



---

## **DAR-INF-07**

---

# Hinweise zum Einsatz von Computersystemen in akkreditierten Laboratorien

## **1. Zielsetzung**

In akkreditierten Laboratorien werden Computersysteme für unterschiedlichste Aufgaben eingesetzt. Dazu gehören u.a.:

- Erstellung, Bearbeitung, Speicherung und Versand von Prüfergebnissen,
- Steuerung und Regelung von Prüfeinrichtungen,
- Messdatenerfassung, -auswertung, -speicherung, -ausgabe und -fernübertragung
- FEM-Berechnungen und Simulationsrechnungen,
- Datenbankanwendungen (z. B. Mess- und Prüfergebnisse, Prüfberichte, Kundenkartei, Referenzdaten),
- Labororganisation.

Aus der Verschiedenartigkeit der Einsatzgebiete und den unterschiedlichen Risiken, die mit dem Computereinsatz verbunden sind, folgt, daß keine generellen Festlegungen bezüglich des Sicherheitsniveaus und der daraus abzuleitenden QM-Maßnahmen getroffen werden können.

Das hier vorliegende Dokument basiert auf einer in der BAM erarbeiteten internen Richtlinie /1/ und dem EA-Dokument "Guidelines for the use of computers and computer systems in accredited laboratories" (Version 2, März 1998) /2/. Das Dokument gibt umfassende Hinweise hinsichtlich der Erfüllung der Forderungen der ISO/IEC 17025 beim Einsatz von Computersystemen in akkreditierten Laboratorien. Das Dokument nennt die Grundprinzipien und Gesichtspunkte, die in Abhängigkeit vom jeweiligen Sicherheitsniveau zu berücksichtigen und erforderlichenfalls umzusetzen sind.

## **2. Begriffe**

### **Computersysteme**

Einzelne, vernetzte oder in Mess- und Prüfeinrichtungen integrierte Computer mit ihrer zugehörigen Hardware und Software.

### **Validierung**

Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, daß die besonderen Forderungen für einen speziellen beabsichtigten Gebrauch erfüllt worden sind.

(DIN EN ISO 8402)

### **Rohdaten**

Rohdaten sind alle ursprünglichen Aufzeichnungen und Unterlagen der Prüfeinrichtung oder deren überprüfte Kopien, die als Ergebnis der ursprünglichen Beobachtungen oder Tätigkeiten bei einer Prüfung anfallen. (GLP)

## **3. Zuständigkeiten**

Die allgemeinen QM-Grundsätze für Mess- und Prüfmittel finden auch beim Einsatz von Computersystemen Anwendung. Das betrifft z.B. die Festlegung der Zuständigkeiten der mit den Computersystemen befassten Mitarbeiter, ihre Einweisung oder Schulung sowie die Einbeziehung der Computersysteme in die QM-Dokumentation und die internen Audits und Reviews.

Für eingesetzte Computersysteme sind unter Berücksichtigung des Einsatzzweckes angemessene Sicherheitsniveaus festzulegen und daraus die erforderlichen QM-Maßnahmen abzuleiten. Die Mitarbeiter sind für die Konsequenzen zu sensibilisieren, die für Arbeitsabläufe und -ergebnisse aus der wachsenden Abhängigkeit von der Funktionsfähigkeit der Computersysteme folgen können. In der Praxis können besondere Umstände eintreten, die es erforderlich machen, daß von QM-Regelungen im Einzelfall abgewichen werden muss. In den QMH muss festgelegt werden, wer in diesen Fällen das abweichende Vorgehen genehmigen darf und wie das jeweils zu dokumentieren ist.

## **4. Regelungsrelevante Gesichtspunkte beim Computereinsatz**

Ob und in welchem Umfang die nachfolgend genannten Gesichtspunkte beim Einsatz der Computersysteme umgesetzt werden müssen, hängt von der Festlegung des erforderlichen Sicherheitsniveaus und damit von der Risikoeinschätzung ab. Das Risiko für ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit von Daten und ihrer Verarbeitung gefährden kann, ist ein Wertepaar, das sich aus den beiden Komponenten Eintrittshäufigkeit und Schadenshöhe des Ereignisses zusammensetzt /3/. Als Hilfestellung bei den notwendigen Entscheidungen können die Fragen und technischen Hinweise im Anhang herangezogen werden.

### **4.1 Abnahmeprüfung, Validierung**

Grundsätzlich sind beschaffte Computersysteme und die zugehörige Software vor Abnahme zu prüfen. Das sollte in der Regel durch denjenigen Mitarbeiter geschehen, der die Spezifikationen festgelegt hat. Das Ausmaß der Abnahmeprüfung richtet sich nach den geforderten Spezifikationen, sie kann im Falle von Standardspezifikationen aus einer einfachen Funktionsprüfung bestehen. Berücksichtigt werden können auch Unterlagen über Validierungen durch den Hersteller, insbesondere wenn dieser ein zertifiziertes QM-System z. B. nach DIN EN ISO 9001 betreibt. In jedem Fall sind die Abnahmeprüfung, ihr Umfang und ihre Ergebnisse im Geräteordner zu dokumentieren. Die Freigabe zum Einsatz neu beschaffter Hardware und Software auf dieser Basis ist zu regeln und zu dokumentieren.

Im Laboratorium entwickelte oder modifizierte Software ist vor ihrem Einsatz im erforderlichen Umfang zu validieren. Zur Software gehören nicht nur Programme, die mit klassischen Programmiersprachen erstellt worden sind, sondern auch vom Benutzer erstellte "Makros", die bestimmte Vorgänge innerhalb eines Programms automatisch nach Aufruf steuern. Durch die Validierung soll sichergestellt werden, daß die Software für den vorgesehenen Einsatzzweck geeignet ist. In Abhängigkeit vom Validierungsergebnis, das zu dokumentieren ist, ist über den Einsatz der Software vom zuständigen Mitarbeiter zu entscheiden

Bei bereits im Gebrauch befindlichen Computersystemen sollten zunächst die Unterlagen gesammelt werden, die Vertrauen in die Gebrauchstauglichkeit der Systeme begründen. Auf dieser Basis kann der zuständige Mitarbeiter entscheiden, ob weitere Validierungsmaßnahmen erforderlich sind.

Computersysteme, die Teil eines Mess- oder Prüfmittels sind, können mit diesem zusammen validiert werden /4/.

Für die Validierung kommen u. a. folgende Vorgehensweisen in Frage:

- Einsatz von Test-Software
- Simulation von realen Eingabewerten durch theoretisch ermittelte Werte und Ergebnisvergleich
- Einsatz von Referenzdaten mit anschließendem Ergebnisvergleich
- Durchführung von Messungen oder Prüfungen mit Prüfgegenständen mit bekannten Kennwerten (Referenzobjekte oder –materialien)

Ein besonderes Augenmerk ist bei der Software-Validierung auf die Verträglichkeit und Wechselwirkung zwischen verschiedenen Programmen bzw. zwischen Software und Hardware zu richten. Dies gilt insbesondere dann, wenn durch Software die Hardware-Konfiguration nachhaltig verändert wird.

#### **4.2 Aufzeichnungen über Computersysteme**

Analog zu Prüfmitteln sollten für Computersysteme beispielsweise in einem Geräteordner die zugehörigen Unterlagen und Aufzeichnungen gesammelt werden. Hierzu gehören insbesondere Beschreibungen der jeweiligen Hardware- und Software-Konfiguration sowie der eingesetzten Softwareversionen. Ein besonderes Augenmerk ist auf austauschbare Hardware-Module (z. B. A/D-Wandlerkarten) zu richten.

Hard- und Software müssen eindeutig gekennzeichnet bzw. identifiziert werden. Dies gilt auch für austauschbare Module, wenn nicht durch andere Maßnahmen (z. B. Siegel) die Hardware als "Black Box" betrachtet werden kann.

Konfigurations- und Softwareänderungen müssen dokumentiert, ebenso wie die Ergebnisse einer ggf. erforderlichen Revalidierung, über deren Notwendigkeit der zuständige Mitarbeiter zu entscheiden hat.

#### **4.3 Geeignete Umgebungsbedingungen**

Für die Nutzung der Computersysteme und die Lagerung der Speichermedien sind geeignete Umgebungsbedingungen zu wählen, die die Funktion der Computersysteme bzw. die Qualität und Lesbarkeit der gespeicherten Daten nicht beeinträchtigen. Erforderlichenfalls sind die Umgebungsbedingungen zu überwachen und aufzuzeichnen.

Soweit zutreffend ist auch die EG-Richtlinie über die Mindestvorschriften bezüglich der Sicherheit und des Gesundheitsschutzes bei der Arbeit an Bildschirmgeräten (90/270/EWG) hinsichtlich der ergonomischen Gestaltung des Arbeitsplatzes zu berücksichtigen (siehe auch DIN EN ISO 9241 Teil 3,7 und 8).

#### **4.4 Einweisung der Mitarbeiter**

Soweit erforderlich sollte die Einweisung der Mitarbeiter in die Nutzung neuer Hard- und Software durch die Lieferfirma oder durch kompetente Mitarbeiter des Laboratoriums erfolgen. Hierzu gehört insbesondere die Belehrung über das Verhalten im Systemaus- und -störfall sowie die Behandlung und Bedeutung von Fehlermeldungen. Umfangreichere Einweisungen sollten dokumentiert werden.

#### **4.5 Zugangs-, Benutzer- und Zugriffskontrolle**

Notwendige Maßnahmen bezüglich der Zugangs-, Benutzer- und Zugriffskontrolle, z. B. durch besondere Schlüsselregelungen, Vergabe von Passwörtern oder abgestimmte Zugriffregelungen sind durch die verantwortlichen Personen zu regeln.

#### **4.6 Kalibrierung, Wartung und Funktionsprüfung**

Analog zu anderen Mess- und Prüfmitteln muss beim Einsatz von Computersystem die metrische Rückführung auf SI-Einheiten bzw. die Rückverfolgbarkeit sichergestellt werden. Es ist festzulegen, in welchen Intervallen und in welchem Umfang Kalibrierungen, Wartungen und Funktionsprüfungen vorgenommen werden sollen. Die Festlegung, Wartungen nur im Störfall vorzunehmen (Bedarfwartungen), kann durchaus ausreichend sein. Computersysteme, die Teil eines Mess- oder Prüfmittels sind, werden in der Regel in dessen Kalibrierung und Wartung einbezogen. Dabei gelten die gleichen Grundsätze und Verfahrensweisen hinsichtlich der Kalibrierung wie bei konventionellen Mess- und Prüfmitteln. Es können sowohl einzelnen Module als auch das Gesamtsystem kalibriert bzw. gewartet werden.

#### **4.7 Virenschutz**

Falls ein Datenaustausch mit anderen Computersystemen z. B. über Netzwerke besteht, ist für einen ausreichenden Virenschutz zu sorgen. Empfehlenswert ist eine Automatisierung des Virenschutzes.

Für den Fall eines Verdachts auf Virenbefall sind geeignete Maßnahmen festzulegen. Beispielsweise sollte das betroffene Computersystem sofort vom Netz getrennt und außer Betrieb genommen werden. Dabei ist auch zu prüfen, ob bereits andere Computersysteme ebenfalls betroffen sind; in diesem Fall sind die zuständigen Mitarbeiter umgehend zu informieren.

#### **4.8 Behandlung der Daten**

Rohdaten sind alle ursprünglichen Laboraufzeichnungen und Unterlagen oder darin überprüfte Kopien, die als Ergebnis der ursprünglichen Beobachtungen oder Tätigkeiten bei einer Prüfung anfallen /5/. Dabei kann es sich auch um mit einer zutreffenden Vorschrift verständlich aufbereitete Messergebnisse handeln, die von einer hierzu autorisierten Person auf Plausibilität geprüft und akzeptiert sind /6/. Für jedes Computersystem ist festzulegen, in welcher Form Rohdaten gespeichert werden sollen (z.B. in elektronischer Form, als Ausdruck oder graphische Darstellung). Kriterium hierbei ist, daß die Rückverfolgbarkeit einer Messung oder Prüfung sowie erforderlichenfalls eine Wiederholung sichergestellt sind.

Wenn Daten manuell in das Computersystem eingegeben werden, sollte der Name der Person, die die Eingabe vornimmt, zum Zeitpunkt der Eingabe angegeben werden. Bei automatischer Datenerfassung sollten das zur Datenübertragung verwendete Gerät und der Zeitpunkt der Übertragung aufgezeichnet werden.

Beim automatischen Betrieb computergestützter Prüfmittel ist darauf zu achten, daß die Beziehung zwischen den einzelnen Prüfgegenständen und den im Ergebnis anfallenden Daten eindeutig hergestellt werden kann.

Die Anforderung, jede ggf. erforderliche Änderung von Rohdaten so vorzunehmen, daß

- die vorherigen Eingaben nicht unleserlich werden,
- der Grund angegeben wird,
- die Person, die die Änderung vornimmt, und das Datum festgehalten werden,

bleibt auch für in Computersystemen gespeicherte Daten gültig.

Alle Aufzeichnungen, die zu einem bestimmten Auftraggeber, Prüfgegenstand und einer bestimmten Prüfung gehören, sollen so gekennzeichnet werden, daß Rückverfolgbarkeit zwischen ihnen unabhängig davon besteht, ob sie elektronisch oder andersartig gespeichert sind.

Sicherungskopien aller Daten sollen in angemessenen Zeitabständen nach geeigneten Verfahren gemacht und sicher gelagert werden. Um den Datenzugriff über den gesamten Aufbewahrungszeitraum sicherzustellen, muss bei jedem Wechsel von Hard- und Software geprüft werden, ob die gespeicherten Daten umformatiert werden müssen.

Analoge Überlegungen sind bei Datenbanken anzustellen.

#### **4.9 Elektronische Übermittlung von Prüfergebnissen**

Bei einer elektronischen Übermittlung von Prüfergebnissen (z. B. per Diskette oder Email) muß insbesondere die Integrität und Vertraulichkeit der Daten durch geeignete Verfahren (z. B. digitale Signatur) sichergestellt werden.

#### 4.10 Auswirkungen auf die Ergebnisunsicherheit

Insbesondere in den Bereichen der Messdatenerfassung und –verarbeitung, der Simulationsrechnung sowie bei der Steuerung und Regelung von Prüfeinrichtungen können eingesetzte Computersysteme einen Einfluss auf die Genauigkeit des Prüfergebnis haben. Bei einer erforderlichen Abschätzung der Unsicherheit des Prüfergebnis ist dies zu berücksichtigen.

### 5. Literatur, Normen und Richtlinien

- /1/ M. Golze, Gutmann, D.  
Qualitätsmanagement beim Einsatz von Computersystemen in der BAM  
BAM-QMH-P-2.7, 02.11.1998
- /2/ EA-Dokument "Guidelines for the use of Computers and computer systems in accredited laboratories", Version 2, März 1998
- /3/ T-Grundschutzhandbuch 1998 - Maßnahmenempfehlungen für den mittleren Schutzbedarf, veröffentlicht im Bundesanzeiger Nr. 123a vom 8. Juli 1998,
- /4/ Software in Scientific Instruments  
NPL-Measurement Good Practice Guide No. 5, Ausgabe 1999
- /5/ Grundsätze der Guten Laborpraxis (GLP)  
Bundesgesetzblatt 1994 Teil 1, S. 1724 – 1732
- /6/ G. Christ u.a.  
Einsatz computergestützter Systeme bei GLP-Prüfungen  
Pharm. Ind. **59** (1997) 1, 24-29, 2, 116-120
- /7/ GLP-Konsensdokument,  
Die Anwendung der GLP-Grundsätze auf computergestützte Systeme  
Bundesanzeiger Nr. 231, S. 12750 ff., 10. Dez. 1996
  
- DIN EN ISO 8402 Qualitätsmanagement - Begriffe, 1995
- DIN EN ISO 9001 Qualitätsmanagementsysteme - Modell zur Qualitätssicherung/QM-Darlegung in Design, Entwicklung, Produktion, Montage und Wartung, 1994
- DIN EN ISO 9241 Teil 3, 7 und 8: Anforderungen für Monitore an Bildschirmarbeitsplätzen
- 90/270/EWG EU-Richtlinie über die Mindestvorschriften bezüglich der Sicherheit und des Gesundheitsschutzes bei der Arbeit an Bildschirmgeräten
- DGQ-Richtlinie 17-01 Zuverlässigkeit komplexer Systeme aus Hardware und Software, 1998

## Anhang

### Fragenkatalog und technische Hinweise zur Risikoanalyse beim Einsatz von Computersystemen

#### 1. Risiken bei der Gewährleistung der Datensicherheit

##### 1.1 Technische Risiken

Dazu gehören

- Fehler der Computer und der Peripheriegeräte
- Fehler der Datenträger
- ungeeignete Umgebungsbedingungen
- Fehler oder unzureichende Bedienersicherheit der eingesetzten Software

##### 1.2 Organisatorische Risiken

Dazu gehören

- Unzureichende oder unklare Aufgabenabgrenzung (z.B. Anwendungsbetreuung, Dateneingabe, Kontrolle, Schreibrechtteilung)
- Bedienfehler durch Unerfahrenheit der Nutzer
- Bedienfehler durch Hektik im Arbeitsablauf
- bewusste Verfälschung von Datenbeständen und Programmen

#### 2. Risikoanalyse - Sicherheitsbedarfsanalyse

##### 2.1 Ist-Zustand

- Welche Daten werden mittels EDV verarbeitet?
- Welche Programme werden dazu eingesetzt und in welchen Dateien werden welche Daten gehalten?
- Auf welchen Datenträgern liegen welche Dateien? Gibt es Kopien? Welchen Aktualisierungsstand haben diese Kopien? Wo werden sie aufbewahrt?
- Wer ist für die Pflege (Erfassung, Veränderung, Löschung) welcher Daten verantwortlich? Wann, wo, wie, warum, von wem werden welche Daten verändert? Was passiert mit den Eingabebelegen? Wer aktualisiert die Kopien?
- Wer nutzt welche Daten? Wann, wozu, wie? Wie ist die Zusammenarbeit organisiert? Welche Daten werden von mehreren gemeinsam genutzt?
- Welche Dateien finden sich noch auf dem Datenträger?
- Gibt es zu jedem eingesetzten Programm eine Lizenzvereinbarung und eine garantiert unveränderte schreibgeschützte Originalversion?
- Sind ausreichende Bedienungsvorschriften vorhanden?
- Gibt es Aufzeichnungen zur Konfigurierung?
- Wann, wo und von wem werden Daten manuell verarbeitet?
- Werden Datenträger, die für die Datenspeicherung zur Übergabe an Dritte vorgesehen sind, so vorbereitet (z.B. mit DOS-Format formatiert), daß sich keine "heimlichen" Daten mehr darauf befinden?
- Sind Festlegungen zur Datensicherung in Verträgen bei Auftragsarbeiten getroffen worden?

## 2.2 Auswirkungen eines Datenverlustes oder eines Hard- und Softwarefehlers

- Welche Arbeiten würden sich dadurch in welchem Maße verlangsamen?
- Welche Arbeiten könnten überhaupt nicht mehr ausgeführt werden?
- Welcher Verlust würde eintreten?
- Wie lange könnte ohne die Daten ausgekommen werden?
- Wie hoch ist der Zeitaufwand zur Herstellung des alten Zustandes?
- Wie hoch sind die Kosten für die Wiederbeschaffung beschädigter Geräte, Programme oder Daten?

## 2.3 Sensibilität der einzelnen Anwendungen

- Dürfen Anwendungen von allen oder nur von einer eingeschränkten bestimmten Mitarbeitergruppe genutzt werden?
- Muss besonders darauf geachtet werden, daß Nutzungsberechtigungen nicht missbraucht werden?
- Darf von allen Berechtigten die volle Anwendung genutzt werden?
- Sind Programme der Anwendung für bestimmte Berechtigte zu sperren?
- Sind besondere Funktionen in den Programmen für bestimmte Berechtigte zu sperren?
  
- Dürfen alle Dateien für alle Berechtigte zugänglich sein?
- Sind besondere Dateien für bestimmte Berechtigte zu sperren?
  
- Dürfen alle Daten für alle Berechtigte zugänglich sein?
- Sind besondere Datenfelder (z.B. in Datenbanken) für bestimmte Berechtigte zu sperren?
- Dürfen alle Berechtigte Daten manipulieren?
- Sind wichtige Daten zusätzlich zu verschlüsseln?
- Dürfen Nutzungsrechte an Dritte weitergegeben werden?
- Welche Vorgänge sind aus Revisionsgründen laufend zu dokumentieren?

## 3. Sicherungsmaßnahmen

### 3.1 Organisatorische Maßnahmen

#### 3.1.1 Verantwortung

- Wer hat Dateien mit personenbezogenen Daten an den Datenschutzbeauftragten zu melden?
- Wer ist für die regelmäßige Datensicherung verantwortlich?
- Wer ist für die Rekonstruktion beschädigter / verlorener Daten zuständig?
- Wer hat die gesicherten Daten zu verwalten?
- Wer ist für die Festlegung der Benutzerprofile zuständig?
- Wer ist mit der Fortschreibung von Hard- und Software und der damit verbundenen Gewährleistung der Verwendbarkeit älterer Datenbestände betraut?
- Wem obliegt die Pflege gemeinsam genutzter Daten?
- Wer ist für die Beratung/Betreuung der Nutzer eingesetzt?
- Wer hat die Pflege bzw. Wartung der Hardware zu organisieren bzw. durchzuführen?

#### 3.1.2 Schulung und Benutzerservice

- Sind spezielle Schulungen zum Umgang mit Hard- und Software für die einzelnen Nutzer erforderlich?
- Werden in den für die Anwendung vorgesehenen Qualifizierungsmaßnahmen die Probleme des Datenschutzes angesprochen?
- Gibt es Ansprechpartner für auftretende Probleme?

### 3.1.3 Zugangskontrolle

Geeignete Maßnahmen dazu können sein:

*organisatorisch*

- Betrieb in zugangskontrollierten Räumen
- Einrichtung von Sicherheitszonen
- Trennung von Datenträger und Computer in Stillstandszeiten
- Protokollierung des Eingabe- oder Veränderungsdatums sowie des eingebenden Nutzers
- ordnungsgemäßes Beenden von Anwendungen bei längeren Arbeitspausen

*Hardwareerschutz*

- elektronische Zugangssicherungen
- (z.B. HardwareBootSperrung - SafeGuard-Karten)
- Verschießbarkeit des Computerzuganges
- (Tastaturschlüssel, Diskettenschloss)
- Softwareschutz
- Zugangsprotokollierung
- Paßwortzugang
- Benutzeridentifikation
- Einrichtung geschlossener Benutzergruppen

### 3.1.4 Notbetrieb planen

- Wer muß benachrichtigt werden?
- Welche Routinearbeiten müssen unterbrochen werden, damit die Restaurierung nicht gestört wird?
- Wie können beschädigte Dateien gefunden werden?
- Wie werden die passenden Sicherungskopien gefunden?

## 3.2 Technische Maßnahmen

### 3.2.1 Datensicherung

- Welche Festlegungen sollten getroffen werden?
    - Verantwortlichkeiten
    - Sicherungsverfahren
    - Sicherungspläne
    - Sicherungsmedien
    - Sicherungsträgerbehandlung
    - Kontrollen
  - Welche Daten sind zu sichern?
    - Originalsoftware (Es sollte eine unveränderte Kopie existieren)
    - Konfigurationsdateien
    - Masken für Eingabe und Reports
    - Daten entsprechend ihrem Wiederbeschaffungsaufwand
    - selbsterstellte Programme, Makros, Text- und Programmbausteine
  - Wann und wie oft sichern?
    - Vor Installationen die aktuellen Konfigurationsdateien sowie die Originalsoftware (Es sollte möglichst von einer Kopie installiert werden)
    - Vor Veränderung von Programmen, Makros und Masken
    - Während der laufenden Arbeit Zwischenstände sichern
    - Nach Beendigung wesentlicher Arbeitsschritte
    - regelmäßige Sicherung des Gesamtstandes
  - Wie sichern?
    - Möglichst konsolidierte Datenbestände sichern, d.h. wenn sich die Daten nicht laufend ändern.
    - kleinere Dateien als Kopie sichern
    - Sicherungen sollten grundsätzlich auf einem anderen (externen) Datenträger erfolgen
    - größere Datenbestände als Backup zu einem festgelegten Zeitpunkt sichern
      1. Gesamt-Backup (alle Dateien)
      2. Fortschritts-Backup (nur geänderte Dateien)
      3. Teil-Backup (alle Daten eines bestimmten Typs, z.B. \*.txt)
- Dabei ist eine geeignete Folge von Gesamt-Backup und den Fortschritts- oder Teil-Backups festzulegen.  
Für erhöhte Anforderungen sollten Mehrgenerationsverfahren sowie evtl. auch mehrere

verschiedene Sicherungsverfahren zum Einsatz kommen.

Backups und die Restaurierung beschädigter Datenbestände sollten nur von erfahrenen Nutzern durchgeführt werden.

- Auf welchen Medien sichern?
  - Streamer
  - Diskette
  - Wechselplatte
  - WORM (Write Once, Read Multiply)
  - PapierformDabei sollten die über die Netzwerkdienste angebotenen Möglichkeiten vorrangig genutzt werden.
- Wie sollte die Aufbewahrung der Sicherungskopien erfolgen?
  - klare Kennzeichnung der Sicherungen nach Inhalt, Zeitpunkt, Reihenfolge und erforderlichenfalls Eigentümer der Daten und Sicherer
  - Erstellung von Datensicherungsprotokollen
  - Aufbewahrung der Kopien getrennt vom Entstehungsort der Daten (gesondertes Behältnis, gesonderter Schrank, gesonderter Raum)
  - Vermeidung von Schäden infolge chemischer oder mikrobieller Verunreinigung, Staubkontamination, Hitze, Dämpfe und Magnetfelder
  - Berücksichtigung der Alterung der Datensicherungsmedien bei Lagerung über größere Zeiträume und bei häufiger Wiederverwendung der Datenträger

### 3.2.2 Virenschutz

- Werden zum Schutz vor Datenverlusten durch Computerviren geeignete Vorsorgemaßnahmen getroffen z.B.:
  - regelmäßige Datensicherung
  - Programmbeschaffungsdocumentation
  - Programminstallation mit schreibgeschützten Dateien
  - permanenter Einsatz von Virensuch- und Virenschutzprogrammen
- Wie werden aufgetretene Viren, wie
  - Systemviren
  - Linkviren
  - Bootviren
  - Hybrideaus den vorangegangenen protokolliert?
- Werden virenverseuchte Dateien, wenn möglich, als Belegexemplare auf besonders gekennzeichneten externen Datenträgern ans Rechenzentrum übergeben?
- Werden Computer, auf denen Viren auftreten, bis zur Behebung des Problems umgehend von jeglichem Netzzugang getrennt und aus dem Arbeitsprozess ausgesondert?

### 3.2.3 Wartung

- Sind die Computer für die vorgesehenen Aufgaben ausreichend dimensioniert und werden sie regelmäßig gepflegt bzw. gewartet, um Datenverluste und Systemabstürze infolge mangelnder Systemressourcen zu vermeiden?
- Erfolgt nach Veränderung der Hardware der Computer und/oder der damit angewendeten Software eine Überprüfung mit bekannten Daten und festgelegten Anwendungen zum Feststellen einer ordnungsgemäßen Datenverarbeitung, die erforderlichenfalls protokolliert wird?  
Für Zwecke der Validierung ist es allgemein akzeptierbar, einen einwandfreien Betrieb des Computers für die Aufgabe anzunehmen, wenn bei der Eingabe gut charakterisierter Parameter der Aufgabe erwartete Antworten produziert werden.
- Werden bei einer Wartung der Computer Maßnahmen ergriffen, die eine Unversehrtheit und Vertraulichkeit wichtiger Daten sicherstellen?  
Wird insbesondere bei einer Wartung durch externe Auftragnehmer eine angemessene Verpflichtung zur Vertraulichkeit über erhaltene Informationen vereinbart?