertung, ungültig gewordene Dokumente (siehe ISO/IEC 17025 Punkt 4.3.1).
Die Aufbewahrungsfrist sollte 5 Jahre nicht unterschreiten.

9.9 Vernichtung von Daten und Datenträgern

Beim Vernichten von Daten auf Datenträgern ist darauf zu achten, dass durch einfaches Löschen am Datenträger der Inhalt der Dateien nicht vollständig beseitigt, sondern nur mit

einfachen Mitteln nicht mehr lesbar ist. Es ist daher mit Mitteln der nachhaltigen Beseitigung z.B. mechanische Zerstörung des Datenträgers, vollständige Formatierung Sorge zu tragen, dass die Daten auf den Datenträgern zerstört sind. Ein entsprechendes, dokumentiertes Verfahren ist im QM-System aufzunehmen.

10 Elektronische Übermittlung von Daten

Die dafür definierten Verfahren sind im QM-System zu beschreiben.
Die elektronische Übermittlung von Daten ist in ISO/IEC 17025 Punkt 5.10.7 geregelt. Darunter fallen z.B.:

- FAX
- e-Mail
- Datentransfer
- Übermittlung auf Datenträgern

Achtung: Bei Übermittlung von Ergebnissen als Email oder in deren Anhängen ist auf die mögliche unterschiedliche Darstellung durch Anwendung unterschiedlicher Formate und Zeichensätze zu achten.

10.1 Vorläufige Information

Elektronische Übermittlung von Prüfergebnissen oder Teilergebnissen als vorläufige Information an Kunden kann durch kompetente Personen autorisiert werden. Derartige Informationen müssen folgenden Mindestkriterien entsprechen:

- Erkennbarkeit des Laboratoriums
- Name des Autorisierenden und des Absenders
- Schutz der Daten vor unbeabsichtigter Veränderungen

Anmerkung: z.B. Schreibzugriff mit Kennwortschutz oder Übermittlung per FAX

Solche Informationen entheben das Laboratorium nicht der Verpflichtung einen rechtsgültigen Prüfbericht zu erstellen.

10.2 Prüfbericht

10.2.1 Begleitende Übermittlung eines elektronischen Prüfberichts:

Wenn ein Labor beabsichtigt, neben dem offiziellen Prüfbericht auf Papier (siehe ISO/IEC 17025 Punkt 5.10), den Bericht oder Auszüge daraus, elektronisch zu übermitteln, so ist Sorge zu tragen, dass eine Veränderung der übermittelten Dateien angemessen verhindert wird.
Bei der Übermittlung ist ein Hinweis anzubringen, dass im Zweifel der Originalbericht (Papierausgabe) als gültiges Dokument heranzuziehen ist.

Anmerkung: z.B. Schreibzugriff mit Kennwortschutz oder Übermittlung per FAX

10.2.2 Rein elektronischer Prüfbericht:

Falls ein Labor beabsichtig Berichte ausschließlich elektronisch zu versenden, so ist Augenmerk auf besonders hohen Schutz gegen Veränderung zu legen. Im Rahmen des QM-Systems ist das Verfahren zu dokumentieren. Die Korrektur derartiger Berichte hat nach

den gleichen Gesichtspunkten (ISO/IEC 17025 Punkt 5.10.9) wie bei Dokumenten, die auf Papier ausgefertigten wurden, zu erfolgen. Ebenso sind die Anforderungen hinsichtlich Lenkung, Aufbewahrung, Unveränderbarkeit und Vertraulichkeit der ISO/IEC 17025 zu erfüllten, z.B. ist sicherzustellen, dass für den Empfänger nachvollziehbar ist, dass die Freigabe durch eine befugte Person erfolgt ist.

Anmerkung: Derartige Dokumente können z.B. durch Erstellen eines PDF-Files mit kennwortgeschütztem Kopier-, Änderungs- und Datenentnahmeschutz erhalten oder per FAX übermittelt werden. Die Verwendung einer elektronischen Signatur gem. Signaturgesetz kann vereinbart werden.

Anhang A (informativ)

RISIKOANALYSE beim Einsatz von COMPUTERSYSTEMEN:

Fragenkatalog und technische Hinweise zur Risikoanalyse beim Einsatz von Computersystemen

1. Risiken für die Datensicherheit:

1.1 Technische Risiken

- technische Fehler Computer und Peripheriegeräte
- technische Fehler Datenträger
- ungeeignete Umgebungsbedingungen
- Fehlerhafte Software
- Computerviren

1.2 Organisatorische Risiken

- unzureichende Definition der Zuständigkeiten
- Bedienerfehler durch Unerfahrenheit der Benutzer
- Bedienerfehler durch Stress oder Arbeitsüberlastung
- bewusste Verfälschungen/Veränderung von Daten oder Programmen
- Verwendung von nicht verifizierter Software

2. Sicherheitsanalyse

2.1 Ist-Zustand

- Welche Daten werden verarbeitet?
- Welche Programme werden eingesetzt, welche Dateien werden dabei generiert?
- Welche Datenträger enthalten welche Dateien, sind Kopien verfügbar?
- Verantwortlichkeiten für Datenpflege
- Sind für jedes eingesetzte Programm unveränderte Originalversionen vorhanden?
- Sind Bedienungsanleitungen vorhanden?
- Ist die Konfiguration ausreichend dokumentiert?
- Wenn Daten an Dritte abgegeben werden, ist sichergestellt, dass nicht irrtümlich andere Daten übermittelt bzw. mit übermittelt werden?

2.2 Auswirkungen bei Verlust von Daten

- Welche Arbeiten werden dadurch verlangsamt oder können überhaupt nicht ausgeführt werden?
- Wie lang kann ohne die Daten ausgekommen werden?
- Wie groß sind der Zeitaufwand und die Kosten für die Herstellung des vorigen Zustands?

2.3 Sensibilitäten der einzelnen Anwendungen

- Welche Anwendungen und Daten dürfen von wem genutzt werden?
- Wie wichtig sind die Nutzungsberechtigungen?
- Sind Programme für bestimmtes Personal zu sperren?

- Sind besondere Dateien (Daten, Datenfelder) für bestimmte Berechtigte zu sperren?
- Was ist aus Revisionsgründen zu dokumentieren?

2.4 Welcher Zustand kann schlimmstenfalls eintreten?

3.Sicherungsmaßnahmen

3.1 Organisatorische Maßnahmen

3.1.1 Verantwortung

- für regelmäßige Datensicherung
- für Wiederherstellung verlorener bzw. beschädigter Daten
- für gesicherte Daten und die Aufbewahrung der Datenträger
- für Beschaffung, Pflege bzw. Wartung der Hardware und Software

3.1.2 Schulung und Benutzerservice

- Sind spezielle Schulungen zum Umgang mit Hard- und Software erforderlich?
- Gibt es bei Problemen qualifizierte Ansprechpartner?

3.1.3 Zugangsregelung

Sind geeignete organisatorische oder technische Maßnahmen vorhanden?

- Zutritt zu Räumen
- Passwortanmeldung mit personifizierter Benutzeridentifikation
- Sonstige Zugangssicherungen
  (z.B.: Fingerprint, Zugangskarten)

3.1.4 Notbetrieb und Störungen

- Vorhersehbare Beeinträchtigungen (z.B. Wartungsarbeiten, Stromabschaltungen)
  - Wer ist von wem zu benachrichtigen?
  - Welche Arbeiten müssen während dieser Beeinträchtigungen unterbrochen werden?
  - Welche Arbeiten müssen aufrechterhalten werden?
  - Informationen über das Ende der Beeinträchtigungen?
- Störungen
  - Wer ist zu benachrichtigen?
  - Welche Arbeiten müssen während dieser Beeinträchtigungen unterbrochen werden?
  - Welche Arbeiten müssen aufrechterhalten werden?
  - Wo und wie werden entsprechenden Sicherungskopien gefunden?
  - Informationen über das Ende der Beeinträchtigungen?
- Welcher Zustand kann schlimmstenfalls eintreten?

3.2 Technische Maßnahmen

3.2.1 Datensicherung

- Welche Festlegungen sind notwendig?
  - Verantwortlichkeiten
  - Sicherungsverfahren
  - Sicherungspläne
  - Sicherungsmedien
  - Sicherungsträgerbehandlung
- Welche Daten sind zu sichern?

- Aufzeichnungen
- Originalsoftware (unveränderte Kopie)
- Konfigurationsdateien
- Masken für Eingabe und Reports
- Daten entsprechend Aufwand für Wiederbeschaffung
- selbsterstellte Programme, Makros, Text- und Programmbausteine

- Wann und wie oft sichern?
  - Regelmäßige Sicherung der Aufzeichnungen
  - Vor Installationen aktuelle Konfigurationsdateien und Originalsoftware
  - Vor jeder Veränderung von Programmen, Makros und Masken
  - Während der laufenden Arbeit Zwischensicherungen vornehmen!
  - Nach Beendigung jedes wesentlichen Arbeitsschrittes
  - Regelmäßige Sicherung des Gesamtstandes
- Wie sichern?
  - Sicherung auf einem anderen Datenträger
  - Dateibestände zu einem festgelegten Zeitpunkt sichern (z.B. Backup)
  - Möglichst Datenstände sichern, wenn sich nicht diese dauernd verändern
- Auf welchen Medien sichern?
  - Streamer
  - CD / DVD
  - Diskette
  - Wechselplatte
  - andere elektronischen oder optischen Medien
  - Papierform
- Wie sollte Aufbewahrung der Sicherungskopien erfolgen?
  - Klare Kennzeichnung (Inhalt, Zeitpunkt, Reihenfolge, Eigentümer der Daten etc.)
  - Erstellung von Dateisicherungsprotokollen
  - Aufbewahrung der Kopien getrennt vom Entstehungsort der Daten (Behälter, Schrank, Raum)
  - Vermeidung von Beeinträchtigungen (chemisch, mikrobiologisch, Staub, Hitze, Magnetfelder)
  - Berücksichtigung der Alterung der Medien während der Lagerung
  - Ist die Lesbarkeit der Daten während der Lagerdauer gewährleistet?

3.2.2 Virenschutz

- Sind die Daten vor Computerviren geschützt?
  - permanenter Einsatz und Aktualisierung von Virenschutz- und Virensuchprogrammen
  - Regelungen über Maßnahmen bei Vermutungen eines Virenbefalls.
  - Keine Verwendung von Raubkopien
  - Vorsicht bei Verwendung von Free- und Sharewareprogrammen

3.2.3 Unberechtigte Zugriffe von außen

- Kann auf das Computersystem von außen (Internet, Telefon) zugegriffen werden?
  - Art und Dauer der Verbindung nach außen
  - Modem (aktiv und passiv)
  - Standleitung
  - Funknetzwerke
  - Remote Zugriff
- Sind die Computersysteme vor unberechtigtem Zugriff von außen (Internet, Telefon) geschützt?
  - Firewall (Hard- und/oder Software)
  - Rückwählverbindung
  - Usw.

Anhang B (informativ)

Beispiele:

Nachfolgende Beispiele sind nicht vollständig und dienen dem Anwender nur zur Erläuterung einzelner Punkt. Sie sollen nicht als Vorlage, sondern nur zu Orientierung dienen. Weiters ist zu den einzelnen angeführten Punkten nur die Unterschiede zu den vorgehenden Punkten dargestellt. Ebenso erheben die Aufzählungen in den einzelnen Punkten keinen Anspruch auf Vollständigkeit.

Zu Punkt 6 Anforderungen an Aufzeichnungen über Computer und -systeme

Büro-PC

Verwendungszweck

Erstellung von Schriftstücken (Korrespondenz, Berichte, Dokumente, Protokolle, usw.)
Verwaltung von Daten (Adressen, Gerätelisten usw.)

Hersteller und Typenbezeichnung

Firmenbezeichnung, Modellbezeichnung (z.B.: Lieferscheinangabe)
Bei Eigenbau Angaben zu den wesentlichen Bauteilen (z.B. Prozessor, Grafikkarte, Speichergröße).

zusätzliche Komponenten
z.B.: Bandlaufwerk, CD-Brenner
Modem, Netzwerkanschluss
Grundsätzlich nicht anzugeben sind zusätzliche Angaben zu Drucker, Bildschirm, Maus, Tastatur udgl.

Software:
Betriebsystem: Angaben zu Betriebssystem und der Version (z.B. SuSe Linux 8.2, Windows 2000, XP, usw.)
Applikationssoftware: Angaben zur wesentlichen Anwendung und der Version (z.B. MS-Office 2000, Open Office, Staroffice 6.0 usw.)

eindeutige Identifikation des Systems:
Inventarnummer, Seriennummer, interne Bezeichnung

Mess- und Auswerte - PC

Verwendungszweck
Steuer- und Auswerterechner für Gaschromatographie
Steuer- und Datenerfassung von Zugprüfmaschinen
Hersteller und Typenbezeichnung siehe oben

Zusätzliche Komponenten:
Interfacekarten, Datalogger

Software
Galaxie 1.0, Zwick 8.0, etc.

Netzwerk

Verwendungszweck:
Kommunikation, Datenaustausch, Zentrale Datenverwaltung und –sicherung, Bereitstellung von Dokumenten

Art und Struktur des Netzwerkes
Ringverkabelung, Sternverkabelung, Funknetz, WAN, LAN….
Hersteller und Typenbezeichnung der Netzwerkkomponenten
Server, Router, Switch, Firewall

zusätzliche Komponenten
Geräte zur Erfassung biometrischer Daten (Fingerprinterkennung)

Software
Serversoftware: Betriebssystem (Novell 4.12, LINUX, Windows 2000 Server, etc.)
Mailserver (MS Exchange 2000, Lotus Notes, etc.)
Backupsoftware (NT Backup, Veristas)

Protokolle: TCP/IP; Netbio, IPX usw.

Laborinformations- und Datenmanagementsystem

Das Risiko derartiger Systeme liegt vor allem in der Tatsache, dass die Daten nicht mehr als allein stehende Dokumente bestehen, sondern dass alle behandelten Dokumente in einer oder mehreren verschlüsselter Gesamtdateien vorhanden sind.

Systembeschreibung des Netzwerkes

Art des Workflows
Spezifikation der durch dieses System abgedeckten Bereiche:
Dokumentenlenkung, Datenauswertung, Berichtserstellung usw.

Zu Punkt 7 Beschaffung und Abnahme und 8 Verifizierung des Systems nach einer Systemänderung

Büro-PC

Einfache Funktionsprüfung und der Peripherie
Prüfung der Software auf Vollständigkeit und Lauffähigkeit

Mess- und Auswerte-PC

Prüfung des Zusammenspiels mit den Messgeräten
Prüfung der Funktionstüchtigkeit

- Im Zuge der Methodenerstellung und Validierung
- Durch Methodenkontrolle

Netzwerk

Prüfung der Verfügbarkeit aller Komponenten mit der geforderten Leistungsfähigkeit

LIMS

Bei LIMS ist ein der geplanten Anwendung entsprechender Prüfplan (Pflichtenheft) zu erstellen und seine Erfüllung im Zuge der Funktionsprüfung zu kontrollieren.

Zu Punkt 9 Betreiben von Computern und Computersystemen

Datenschutz

Zutrittsrechte zu Eingabeplätzen

- Schlüsselplan

Zugriffrechte auf Computer

- Loginbeschränkungen (personenbezogen)
- Maßnahmen für Zugriffe aus Netzwerken (z.B. Internet)
- Maßnahmen für externe Zugriffe über Einwählverbindungen (z.B. RAS, VPN)

Zugriffsrechte auf Dateien, Verzeichnisse und Strukturen

- Beschränkung durch Zugriffsrechte (Lesen, Schreiben, Ändern, Löschen…)
- Verwendung spezieller Datenformate (z.B. PDF)
- Physikalische Trennung

Zugriffrechte auf Datenmedien

- Physikalischer Zugriff auf gelagerte Medien (z.B. CD´s)

Regelungen zum Virenschutz

- Verwendung aktueller Virenschutzprogramme und regelmäßige Aktualisierung
- Firewall
- Schulung der Mitarbeiter über das Verhalten

Datensicherung

Spiegelung von Datenträgern

- Verwendung von speziellen Festplattensystemen (RAID Systemen)
- Synchronisierte Daten (Offlineordner, Replikation)

Backup auf Datenträger

- Verwendung von automatischen Backupsystemen (Bandsicherungsgeräten, Spindelbrenner)
- Verwendung von manuellen Backupsystemen (Backup auf CD´s, externen Festplatten usw.)

Kopien von Datenträgern

- Automatische oder manuelle Kopien von Dateien oder ganzen Verzeichnissen auf externe Datenträger (Diskette, CD´s usw.)

Beachtung der Haltbarkeit von Datenträgern:
Bei der Verwendung von magnetischen Medien ist auf die Lagerbedingungen zu achten (Strom- und Magnetfelder, Temperatur, Feuchtigkeit usw.). Die Datenträger sollten in regelmäßigen Abständen (z.B. jährlich) auf neue Medien kopiert werden.
Bei Verwendung optischer Medien (z.B. CD´s, DVD) ist neben den Lagerbedingungen (Temperatur, Feuchtigkeit) auch auf den mechanischen Schutz (Zerkratzen) zu achten. Über die (Langzeit) Haltbarkeiten von optischen Medien sind keine gesicherten Informationen verfügbar.

Archivierung von Daten:
Aufgrund der begrenzten Verwend- und Haltbarkeit von Datenträgern und dem systematischen Überschreiben von Daten inkl. fehlerhafter oder unbeabsichtigt geänderter Daten sollten im Generationsprinzip verwaltet werden. D.h. es werden in regelmäßigen Abständen die Datenträger getauscht oder durch Neue ersetzt.

Beispiel:

Sicherung: täglich MO-DI-MI-DO-FR
(überschreiben des ersten Bandes nach einer Woche),
Archivierung der Freitagskopie über ein Monat,
Archivierung einer Monatskopie, Quartalskopie, Jahreskopie….

Wartung:

Softwarepflege:

- Aktualisierung von Virensoftware und Firewalls,
- Pflege von Datenbeständen,
- Pflege von Zugriffberechtigungen,
- Pflege von Netzwerkstrukturen

Hardwarepflege:

- Reinigung von Bauteilen,
- Austausch von Verbrauchsmaterial (Druckerpatronen)

Lenkung von elektronischen Dokumenten

Die Nachvollziehbarkeit von Änderungen kann direkt im Dokument (Kennzeichnung der Änderungen) oder durch eine Änderungshistorie (Liste der Änderungen) gewährleistet werden.

	Leitfaden Computer in Prüflaboratorien	Nr.: **L 18**
Version/Datum 01 / 2003		Seite: 18 von 18
Erstellt: Fostel 10.12.2003	Geprüft: Beirat (95.Sitzung) 20.1.2004	Freigabe: Friers 20.1.2004

Inhaltsverzeichnis: