

**Checkliste für den Baustein  
„PC mit Windows 95“**

---

## Inhalt

<b>1 Administrator .....</b>	<b>7</b>
1.1 Übergeordnete Fragen .....	7
1.1.1 Allgemeine Fragen zur Organisation .....	7
1.1.2 Datensicherung .....	9
1.1.3 Datenträger .....	11
1.1.4 Identifikation und Authentisierung.....	11
1.1.5 Peripheriegeräte.....	12
1.1.6 Protokollierung .....	13
1.1.7 Schulung .....	14
1.1.8 Software.....	15
1.1.9 Virenschutz .....	18
1.1.10 Windows 95 .....	21
1.1.11 Zugriffsschutz.....	26
<b>2 Archivverwalter .....</b>	<b>27</b>
2.1 Übergeordnete Fragen .....	27
2.1.1 Allgemeine Fragen zur Organisation .....	27
2.1.2 Datensicherung .....	27
2.1.3 Datenträger .....	28
2.1.4 Identifikation und Authentisierung.....	31
2.1.5 Peripheriegeräte.....	31
2.1.6 Protokollierung .....	31
2.1.7 Schulung .....	31
2.1.8 Software.....	31
2.1.9 Virenschutz .....	31
2.1.10 Windows 95 .....	31
2.1.11 Zugriffsschutz.....	31
<b>3 Beschaffungsstelle .....</b>	<b>32</b>
3.1 Übergeordnete Fragen .....	32
3.1.1 Allgemeine Fragen zur Organisation .....	32
3.1.2 Datensicherung .....	33
3.1.3 Datenträger .....	33

---

3.1.4	Identifikation und Authentisierung.....	33
3.1.5	Peripheriegeräte.....	33
3.1.6	Protokollierung .....	33
3.1.7	Schulung .....	33
3.1.8	Software.....	33
3.1.9	Virenschutz .....	33
3.1.10	Windows 95 .....	33
3.1.11	Zugriffsschutz.....	33
<b>4</b>	<b>Haustechnik .....</b>	<b>34</b>
4.1	Übergeordnete Fragen .....	34
4.1.1	Allgemeine Fragen zur Organisation .....	34
4.1.2	Datensicherung .....	36
4.1.3	Datenträger .....	36
4.1.4	Identifikation und Authentisierung.....	36
4.1.5	Peripheriegeräte.....	36
4.1.6	Protokollierung .....	36
4.1.7	Schulung .....	36
4.1.8	Software.....	36
4.1.9	Virenschutz .....	36
4.1.10	Windows 95 .....	36
4.1.11	Zugriffsschutz.....	36
<b>5</b>	<b>IT-Benutzer .....</b>	<b>37</b>
5.1	Übergeordnete Fragen .....	37
5.1.1	Allgemeine Fragen zur Organisation .....	37
5.1.2	Datensicherung .....	38
5.1.3	Datenträger .....	39
5.1.4	Identifikation und Authentisierung.....	41
5.1.5	Peripheriegeräte.....	41
5.1.6	Protokollierung .....	41
5.1.7	Schulung .....	42
5.1.8	Software.....	42
5.1.9	Virenschutz .....	43
5.1.10	Windows 95 .....	43

---

5.1.11	Zugriffsschutz.....	43
5.2	Fragen zu einem konkreten IT-System .....	44
5.2.1	Allgemeine Fragen zur Infrastruktur .....	44
5.2.2	Allgemeine Fragen zur Organisation .....	45
5.2.3	Datensicherung .....	46
5.2.4	Identifikation und Authentisierung.....	48
5.2.5	Peripheriegeräte.....	50
5.2.6	Software (optional) .....	51
5.2.7	Windows 95 .....	52
<b>6</b>	<b>IT-Sicherheitsmanagement .....</b>	<b>54</b>
6.1	Übergeordnete Fragen .....	54
6.1.1	Allgemeine Fragen zur Infrastruktur .....	54
6.1.2	Allgemeine Fragen zur Organisation .....	54
6.1.3	Datensicherung .....	54
6.1.4	Datenträger .....	54
6.1.5	Identifikation und Authentisierung.....	54
6.1.6	Peripheriegeräte.....	54
6.1.7	Protokollierung .....	54
6.1.8	Schulung .....	55
6.1.9	Software.....	56
6.1.10	Virenschutz .....	57
6.1.11	Windows 95 .....	57
6.1.12	Zugriffsschutz.....	57
<b>7</b>	<b>IT-Verfahrensverantwortlicher .....</b>	<b>58</b>
7.1	Übergeordnete Fragen .....	58
7.1.1	Allgemeine Fragen zur Infrastruktur .....	58
7.1.2	Allgemeine Fragen zur Organisation .....	58
7.1.3	Datensicherung .....	58
7.1.4	Datenträger .....	58
7.1.5	Identifikation und Authentisierung.....	58
7.1.6	Peripheriegeräte.....	58
7.1.7	Protokollierung .....	58
7.1.8	Schulung .....	59

7.1.9	Software (optional) .....	59
7.1.10	Virenschutz .....	59
7.1.11	Windows 95 .....	59
7.1.12	Zugriffsschutz.....	59
<b>8</b>	<b>Leiter IT .....</b>	<b>60</b>
8.1	Übergeordnete Fragen .....	60
8.1.1	Allgemeine Fragen zur Organisation .....	60
8.1.2	Datensicherung .....	66
8.1.3	Datenträger.....	66
8.1.4	Identifikation und Authentisierung.....	67
8.1.5	Peripheriegeräte.....	68
8.1.6	Protokollierung .....	68
8.1.7	Schulung .....	68
8.1.8	Software.....	69
8.1.9	Virenschutz .....	70
8.1.10	Windows 95 .....	70
8.1.11	Zugriffsschutz.....	70
<b>9</b>	<b>Personalabteilung .....</b>	<b>71</b>
<b>10</b>	<b>Personalrat/Betriebsrat .....</b>	<b>72</b>
<b>11</b>	<b>Revisor .....</b>	<b>73</b>
11.1	Übergeordnete Fragen .....	73
11.1.1	Allgemeine Fragen zur Organisation .....	73
11.1.2	Datensicherung .....	73
11.1.3	Datenträger.....	73
11.1.4	Identifikation und Authentisierung.....	73
11.1.5	Peripheriegeräte.....	73
11.1.6	Protokollierung .....	74
11.1.7	Schulung .....	76
11.1.8	Software.....	76
11.1.9	Virenschutz .....	76
11.1.10	Windows 95 .....	76
11.1.11	Zugriffsschutz.....	76

<b>12 Vorgesetzte .....</b>	<b>77</b>
-----------------------------	-----------



# 1 Administrator

## 1.1 Übergeordnete Fragen

### 1.1.1 Allgemeine Fragen zur Organisation

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	<b>Wartung und Reparatur</b>					
1.1	Werden Wartungs- und Reparaturarbeiten im Hause durch eine fachkundige Kraft beaufsichtigt, um die Durchführung von nichtautorisierten Handlungen durch das Wartungspersonal zu verhindern?	M 2.4				
1.2	Weist sich das Wartungspersonal auf Verlangen aus?	M 2.4				
1.3	Werden vor Wartungs- und Reparaturarbeiten alle Speichermedien ausgebaut oder gelöscht, um einen Zugriff auf Daten durch das Wartungspersonal zu vermeiden?	M 2.4				

Befragte Person:

Geprüft von:

Datum:



Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.4	Werden nach der Durchführung der Wartungs- und Reparaturarbeiten alle Paßwörter geändert?	M 2.4				
1.5	Wird nach der Durchführung der Wartungs- und Reparaturarbeiten ein Viren-Check durchgeführt?	M 2.4				

Befragte Person:

Geprüft von:

Datum:

## 1.1.2 Datensicherung

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Existiert ein Datensicherungskonzept?	M 6.32				
1.1	Ist das Zeitintervall festgelegt, wie oft die Daten gesichert werden (z.B. täglich, wöchentlich)?	M 6.32				
1.2	Ist der Zeitpunkt festgelegt, wann die Daten gesichert werden (z.B. nachts, freitags abends)?	M 6.32				
1.3	Ist die Anzahl der aufzubewahrenden Generationen der Datensicherungen festgelegt?	M 6.32				
1.4	Ist der Umfang der zu sichernden Daten festgelegt (z.B. bestimmte Partitionen oder Verzeichnisse)?	M 6.32				
1.5	Sind die eingesetzten Speichermedien festgelegt (z.B. Bänder, Disketten)?	M 6.32				
1.6	Ist die vorherige Löschung der Datenträger vor deren Wiederverwendung festgeschrieben?	M 6.32				
1.7	Ist die Zuständigkeit für die Durchführung der Datensicherungen geregelt (z.B. Administrator, IT-Benutzer)?	M 6.32				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.8	Ist die Zuständigkeit für die Überwachung der Datensicherungen, insbesondere bei automatischer Durchführung geregelt?	M 6.32				
1.9	Ist die Art der Datensicherung festgelegt evtl. in Abhängigkeit vom Zeitpunkt (z.B. Komplettsicherung, inkrementelle Sicherung)?	M 6.32				
1.10	Ist die Dokumentation der erstellten Datensicherungen gewährleistet?	M 6.32				
2	Sind die Benutzer über die Regelungen zur Datensicherung informiert?	M 6.32				
3	Werden auf allen PCs die Einträge im CMOS-RAM schriftlich dokumentiert oder mit einem entsprechenden Programm auf Diskette gespeichert?	M 6.27				

Befragte Person:

Geprüft von:

Datum:

### 1.1.3 Datenträger

### 1.1.4 Identifikation und Authentisierung

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	<b>Paßwortschutz</b>					
1.1	Wurde auf allen PCs der BIOS-Paßwortschutz aktiviert?	M 4.1				
1.1.1	Wurde der Zugriff auf die Diskettenlaufwerke durch ein BIOS-Paßwort geschützt?	M 4.1				

Befragte Person:

Geprüft von:

Datum:

### 1.1.5 Peripheriegeräte

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>CD-ROM</b>					
1.1	Wurde bei Rechnern mit Windows 95 auf der Registerkarte GERÄTEMANAGER unter der Systemsteuerungsoption SYSTEM für die CD-ROM die Eigenschaft „Automatische Benachrichtigung beim Wechsel“ deaktiviert?	M 4.57				
1.2	Falls die automatische CD-ROM Erkennung gewünscht wird, sind die Benutzer darüber informiert, wie sie dies für jede CD-ROM einzeln manuell verhindern können?	M 4.57				
<b>2</b>	<b>Diskettenlaufwerk (optional)</b>					
2.1	Ist sichergestellt, daß alle Diskettenlaufwerke der PCs mittels spezieller Einschiebvorrichtungen verschlossen sind und nur im Falle einer autorisierten Nutzung geöffnet werden?	M 4.4				
2.1.1	Existiert eine Schlüsselverwaltung?	M 4.4				
2.1.2	Sind Duplikate der Schlüssel sicher hinterlegt?	M 4.4				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
2.1.3	Ist sichergestellt, daß die Schlüssel der eingesetzten Schlösser verschieden sind?	M 4.4				
2.2	Wurde ersatzweise der Ausbau der Diskettenlaufwerke erwogen, falls ein Verschluß nicht möglich ist?	M 4.4				

### 1.1.6 Protokollierung

Befragte Person:

Geprüft von:

Datum:

## 1.1.7 Schulung

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	<b>Mehrbenutzerbetrieb für Windows 95 Rechner</b>					
1.1	Werden die entsprechenden Administratoren ausreichend geschult?	M 3.11				
1.1.1	Können alltägliche Administrationsarbeiten selbst durchgeführt werden?	M 3.11				
1.1.2	Können einfache Fehler selbst erkannt und behoben werden?	M 3.11				
1.1.3	Können Datensicherungen selbstständig durchgeführt werden?	M 3.11				
1.1.4	Können Eingriffe von externem Wartungspersonal nachvollzogen werden?	M 3.11				

Befragte Person:

Geprüft von:

Datum:

## 1.1.8 Software

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>Einschränkung der Benutzerumgebung (Windows 95)</b>					
1.1	Wird auf den betroffenen Rechnern ein angemessenes PC-Sicherheitsprodukt eingesetzt?	M 4.41				
1.1.1	Führt das Produkt eine Identifikation und Authentisierung des Administrators und der Benutzer durch?	M 4.41				
1.1.1.1	Wird das System nach drei fehlerhaften Authentisierungsversuchen gesperrt, die nur der Administrator aufheben kann?	M 4.41				
1.1.1.2	Wird das Paßwort verschlüsselt im System gespeichert, falls ein Paßwort verwendet wird?	M 4.41				
1.1.2	Stellt das Produkt eine Rechteverwaltung und -kontrolle zur Verfügung?	M 4.41				
1.1.2.1	Wird dabei zwischen lesendem und schreibendem Zugriff unterschieden?	M 4.41				
1.1.3	Unterstützt das Produkt eine Rollentrennung zwischen Administrator, Revisor und Benutzer?	M 4.41				

Befragte Person:

Geprüft von:

Datum:



Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.1.4	Können mit dem Produkt die An- und Abmeldevorgänge, auftretende Rechteverletzungen sowie durchgeführte Administrationstätigkeiten protokolliert werden?	M 4.41				
1.1.5	Ist der Systemzugriff auf Betriebssystemebene für die Benutzer gesperrt?	M 4.41				
1.1.6	Stellt das Produkt eine Bildschirmsperre zur Verfügung?	M 4.41				
1.1.7	Verfügt das Produkt über einen Boot-Schutz, der verhindert, daß der PC unbefugt von Diskette gebootet werden kann?	M 4.41				
1.1.8	Bietet das Produkt eine Verschlüsselung der Datenbestände?	M 4.41				
1.1.9	Verfügt das Produkt über eine benutzerfreundliche Oberfläche?	M 4.41				
1.1.10	Existiert eine aussagekräftige und nachvollziehbare Dokumentation für Administrator und Benutzer?	M 4.41				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.1.11	Hat das Produkt eine minimale Evaluationstiefe von <i>E2</i> und eine Mindeststärke der Mechanismen von <i>mittel</i> , falls es über ein Sicherheitszertifikat nach ITSEC verfügt?	M 4.41				
1.2	Ist eine aktuelle Übersicht über PC-Sicherheitsprodukte und deren Funktionalitäten vorhanden?	M 4.41				

Befragte Person:

Geprüft von:

Datum:

### 1.1.9 Virenschutz

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Wird bei allen PCs ein anerkannt gutes Viren-Suchprogramm eingesetzt?	M 4.3				
1.1	Werden mit dem Viren-Suchprogramm die Viren auch möglichst exakt identifiziert?	M 4.3				
1.2	Erkennt das Viren-Suchprogramm auch Makro-Viren?	M 4.44				
1.3	Wird das Viren-Suchprogramm regelmäßig aktualisiert?	M 4.3				
1.4	Wird das Viren-Suchprogramm im Hintergrund (resident) genutzt?	M 4.3				
1.5	Ist das Viren-Suchprogramm sinnvoll konfiguriert (z.B. welche Dateiarnten überprüft werden sollen)?	M 4.3				
2	Wird dem Virenbefall durch die Möglichkeit, über das BIOS-Setup die Boot-Reihenfolge zu vertauschen (erst C:, dann A:) oder das Booten von Diskette ganz zu unterbinden, vorgebeugt?	M 4.1, M 4.3				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
3	Wurde im BIOS-Setup die Virus-Warnfunktion aktiviert, um vor der Veränderung des Bootsektors vom Benutzer eine Bestätigung einzuholen?	M 4.1				
4	Wird ein Checksummen-Prüfprogramm zum Schutz vor Veränderung der Dateien eingesetzt?	M 4.3				
5	Wird das Programm <i>ghostscript</i> ( <i>gs</i> ) eingesetzt?					
5.1	Wurde überprüft, daß per Default die Schreibmöglichkeit auf Dateien abgeschaltet ist gemäß den Sicherheitsbulletins des DFN-CERT (DSB-95:02 und DSB-95:03 vom 24.08.1995)?	M 4.44				
5.2	Werden nur <i>ghostscript</i> -Versionen eingesetzt, bei denen eine Modifikation von Dateien ausgeschlossen werden kann?	M 4.44				
6	Kommen PDF-Dateien in der Behörde bzw. im Unternehmen zum Einsatz?					
6.1	Werden für das Lesen von PDF-Dateien nur Viewer eingesetzt, die eventuell eingebettete Funktionen nicht verarbeiten können, oder eine Version des Acrobat Reader bzw. des Acrobat Exchange, bei denen der Benutzer einer Ausführung explizit zustimmen muß?	M 4.44				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
7	Wurden die Verhaltensregeln bei Auftreten eines Computer Virus allen betroffenen Mitarbeitern bekanntgegeben?	M 6.23				
8	Gibt es sachkundige Personen, die beim Auftreten eines Virus die erforderlichen Schritte durchführen können?	M 6.23				
9	Trat seit der letzten Revision ein Virenbefall auf?					
9.1	Wurde der Virus beseitigt?					
9.2	Wurde die Ursache bekämpft, so daß sich der Fall nicht wiederholen kann?					

Befragte Person:

Geprüft von:

Datum:

### 1.1.10 Windows 95

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>Papierkorb</b>					
1.1	Ist die maximale Größe des Papierkorbes bei Rechnern mit Windows 95 auf einen sinnvollen Wert (z.B. 2 MB) voreingestellt?	M 4.56				
<b>2</b>	<b>Rettungsdisketten</b>					
2.1	Wurde für alle Rechner mit Windows 95 eine startfähige Systemdiskette erstellt?	M 6.46				
2.1.1	Wurde dazu die Registerkarte <i>STARTDISKETTE</i> unter der Systemsteuerungsoption <i>SOFTWARE</i> verwendet?	M 6.46				
2.1.2	Wurden stattdessen alle relevanten Dateien manuell auf Diskette kopiert, falls keine Windows 95 CD zur Verfügung steht?	M 6.46				
2.1.3	Wurde für andere notwendige Dateien (z.B. Editor, Backup-Programm) ggf. eine zusätzliche Diskette verwendet?	M 6.46				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
2.2	Wurden die erstellten Rettungsdisketten auf Computer-Viren überprüft?	M 6.46				
2.3	Wurden die erstellten Rettungsdisketten schreibgeschützt?	M 6.46				
<b>3</b>	<b>Mehrbenutzerbetrieb für Windows 95 Rechner</b>					
3.1	Wurden die Benutzerprofile unter Windows 95 für alle betroffenen Rechner aktiviert?	M 2.103				
3.1.1	Wurde dazu die Schaltfläche <i>KENNWÖRTER</i> der Programmgruppe <i>SYSTEMSTEUERUNG</i> verwendet?	M 2.103				
<b>4</b>	<b>Einschränkung der Benutzerumgebung (Windows 95)</b>					
4.1	Wurde die Benutzerumgebung durch die Verwendung von Systemrichtlinien eingeschränkt?	M 2.104				
4.1.1	Wurde der Zugriff auf die Schaltflächen <i>ANZEIGE</i> , <i>NETZWERK</i> , <i>KENNWÖRTER</i> , <i>DRUCKEREINSTELLUNGEN</i> und <i>SYSTEM</i> der Programmgruppe <i>SYSTEMSTEUERUNG</i> eingeschränkt?	M 2.104				
4.1.1.1	Wurden Vorgaben für die Bildschirmfarben gemacht?	M 2.104				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
4.1.1.2	Wurde vorgesehen, eigene Kennwörter durch den Benutzer ändern zu lassen?	M 2.104				
4.1.1.3	Wurden Vorgaben für die Druckerkonfiguration und die Hardware-Einstellungen gemacht?	M 2.104				
4.1.1.4	Wurde die Registerkarte <i>BENUTZERPROFILE</i> für die Systemsteuerungsoption <i>KENNWÖRTER</i> ausgeblendet?	M 2.104				
4.1.1.5	Wurde die Option <i>ORDNER UNTER EINSTELLUNGEN IM MENÜ „START“ ENTFERNEN</i> aktiviert, um die System- und Druckersteuerung zu deaktivieren?	M 2.104				
4.1.2	Wurden Zugriffe auf einzelne Funktionen der Benutzeroberfläche von Windows 95 eingeschränkt?	M 2.104				
4.1.2.1	Wurden die Befehle <i>AUSFÜHREN</i> , <i>SUCHEN</i> und <i>BEENDEN</i> von der Benutzeroberfläche entfernt?	M 2.9, M 2.104				
4.1.2.2	Wurden alle Laufwerke bzw. Partitionen ausgeblendet, so daß im <i>ARBEITSPLATZ</i> und im <i>EXPLORER</i> nur noch die Start-Partition (z.B. C:) zur Verfügung steht?	M 2.104				

Befragte Person:

Geprüft von:

Datum:



Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
4.1.3	Wurde der Programmstart von ausführbaren Dateien eingeschränkt?	M 2.9, M 2.104				
4.1.3.1	Wurden die für den einzelnen Benutzer erlaubten Anwendungen explizit vorgegeben (z.B. <i>WINWORD.EXE</i> , <i>EXCEL.EXE</i> und <i>EXPLORER.EXE</i> )?	M 2.9, M 2.104				
4.1.3.2	Wurde die Option <i>LAUFWERKE IM FENSTER „ARBEITSPLATZ“ AUSBLENDEN</i> aktiviert, falls die Benutzung des <i>EXPLORERS</i> nicht erlaubt sein soll?	M 2.104				
4.1.4	Wurde die Option <i>PROGRAMME ZUM BEARBEITEN DER REGISTRIERUNG DEAKTIVIEREN</i> aktiviert?	M 2.104				
4.1.5	Wurde die MS-DOS-Eingabeaufforderung deaktiviert?	M 2.104				
4.1.6	Wurde ein alphanumerisches Windows 95 Anmeldekennwort und eine Mindestlänge von sechs Zeichen eingestellt?	M 2.104				
4.2	Ist die Einschränkung der Benutzerumgebung aus betrieblicher Sicht notwendig?	M 2.104				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
4.3	Wurde für den Administrator ein eigener Benutzer eingerichtet, für den keine Einschränkungen gelten?	M 2.104				
4.4	Wurde der Systemrichtlinien-Editor ( <i>POLEDIT.EXE</i> ) abschließend von der Festplatte gelöscht?	M 2.104				

Befragte Person:

Geprüft von:

Datum:

### 1.1.11 Zugriffsschutz

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>Mehrbenutzerbetrieb für Windows 95 Rechner</b>					
1.1	Wurden für alle betroffenen Windows 95 Rechner die Zugriffsrechte eingerichtet?	M 2.63				
1.1.1	Wurden die Benutzer den einzelnen Funktionen zugeordnet, die der Windows 95 Rechner zur Verfügung stellt?	M 2.63				
1.1.2	Können die Benutzer damit den Rechner nur gemäß ihren Aufgaben nutzen?	M 2.63				
1.1.3	Wurden die Ergebnisse schriftlich dokumentiert?	M 2.63				
1.2	Werden die erforderlichen Zugriffsrechte im Vertretungsfall erst dann eingerichtet, wenn kontrolliert wurde, ob der Vertreter vom Fachverantwortlichen autorisiert ist?	M 2.63				
1.3	Wurden die sinnvoll einsetzbaren Protokollfunktionen zur Beweissicherung aktiviert (z.B. Fehlermeldungen des Systems, unerlaubte Zugriffsversuche)?	M 2.63				
1.4	Werden die eingerichteten Zugriffsrechte sporadisch überprüft?	M 2.63				

Befragte Person:

Geprüft von:

Datum:

## **2 Archivverwalter**

### **2.1 Übergeordnete Fragen**

#### **2.1.1 Allgemeine Fragen zur Organisation**

#### **2.1.2 Datensicherung**

Befragte Person:

Geprüft von:

Datum:

### 2.1.3 Datenträger

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Werden Bestandsverzeichnisse für die Datenträgerverwaltung geführt?	M 2.3				
1.1	Gibt das Bestandsverzeichnis Auskunft über den Aufbewahrungsort der Datenträger?	M 2.3				
1.2	Gibt das Bestandsverzeichnis Auskunft über die Aufbewahrungsdauer der Datenträger?	M 2.3				
1.3	Gibt das Bestandsverzeichnis Auskunft über berechnete Empfänger der Datenträger?	M 2.3				
2	Werden die Datenträger einheitlich gekennzeichnet?	M 2.3				
2.1	Wurde eine Struktur von Kennzeichnungsmerkmalen festgelegt?	M 2.3				
2.2	Ist sichergestellt, daß Unbefugte aufgrund der Kennzeichnung keinen Rückschluß auf den Inhalt der Datenträger erlangen?	M 2.3				
3	Ist eine sachgerechte Behandlung der Datenträger sichergestellt?	M 2.3				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
4	Ist eine sachgerechte Aufbewahrung der Datenträger sichergestellt?	M 2.3				
4.1	Wurden Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) getroffen?	M 2.3				
4.2	Wurden Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) getroffen?	M 2.3, M 6.20, M 6.21				
4.3	Ist im Bedarfsfall ein ausreichend schneller Zugriff auf die Datenträger gewährleistet?	M 6.20				
4.4	Werden Originaldatenträger und Sicherungskopien der eingesetzten Software getrennt voneinander aufbewahrt?	M 6.21				
5	Ist ein ordnungsgemäßer Versand oder Transport der Datenträger sichergestellt?	M 2.3				
5.1	Werden die Datenträger gemäß ihrer Schutzbedürftigkeit verpackt (z.B. Magnetbandversandtasche, luftgepolsterte Umschläge)?	M 2.3				
5.2	Sind die zulässigen Versand- und Transportarten festgelegt?	M 2.3				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
5.3	Ist ein Nachweisverfahren über den Versand und den Eingang beim Empfänger festgelegt?	M 2.3				
5.4	Werden vor Abgabe wichtiger Datenträger Sicherungskopien erstellt?	M 2.3				
6	Wurden Regelungen über die Behandlung von Datenträgern getroffen, die von Dritten stammen?	M 2.3				
7	Existiert eine geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern?	M 2.3				
7.1	Wird beim Formatieren von DOS-Datenträgern der Parameter /U verwendet?	M 2.3				
7.2	Wird beim Formatieren unter Windows 95 der Parameter <i>Vollständig</i> verwendet?	M 2.3				
8	Werden Vollständigkeitskontrollen des Datenträgerbestandes vorgenommen?	M 2.3				

Befragte Person:

Geprüft von:

Datum:

**2.1.4 Identifikation und Authentisierung**

**2.1.5 Peripheriegeräte**

**2.1.6 Protokollierung**

**2.1.7 Schulung**

**2.1.8 Software**

**2.1.9 Virenschutz**

**2.1.10 Windows 95**

**2.1.11 Zugriffsschutz**

Befragte Person:

Geprüft von:

Datum:



### 3 Beschaffungsstelle

#### 3.1 Übergeordnete Fragen

##### 3.1.1 Allgemeine Fragen zur Organisation

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	<b>Einschränkung der Benutzerumgebung (Windows 95)</b>					
1.1	Wird bei der IT-Beschaffung ein eventuell vorhandenes Sicherheitszertifikat als Auswahlkriterium berücksichtigt?	M 2.66				
1.1.1	Ist eine aktuelle Übersicht über zertifizierte Produkte vorhanden?	M 2.66				
1.1.2	Werden die relevanten Zertifizierungsreports des BSI regelmäßig angefordert?	M 2.66				

Befragte Person:

Geprüft von:

Datum:

- 3.1.2    Datensicherung**
- 3.1.3    Datenträger**
- 3.1.4    Identifikation und Authentisierung**
- 3.1.5    Peripheriegeräte**
- 3.1.6    Protokollierung**
- 3.1.7    Schulung**
- 3.1.8    Software**
- 3.1.9    Virenschutz**
- 3.1.10    Windows 95**
- 3.1.11    Zugriffsschutz**

Befragte Person:

Geprüft von:

Datum:

## 4 Haustechnik

### 4.1 Übergeordnete Fragen

#### 4.1.1 Allgemeine Fragen zur Organisation

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>Entsorgung von Betriebsmitteln</b>					
1.1	Existiert eine Anordnung, die die Art der Entsorgung schutzbedürftigen Materials regelt?	M 2.13				
1.1.1	Werden in der Anordnung alle Betriebs- oder Sachmittel behandelt, die schützenswerte Daten enthalten (z.B. Druckerpapier, Disketten, Festplatten oder spezielle Tonerkassetten)?	M 2.13				
1.1.2	Werden entsprechende Entsorgungseinrichtungen vorgehalten?	M 2.13				
1.2	Ist die Sammelstelle für zu entsorgendes, schutzbedürftiges Material vor unberechtigtem Zugriff geschützt?	M 2.13				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.3	Werden bei einer Entsorgung durch externe Unternehmen diese auf die Einhaltung erforderlicher IT-Sicherheitsmaßnahmen verpflichtet?	M 2.13				
1.4	Ist bei der Entsorgung gewährleistet, daß keine Rückschlüsse auf vorher gespeicherte Daten möglich sind?	M 2.13				
1.4.1	Werden funktionstüchtige Datenträger vor der Entsorgung physikalisch gelöscht?	M 2.13				
1.4.2	Werden nicht mehr funktionierende Datenträger vor der Entsorgung mechanisch zerstört?	M 2.13				

Befragte Person:

Geprüft von:

Datum:

**4.1.2    Datensicherung**

**4.1.3    Datenträger**

**4.1.4    Identifikation und Authentisierung**

**4.1.5    Peripheriegeräte**

**4.1.6    Protokollierung**

**4.1.7    Schulung**

**4.1.8    Software**

**4.1.9    Virenschutz**

**4.1.10   Windows 95**

**4.1.11   Zugriffsschutz**

Befragte Person:

Geprüft von:

Datum:

## 5 IT-Benutzer

### 5.1 Übergeordnete Fragen

#### 5.1.1 Allgemeine Fragen zur Organisation

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	<b>Wartung und Reparatur</b>					
1.1	Werden Wartungs- und Reparaturarbeiten im Hause durch eine fachkundige Kraft beaufsichtigt, um die Durchführung von nichtautorisierten Handlungen durch das Wartungspersonal zu verhindern?	M 2.4				
1.2	Weist sich das Wartungspersonal auf Verlangen aus?	M 2.4				
1.3	Werden vor Wartungs- und Reparaturarbeiten alle Speichermedien ausgebaut oder gelöscht, um einen Zugriff auf Daten durch das Wartungspersonal zu vermeiden?	M 2.4				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.4	Werden nach der Durchführung der Wartungs- und Reparaturarbeiten alle Paßwörter geändert?	M 2.4				
1.5	Wird nach der Durchführung der Wartungs- und Reparaturarbeiten ein Viren-Check durchgeführt?	M 2.4				

### 5.1.2 Datensicherung

Befragte Person:

Geprüft von:

Datum:

### 5.1.3 Datenträger

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Ist eine sachgerechte Behandlung der eingesetzten Datenträger sichergestellt?	M 2.3				
2	Ist eine sachgerechte Aufbewahrung der eingesetzten Datenträger sichergestellt?	M 2.3				
2.1	Wurden Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) getroffen?	M 2.3				
2.2	Wurden Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) getroffen?	M 2.3, M 6.20, M 6.21				
2.3	Ist im Bedarfsfall ein ausreichend schneller Zugriff auf die Datenträger gewährleistet?	M 6.20				
2.4	Werden die Backup-Datenträger für den Katastrophenfall räumlich getrennt vom zugehörigen Rechner aufbewahrt?	M 6.20				
2.5	Werden Originaldatenträger und Sicherungskopien der eingesetzten Software getrennt voneinander aufbewahrt?	M 6.21				

Befragte Person:

Geprüft von:

Datum:



Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
3	Ist ein ordnungsgemäßer Versand oder Transport der eingesetzten Datenträger sichergestellt?	M 2.3				
3.1	Werden die Datenträger gemäß der Schutzbedürftigkeit verpackt (z.B. Magnetbandversandtasche, luftgepolsterte Umschläge)?	M 2.3				
3.2	Wird das Nachweisverfahren über den Versand und den Eingang beim Empfänger angewendet?	M 2.3				
3.3	Ist sichergestellt, daß die Datenträger über die zu versendenden Daten hinaus keine „Restdaten“ enthalten?	M 2.3				
3.4	Werden vor Abgabe wichtiger Datenträger Sicherungskopien erstellt?	M 2.3				
4	Werden die Regelungen über die Behandlung von Datenträgern, die von Dritten stammen, beachtet?	M 2.3				
4.1	Werden die Datenträger beim Empfang auf Computer-Viren überprüft?	M 2.3				
4.2	Werden die Datenträger beim Versenden auf Computer-Viren überprüft?	M 2.3				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
5	Wird die geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern angewendet?	M 2.3				
5.1	Wird beim Formatieren von DOS-Datenträgern der Parameter <i>/U</i> verwendet?	M 2.3				
5.2	Wird beim Formatieren unter Windows 95 der Parameter <i>Vollständig</i> verwendet?	M 2.3				

#### 5.1.4 Identifikation und Authentisierung

#### 5.1.5 Peripheriegeräte

#### 5.1.6 Protokollierung

Befragte Person:

Geprüft von:

Datum:

### 5.1.7 Schulung

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Werden Mitarbeiter, die eine IT-gestützte Aufgabe neu übernehmen sollen, ausreichend geschult?	M 3.4				
2	Werden regelmäßig Schulungen zum Thema IT-Sicherheit veranstaltet?	M 3.5				

### 5.1.8 Software

Befragte Person:

Geprüft von:

Datum:

### 5.1.9 Virenschutz

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Sind die Verhaltensregeln bei Auftreten eines Computer Virus bekannt?	M 6.23				

### 5.1.10 Windows 95

### 5.1.11 Zugriffsschutz

Befragte Person:

Geprüft von:

Datum:

## 5.2 Fragen zu einem konkreten IT-System

### 5.2.1 Allgemeine Fragen zur Infrastruktur

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>Aufstellung des IT-Systems (optional)</b>					
1.1	Wird eine Überhitzung des IT-Systems durch die Aufstellung in ausreichender Entfernung zur Heizung vermieden?	M 1.29				
1.2	Ist gewährleistet, daß das IT-System keiner direkten Sonneneinstrahlung ausgesetzt ist?	M 1.29				
1.3	Wird eine direkte Lichteinstrahlung auf den Bildschirm des IT-Systems vermieden?	M 1.29				
1.4	Wird das IT-System regelmäßig von Staub oder anderen Verschmutzungen gereinigt?	M 1.29				
1.5	Ist das IT-System in ausreichender Entfernung von Fenstern oder Türen aufgestellt, um eine unbefugte Kenntnisnahme von Außerhalb zu verhindern?	M 1.29				

Befragte Person:

Geprüft von:

Datum:

## 5.2.2 Allgemeine Fragen zur Organisation

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	<b>Umgang mit PCs (optional)</b>					
1.1	Werden alle durchgeführten IT-Sicherheitsmaßnahmen und Änderungen am PC mittels eines PC-Checkheftes dokumentiert?	M 2.24				

Befragte Person:

Geprüft von:

Datum:

### 5.2.3 Datensicherung

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Wird eine regelmäßige Datensicherung durchgeführt?	M 6.32				
2	Ist das Datensicherungskonzept der Behörde bzw. des Unternehmens bekannt?	M 6.32				
2.1	Ist der Datensicherungsvorgang konform zum vorhandenen Datensicherungskonzept?	M 6.32				
2.2	Wurden ggf. Ergänzungen vorgenommen, um individuelle Anforderungen abdecken zu können?	M 6.32				
3	Wird der Datensicherungsvorgang dokumentiert?	M 6.32				
4	Werden unter MS Windows 95 nur Programme zur Datensicherung eingesetzt, die lange Dateinamen verarbeiten können (z.B. <i>BACKUP.EXE</i> )?	M 6.45				
5	Wird sporadisch überprüft, ob die gesicherten Daten wiederhergestellt werden können?	M 6.22				
6	Wurde auch von den Originaldatenträgern erworbener Software bzw. von der Originalsoftware bei Eigenentwicklungen eine Sicherungskopie erstellt?	M 6.21				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
6.1	Wird alternativ eine Sicherungskopie der installierten Software erstellt, falls die Software auf CD-ROM ausgeliefert wird?	M 6.21				
7	Werden alle Änderungen im CMOS-RAM des Rechners schriftlich dokumentiert oder mit einem entsprechenden Programm auf Diskette gespeichert?	M 6.27				

Befragte Person:

Geprüft von:

Datum:



## 5.2.4 Identifikation und Authentisierung

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>Bildschirmsperre</b>					
1.1	Ist auf den betreffenden Rechnern eine Bildschirmsperre installiert?	M 4.2				
1.2	Aktiviert sich die Bildschirmsperre bei längerer Pausenzeit automatisch?	M 4.2				
1.3	Wird die Bildschirmsperre konsequent eingesetzt?	M 4.2				
1.4	Verfügt die Bildschirmsperre über eine Paßwort-Abfrage?	M 4.2				
1.5	Funktioniert die Bildschirmsperre für alle Anwendungen, auch wenn es sich um eine Non-Windows-Anwendung handelt?	M 4.2				
<b>2</b>	<b>Paßwortschutz</b>					
2.1	Ist auf den betreffenden Rechnern ein Paßwortschutz installiert?	M 4.1				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
2.2	Wird das Paßwort für das betreffende IT-System an einer geeigneten Stelle in einem geschlossenen Umschlag hinterlegt?	M 2.22				
2.2.1	Sind die hinterlegten Paßwörter vollständig und aktuell?	M 2.22				
2.3	Wird das Paßwort regelmäßig geändert?	M 4.1				

Befragte Person:

Geprüft von:

Datum:

## 5.2.5 Peripheriegeräte

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	CD-ROM					
1.1	Sind die Benutzer darüber informiert, wie sie die automatische CD-ROM Erkennung für jede CD-ROM einzeln manuell verhindern können?	M 4.57				

Befragte Person:

Geprüft von:

Datum:

### 5.2.6 Software (optional)

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Werden die Sicherheitsfunktionen der eingesetzten Softwareprodukte regelmäßig genutzt?	M 4.30				
1.1	Wird der Paßwortschutz bei Programmaufruf genutzt?	M 4.30				
1.2	Wird der Zugriffsschutz auf einzelne Dateien mittels Paßwort genutzt?	M 4.30				
1.3	Wird die automatische Speicherung von Zwischenergebnissen genutzt?	M 4.30				
1.4	Wird die automatische Sicherung der Vorgängerdatei genutzt?	M 4.30				
1.5	Wird die Verschlüsselung von Dateien genutzt?	M 4.30				

Befragte Person:

Geprüft von:

Datum:

## 5.2.7 Windows 95

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>Papierkorb</b>					
1.1	Wird der Inhalt des Papierkorbes unter Windows 95 regelmäßig gelöscht?	M 4.56				
1.2	Ist die maximale Größe des Papierkorbes auf einen sinnvollen Wert (z.B. 2 MB) eingestellt?	M 4.56				
1.3	Werden Dateien mit sensitivem Inhalt nicht in den Papierkorb verschoben, sondern explizit gelöscht?	M 4.56				
<b>2</b>	<b>Rettungsdisketten</b>					
2.1	Wurde für den Windows 95 Rechner eine rechner- und benutzerspezifische Rettungsdiskette erstellt?	M 6.46				
2.1.1	Wurde dazu das Programm <i>EMERGENCY RECOVERY UTILITY (ERU)</i> verwendet, welches sich auf der Windows 95 CD befindet?	M 6.46				
2.2	Wird die Rettungsdiskette bei umfangreichen oder wichtigen Änderungen an der Konfiguration oder an den Benutzereinstellungen aktualisiert?	M 6.46				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
2.3	Werden die erstellten Rettungsdisketten auf Computer-Viren überprüft?	M 6.46				
2.4	Werden die erstellten Rettungsdisketten schreib-geschützt?	M 6.46		optional		

Befragte Person:

Geprüft von:

Datum:

## **6 IT-Sicherheitsmanagement**

### **6.1 Übergeordnete Fragen**

#### **6.1.1 Allgemeine Fragen zur Infrastruktur**

#### **6.1.2 Allgemeine Fragen zur Organisation**

#### **6.1.3 Datensicherung**

#### **6.1.4 Datenträger**

#### **6.1.5 Identifikation und Authentisierung**

#### **6.1.6 Peripheriegeräte**

#### **6.1.7 Protokollierung**

Befragte Person:

Geprüft von:

Datum:

### 6.1.8 Schulung

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Werden Schulungen zu IT-Sicherheitsmaßnahmen durchgeführt?	M 3.5				
1.1	Wird der Inhalt der PC-Richtlinie im Rahmen einer Schulung erläutert?	M 2.23		optional		

Befragte Person:

Geprüft von:

Datum:



### 6.1.9 Software

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Wird der vorhandene Software-Bestand regelmäßig überprüft, um feststellen zu können, ob gegen das Verbot der Nutzung nicht freigegebener Software verstoßen wurde?	M 2.10				
1.1	Existiert ein geregeltes Verfahren, welches bei einem Verstoß gegen das Verbot angewendet wird?	M 2.10				
1.2	Wurde dem IT-Sicherheitsmanagement durch die Unternehmens- bzw. Behördenleitung die Befugnis verliehen, eine solche Überprüfung durchzuführen?	M 2.10				
1.3	Werden die Ergebnisse der Überprüfung dokumentiert?	M 2.10				
<b>2</b>	<b>Einschränkung der Benutzerumgebung (Windows 95)</b>					
2.1	Wird bei der Entwicklung neuer IT-Anwendungen systematisch festgestellt, welche Sicherheitsfunktionen die Anwendung bereitstellen muß?	M 4.42		optional		

Befragte Person:

Geprüft von:

Datum:

**6.1.10 Virenschutz**

**6.1.11 Windows 95**

**6.1.12 Zugriffsschutz**

Befragte Person:

Geprüft von:

Datum:

## **7 IT-Verfahrensverantwortlicher**

### **7.1 Übergeordnete Fragen**

#### **7.1.1 Allgemeine Fragen zur Infrastruktur**

#### **7.1.2 Allgemeine Fragen zur Organisation**

#### **7.1.3 Datensicherung**

#### **7.1.4 Datenträger**

#### **7.1.5 Identifikation und Authentisierung**

#### **7.1.6 Peripheriegeräte**

#### **7.1.7 Protokollierung**

Befragte Person:

Geprüft von:

Datum:

### 7.1.8 Schulung

### 7.1.9 Software (optional)

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Werden die Benutzer auf die Sicherheitsfunktionen der eingesetzten Softwareprodukte hingewiesen?	M 4.30				
1.1	Werden dabei die sicherheitsrelevanten Hinweise in Handbüchern oder Zertifizierungsreports beachtet?	M 4.30				

### 7.1.10 Virenschutz

### 7.1.11 Windows 95

### 7.1.12 Zugriffsschutz

Befragte Person:

Geprüft von:

Datum:

## 8 Leiter IT

### 8.1 Übergeordnete Fragen

#### 8.1.1 Allgemeine Fragen zur Organisation

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	<b>Wartung und Reparatur</b>					
1.1	Werden Wartungs- und Reparaturarbeiten den betroffenen Mitarbeitern angekündigt?	M 2.4				
1.2	Wurden Regelungen über die Beaufsichtigung des Wartungspersonals getroffen?	M 2.4				
1.3	Werden die Mitarbeiter zur Wahrnehmung der Aufsicht angehalten?	M 2.4				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.4	Ist sichergestellt, daß die dem Wartungspersonal eingeräumten Zutritts-, Zugangs- und Zugriffsrechte auf ein Minimum beschränkt sind und nach den Arbeiten widerrufen bzw. gelöscht werden?	M 2.4				
1.5	Ist eine Regelung zum Ausbau oder zur Löschung von Speichermedien vor Durchführung der Wartungs- und Reparaturarbeiten getroffen, um einen Zugriff auf Daten durch das Wartungspersonal zu vermeiden?	M 2.4				
1.5.1	Werden die Wartungs- und Reparaturarbeiten auch extern beobachtet bzw. sind besondere vertragliche Vereinbarungen über die Geheimhaltung von Daten getroffen, falls ein Löschen der Speichermedien nicht möglich ist?	M 2.4				
1.6	Ist ein ordnungsgemäßer Versand oder Transport der extern zu reparierenden IT-Komponenten sichergestellt?	M 2.4				
1.6.1	Werden die IT-Systeme gemäß ihrer Schutzbedürftigkeit transportiert (z.B. verschlossene Behältnisse, Kurier)?	M 2.4				
1.6.2	Ist ein Nachweisverfahren über den Versand und den Eingang beim Empfänger festgelegt?	M 2.4				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.7	Wird überprüft, ob der Wartungsauftrag ausgeführt wurde?	M 2.4				
1.8	Wird die Vollständigkeit der IT-Systeme oder Komponenten nach der Rückgabe überprüft?	M 2.4				
1.9	Werden die Mitarbeiter verpflichtet, nach Durchführung der Wartungs- und Reparaturarbeiten alle Paßwörter zu ändern und einen Viren-Check durchzuführen?	M 2.4				
1.10	Werden die durchgeführten Wartungsarbeiten dokumentiert?	M 2.4				
1.10.1	Werden zu diesem Zweck die zu reparierenden IT-Systeme oder Komponenten einheitlich gekennzeichnet?	M 2.4				
1.10.2	Wird der Zeitpunkt überwacht, wann eine externe Reparatur voraussichtlich abgeschlossen sein sollte?	M 2.4				
<b>2</b>	<b>Umgang mit PCs (optional)</b>					
2.1	Existiert eine PC-Richtlinie?	M 2.23				
2.1.1	Werden die IT-Sicherheitsziele erläutert und die für das gemeinsame Verständnis notwendigen Begriffe definiert?	M 2.23				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
2.1.2	Wird innerhalb der PC-Richtlinie verbindlich festgelegt, für welche Teile des Unternehmens bzw. der Behörde die PC-Richtlinie gilt?	M 2.23				
2.1.3	Werden alle Rechtsvorschriften wie z.B. das Bundesdatenschutzgesetz und das Urheberrechtsgesetz aufgeführt, die von den Mitarbeitern einzuhalten sind?	M 2.23				
2.1.4	Werden alle relevanten betriebsinternen Regelungen aufgelistet?	M 2.23				
2.1.5	Wird innerhalb der PC-Richtlinie definiert, welcher Funktionsträger im Zusammenhang mit dem PC-Einsatz welche Verantwortung trägt?	M 2.23				
2.1.6	Sind alle IT-Sicherheitsmaßnahmen enthalten, die von einem IT-Benutzer einzuhalten bzw. umzusetzen sind?	M 2.23				
2.2	Werden die Inhalte der PC-Richtlinie regelmäßig aktualisiert?	M 2.23				
2.3	Erhalten alle Mitarbeiter ein Exemplar der jeweils aktuellen PC-Richtlinie ausgehändigt?	M 2.23				

Befragte Person:

Geprüft von:

Datum:



Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
2.4	Wird ein PC-Checkheft eingesetzt?	M 2.24				
2.4.1	Wird der Name des PC-Benutzers dokumentiert?	M 2.24				
2.4.2	Wird der Aufstellungsort des PC dargestellt?	M 2.24				
2.4.3	Wird die Konfiguration des PC beschrieben?	M 2.24				
2.4.4	Werden die Zugangsmittel aufgelistet?	M 2.24				
2.4.5	Wird die eingesetzte Hard- und Software dokumentiert?	M 2.24				
2.4.6	Werden die planmäßigen Zeitpunkte für die Datensicherungen eingetragen?	M 2.24				
2.4.7	Werden alle durchgeführten Wartungen und Reparaturen dokumentiert?	M 2.24				
2.4.8	Werden alle durchgeführten Computer-Viren-Kontrollen vermerkt?	M 2.24				
2.4.9	Wird der Zeitpunkt von Paßwort-Änderungen festgelegt?	M 2.24				
2.4.10	Wird das zur Verfügung stehende Zubehör beschrieben?	M 2.24				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
2.4.11	Werden alle durchgeführten Revisionen vermerkt?	M 2.24				
2.4.12	Werden die Ansprechpartner für Problemfälle benannt?	M 2.24				
2.4.13	Werden die Zeitpunkte der durchgeführten Datensicherungen dokumentiert?	M 2.24				
<b>3</b>	<b>Mehrbenutzerbetrieb für Windows 95 Rechner</b>					
3.1	Wurde für die Windows 95 Rechner ein Administrator bestimmt, der insbesondere die Benutzerverwaltung einschließlich der Verwaltung der Zugriffsrechte durchführt?	M 2.26				
3.2	Wurde ein Vertreter benannt, um beim Ausfall des Administrators die Funktionen weiter aufrechterhalten zu können?	M 2.26				
3.3	Ist das hierfür eingesetzte Personal vertrauenswürdig?	M 3.10				
3.4	Werden Administrator und Vertreter regelmäßig darüber belehrt, daß sie ihre Befugnisse nur für die erforderlichen Administrationsaufgaben verwenden dürfen?	M 3.10				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
3.5	Wurden der Administrator und der Vertreter ausreichend geschult?	M 2.26				
3.6	Stehen dem Administrator und dem Vertreter für eine sorgfältige Aufgabenerfüllung die hierfür erforderliche Zeit zur Verfügung?	M 2.26				

### 8.1.2 Datensicherung

### 8.1.3 Datenträger

Befragte Person:

Geprüft von:

Datum:

## 8.1.4 Identifikation und Authentisierung

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>Paßwortschutz</b>					
1.1	Existiert eine geeignete Stelle, an der alle Paßwörter für einzelne IT-Systeme in einem geschlossenen Umschlag hinterlegt sind?	M 2.22				
1.1.1	Ist die ordnungsgemäße Verwendung eines hinterlegten Paßwortes geregelt?	M 2.22				
1.1.2	Wird das hinterlegte Paßwort nur nach dem Vier-Augen-Prinzip genutzt?	M 2.22				
1.1.3	Werden auch die Paßwörter der Telearbeiter hinterlegt?	M 2.22				
<b>2</b>	<b>Mehrbenutzerbetrieb für Windows 95 Rechner</b>					
2.1	Werden alle Mitarbeiter verpflichtet, sich nach Aufgabenerfüllung an ihrem PC abzumelden?	M 3.18				
2.1.1	Wird an die Verpflichtung zum Abmelden regelmäßig erinnert?	M 3.18				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
2.1.2	Wird alternativ bei einer kurzen Unterbrechung der Arbeit die manuelle Aktivierung der Bildschirmsperre empfohlen?	M 3.18				

### 8.1.5 Peripheriegeräte

### 8.1.6 Protokollierung

### 8.1.7 Schulung

Befragte Person:

Geprüft von:

Datum:

## 8.1.8 Software

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1	Gibt es ein Genehmigungs- und Registrierverfahren für Software?	M 2.9				
2	Ist das Nutzungsverbot nicht freigegebener Software schriftlich fixiert?	M 2.9				
2.1	Sind alle Mitarbeiter über das Nutzungsverbot unterrichtet?	M 2.9				
2.2	Wird in regelmäßigen Abständen an das Nutzungsverbot erinnert?	M 2.9				
2.3	Existieren Listen mit den freigegebenen Versionen ausführbarer Dateien je IT-System, die insbesondere Erstellungsdatum und Dateigröße beinhalten (Software-Bestandsverzeichnis)?	M 2.9				
2.4	Wird regelmäßig überprüft, ob die freigegebenen Versionen ausführbarer Dateien verändert wurden?	M 2.9				
3	Gibt es Regelungen über die Programmierung und die Weitergabe von Makros aus leistungsfähigen Standardprodukten wie z.B. Textverarbeitung, Tabellenkalkulation und Datenbanken?	M 2.9				

Befragte Person:

Geprüft von:

Datum:

**8.1.9 Virenschutz**

**8.1.10 Windows 95**

**8.1.11 Zugriffsschutz**

Befragte Person:

Geprüft von:

Datum:

## **9      Personalabteilung**

Befragte Person:

Geprüft von:

Datum:



## 10      **Personalrat/Betriebsrat**

Befragte Person:

Geprüft von:

Datum:

## **11 Revisor**

### **11.1 Übergeordnete Fragen**

#### **11.1.1 Allgemeine Fragen zur Organisation**

#### **11.1.2 Datensicherung**

#### **11.1.3 Datenträger**

#### **11.1.4 Identifikation und Authentisierung**

#### **11.1.5 Peripheriegeräte**

Befragte Person:

Geprüft von:

Datum:

## 11.1.6 Protokollierung

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
<b>1</b>	<b>Einschränkung der Benutzerumgebung (Windows 95)</b>					
1.1	Werden die protokollierten Daten sicherheits-relevanter Ereignisse des Windows 95 Rechners regelmäßig kontrolliert?	M 2.64				
1.1.1	Wird kontrolliert, ob die An- und Abmeldezeiten außerhalb der Arbeitszeit liegen?	M 2.64				
1.1.2	Wird die Anzahl der fehlerhaften Anmeldeversuche überprüft?	M 2.64				
1.1.3	Wird die Anzahl der unzulässigen Zugriffsversuche überprüft?	M 2.64				
1.1.4	Wird bei auffällig großen Zeitintervallen, in denen keine Protokolldaten aufgezeichnet wurden, nach gelöschten Protokolldatensätzen gesucht?	M 2.64				
1.1.5	Wird bei auffällig großen Zeitintervallen, in denen kein Benutzer-Wechsel stattgefunden hat, das Abmelden nach Aufgabenerfüllung kontrolliert?	M 2.64, M 2.65				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.2	Wird ein Werkzeug zur Auswertung benutzt?	M 2.64				
1.2.1	Können die Auswertungskriterien ausgewählt werden?	M 2.64				
1.2.2	Werden besonders kritische Einträge (z.B. mehrfacher fehlerhafter Anmeldeversuch) hervorgehoben?	M 2.64				
1.3	Wird das IT-Sicherheitsmanagement bei Auffälligkeiten unterrichtet?	M 2.64				
1.4	Ist sichergestellt, daß die Protokolldaten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden?	M 2.64				
1.5	Werden die Protokolldaten nach erfolgter Kontrolle regelmäßig gelöscht?	M 2.64				
1.6	Wird das Abmelden nach Aufgabenerfüllung in angemessenen Zeitabständen auch durch Stichproben überprüft?	M 2.65				
1.6.1	Werden die Benutzer bei festgestellten Verstößen auf die Verpflichtung zum Abmelden nach Aufgabenerfüllung hingewiesen?	M 2.65				

Befragte Person:

Geprüft von:

Datum:

Nr.	Frage	Maßnahme	Relevant ?	Begründung / Kommentar	Ja	Nein
1.6.2	Wird ihnen auch der Sinn dieser Maßnahme erläutert?	M 2.65				

### **11.1.7 Schulung**

### **11.1.8 Software**

### **11.1.9 Virenschutz**

### **11.1.10 Windows 95**

### **11.1.11 Zugriffsschutz**

Befragte Person:

Geprüft von:

Datum:

## 12 Vorgesetzte

Befragte Person:

Geprüft von:

Datum: