# CGM Clinical Systeminformationen Edition 2016-1

Versionsinformationen
Systeminformationen IT D&S
Systeminformationen Produkte
Produktspez. Anforderungen
Drucken Terminalserver IT D&S
Fernwartungskonzept
Betreiberverantwortung
Grundlagen Datensicherung
Empfehlung Datensicherung

2016-1

Synchronizing Healthcare



CompuGroup Medical

## INHALT

# CGM Clinical Systeminformationen Edition 2016-1

Editionsinformationen

# Editionsinformationen

## Aktuelle Edition

| Produkte | CGM Clinical Edition 2016-1 | |
|---|---|---|
| | Version | Hinweise |
| CGM RECHNUNGSWESEN | 5.3 | |
| CGM REHA | 5.17 | |
| CGM SOZIAL TOPSOZ | 9.1 | |
| CGM SOZIAL DP | 10.1 | |
| CGM SOZIAL PEP | 2.11 | |
| CGM SOZIAL P&D | 4.2 | |
| CGM SOZIAL BA | 5.3 | |
| CGM SOZIAL SIC | 2.18 | |
| CGM SOZIAL OPAS | 3.7 | |
| CGM SOZIAL MOBILE | 1.1 | |
| CGM DMS FAME | 5.3 | |
| CGM DMS RECHNUNGSEINGANG | 1.4 | |
| Partnerprodukte | | |
| mps All for public | 5.3 | |
| P&I Loga | 9.0 | |
| WIN-EV | 1.1.057 WinEV Tarif/SVK | |
| FACTIS | 2013-12 (1.8) | |
| DAKOTA | 6.3 Build 1 | PKCS#7-Zertifikate |
| ID Diacos | 7.3.43 | Quartalsupdate 3/2016 – SP1 |
| 3M Kodip II | 5.5.6 | Patch Juli |
| 3M Kodip DRG Scout | 9.8.0 | |
| 3M Kodip DRG Proof | 3.6 | |
| 3M 360 Encompass (ehemals KODIP Suite) | 1.6.3 | |
| ifap praxisCENTER | Quartal 4/16 (3.20.0.963) | Datenbestand 15.10.2016 |
| i:fox | Quartal 4/16 (3.21.0.959) | |

## Versionsvoraussetzung für aktuellen Releasewechsel

| Produkte | | |
|---|---|---|
| CGM RECHNUNGSWESEN | 5.0 (Edition 2013-1) | |
| CGM REHA | 5.5 (Edition 2014-1) | |
| CGM SOZIAL TOPSOZ | 8.6 (Edition 2012-1) | |
| CGM SOZIAL DP | 8.4 (Edition 2006-3) | |
| CGM SOZIAL PEP | 1.0 (Edition 2011-1) | |
| CGM SOZIAL P&D | 4.0 (Edition 2015-1) | Version 4.0 muss vor Version 4.2 installiert werden. |
| CGM SOZIAL BA | 5.0.2.1 (Edition 2013-1) | |
| CGM SOZIAL SIC | 2.8 (Edition 2011-1) | |
| CGM OPAS SOZIAL | 3.3 | |
| CGM DMS FAME | 4.8 (Edition 2012-1) | |
| CGM DMS SMARTWAY | 1.0 | |
| Partnerprodukte | | |
| mps All for public | 5.0 | |
| P&I Loga | 3.x | |
| FACTIS | 2013-12 (1.8) | |
| DAKOTA | 6.3 Build 1 | |

## Nicht mehr unterstützte Versionen

| Produkte | | |
|---|---|---|
| CGM RECHNUNGSWESEN | 5.1 (Edition 2014-1) | Auch alle älteren Vorgängerversionen |
| CGM REHA | 5.9 (Edition 2014-1) | Auch alle älteren Vorgängerversionen |
| CGM SOZIAL TOPSOZ | 8.8 (Edition 2014-1) | Auch alle älteren Vorgängerversionen |
| CGM SOZIAL DP | 9.8 (Edition 2014-1) | Auch alle älteren Vorgängerversionen |
| CGM SOZIAL PEP | 2.9 (Edition 2014-1) | Auch alle älteren Vorgängerversionen |
| CGM SOZIAL P&D | 4.0 (Edition 2015-1) | Auch alle älteren Vorgängerversionen |
| CGM SOZIAL BA | 5.1 (Edition 2014-1) | Auch alle älteren Vorgängerversionen |
| CGM SOZIAL SIC | 2.11 (Edition 2014-1) | Auch alle älteren Vorgängerversionen |
| CGM OPAS SOZIAL | 3.5 | |
| CGM DMS FAME | 4.10 (Edition 2014-1) | Auch alle älteren Vorgängerversionen |
| CGM DMS SMARTWAY | 1.2 (Edition 2014-1) | Auch alle älteren Vorgängerversionen |
| Partnerprodukte | | |
| mps All for public | 5.1 | Auch alle älteren Vorgängerversionen |
| FACTIS | < 1.8 (2013-12) | Auch alle älteren Vorgängerversionen |
| DAKOTA | 6.0 Build 18 ab 01.03.2016<br>4.1.0.6 bis 5.2 ab 01.01.2015 | Auch alle älteren Vorgängerversionen |

# Systemumgebung

## Hardwarevoraussetzungen 32/64 Bit

### Client

| Detail | Mindestvoraussetzung | Empfohlen |
|---|---|---|
| Prozessortyp | PC Intel® Pentium® AMD Athlon ™ oder vergleichbarem Prozessor | PC mit Intel® Core ™ i5 AMD Athlon ™ oder vergleichbarem Prozessor |
| Taktfrequenz | 2 GHz | > 2 GHz |
| Hauptspeicher | mind.2 GB | 4-8 GB |
| Netzwerkanbindung | 100Mbit/s | 1Gbit/s oder 10Gbit/s |
| Bildschirmauflösung | 1024x768 | > 1280x1024 |

### Anwendungsserver

| Detail | Mindestvoraussetzung | Empfohlen [1] |
|---|---|---|
| Prozessortyp | PC Intel® Pentium® AMD Athlon ™ | Server Intel Xeon AMD Athlon ™ |
| Taktfrequenz | 1,4 GHz | 2.8 GHz (100 - 150 User) |
| Hauptspeicher | 1 GB | > 2 GB |
| Netzwerkanbindung | 100Mbit/s | 1Gbit/s oder 10Gbit/s |

### Datenbank-Sizing

| Bezeichnung | User-Anzahl |
|---|---|
| klein | Bis zu 20 User |
| mittel | Bis zu 80 User |
| groß | Bis zu 200 User |

**Die Sizingangaben für den/die jeweiligen Datenbank-Server beziehen sich auf typische Installationsgrößen. Konkrete Empfehlungen zum Sizing werden durch ein Feinkonzept erstellt**.

[1] Hardwareanforderung ist abhängig von der Anzahl der Clients sowie vom Datenvolumen.

*Datenbank-Server (klein) (1- 20 User)*

| Detail | Mindestvoraussetzung | Empfohlen [1] |
|---|---|---|
| Prozessortyp | PC Intel® Pentium®<br>AMD Athlon ™ | PC Intel® Pentium® Xeon Quad Core<br>AMD Athlon ™ |
| Taktfrequenz | 1,4 GHz | 2.0 GHz |
| Hauptspeicher<br>mit BI-Datenbank | 4 GB<br>6 GB | 6 GB<br>12 GB |
| Netzwerkanbindung | 100Mbit | 1Gbit/s oder 10Gbit/s |

*Datenbank-Server (mittel) (ab 20 User)*

| Detail | Mindestvoraussetzung | Empfohlen [1] |
|---|---|---|
| Prozessortyp<br><br>mit BI-Datenbank | PC Intel® Pentium®<br>AMD Athlon ™ | PC Intel® Pentium® Xeon Quad Core<br>AMD Athlon ™<br>Dual Core |
| Taktfrequenz | 1,4 GHz | 2 x 2.0 GHz |
| Hauptspeicher | 8 GB | > 12 GB |
| Netzwerkanbindung | 1 Gbit/s | 1Gbit/s oder 10Gbit/s |
| Raid-Controller | | Raid 1 73 GB SAS (BS + Swap + Logs)<br>Raid 10 6 x 73 o. 4 x 146 GB SAS (Data) |

*Datenbank-Server (groß) (ab 80 User)*

| Detail | Mindestvoraussetzung | Empfohlen |
|---|---|---|
| Prozessortyp<br><br>mit BI-Datenbank | PC Intel® Pentium®<br>AMD Athlon ™<br>Dual Core | PC Intel® Pentium®<br>AMD Athlon ™<br>Quad/Six/Eight Core |
| Taktfrequenz | 2,0 GHz | 2x aktuelle CPU - Systeme |
| Hauptspeicher | 12 GB | > 24 GB |
| Netzwerkanbindung | 1 Gbit/s | 1Gbit/s oder 10Gbit/s |
| Raid-Controller | | Raid 1 73 GB SAS (BS + Swap)<br>Raid 1 146 GB SAS (Logs)<br>Raid 10 10 x 73 o. 10 x 146 GB SAS (Data) |

### Web-Server

| Detail | Mindestvoraussetzung | Empfohlen [1] |
|---|---|---|
| Prozessortyp | PC Intel® Pentium®<br>AMD Athlon ™ | PC Intel® Pentium®<br>AMD Athlon ™ |
| Taktfrequenz | 1,4 GHz | 2.8 GHz |
| Hauptspeicher | 2 GB | > 4 GB |
| Netzwerkanbindung | 100Mbit/s | 1Gbit/s oder 10Gbit/s |

### Drucker in Client/Server -Umgebung

| | |
|---|---|
| Sonstige | Auf Anfrage (alle gängigen PCL treiberunterstütze Druckertypen) |

## Übersicht der Betriebssystem- und Softwareanforderungen

In der folgenden Tabelle sind die Anforderungen als Übersicht zusammengefasst. Weitere Details müssen dem nachfolgenden Dokument entnommen werden.

| | Produkt | CGM REHA | | | | | CGM RECHNUNGSWESEN | | | | CGM DMS | | | | | CGM SOZIAL | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Komponente | Anwendungsserver | XREHA-Sever | DB-Server | Terminalserver | Client | Anwendungsserver | DB-Server | Terminalserver | Client | Anwendungsserver | Rechnungseingang-AppLink | DB-Server | Terminalserver | Client | Anwendungsserver | DB-Server | Terminalserver | Client |
| Betriebssysteme | Windows 7 Prof. | | X[4] | | | X | | | | X[6] | | | | | X | | | | X[6] |
| | Windows 8.1 | | X[4] | | | X | | | | X[6] | | | | | X | | | | X[6] |
| | Windows 10 | | | | | X | | | | X[6] | | | | | X | | | | X[6] |
| | Windows Server 2008 R2 (SP1) [3] | X | X[4] | X | X | | X[6] | X | X[6] | | X | X[5] | X | X | | X[6] | X | X[6] | |
| | Windows Server 2012 [3] | X | X[4] | X | X | | X[6] | X | X[6] | | X | X[5] | X | X | | X[6] | X | X[6] | |
| | Windows Server 2012 R2 [3] | X | X[4] | X | X | | X[6] | X | X[6] | | X | X[5] | X | X | | X[6] | X | X[6] | |
| | Windows Server 2016 [3] | X | | X | X | | X[6] | X | X[6] | | X | X[5] | X | X | | X[6] | X | X[6] | |
| Citrix | CITRIX XenApp 6.5 (Win Srv 2008 R2) | | | | X | | | | X | | | | | X | | | | X | |
| | CITRIX XenApp 7.6 | | | | X | | | | X | | | | | X | | | | X | |
| Datenbanken | SQL Server 2008 Standard 32/64 Bit SP3 | | | X[1] | | | | X[8] | | | | | X | | | | X | | |
| | SQL Server 2008 Enterprise 32/64 Bit SP3 | | | X[1] | | | | X[8] | | | | | X | | | | X | | |
| | SQL Server 2008 R2 Standard 32/64 Bit SP2 | | | X[1] | | | | X | | | | | X | | | | X | | |
| | SQL Server 2008 R2 Enterprise 32/64 Bit SP2 | | | X[1] | | | | X | | | | | X | | | | X | | |
| | SQL Server 2012 Standard 32/64 Bit SP2 | | | X | | | | X | | | | | X | | | | X | | |
| | SQL Server 2012 Enterprise 32/64 Bit SP2 | | | X | | | | X | | | | | X | | | | X | | |
| | SQL Server 2012 Business Intelligence 32/64 Bit | | | X | | | | X | | | | | X | | | | X | | |
| | SQL Server 2014 Standard 32/64 Bit | | | X | | | | X | | | | | X | | | | X | | |
| | SQL Server 2014 Business Intelligence 32/64 Bit | | | X | | | | X | | | | | X | | | | X | | |
| | SQL Server 2014 Enterprise 32/64 Bit | | | X | | | | X | | | | | X | | | | X | | |
| | SQL Server 2016 Standard | | | | | | | | | | | | | | | | X | | |
| | SQL Server 2016 Enterprise | | | | | | | | | | | | | | | | X | | |
| | Oracle 11g (11.1.0.7 und 11.2.0.2) | | | X | | | | X | | | | | X | | | | X[7] | | |
| | Oracle 12c (12.1.0.1) | | | X | | | | X | | | | | X | | | | X[7] | | |
| | SQL-Client passend zum DBMS | | | | X | X | | | X | X | | | | X | X | | | X | X |
| Office | Office 2010 32 Bit (Word / Excel) | | | | X | X | | | X | X | | | | X | X | | | X | X |
| | Office 2013 32 Bit (Word / Excel) | | | | X | X | | | X | X | | | | X | X | | | X | X |
| | Office 365 | | | | | | | | | | | | | | | | | | |
| Browser | Microsoft Internet Explorer 9.0 | | | | | X[1] | | | | X | | | | | X | | | | X |
| | Microsoft Internet Explorer 10.0 | | | | | X[1] | | | | X | | | | | X | | | | X |
| | Microsoft Internet Explorer 11.0 | | | | | X | | | | X | | | | | X | | | | X |
| | Mirth Connect 3.3.1 | X[2] | X[2] | | | | | | | | | | | | | | | | |

1) Für den Einsatz der CGM REHA G3-Module werden diese Versionen nicht unterstützt.
2) Für den Betrieb des Mirth Connect ist eine zusätzliche Datenbank erforderlich. Um die bestehende Datenbank bzgl. der Priorität performancekritischer Aktionen nicht zu beeinflussen, wird die Anlage in einer separaten Datenbankinstanz empfohlen.
3) Die Nutzung von RemoteApps wird nicht unterstützt.
4) Microsoft Internet Information Services (IIS) Version 7.5 oder 8 wird benötigt mit den Features „URL Rewrite“, „Application Request Routing”, „Ablaufverfolgungsregeln für Anforderungsfehler“ und „Serverzertifikate“
5) Microsoft .NET Framework 4.0 FULL wird benötigt.
6) Für den Offline-Schnittstellen-Converter wird Java JRE benötigt.
Bei einem x64 Betriebssystem wird Java x64 SE 7 und Java x86 SE 7 benötigt.
7) Für CGM SOZIAL P&D und CGM OPAS SOZIAL keine Freigabe für Oracle-Systeme
8) DS BI erfordert mindesten die SQL Server 2008 R2 Version.

## Hinweis zur Unterstützung von Microsoft-Produkten

Für jedes seiner Produkte definiert Microsoft einen aktiven Lebenszyklus. Dieser besteht bei den Softwareprodukten aus einem bestimmten Zeitraum und unterteilt sich in den Mainstream-Support und dem sich daran anschließenden Extended-Support. Während des Mainstream-Supports gewährt Microsoft einen umfassenden Support. In der Produktlebenszyklusphase „Extended-Support“ ist dieser erheblich eingeschränkt. Details dazu siehe https://support.microsoft.com/de-de/lifecycle.

Für den Betrieb der eigenen Produkte werden bestimmte Versionen der Microsoftprodukte mit möglichst optimalem Support vorausgesetzt. Aufgrund der Häufigkeit des Erscheinens neuer Microsoft-Versionen ist es nicht möglich, alle Versionen bis zum Ende des definierten Lebenszyklus zu unterstützen. Microsoft-Produkte werden bis zum Ende des Mainstream-Supportes unterstützt, aber nicht zwingend bis zum Ende des Extended-Supportes. Sind mehr als zwei Versionen eines Microsoft-Produktes verfügbar, so werden die Microsoft-Produkte ohne Mainstream-Support nicht mehr unterstützt.

## Betriebssysteme

**Die folgenden Freigaben und Empfehlungen beziehen sich ausschließlich auf CGM Clinical Produkte!**
**Freigaben, Empfehlungen und Systemvoraussetzungen anderer Hersteller, deren Produkte ebenfalls auf dem Server installiert sind und die ggf. mit den CGM Clinical Produkten interagieren (z.B. Com4Cure, DIACOS, KODIP, WINEV, etc.) müssen ebenfalls beachtet werden.**

### Client

| | |
|---|---|
| Freigegebene Betriebssysteme | Microsoft® Windows 7 (ab Edition Professional)<br>Microsoft® Windows 8.1<br>Microsoft® Windows 10 |

**Bitte beachten Sie, dass Oracle von Herstellerseite erst ab der Version 11gR2 (11.2.0.x) für Microsoft® Windows 7 freigegeben wird.**

### Anwendungsserver

| | |
|---|---|
| Freigegebene Betriebssysteme | Microsoft® Windows Server 2008 R2® SP1<br>Microsoft® Windows Server 2012® 64 Bit<br>Microsoft® Windows Server 2012 R2® 64 Bit<br>Microsoft® Windows Server 2016 |

### Datenbank-Server

| | |
|---|---|
| Freigegebene Betriebssysteme | Microsoft® Windows Server 2008 R2® SP1<br>Microsoft® Windows Server 2012® 64 Bit<br>Microsoft® Windows Server 2012 R2 ® 64 Bit |

### Terminal-Server

| | |
|---|---|
| Freigegebene Betriebssysteme | Microsoft® Windows Server 2008 R2® SP1<br>Microsoft® Windows Server 2012® 64 Bit<br>Microsoft® Windows Server 2012 R2 ® 64 Bit<br>Microsoft® Windows Server 2016 |
| Einschränkung | Die Nutzung von RemoteApps wird nicht unterstützt. |
| Freigegebene Versionen | CITRIX® XenApp 6.5 (Windows Server 2008 R2)<br>CITRIX® XenApp 7.6 |

## Datenbankmanagement

| | |
|---|---|
| Freigegebene Versionen | Microsoft® SQL-Server 2008 Standard 32/64 Bit SP3<br>Microsoft® SQL-Server 2008 Enterprise 32/64 Bit SP3<br>Microsoft® SQL-Server 2008 Standard R2 32/64 Bit SP2<br>Microsoft® SQL-Server 2008 Enterprise R2 32/64 Bit SP2<br>Microsoft® SQL-Server 2012 Standard 32/64 Bit SP2*<br>Microsoft® SQL-Server 2012 Business Intelligence 32/64 Bit SP2*<br>Microsoft® SQL-Server 2012 Enterprise 32/64 Bit SP2*<br>Microsoft® SQL-Server 2014 Standard 32/64 Bit SP1<br>Microsoft® SQL-Server 2014 Business Intelligence 32/64 Bit SP1<br>Microsoft® SQL-Server 2014 Enterprise 32/64 Bit SP1<br>Oracle 11g (11.1.0.7 und 11.2.0.2)<br>Oracle 12c (12.1.0.1) |
| Zusatzinformation CGM SOZIAL | Die CGM SOZIAL Produkte sind zusätzlich für Microsoft® SQL-Server 2016 Standard und Enterprise freigegeben. |
| Zusatzinformationen für Oracle | **ACHTUNG: Neuer Zeichensatz WE8MSWIN1252, Konvertierung der Datenbanken erforderlich. Bei systema.SIC muss der Oracle ODBC-Treiber 11.1.0.6 verwendet werden.** |
| Einschränkungen CGM SOZIAL PEP CGM DMS Rechnungseingang | Voraussetzung für den Zugriff auf Oracle-Datenbanken ist die Installation des **Oracle Data Provider für .NET 4.0 (ODP.NET)** in der entsprechenden Version |
| Einschränkung CGM SOZIAL P&D und CGM OPAS SOZIAL | CGM SOZIAL P&D und CGM OPAS SOZIAL sind nicht für Oracle freigegeben. |
| Einschränkungen CGM REWE | Voraussetzung für den Betrieb von DS BI ist mindesten die Version SQL-Server 2008 R2 |
| Einschränkungen CGM REHA | Für den Einsatz der CGM REHA G3-Module sind die Versionen Microsoft® SQL-Server 2012 und Microsoft® SQL-Server 2014 erforderlich. |

*Bitte beim SQL Server 2012 den CU7 (KB KB3065718 Cumulative Update package 7 for SQL Server 2012 Service Pack 2) installieren.

### Client

| | |
|---|---|
| Freigegebene Versionen | Microsoft SQL Client<br><br>Oracle 11g (11.1.0.7 und 11.2.0.2)<br>Oracle 12c (12.1.0.1)<br>Die Oracle Client-Versionen müssen der eingesetzten Serverdatenbankversion entsprechen. |

Oracle wird clientseitig (Client & Terminalserver) in x64-Umgebung eingeschränkt unterstützt. Ab Oracle Version 11g kann ein 32-Bit-Treiber in x64-Umgebungen installiert werden.

## Softwarevoraussetzungen für Microsoft Office und weitere Systemkomponenten

Folgende Voraussetzungen betreffen nur Produkte, die Microsoft Office, den Internet Explorer bzw. Java verwenden.

### Microsoft Office

| Freigegebene Versionen |
|---|
| Microsoft® Office® 2010 (Word / Excel) |
| Microsoft® Office® 2013 (Word / Excel) |
| Microsoft® Office: nur in 32 Bit Versionen, auch auf 64 Bit Betriebssystemen! |
| Um einen störungsfreien Betrieb sicherzustellen empfehlen wir keinen Mischbetrieb bei den Office-Versionen.<br>Sollte dies aus technischen oder organisatorischen Gründen dennoch notwendig sein, so müssen kundenindividuell die Rahmenbedingungen und möglichen Einschränkungen geprüft und ggf. mit geeigneten Maßnahmen belegt werden. |

### Internet-Explorer

| | |
|---|---|
| Freigegebene Versionen | Microsoft® Internet Explorer® 9.0<br>Microsoft® Internet Explorer® 10.0<br>Microsoft® Internet Explorer® 11.0<br>Zusätzlich aktivierter Scriptinghost |
| Einschränkungen CGM REHA | Für den Einsatz der CGM REHA G3-Module ist die Version Microsoft® Internet Explorer® 11.0 erforderlich |

### Weitere Systemkomponenten

| Produkt | System-komponente | Voraussetzungen |
|---|---|---|
| CGM RECHNUNGSWESEN<br>CGM SOZIAL | JAVA JRE | Offline-Schnittstellen-Converter<br>Bei einem x64 Betriebssystem wird Java x64 SE 7 und Java x86 SE 7 benötigt |
| CGM SOZIAL PEP<br>CGM SOZIAL P&D | .NET Framework | Es wird das **Microsoft .NET-Framework 4.6.1 FULL** auf dem Anwendungsserver und den Clients benötigt. |
| CGM OPAS SOZIAL Mobil Touch | .NET Framework | Es wird das Microsoft .NET-Framework 3.5 FULL auf dem Anwendungsserver sowie auf den mobilen Endgeräten benötigt. |
| CGM OPAS SOZIAL Mobil Touch | MS IIS | Es wird Microsoft Internet Information Services ab Version 5 benötigt. |
| CGM DMS Rechnungseingang | .NET Framework | Es wird das Microsoft .NET-Framework 4.0 **FULL** auf dem Anwendungsserver benötigt. |
| CGM DMS FAME | .NET Framework | Modul “Volltext” mit GdPicture<br>Modul “Akten-Output-Converter (PDF-Generator)”<br>Vorschau in der Akte von XPS-Dokumenten<br>Es wird das Microsoft .NET-Framework 3.5 FULL auf dem Anwendungsserver und ggf. auf den Clients benötigt. |

| | | |
|---|---|---|
| mps All for Public | JAVA (JDK 5.0) | Offline-Schnittstellen-Converter |
| CGM DMS Rechnungseingang | MS IIS | Es wird Microsoft Internet Information Services ab Version 6 benötigt. |
| CGM REHA XReha | MS IIS | Es wird Microsoft Internet Information Services (IIS) Version 7.5 oder 8 benötigt mit den Features „URL Rewrite“, „Application Request Routing”, „Ablaufverfolgungsregeln für Anforderungsfehler“ und „Serverzertifikate“. |
| CGM REHA XReha, CGM REHA Connect | Mirth Connect | Beim Einsatz von CGM REHA XReha oder CGM REHA Connect wird die Installation des Kommunikationsservers Mirth Connect ab Version 3.3.1 auf dem Anwendungsserver bzw. auf dem Kommunikationsserver vorausgesetzt. Des Weiteren ist eine zusätzliche Datenbank für den Betrieb des Mirth Connect erforderlich. Um die bestehende Datenbank bzgl. der Priorität performancekritischer Aktionen nicht zu beeinflussen, wird die Anlage in einer separaten Datenbankinstanz empfohlen. |

Voranstehende Angaben beruhen auf unseren Erfahrungen entsprechenden normalen Anforderungsbedürfnissen. Im Einzelfall kann es, insbesondere bei besonderen System-Konstellationen oder individuellen Bedürfnissen und Wünschen, jedoch zu Abweichungen hiervon kommen. In diesem Fall ist eine vorherige Überprüfung und Beratung im Hinblick auf die Systemvoraussetzungen unerlässlich.

Bitte beachten Sie auch die Life Cycle Status-Information der Hersteller.

Microsoft®: http://support.microsoft.com/lifecycle/

Citrix®: http://www.citrix.com/support/product-lifecycle

## Netzwerkprotokolle

Die Anbindung der Clients erfolgt in einem lokalen Netzwerk unter Verwendung des TCP/IP-Protokolls. Anbindungen über WAN-Strecken sind mittels TCP/IP ebenfalls möglich. Entscheidend für die Performance und Stabilität sind die verwendeten Bandbreiten. Im lokalen Netzwerk muss eine Mindestbandbreite von 100 Mbit/s bis zu den Arbeitsplätzen vorhanden sein. Bei der Verwendung von Terminalserverkonzepten sind je nach Ausbaustufe sog. BackBones von min. 1 Gbit/s empfehlenswert. Die notwendigen Bandbreiten bei Anbindung über WAN-Strecken hängen stark vom verwendeten Client-Konzept sowie von den anwendungsspezifischen Datenmengen ab. Daher muss dies im Einzelfall in enger Abstimmung mit der CGM Clinical geschehen. Bei Architekturen im Citrix XenApp-Umfeld gilt die Empfehlung von 2 Mbit-Standleitung (synchron) bei ca. 100 anzubindenden Anwendern, die im durchschnittlichen Regelbetrieb mit CGM Clinical – Applikationen arbeiten. Empfehlenswert sind im Einzelfall Tools zum Bandbreitenmanagement, um vor allem Performanceengpässe beim Abarbeiten von großen Druckaufträgen zu vermeiden.

## Virtuelle Umgebungen

Die Architektur der CGM Clinical Software ermöglicht den Einsatz innovativer Serverkonzepte. Hierzu zählt beispielsweise die Servervirtualisierung.

Beim Einsatz von virtuellen Umgebungen wie beispielsweise VmWare oder Citrix XenServer weisen wir ausdrücklich auf die Freigabehinweise sowie technischen Informationen der Hersteller hin. (Hersteller z.B.: Hewlett-Packard, Fujitsu, Microsoft, Oracle, Citrix und VmWare)

Eventuelle Einschränkungen der Hersteller bzw. besondere Verfahren im Supportfall bei virtuellen Umgebungen gelten uneingeschränkt auch für Systeme aus unserem Hause.

# Systemanforderungen

Hier erhalten Sie eine generelle Übersicht über die globalen Systemanforderungen und Sicherheitseinstellungen der aktuellsten CGM Clinical - Applikationen.

## Windows-Systemberechtigungen

### Allgemeine Anforderungen

| Rubrik | Erläuterung |
|---|---|
| Domäne | Microsoft Windows Domäne (ab Windows 2008) muss im Einsatz sein |
| Service-User | Es muss ein Windows-Domänenuser für Windows/COM+ - Services vorhanden sein.<br><br>Das Passwort dieses Users darf nicht ablaufen.<br>Empfohlener Name des Users <A41svcuser>. Dieser User wird bei Windows-Diensten als Laufzeit-Benutzer zugeordnet bzw. bei COM+-Diensten als Laufzeitidentität eingetragen. |

### Registry

| Securitylevel | Schlüssel |
|---|---|
| Vollzugriff | HKEY_LOCAL_MACHINE\SOFTWARE\All for One\Cobra<br>HKEY_CURRENT_USER\SOFTWARE\All for One\ |
| Leserecht | HKEY_LOCAL_MACHINE<br>HKEY_CLASSES_ROOT |
| Lese&Schreibrecht | HKEY_CURRENT_USER |
| Vollzugriff bei Installation | HKEY_LOCAL_MACHINE<br>HKEY_CLASSES_ROOT |

### Dateisystem / NTFS (CGM RECHNUNGSWESEN, CGM REHA, CGM DMS, mps All for public)

| Securitylevel | Verzeichnis |
|---|---|
| Vollzugriff | User-Temp |
| Leserecht | <Freigabe>\Cobra\Resource\Forms (Anmelde-Dialog)<br><Freigabe>\Cobra\Typelib (registrierte Typbibliotheken) |
| Lese&Schreibrecht | <Freigabe>\Cobra\Help (Online-Hilfe) |
| Ausführungsrecht | <Freigabe>\cobra\apps\<Anwendungsgebiet>\Bin |
| Vollzugriff bei Installation | \\SERVERNAME\CGM$ (ältere Installationen *SERVERNAME*\AllforOne$)<br><%systemroot%>\System32<br>Lokales Applikationsverzeichnis |

### Dateisystem/NTFS (CGM SOZIAL TOPSOZ)

| Securitylevel | Verzeichnis |
|---|---|
| Vollzugriff | User-Temp |
| Leserecht | <Clientverzeichnis>\Custom\<br><Topsoz-Serverfreigabe>\Custom\ |
| Lese&Schreibrecht | <Clientverzeichnis>\Custom\Tmp<br><Topsoz-Serverfreigabe>\Custom\ |
| Ausführungsrecht | <Clientverzeichnis>\Custom\<br><Clientverzeichnis>\Custom\Bin |
| Vollzugriff bei Installation | <Topsoz-Serverfreigabe>\Custom\<br><Clientverzeichnis>\Custom<br><%systemroot%>\system32 |

### Dateisystem/NTFS (CGM SOZIAL DP)

| Securitylevel | Verzeichnis |
|---|---|
| Vollzugriff | User-Temp |
| Leserecht | <Dienstplan-Serverfreigabe>\VIPP\ |
| Lese&Schreibrecht | <Dienstplan-Serverfreigabe>\VIPP\ |
| Ausführungsrecht | <Dienstplan-Serverfreigabe>\VIPP\programs\ |
| Vollzugriff bei | <Dienstplan-Serverfreigabe>\VIPP |
| Installation | <%CommonProgramFiles%> |
| | <%systemroot%>\system32 |

### Dateisystem/NTFS (CGM SOZIAL PEP/CGM SOZIAL P&D)

| Securitylevel | Verzeichnis |
|---|---|
| Vollzugriff | User-Temp |
| Lese&Schreibrecht | <Installationsverzeichnis><br><br>Folgende Rechte werden benötigt, werden aber standardmäßig vom Betriebssystem gewährt:<br><br>Anwendungsserver:<br>• Windows Server 2008 / 2012 / 2016: <%ProgramData%>\system.SOZIAL<br><br>Client:<br>• Windows 7 / Windows Server 2008 / 2012 /2016: C:\Users\<USER>\AppData\Local\AllForOne |
| Ausführungsrecht | <Installationsverzeichnis> |
| Vollzugriff bei Installation | <Installationsverzeichnis><br><br>Bei Neuinstallation des Servers werden Leserechte auf das TOPSOZ-Serverzeichnis benötigt. |

### Dateisystem/NTFS (CGM SOZIAL BA)

| Securitylevel | Verzeichnis |
|---|---|
| Vollzugriff | User-Temp |
| Leserecht | <Ba-Clientverzeichnis> |
| Lese&Schreibrecht | Keine Schreibrechte, Ablage von Dokumenten in <%USERPROFILE%>\Eigene Dateien |
| Ausführungsrecht | <Ba-Clientverzeichnis><br><Ba-Clientverzeichnis>\Tools |
| Vollzugriff bei Installation | <Ba-Clientvereichnis><br><%CommonProgramFiles%><br><%systemroot%>\system32 |

### Dateisystem/NTFS (CGM SOZIAL SIC)

| Securitylevel | Verzeichnis |
|---|---|
| Vollzugriff | User-Temp |
| Leserecht | <SIC-PA-Clientverzeichnis> (sofern lokaler Client installiert) |
| Lese&Schreibrecht | <SIC-PA-Clientverzeichnis> (sofern lokaler Client installiert)<br><SIC-PA-Serverfreigabe>\SICPA |
| Ausführungsrecht | <SIC-PA-Clientverzeichnis> (sofern lokaler Client installiert)<br><SIC-PA-Serverfreigabe>\SICPA |
| Vollzugriff bei Installation | <SIC-PA-Serverfreigabe>\SICPA<br>(ggf. <SIC-PA-Clientverzeichnis> bei lokalem Client)<br><%CommonProgramFiles%><br><%systemroot%>\system32 |

### Dateisystem/NTFS (CGM OPAS SOZIAL)

| Securitylevel | Verzeichnis |
|---|---|
| Vollzugriff | User-Temp |
| Leserecht | <OPAS SOZIAL-Clientverzeichnis> (sofern lokaler Client installiert) |
| Lese&Schreibrecht | <OPAS SOZIAL-Clientverzeichnis> (sofern lokaler Client installiert)<br><OPAS SOZIAL-Serverfreigabe>\Image |
| Ausführungsrecht | <OPAS SOZIAL-Clientverzeichnis> (sofern lokaler Client installiert)<br><OPAS SOZIAL-Serverfreigabe>\Client |
| Vollzugriff bei Installation | <OPAS SOZIAL-Serverfreigabe><br>(ggf. <OPAS SOZIAL-Clientverzeichnis> bei lokalem Client)<br><%CommonProgramFiles%><br><%systemroot%>\system32 |

### Dienste

| Rubrik | Erläuterung |
|---|---|
| Service-User | Es muss ein Windows-Domänenuser für Windows/COM+ - Services vorhanden sein.<br><br>Das Passwort dieses Users darf nicht ablaufen.<br>Empfohlener Name des Users <A41svcuser>. Dieser User wird bei Windows-Diensten als Laufzeit-Benutzer zugeordnet bzw. bei COM+-Diensten als Laufzeitidentität eingetragen. |
| CGM SOZIAL | Der Dienst „SocialService“ benötigt lokale Adminrechte. |
| CGM OPAS SOZIAL | Die Dienste „ITSRVANY“ sowie „OPASServer3“ benötigen lokale Adminrechte. |
| CGM DMS | Der Dienst AppLink Connector Server benötigt lokale Adminrechte |

### Zusätzliche Berechtigungen

In Verbindung mit verschiedenen Fremdanwendungen (z.B. Elster, Fakturasysteme) kommen unter Umständen weitere Technologien zum Einsatz, die ihrerseits weitere Berechtigungseinstellungen in verschiedenen Systemkomponenten benötigen.

Dies ist jedoch abhängig vom lokalen Betriebssystem und von der spezifischen Systemumgebung.

### Weitere produktspezifische Berechtigungen

Siehe < Produktfamilienspezifische Anforderungen>

## Erforderliche DB-Einstellungen & Benutzer

### MSSQL Server

***Parameter & Werte***

| Bereich | Wert |
|---|---|
| Sprache | Deutsch |
| Sortierungskennzeichen | German_PhoneBook_CS_AI_KS_WS<br>ACHTUNG: ab SQL Server 2008 KEINESFALLS German_PhoneBook_100_CS_AI_KS_WS verwenden! |
| Sortierreihenfolge: | Groß-/Kleinschreibung<br>Unterscheidung nach Kana<br>Unterscheidung nach Breite. |

Der Datenbankname und Benutzer richtet sich nach dem jeweiligen Produkt.
Der Benutzer muss immer die Rolle <db_owner> haben

***Datenbank-User***

| Produkt | Datenbankname | Benutzer |
|---|---|---|
| Cobra-Applikationen<br>• CGM RECHNUNGSWESEN<br>• CGM REHA<br>• mps All for Public | Cobra | Cobra |
| CGM DMS FAME (in Verbindung mit anderen Cobra Applikationen) | Cobra | Cobra |
| CGM DMS FAME (in Verbindung mit CGM SOZIAL TOPSOZ und/oder PO) | Fameaim | Cobra |
| CGM SOZIAL DP (stationär) | DPPEP | DPPEP<br><dem Benutzer muss die DPPEP Datenbank als **Standard** eingetragen werden, Sprache „German“> |
| CGM SOZIAL TOPSOZ,<br>CGM SOZIAL PEP,<br>CGM SOZIAL P&D und<br>CGM SOZIAL DP | TOPSOZ | TOPSOZ<br><dem Benutzer muss die TOPSOZ Datenbank als **Standard** eingetragen werden, Sprache „German“> |
| CGM SOZIAL SIC | SICPA | SICPA |
| CGM SOZIAL BA | BA_DOKU | Cobra |
| CGM OPAS SOZIAL | OPASxxxx | OPASADM<br>SPMAN |
| CGM DMS Rechnungseingang | AppLink | AppLink<br>Das Schema des Benutzers AppLink muss dbo sein. |

**Bei Einsatz von Cobra Applikationen muss ein Schema <cobra> in der Datenbank angelegt werden.**

## Oracle

***Parameter & Werte***

| Bereich | Wert |
|---|---|
| Initialisierungsparameter | processes=300<br>OPEN_CURSORS=2048 |
| Einstellungen zum Zeichensatz der Datenbank | WE8ISO8859P1<br><br>Ab Version 11.1<br>WE8MSWIN1252, Konvertierung bestehender Datenbanken erforderlich |
| NLS_LANG | GERMAN_GERMANY.WE8ISO8859P1<br><br>Ab Version 11.1<br>GERMAN_GERMANY. **WE8MSWIN1252**<br>zwingend notwendig am Oracle Client |

***Datenbankuser***

| Produkt | Benutzer |
|---|---|
| Cobra-Applikationen<br>• CGM RECHNUNGSWESEN<br>• CGM REHA<br>• CGM DMS FAME<br>• mps All for Public | cobra |
| CGM SOZIAL DP (stationär) | dppep |
| CGM SOZIAL TOPSOZ,<br>CGM SOZIAL PEP,<br>CGM SOZIAL P&D und<br>CGM SOZIAL DP | topsoz |
| CGM SOZIAL SIC | sicpa |
| CGM SOZIAL BA | gbm |
| CGM DMS Rechnungseingang | AppLink |
| CITRIX | metaframe |

***Berechtigungen***

| Berechtigungen | Rechte |
|---|---|
| Rolle All41<br>Den ALL41 Usern dann diese Rolle zuweisen | CLUSTER, DATABASE LINK, DIMENSION, EVALUATION CONTEXT, EXTERNAL JOB, INDEXTYPE, JOB, LIBRARY, MATERIALIZED VIEW, OPERATOR, PROCEDURE, PROFILE, PUBLIC DATABASE LINK, PUBLIC SYNONYM, ROLE, ROLLBACK SEGMENT, RULE, RULE SET, SEQUENCE, SESSION, SYNONYM, TABLE, TABLESPACE, TRIGGER, TYPE, USER, VIEW |
| Systemberechtigungen | CREATE PROCEDURE, CREATE TRIGGER |

### Unbedingt beachten

1. Die Installationsrichtlinien der CGM Clinical Deutschland GmbH sind zu beachten.
2. Datensicherungskonzept muss seitens Kunde gewährleistet sein.

## Produktfamilienspezifische Anforderungen

### CGM SOZIAL

| Bereich | Hinweise |
|---|---|
| Integration<br>CGM SOZIAL TOPSOZ<br>mit CGM RECHNUNGS-WESEN<br>oder SAP<br>oder LOGA<br>über CGM Clinical EAI | Damit diese Integration eingesetzt werden kann ist es erforderlich, dass auf den Clients DCOM aktiviert ist, dass auf dem Server, auf dem die EAI-Komponente eingesetzt wird (im Normalfall der Datenbankserver) ebenfalls das DCOM-Protokoll aktiviert ist. Des Weiteren wird in dieser Konstellation nur ein Netzwerk mit Windows- bzw. Activedirectory-Domäne unterstützt. Für Konstellationen ohne AD- oder Windowsdomäne (z.B. Workgroup oder Novell Verzeichnisdienst) kann keine Funktionsgarantie übernommen werden. |
| CGM SOZIAL PEP<br>CGM SOZIAL P&D | CGM SOZIAL PEP und CGM SOZIAL P&D werden in einem Client-Server-System betrieben, wobei der Social.NET-Server als Windows-Dienst ausgeführt wird. Dadurch wird kein Webserver o. ä. benötigt.<br><br>Wenn es die Infrastruktur bzw. Hardware zulässt, kann der Dienst physikalisch auf dem Datenbankserver laufen. Ein separater Anwendungsserver wird allerdings empfohlen.<br><br>Spezifische Anforderungen:<br>• Es wird das **Microsoft .NET-Framework 4.6.1** auf dem Anwendungsserver und den Clients benötigt.<br>• Bildschirmauflösung mind. 1280 x 1024<br>• VFP-Datenbanken werden nicht unterstützt! |
| CGM SOZIAL PEP | Voraussetzung für den Zugriff auf **Oracle-Datenbanken** ist die Installation des **Oracle Data Provider für .NET 4.0 (ODP.NET)**. |
| CGM SOZIAL P&D | Bei Verwendung des Formulardrucks wird Microsoft Word bzw. Excel ab Version 2010 sowie ein PDF-Reader (z.B. Adobe Acrobat Reader) auf jedem Terminalserver bzw. zu jeder lokalen Client-Installationen benötigt.<br><br>Die Server- und Einzelplatzinstallation von CGM SOZIAL P&D benötigt ein 64 Bit Betriebssystem. Der Client kann auf 32 und 64 Bit Betriebssystemen verwendet werden. |
| CGM SOZIAL MOBILE | CGM SOZIAL MOBILE ist eine Android-App, die über Synchronisierungs-dienste mit CGM SOZIAL SIC oder CGM SOZIAL P&D kommunizieren kann.<br><br>Zur Synchronisation der Mobilen Anwendung mit dem jeweiligen Dokumentationsprogramm wird ein WLAN-Netz benötigt. Da die App offlinefähig ist, ist eine punktuelle WLAN-Ausleuchtung ausreichend.<br><br>Voraussetzung ist ein Smartphone oder Tablet mit<br>• Android ab Version 4.2 (empfohlen ab Version 5.0)<br>• 16 GB Speicher<br>• 1 GB Arbeitsspeicher (empfohlen 2 GB)<br>• minimaler Bildschirmgröße 4,5 Zoll |

| | |
|---|---|
| | Die Systemvoraussetzungen für die Synchronisierungsdienste sind dieselben wie für die CGM SOZIAL SIC bzw. den Anwendungsserver von CGM SOZIAL P&D.<br>Wir empfehlen eine SSL Verschlüsselung bei der Kommunikation mit dem Webservice (https). Dazu wird ein SSL-Zertifikat für den Anwendungsserver benötigt, welches von einer CA ausgestellt sein muss (kein selbstsigniertes). Diese Zertifikate sind z.B. bei https://www.psw-group.de/ssl-zertifikate erhältlich. |
| CGM SOZIAL OPAS | **OPAS Mobil Touch**<br><br>Bei OPAS Mobil Touch erfolgt eine Installation auf dem mobilen Gerät, das auch eine kleine Daten- bank als Cache der aktuell benötigen Daten vorhält. Die Anwendung greift immer nur lokal auf die Datenbank zu. Hat das Gerät eine Online-Verbindung (z. B. bei komplett verfügbarem WLAN oder eingesteckten LAN) erfolgt der Datenaustausch mit nur geringer Zeitverzögerung. Bei nur eingeschränkter Konnektivität (z. B. WLAN nur im Bereich des Pflegestützpunktes oder bei manuellem Datenabgleich), wird von Zeit zu Zeit bei vorhandener Verbindung der Datenaustausch initiiert.<br><br>Für den Einsatz von OPAS Mobil Touch werden gängige Netbooks mit Touchscreen empfohlen. Hierzu stellt CGM Clinical ein separates Dokument bereit.<br><br>**OPAS SOZIAL Datenreplikation**<br><br>Für die OPAS Sozial Datenreplikation empfehlen wir eine ISDN oder DSL-Verbindung (z. B. über ein VPN). Dazu muss vom zentralen OPAS Sozial Server nur über die IP-Adresse der Gegenstelle automatisch eine Verbindung aufgebaut werden können. Eine Unterstützung für Passwort-Abfragen oder den Start spezieller Programme ist nicht vorhanden.<br>Wir empfehlen den Einsatz von DSL-Routern oder VPN-Routern, die automatisch die Verbindungen herstellen, sobald ein „PING“ ausgeführt wird.<br><br>**OPAS SOZIAL Web-Client (Kassenbuch)**<br><br>Für die Installation des Web-Clients ist ein Microsoft Internet Information Server erforderlich. Für detaillierte Angaben wenden Sie sich bitte an den OPAS Sozial Support. |
| CGM SOZIAL DP | Spezifische Anforderungen:<br>• Aus technischen Gründen darf keine Bildschirmauflösung größer Full HD (1900 x 1080) eingestellt sein. |

### CGM RECHNUNGWESEN

| Bereich | Hinweise |
|---|---|
| CGM RECHNUNGSWESEN CP Kassenterminals | Hersteller der Kartenterminals:<br>Giesecke & Devrient: alle ZVT 700 - kompatiblen Geräte<br>Ingenico: alle ZVT 700 - kompatiblen Geräte; namentlich die ELITE - Produktreihe<br><br>Provider und deren Terminals:<br>TeleCash: Giesecke & Devrient - Terminals.<br>InterCard: Inegnico - "Elite" - Terminals.<br><br>Generell gilt<br>Alle Geräte der nicht genannten Hersteller (oder nicht ZVT 700 kompatiblen Geräte der genannten Hersteller) müssen getestet werden, auch wenn die Geräte angeblich den ZVT 700 Standard unterstützen. |
| CGM RECHNUNGSWESEN FS Integration CGM AKUT | Beachten sie die Voraussetzungen zur Integration mit CGM AKUT, die in den dazu gültigen Softwarevoraussetzungen beschrieben sind. |

| Rechte | Hinweise |
|---|---|
| CGM RECHNUNGSWESEN AS Jahresabschluss | Create/Write/Read unter <Freigabe>\Cobra\Apps\AS\Database für Backup-Dateien und –Ordner |
| CGM RECHNUNGSWESEN FS Elster-Modul | Windows XP wird nicht mehr unterstützt<br>Für die Ausführung werden die „Visual C++ Redistributable Packages für Visual Studio 2013 x86 (32bit)“ benötigt.<br>http://www.microsoft.com/de-de/download/details.aspx?id=40784<br>Vollzugriff auf <Freigabe>\Cobra\Apps\FS\Bin (MSAccess-DB, Temporärdateien, STADUEV0.UST, STADUEV0.UST.cry, STADUEV0.UST.cry.bes).<br>Zusätzlich bei Terminalserverbetrieb auf dem Terminalserver:<br>Vollzugriff auf<br>..\Cobra\Apps\FS\Bin (MSAccess-DB, Temporärdateien, STADUEV0.UST, STADUEV0.UST.cry, STADUEV0.UST.cry.bes). |
| CGM RECHNUNGSWESEN FS Datei-Import | Create/Write/Read für Stammdaten, Bewegungsdaten von Fakturasystemen<br>Create/Write fürLog-Dateien und –Ordner unterhalb des zu definierenden Importverzeichnisses |
| CGM RECHNUNGSWESEN CP Datei-Import | Create/Write für Log-Dateien und –Ordner unterhalb des zu definierenden Importverzeichnisses.<br>Execute für Konverter (je nach Bedarf). |
| CGM RECHNUNGSWESEN DS Konverter | Execute für Java-Konverter |

### CGM RECHNUNGWESEN DS BI

| Bereich | Hinweise |
|---|---|
| Allgemeine Systemvoraussetzung | Für DS BI wird ein SQL Server ab der Version 2008 R2 oder höher benötigt.<br><br>Die CGM RECHNUNGSWESEN BI Analyse Lösung basiert auf den Microsoft SQL Server 2008 R2/2012 Analysis Services in Verbindung mit Excel 2010/2013.<br><br>Für die Aufbereitung der Daten (Staging) ist CGM RECHNUNGEWSEN DS erforderlich.<br><br>Spezifische Anforderungen:<br>• Es wird das Microsoft .NET-Framework 4.0 **FULL** auf dem Anwendungsserver und den Clients benötigt. |
| Benutzerberechtigung | Für die Steuerung der Berechtigungen in DS BI, wird die Windows Authentifizierung (Microsoft Active Directory) verwendet. |
| Voraussetzung bei Oracle Datenbanken | Spezifische Anforderungen:<br>• Bei einer Konstellation BI-Server auf SQL Server x64 und CGM RECHNUNGSWESEN DS auf einem Oracle Server ist auf dem SQL Server x64 der **32bit Oracle Client** zu installieren.<br>• Auf dem SQL Server muss der Oracle OLE-DB Treiber installiert werden, sofern dieser nicht bereits durch eine vorhandene Oracle Clientinstallation verfügbar ist. |
| Excel Version Allgemein | Für eine Verbindung zu SQL Server 2012 ist mindestens Excel 2010 erforderlich. |
| Voraussetzungen Berichtsersteller | Berichtsersteller benötigen mindestens die Excel Version 2007 SP 1 oder höher. |
| Vorrausetzungen Berichtsempfänger | Excel 2007 SP 1 /2010 oder höher<br><br>Alternativ:<br>Excel Services über Microsoft Internet Explorer 7 oder höher<br><br>Alternativ:<br>Excel Services über Microsoft SharePoint Server 2007 oder Microsoft SharePoint Server 2010 |

### CGM DMS Rechnungseingang

| Bereich | Hinweise |
|---|---|
| Browser | Freigegebene Browser:<br>• Microsoft Internet Explorer ab Version 9<br>  ○ Kompatibilitätsmodus wird nicht unterstützt<br>• Mozilla Firefox ab Version 15<br>• Google Chrome ab Version 20 |
| Spezifische Anforderungen | • Es wird das Microsoft .NET-Framework 4.5.1 oder höher vorausgesetzt.<br>  • Installation auf Windows Server 2003 und XP nicht möglich.<br>• Bildschirmauflösung mind. 1280 x 1024 für den Einsatz des DMS Rechnungseingang.WebClients.<br>• Die Software wird als virtuelles Server-Image auf einer USB-Platte oder USB-Stick zur Verfügung gestellt (für VMWare, HyperV oder Citrix XenServer).<br>• Das Image hat den Namen ´SmartDMSWF´.<br>• Das Image muss mit einer Microsoft Windows 2012R2 Standard/Enterprise oder Datacenter-Edition Lizenz aktiviert werden.<br>• Das Image benötigen 1 fixe IP-Adressen für das Image.<br>• Für die Windows-Dienste ist ein eigener Dienste-Benutzer erforderlich. Gerne würden wir hier einen Benutzer mit dem Namen „dmsServices“ verwenden.<br>• Die Software benutzt derzeit eine lokale MS SQL-Express Installation.<br>• Für die Anbindung an den vorhandenen Oracle Datenbank-Server wird ein eigenes Schema in einer Oracle-Datenbank mit folgendem Zeichensatz benötigt: WE8MSWIN1252.<br>• Für die Anbindung an den vorhandenen SQL-Server wird eine eigene Instanz DMS / Port 1429 mit einer anderen als die Standard-MPS/CGM Systema Sortierreihenfolge benötigt. Die Sortierreihenfolge lautet : Latin1_General_CI_AS . Diese Instanz sollte dann auch mit in den Sicherungsplan aufgenommen werden.<br>• Derzeit gelten für die geplante Inbetriebnahme der Software folgende HW-Eckdaten für die virtuelle Maschine : 4x vCPU (Virtuell CPU mit je 2 Kernen ), 8 GB RAM, Laufwerk C:\ 50 GB Laufwerk D:\ 40GB, Laufwerk E:\ und F:\ mit je 20 GB Speicherkapazität. Für das revisionssichere Archiv werden zusätzlich 2x 50GB als Freigabe oder Laufwerk benötigt<br>• IRISPowerscan9 ist unter Windows 10 nicht mehr freigegeben. |
| formcraft FCI Invoice (Rechnungsleser) ab Version 4.90.5 | Systemvoraussetzungen, siehe Dokumentation:<br>• EMC Captiva InputAccel Version 7.5 Release Notes<br>  • Server: mindestens Prozessor 2,4 GHz Pentium, 6 GB Arbeitsspeicher, 4 GB freier Plattenplatz<br>  ○ 64bit Windows-OS (kein 32bit !)<br>  ○ .Net 4.5.2 oder 3.5 SP 1 muss vor der eigentlichen Installation installiert werden<br>  ○ Betriebssysteme: Windows Server 2012 Standard, |

| | |
|---|---|
| | Windows Server 2012 R2, Windows Server 2008 R2 oder R2 SP1 Standard oder höher<br>• Client: unter einem 64bit System läuft der Client als 32bit Anwendung<br>○ .Net 4.5.2 muss vor der eigentlichen Installation installiert werden<br>○ Betriebssysteme: Windows Server 2012 Standard, Windows Server 2012 R2, Windows Server 2008 R2 oder R2 SP1 Standard oder höher, Windows 8.1 Update 1 Pro (64/32bit), Windows 8 Pro (32bit), Windows 7 SP1 - Professional, Enterprise, oder Ultimate Edition (64/32bit)<br>• Kurzanleitung Installation FCI 4.90 & IA6.0.2 unter Windows Server 2008 R2 x64 |
| Saperion Archivsoftware ab Version 7.5.5 | Systemvoraussetzungen, siehe Dokumentation:<br>• SAPERION Technical Specifications Version 7.5.5 |

### CGM REHA

| Bereich | Hinweise |
|---|---|
| Infrastruktur | CGM REHA basiert auf einer Client - Server Architektur. Die Serverkomponenten sind zentrale Datenbank-, Anwendungs- und Kommunikationsserver.<br>Änderungen, die dem technischen Fortschritt oder organisatorischen Verbesserungen dienen, behalten wir uns vor. |
| Serverkomponenten | Bei allen unter CGM REHA eingesetzten Serversystemen ist bei der Parametrierung eine enge Abstimmung mit CGM Clinical Deutschland GmbH notwendig. Dies gilt sowohl für das Einspielen von Servicepacks bzw. weiterer Systemsoftware als auch für die Parametrierung der DB-Systeme, da dies entscheidenden Einfluss auf Performance und Stabilität hat und ansonsten keine Funktionsgarantie für das CGM REHA-System übernommen werden kann. Je nach Größe der Installation können dedizierte Serversysteme zwingend notwendig sein. |
| Anwendungsserver | CGM REHA verwendet verschiedene Dienste, welche die zentrale Verarbeitung von Aufgaben übernehmen. Diese Dienste werden auf dem Anwendungsserver konfiguriert und erfordern je nach Konfigurationsgröße entsprechende Systemressourcen wie Hauptspeicher und Prozessorleistung. In komplexen Umgebungen kann daher der Einsatz von mehreren Anwendungsservern sinnvoll und notwendig sein um einen performanten und stabilen Betrieb zu gewährleisten. |
| Kommunikations-server | Auf Kommunikationsservern werden unter CGM REHA die Prozesse bzw. Dienste ausgeführt, die dem Datenaustausch bzw. der Integration von Partner- und Fremdsystemen dienen. Die Anzahl der Dienste sowie der |

| | |
|---|---|
| | damit verbundene Ressourcenbedarf hängt sowohl von der Anzahl und Integrationstiefe der im Einsatz befindlichen Partner- und Fremdsysteme als auch von der Konfigurationsgröße ab.<br><br>Bei einer Anbindung von Systemen mittels dem HL7-Protokoll-Standard werden je nach Integrationstiefe und Partnersystem mehrere Dienste benötigt, welche die Kommunikation mit diesen Systemen zentral übernehmen. Die Serverkonfiguration muss daher im Einzelfall in enger Abstimmung mit der CGM Clinical Deutschland GmbH erfolgen.<br><br>Bei der Nutzung von Fremdsoftware und -hardware sind die Anforderungen der jeweiligen Hersteller zu beachten.<br><br>Zur Integration der gesetzlich vorgeschriebenen §30x-Kommunikation mit den Kostenträgern dient ein dedizierter Kommunikationsserver, auf dem das Partnersystem Com4Cure (ehemals ProSoft) konfiguriert ist. Bei größeren Installationen, insbesondere bei einer zentralen Abwicklung der §30x-Kommunikation für mehrere Häuser, muss ggf. ein leistungsstärkerer Rechner eingesetzt werden. |
| Durchführung von Updates | Bei allen Updates von CGM REHA- und MPS-Produkten gilt als Voraussetzung, dass keine Datenbankverbindungen von Anwendungen und Services bestehen dürfen. Vor einem Update müssen die Anwendungen geschlossen und die Dienste beendet werden. |
| Spezifische Anforderungen | Bildschirmauflösung mind. 1280 x 1024 |

| Rechte | Hinweise |
|---|---|
| Windows-User/Gruppen | Für den Zugriff auf die CGM REHA Module werden üblicherweise Windows-User bzw. –Gruppen verwendet. Die Organisation und Konfiguration der Security-Policies hängt von den Sicherheitsansprüchen der jeweiligen Organisation ab und wird üblicherweise durch die lokale System-Administration des Kunden durchgeführt.<br><br>Für die Installation sowie Updates wird ein dedizierter User (im folgenden CGMUser) benötigt. Dieser User wird üblicherweise auch für Tätigkeiten im Rahmen der Fernwartung verwendet. Dieser User muss für das CGM REHA-System konfiguriert, und in die lokale Gruppe der Administratoren des lokalen Systems aufgenommen werden.<br><br>Darüber hinaus wird empfohlen, einen dedizierten User (CGMServices) für CGM REHA-Services zu definieren. Da dieser User normalerweise nicht für administrative Zwecke verwendet wird (keine Systemanmeldung) kann ein besonderes Kennwortes ohne Ablauf verwendet werden. |

| | |
|---|---|
| | Der lifeWATCH-Service verwendet zur Steuerung (Starten, Beenden, Neu starten) und Überwachung der CGM REHA-Dienste den WMI-Mechanismus (Windows Management Instrumentation) von Microsoft Windows. WMI wurde mit Windows 2000 eingeführt und ist seitdaher Bestandteil aller Windows-Versionen. Damit der lifeWATCH -Service alle installierten CGM REHA-Dienste per WMI ansteuern kann, muss der Benutzer, unter dem sich der lifeWATCH -Service bei Windows anmeldet, der Gruppe „Distributed COM-Benutzer“ zugewiesen werden. Zusätzlich muss der Benutzer Schreibrechte auf das Verzeichnis <Freigabe>\cobra\etc\config besitzen. |
| Netzwerk-komponenten | CGM REHA kann für die interne Kommunikation der Services TCP-Ports verwenden. Diese dürfen nicht von der Firewall o.ä. blockiert werden. Folgende Port-Ranges sind vorkonfiguriert und können kundenindividuell angepasst werden:<br><br>• CGM REHA-Dienste (GTP/SQL): 2001-2200; 3100-3150<br>• lifeWATCH: 51000<br>• lifeWATCH-Diensteüberwachung: 50000 - 50200 |
| Windows Netzwerk-Freigaben | Die Installation der CGM REHA-Module kann in ein beliebiges Verzeichnis auf dem Anwendungsserver erfolgen. Beim Einsatz von Terminalservern werden die CGM REHA-Module ebenfalls auf den Terminalservern in ein lokales Verzeichnis installiert. Nähere Informationen hierzu sind in der CGM REHA Systemkonzeption enthalten. Um den Zugriff auf zentrale Dateien zur Laufzeit sowie zur Client-Installation zu ermöglichen, werden von CGM REHA verschiedene Netzwerk-Freigaben, sog. Shares benötigt. Die notwendigen Zugriffseinstellungen beziehen sich dabei auf die sicherheitsrelevanten Einstellungen der Freigaben (Freigabeberechtigungen). Zugriffseinstellungen auf Dateiebene werden im folgenden Abschnitt beschrieben.<br><br>\\SERVERNAME\CGM$<br>(auch <Freigabe> genannt).<br>Hier werden alle zum Betrieb der CGM REHA-Module benötigten Dateien zentral abgelegt. Auf diesen Share müssen alle CGM REHA-User Vollzugriff auf Freigabe-Ebene erhalten.<br><br>Darüber hinaus können für Schnittstellen sowie Partnersysteme wie z.B. Com4Cure (ehemals ProSoft), KODIP, DIACOS, etc. weitere Netzwerkfreigaben notwendig sein. Die Einstellungen sowie besonderen Berechtigungen müssen den entsprechenden Dokumentationen entnommen werden. |
| Windows Dateisystem | Die Installation der CGM REHA-Module erfolgt wie beschrieben in ein Verzeichnis auf dem Anwendungs- bzw. Terminalserver. Auf dieses Installationsverzeichnis sowie alle darunter liegenden Verzeichnisse |

| | |
|---|---|
| | benötigen alle User von CGM REHA lesenden und ausführenden Zugriff.<br>In den Betriebsparametern des Moduls Patientenmanagement müssen verschiedene Pfade im Zusammenhang mit Schnittstellen angegeben werden, beispielsweise zum Austausch von Daten gemäß §301ff, Datenaustausch im HL7-Standard oder für den internen Datenaustausch gemäß dem DTA-Protokoll. Auf die dort angegebenen Verzeichnisse benötigen die betroffenen User Vollzugriff.<br>Da im laufenden Betrieb von CGM REHA an verschiedenen Stellen temporäre Dateien und ggf. Verzeichnisse erzeugt werden, ist ein Vollzugriff auf das temporäre Verzeichnis des angemeldeten Benutzer notwendig.<br>Im Modul Therapieplanung werden verschiedene Statusmeldungen sowie ggf. Trace und Debuginformationen abgelegt. Daher benötigen die User des Moduls Therapieplanung Vollzugriff auf den Verzeichnissen:<br>▪ <Freigabe>\Cobra\Apps\GTP\bin<br>▪ <Freigabe>\Cobra\Apps\GTP\Log<br>für Debug\Tracing<br><br>Anforderungen bzgl. des Moduls GPM-Fallakte sind in den Abschnitten zu FAME zu entnehmen.<br><br>Bei der Nutzung von Fremdsoftware und -hardware sind die Anforderungen der jeweiligen Hersteller zu beachten. |

### CGM DMS FAME

| Bereich | Hinweise |
|---|---|
| Windows Dateisystem | Anwendungsserver:<br>Die Installation der CGM DMS FAME-Module erfolgt wie beschrieben in ein Verzeichnis auf dem Anwendungsserver.<br>Unterhalb dieses Verzeichnisses benötigen die FAME-User mindestens lesend Zugriff.<br><br>User, die Dokumente editieren oder erzeugen, benötigen Vollzugriff im Verzeichnis<br><Freigabe>\Cobra\Apps\Fm\Server\Wordtext<br><br>User, die Vorlagen ändern (i.d.R. FAME-Administratoren), benötigen Vollzugriff auf das Verzeichnis<br><Freigabe>\Cobra\Apps\Fm\Server\Vorlagen<br><br>Anmerkung:<br>Standardmäßig werden die Dokumente und Vorlagen für CGM DMS FAME unterhalb des CGM DMS FAME-Server- |

| | |
|---|---|
| | Verzeichnisses<br><Freigabe>\Cobra\Apps\Fm\Server\<br><br>gespeichert.<br>▪ Dokumente liegen dort im Unterverzeichnis Wordtext<br>▪ Vorlagen liegen dort im Unterverzeichnis Vorlagen<br>Wird jedoch gewünscht, Vorlagen und Dokumente auf einem anderen Server bzw. in einem anderen Verzeichnis abzulegen, kann ein anderer Pfad angegeben werden.<br>Die Zugriffsrechte müssen dann entsprechend auf diesem Pfad vergeben werden.<br><br>Terminalserver:<br>Auf dem Terminalserver erfolgt die Installation der FAME-Komponenten in Abhängigkeit seines Betriebssystems:<br>• ab Windows2008<br>FAME Komponenten liegen nicht lokal, es werden die auf dem Anwendungsserver installierten Komponenten registriert<br><br>Welches FAME-Tmp-Verzeichnis genutzt wird kann im Rahmen der Terminalserver-Installation bestimmt werden:<br><br>Empfohlen wird, das Benutzerbezogene Verzeichnis zu nutzen. Grund ist die Benutzerkontensteuerung UAC ab Windows Vista.<br><br>• Clientbezogenes Verzeichnis soll benutzt werden:<br>Das Verzeichnis *tmp* wird auf dem entsprechenden Client unter …Client\Cobra\Apps\Fm\Client<br>angelegt<br><br>• Benutzerbezogenes Verzeichnis soll benutzt werden:<br>Das Verzeichnis *tmp* wird auf dem entsprechenden Client unter<br><Laufwerk>:\Dokumente_und_Einstellungen\<Benutzer>\Anwendungsdaten\ CGMSYSTEMA bzw AllforOne\Cobra\Apps\Fm\Client<br>bzw.<br><Laufwerk>:\Users\<Benutzer>\AppData\ CGMSYSTEMA bzw AllforOne\Cobra\Apps\Fm\Client<br><br>angelegt.<br><br>Auf diesem Installationsverzeichnis sowie alle darunter liegenden Verzeichnisse benötigen alle User von CGM DMS FAME lesenden und |

| | |
|---|---|
| | ausführenden Zugriff. |
| Verwendung von PDF-Vorlagen | Adobe PDF Reader ab Version 7 |
| Modul Volltextdaten MODI | Microsoft Office Document Imaging (MODI) Komponente (ab Version 2007)<br>Diese ist ab Office Version 2010 nicht mehr enthalten und muss deshalb von einer Vorgängerversion (Office 2007) installiert werden. |
| Modul Volltextdaten GdPicture | .net Framework 3.5.1 Features |
| Akten-Output-Converter (PDF-Generator) | .net Framework 3.5.1 Features |
| Vorschau von XPS Dokumenten | .net Framework 3.5.1 Features |
| FAME STA Diktatplayer | Visual C++2012 Redistributable (32 bit) muss installiert sein. |
| Scanning | IRISPowerscan9 ist unter Windows 10 nicht mehr freigegeben. |

# Drucken in Terminalserver Umgebungen

## Druckprobleme

Das größte Problem stellt die mangelnde Unterstützung der Hersteller für diese Plattform dar. Die Druckertreiber werden hauptsächlich für die Betriebssysteme Windows 7 / 8 entwickelt und warten mit tollen Features wie Tintenstandsanzeige auf.

Diese Funktionen sind in einer Terminalserverumgebung nicht notwendig und verursachen einen Großteil der Probleme.

Für den Einsatz unter Terminalservern würde ein sogenannter Mini-Treiber vollkommen ausreichen. Diese Treiber werden aber nur von den wenigsten Herstellern zur Verfügung gestellt.

Aus diesem Grunde hat die CGM Clinical Deutschland GmbH eine **Printing Policy** definiert, welche Ihnen helfen soll, den richtigen Druckertreiber zu finden und zu verwenden.

## Druckertreiberauswahl

Folgende Punkte sollten Sie in jedem Falle bei der Wahl eines Druckers bzw. Druckertreibers beachten

1. Verwenden Sie keine Tintenstrahldrucker.
    - diese Drucker sind HOST-BASED Drucker => diese Drucker verwenden den Prozessor des PCs bzw. Serversystems zur Abarbeitung des Auftrages. Dadurch werden die verfügbaren Systemressourcen eines Terminalservers stark dezimiert
    - die verwendeten Treiber verursachen die meisten Probleme aufgrund ihrer Menge an Features (wie z.B. Tintenstandanzeige)

2. Verwenden Sie immer den Treiber, welchen das **Betriebssystem** on Board hat. => die Treiber, die mitgeliefert werden.

3. Sollte kein Treiber für Ihren Drucker vorhanden sein, verwenden Sie einen kompatiblen Druckertreiber des Betriebssystems. Die meisten Laserdrucker sind mit dem HP Laserjet 4 oder 5 (PCL-Druckersprache) kompatibel. In Einzelfällen fragen Sie bitte beim Hersteller nach

4. Als letzte Instanz kann der Druckertreiber des Herstellers verwendet werden. Suchen Sie auf der Homepage der Herstellers immer nach einem Mini-Treiber (beinhaltet nur die notwendigsten Komponenten) oder Terminalserver-Treiber.

***Prüfen Sie eine eventuelle Kompatibilität oder Freigabe immer vor Kauf eines neuen Druckers!!***

***Beschränken Sie die Anzahl unterschiedlicher Druckerhersteller und Modelle auf ein Minimum!!***

### Freigaben

| Hersteller | Link/Download |
|---|---|
| HP | Citrix Support Artikel CTX110571 |
| Kyocera | bei Kyocera gibt es sogenannte Classic Mini Treiber.<br>Ausschließlich diese Treiber verwenden, die KX Treiber beeinflussen Ihre Systemumgebung |
| Lexmark | Knowledge Base Lexmark |
| Ricoh/Aficio | bei Ricoh/Aficio gibt es auch sogenannte Mini-Treiber<br>**Achtung:** den Mini-Treiber gibt es nicht für alle Druckertypen |

# Technische Hinweise zur Fernwartung bei CGM Clinical

**(Stand April 2009)**

## Geltungsbereich

Nachstehende Angaben haben Gültigkeit für die Produktbereiche:

- CGM REHA
- CGM SOZIAL
- CGM AKUT
- CGM RECHNUNGSWESEN
- CGM DMS
- CGM IT Design&Service

## Allgemeines

Zur Erbringung von Supportleistungen wie Fehlerbeseitigung, Unterstützung, Systemanpassung, Migration etc. ist es erforderlich, dass die CGM Clinical im Rahmen der Vertragsbeziehungen zeitweise Zugriff auf produktive Netze und Systeme von Kunden erhält, damit diese auf Protokollebene erreichbar und administrierbar sind. Diese Zugriffsmöglichkeiten dienen der schnellen, effektiven und unkomplizierten Unterstützung aus der Ferne.

Die in diesem Dokument beschriebenen Verfahren sind die unterstützten Standard Methoden zur Fernwartung, welche auch durch die ISO 27001 Sicherheitsnorm zertifiziert sind. Alle davon abweichenden Methoden werden durch die CGM Clinical nicht supportet und sind nicht in die ISO 27001 Zertifizierung mit integriert, d.h. die CGM Clinical kann hier keine Zusagen zu Vertraulichkeit, Verfügbarkeit und Integrität machen.

## Der Standard - Fernwartung per VPN

Als Zugangsmethode wird bei der CGM Clinical die Verbindung zum Kundennetz über das Internet mittels eines verschlüsselten VPN Tunnels hergestellt. Dabei wird über zwei VPN Geräte mittels des Standards IPSec eine sichere Verbindung hergestellt

| | |
|---|---|
| Technische Voraussetzungen | IPSec kompatible Hardware<br><br>Internetanschluss mit fester IP Adresse für das VPN Gerät |
| IPSec<br><br>Parameter | Mind. 3DES Verschlüsselung, DH Group 2, SHA-1<br><br>Verwendung von Pre-Shared Keys |
| Zugriff | Freier Zugriff auf gewünschte Zielsysteme für die<br><br>IP Adresse 10.143.167.10 |
| CGM Clinical Hardware | z.B.: Cisco Firewall ASA 5510 |

## Zugangssoftware für VPN Fernwartung

Zum Zugriff auf die gewünschten Systeme nach Herstellung der Verbindung über VPN oder ISDN werden verschiedene Software Tools verwendet

| **Client-Server** | **Software-Version** |
|---|---|
| | Teamviewer |
| **Terminal-Server** | **Software-Version** |
| Mindestens | Microsoft® Terminalserver-Remotedesktop-Client<br>CITRIX – Client |

## Implementierung VPN & ISDN Fernwartung durch die CGM Clinical

Es können bestehende Internet Strukturen durch den Einsatz von Standards zur Implementierung der Fernwartung verwendet werden.

Zur vollständigen Unterstützung von Kunden, bietet die CGM Clinical auch die Möglichkeit, preisgünstig die komplette Struktur mittels bewährten Cisco Hardware Geräten zu besorgen, zu installieren und dafür den Support zu leisten.

## Sicherheit

Der komplette Prozess der CGM Clinical wurde nach sicherheitsrelevanten Aspekten untersucht und angepasst. Relevante Aspekte der Sicherheit für Kunden sind

***Transparenter Zugriff***

Die CGM Clinical empfiehlt die Möglichkeit der Abschaltung des Fernwartungszugriffes bei Nicht-Bedarf einzuführen. Dies kann z. Bsp. bei VPN Devices durch die Verwendung von Skripten geschehen. Dadurch werden Zugriffe auf Kundensysteme erst nach Rücksprache mit dem verantwortlichen Ansprechpartner frei geschalten. Die Implementierung solcher Maßnahmen liegt im Ermessen des Kunden wobei die CGM Clinical bei der Implementierung bei unterstützten Geräten Unterstützung leisten kann.

***Authentifizierung***

Beim Zugriff auf die VPN Fernwartungsstruktur müssen sich interne Mitarbeiter erfolgreich authentifizieren, bevor der Zugriff auf Kundendaten möglich ist. Dadurch wird gewährleistet, dass nur CGM Clinical Mitarbeiter bei Kunden zugreifen können.

***Protokollierung***

Alle Verbindungen und Authentifizierungen werden protokolliert, wodurch eine spätere Überprüfung des Zugriffes möglich ist.

***Sicherheit TeamViewer***

Da beim Zugriff mit TeamViewer der Kunde erst selbstständig die Verbindung initiieren muss, ist eine Kontrolle des Zugriffes stets gegeben.

# Betreiberverantwortung

## Allgemeine Informationen

Eine stabile und gut gewartete IT-Infrastruktur ist eine wichtige Grundvoraussetzung zur Sicherstellung eines performanten und störungsfreien Betriebs von unternehmenskritischen Anwendungen der CGM Clinical Deutschland GmbH.

Nach erfolgreicher Installation und Konfiguration durch unsere Spezialisten geht die weitere Administration und Überwachung normalerweise an den Kunden über. Die daraus resultierenden notwendigen Maßnahmen lassen sich in verschiedene Kategorien und Aufgabenfelder zusammenfassen.

Jedes dieser Aufgabenfelder kann auch im Bedarfsfall an externe Spezialisten ausgelagert werden, gerne natürlich auch an unsere Spezialisten des Bereichs IT-Design&Service der CGM Clinical Deutschland GmbH.

Das vorliegende Dokument fasst die wesentlichen Aufgaben aus Sicht der CGM Clinical-Anwendung zusammen und dient der Unterstützung zur Organisation und Strukturierung der entsprechenden Zuständigkeiten unserer Kunden. Die genannten Punkte stellen dabei lediglich Empfehlungen dar, kundenindividuell können daneben weitere Aufgaben notwendig sein, die hier nicht betrachtet werden können.

### Systems Management

Zur Überwachung und Monitoring der IT-Infrastruktur ist ein ständiger Überblick über alle Ressourcen unbedingt erforderlich. Drohende oder bereits eingetretene Engpässe bei der Verfügbarkeit von Ressourcen müssen zeitnah erkannt und durch geeignete Maßnahmen behoben werden. Daneben müssen Fehlverhalten von Prozessen erkannt und behoben sowie ausgefallene Prozesse bei Bedarf neu gestartet werden. Die Störungserkennung kann beispielsweise durch ständiges Überwachen von Log-Einträgen sichergestellt werden, zur Behebung stehen verschiedene Reaktionsmöglichkeiten zur Verfügung, beispielsweise von der automatisierten Benachrichtigung der IT-Mitarbeiter bis hin zu einer automatisierten Störungsbeseitigung (z.B. Virenscanner) zur Verfügung.

Zur Unterstützung dieser teilweise aufwändigen Tätigkeiten wird der Einsatz von System-Management-Werkzeugen empfohlen. Diese bieten neben vorkonfigurierten und automatisierbaren Überwachungsmodulen auch ausgefeilte Kommunikationsmodule zur zeitnahen Benachrichtigung der zuständigen Mitarbeiter an.

### Reporting

Zur Beurteilung der Ressourcenauslastung sowie der Systemverfügbarkeit sind regelmäßige und standardisierte Reports und Statistiken unerlässlich. Diese sollten sowohl die Leistungsparameter der Systeme, wie Auslastung, Ressourcenverbrauch, Verfügbarkeit etc., als auch eine Statistik über alle festgestellten Problem- und Störungsmeldungen umfassen.

### Dokumentation

Eine umfassende Dokumentation über sämtliche Eigenschaften der IT-Infrastruktur ist wesentliche Voraussetzung zur schnellen und gezielten Analyse, Lokalisierung und Behebung von Störungen. Die Dokumentation sollte möglichst graphisch aufbereitet und muss bei Änderungen unbedingt aktualisiert werden. Sie ist auch eine wichtige Unterstützung bei Entscheidungen für mögliche Erneuerungen bzw. Erweiterungen.

### Betriebsführungshandbuch

Zur transparenten Dokumentation aller notwendigen Abläufe sowie organisatorischen Vorkehrungen und Zuständigkeiten wird das Führen eines Betriebshandbuches empfohlen. Neben den Festlegungen für die Betriebsführung, die zeitlichen Abstände der verschiedenen Maßnahmen etc. werden dort vor allem auch die Prozesse des „Change-Managements“ festgelegt.

### Service-Verträge/Hotline

Zur Sicherstellung der unmittelbaren Unterstützung bei komplexen System-Störungen durch kompetente Spezialisten sowie der zeitnahen Analyse und Behebung von Hardwareproblemen wird der Abschluss sowie die fristgerechte Prüfung und ggf. Verlängerung von Serviceverträgen und Hotline-Vereinbarungen dringend empfohlen.

## Produktiver Betrieb der Systeme

### Betrieb Server-Systeme

- Überwachung aller Serversysteme
  - Zentrales Rechnersystem (z.B. CPU, I/O, HW-Komponenten, etc.)
  - Festplatten-Subsystem (z.B. Plattenauslastung, -Zugriffszeiten, Swap-Space)
  - Netzwerk-Parameter (z.B. IP-Adressierung, DHCP, DNS, WINS)
- Überwachung von Server-Funktionen
  - Standard-Dienste (z.B. Anmeldedienste, Serverdienste)
  - Printing (z. B. Printer-Queues)
  - Netzwerk-Dienste (z.B. DHCP, DNS, WINS)
- Analyse der Serverprotokolldateien auf Probleme oder Fehler
- Überwachung der Kapazität auf den Datenträgern
- Überprüfung und Überwachung der USV-Komponenten
- Einspielen von Servicepacks, Hotfixes oder Patches
- Reorganisation, Löschung und Archivierung von Datenträgerinhalten
- Aktualisierung der aktuellen Anti-Viren-Pattern-Files
- Einrichtung von Druckern (neue Drucker, Berechtigungen, Drucker-Queues)
- Einstellungen der spezifischen Druckeransteuerungen von den Client-Systemen aus
- Optimierung/Tuning-Parameter
  - Anpassung der Systemparameter für Auslagerungsspeicher, Datenträger, etc.
  - Analyse der Reports und Performancedaten zur Ermittlung von notwendigen Systemerweiterungen, Aufrüstungen und Auslagerung von Anwendungen
  - Defragmentierung von Datenträgern und Datenträger-Überprüfungen

### Betrieb Backup-Mechanismen

- Überwachung der Backup-Hardware
- Auswertung von Sicherungsprotokollen und -logfiles
- Wechsel und Aufbewahrung der Datensicherungsmedien
- Konsistenzprüfungen nach Recovery
- Durchführen von Recovery-Tests

### Betrieb Datenbank-Management-System

- Datenbank- und Instanzüberwachung
  - Alert- und Trace-Files
  - Überwachung des Wachstums der DB-Ressourcen (z.B. Tablespaces, tabellen, Archivefilesystem)
- Performance- und Ressourcenüberwachung
  - I/O-Verhalten
  - Zugriffszeiten
  - Hit-Cache-Ratio
  - Connections
- Parameteranpassungen DB-Instanz
- Erweitern von Tablespaces
- Organisation und Pflege des Archiv-Filesystems
- Einspielen von Servicepacks, Hotfixes und Patches
- Reorganisation von DB-Objekten (z.B. Defragmentierung, Rebuild der Indices)
- (Online-)Sicherung der Datenbanken
- Recovery-Tests

### Betreuung Standard-Applikationen

- der Administration ADS/Domänenkonzept (z.B. Loginscripts, Policies, Berechtigungen)
- Administration Citrix- und Terminalserver-Umgebung (z.B. Loadbalancing, Published Applications, Profile)

### Betrieb der Security- & Firewall-Struktur

- Überwachen und Sicherstellen von Security-Policies
- Administration Firewall (z. B. Cisco-PIX)

### Netzwerk-Betreuung

- Überwachung aller managebaren Komponenten im Netzwerk
- Verwalten der LAN-Verbindungen
- Verwalten der Router-Konfiguration
- Diagnose bei Störungen im Netzwerk
- Administration von VPN-Leitungen mit laufender Funktionsprüfung

## Weitere produktspezifische Aufgaben

### Betrieb Management CGM REHA-System

- Überwachung der CGM LIFE CURE-Dienste (z.B. Leistungsjob, DW-Dienste, Druck-Spooler)
- Durchführen und Überwachen von Reorg-Maßnahmen (z.B. temp. Tabellen löschen, Zugriffe optimieren)
- Überwachung der Schnittstellen
- Überwachung der Kommunikationsserver (Com4Cure ehemals ProSoft)
- Überwachung der BediOnline-Konnektivität (XReha)
- Konfiguration von Usern und Berechtigungen
- Einspielen von neuen Releases, Servicepacks, Hotfixes und Patches der CGM LIFE CURE-Softwaremodule
- Installation und Konfiguration von CGM REHA-Clients

Einspielen von Servicepacks, Hotfixes und Patches von CGM REHA Partnersystemen nach Freigabe in CGM REHA (z.B. Com4Cure ehemals ProSoft, KODIP, DIACOS)

## Empfehlungen zum Reboot von Windows Server Systemen

Die Notwendigkeit von regelmäßigen Server-Neustarts (reboot) ist weniger in unserer Software begründet als vielmehr in der Systemarchitektur von Windows. Im Gegensatz zu anderen Betriebssystemen wie z.B. Unix werden dort die Systemressourcen leider nicht vollständig gekapselt und können bei einem Fehler, sei es aufgrund eines Programmabsturzes oder auch aufgrund systembedingter Fehlfunktionen, vom Windows-Betriebssystem nicht immer vollständig freigegeben werden. Durch eine lange Laufzeit des Systems werden damit Systemressourcen immer knapper, was sich leider oft auch auf die Performance des gesamten Systems oder auch nur auf Teilbereiche auswirkt. Nach einem System-Neustart werden diese Ressourcen normalerweise wieder freigegeben, können von den Anwendungen wieder verwendet werden und tragen damit wieder zu einer besseren Performance und teilweise auch Stabilität des Systems bei.

Auch wenn Microsoft die Notwendigkeit von regelmäßige System-Neustarts zumindest auf Marketing-Ebene teilweise verneint und auf die hohe Systemverfügbarkeit aufgrund "neuer" Architekturen verweist, so zeigt doch die Erfahrung, nicht nur in unserem Hause bei zahlreichen Installationen im Microsoft-Windows-Umfeld, dass regelmäßige Reboots leider auch weiterhin notwendig sind. Der Aufwand für solche Reboots hält sich dank der Verfügbarkeit von automatisierbaren sog. Tasks in engen Grenzen.

Die Sicherstellung eines performanten und stabilen Systems gehört zu den Betreiberaufgaben und sollte daher vom Kunden durchgeführt und überwacht werden. Wir sprechen hier nur die Empfehlung aus, die Server im Interesse unserer Kunden regelmäßig neu zu starten. Eine Empfehlung, die im Übrigen auch von anderen namhaften Software-Herstellern wie Citrix etc. kommt und welche auch in verschiedenen Foren immer wieder auftaucht. Gerne sind wir natürlich bereit, im Rahmen von Outsourcing-Verträgen die Administration sowie Überwachung ihres Systems teilweise oder auch komplett zu übernehmen. Sollten Sie hierzu Bedarf haben, so wenden Sie sich bitte an Ihren Ansprechpartner aus unserem Haus.

In der folgenden Tabelle sind unsere Empfehlungen aufgeführt:

| Servertyp | Reboot empfohlen | Warum |
|---|---|---|
| Citrix / Terminalserver | JA (mind. 1x pro Woche) | Speicherfragmentierung |
| Domaincontroller | NEIN | |
| Fileserver | NEIN | |
| reiner Datenbankserver | NEIN | |
| Datenbankserver mit Applikation | JA (1x pro Monat) | „alte“ Prozesse und Threads beenden |
| Applikationsserver | JA (1x pro Monat) | „alte“ Prozesse und Threads beenden |
| Printserver | JA (mind. 1x pro Woche) | Alte Druckaufträge löschen, Speicherfragmentierung |
| Exchange Server | JA (1x pro Monat) | Queues leeren, Speicherfragmentierung |

# Grundlagen Datensicherung

Die hier zusammengestellten Informationen sind auszugsweise dem IT-Grundsatzhandbuch des BSI entnommen.

## Regelmäßige Datensicherung

**Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT**

**Verantwortlich für Umsetzung: Administrator, IT-Benutzer**

Um den eventuellen Verlust von Daten zu verhindern ist es notwendig regelmäßig Datensicherungen durchzuführen. Um den genauen Umfang der zu sichernden Daten und den zugehörigen zeitlichen Rahmen festzulegen wird ein Datensicherungskonzept erstellt. Das Datensicherungskonzept enthält auch den oder die für die Sicherung verantwortlichen Mitarbeiter, der oder die sich auch um die Verwaltung der Speichermedien kümmert. Dieses wird weiterführend im Bänderverwaltungskonzept beschrieben. Die Durchführung der Datensicherung erfolgt in den meisten Fällen vollautomatisch.

Vor Erstellung des Datensicherungskonzeptes sind folgende Punkte festzulegen:

- Zeitintervall

  Beispiele: täglich, wöchentlich, monatlich,

- Zeitpunkt

  Beispiele: nachts, freitags abends,

- Anzahl der aufzubewahrenden Generationen,

  Beispiel: Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitagabend-Sicherungen der letzten zwei Monate.

- Umfang der zu sichernden Daten

  Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie Aufwand und Kosten sparen helfen.

  Beispiel: Selbsterstellte Dateien und individuelle Konfigurationsdateien.

- Speichermedien (abhängig von der Datenmenge)

  Beispiele: Bänder, Backup-To-Disk

- Vorherige Löschung der Datenträger vor Wiederverwendung
- Zuständigkeit für die Durchführung (Administrator, Benutzer)
- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien)

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wiedereingespielt werden. Daher und zur Senkung der Kosten sollen zwischen den Komplettsicherungen regelmäßig inkrementelle Sicherungen durchgeführt werden, das heißt, nur die seit der letzten Komplettsicherung neu erstellten Daten werden gesichert. (Werden zwischen zwei Komplettsicherungen mehrere inkrementelle Sicherungen durchgeführt, können auch jeweils nur die seit der letzten inkrementellen Sicherung neu erstellten Daten gesichert werden.)

Eine inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.

Für eingesetzte Software ist in der Regel die Aufbewahrung der Originaldatenträger und deren Sicherungskopien ausreichend. Sie braucht dann von der regelmäßigen Datensicherung nicht erfasst zu werden.

Alle Benutzer sollten über die Regelungen zur Datensicherung informiert sein, um ggf. auf Unzulänglichkeiten (zum Beispiel zu geringes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können (zum Beispiel zwischenzeitliche Spiegelung wichtiger Daten auf der eigenen Platte). Auch die Information der Benutzer darüber, wie lange die Daten wiedereinspielbar sind, ist wichtig. Werden zum Beispiel bei wöchentlicher Komplettsicherung nur zwei Generationen aufbewahrt, bleiben in Abhängigkeit vom Zeitpunkt des Verlustes nur zwei bis drei Wochen Zeit, um die Wiedereinspielung vorzunehmen.

## Datensicherungsplan

**Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement**

**Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen**

Mit Hilfe des Datensicherungsplans muss ein sachverständiger Dritter in der Lage sein, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten in angemessener Zeit beschaffen und installieren zu können.

Ein Datensicherungsplan muss Auskunft geben können über:

- Speicherungsort der Daten im Normalbetrieb (Plattenspeicher-Belegungsplan),
- den Bestand der gesicherten Daten (Bestandsverzeichnis),
- die Zeitpunkte der Datensicherungen,
- Art und Umfang der Datensicherung (logische/physikalische, Teil-/Vollsicherung),
- das Verfahren zur Datensicherung und zur Rekonstruktion der gesicherten Daten und
- den Ort der Aufbewahrung (Hinweis auf ggf. erforderliche Zutrittsmittel).

## Ersatzbeschaffungsplan

**Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement**

**Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen**

Um die im Falle eines Ausfalles notwendige Ersatzbeschaffung eines Teiles des IT-Systems durch den Verantwortlichen oder einen stellvertretenden Dritten zeitnah zu ermöglichen ist es notwendig einen Ersatzbeschaffungsplan zu erstellen.

Dieser muss die folgenden Angaben enthalten:

Übersicht über alle Teile des mit der Datensicherung verbundenen IT-Systems mit Angaben zu

- Produktbezeichnung
- Hersteller
- Seriennummer
- Kaufdatum
- Support-Hotline
- Support-Vertrag (sofern vorhanden)
- Lieferant
- Desaster Recovery für die Teilkomponente

Ersatzbeschaffungen müssen auch die technische Fortentwicklung der Teilkomponente berücksichtigen, da die Wiederherstellung des ursprünglichen Zustandes nicht ausschließlicher Zweck der Anschaffung ist. Aus diesem Grunde ist auch eine regelmäßige Überprüfung des Planes notwendig.

Für besondere kritische Systeme ist es eventuell notwendig ein entsprechend ausgestattetes Zweitgerät in einem separaten Raum oder Gebäude einsatzbereit vorzuhalten.

## Dokumentation der Datensicherung

**Verantwortlich für Initiierung: IT-Sicherheitsmanagement**

**Verantwortlich für Umsetzung: Verantwortliche für die Datensicherung**

In einem Datensicherungskonzept muss festgelegt werden, wie die Dokumentation der Datensicherung zu erfolgen hat. Für eine ordnungsgemäße und funktionierende Datensicherung ist eine Dokumentation erforderlich. So ist bei der Erstellung der Datensicherung für jedes IT-System zu dokumentieren:

- das Datum der Datensicherung,
- der Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert),
- der Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind,
- der Datenträger, auf dem die Daten gesichert wurden,
- die für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer) und
- die bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.).

Darüber hinaus bedarf es einer Beschreibung der Vorgehensweise für die Wiederherstellung eines Datensicherungsbestandes. Auch hier muss eine Beschreibung der erforderlichen Hard und Software, der benötigten Parameter und der Vorgehensweise, nach der die Datenrekonstruktion zu erfolgen hat, erstellt werden.

## Geeignete Aufbewahrung der Backup Datenträger

**Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement**

**Verantwortlich für Umsetzung: Administrator, IT-Benutzer**

Folgende Punkte sind in Hinblick auf die Aufbewahrung der Sicherungsdatenträger zu beachten:

- Die Sicherungsdatenträger sind nur autorisierten Personen zugänglich zu machen
- Für den Katastrophenfall muss sichergestellt sein, dass sie Datenträger räumlich getrennt vom IT-System aufbewahrt werden muss, wenn möglich in einen anderen Brandabschnitt
- Der schnelle Zugriff auf die Datenträger muss gewährleistet sein.
- Die Aufbewahrungsvorschriften des Herstellers müssen eingehalten werden

## Datenträgerverwaltung

**Verantwortlich für Initiierung: Leiter IT**

**Verantwortlich für Umsetzung: Archivverwalter, IT-Verfahrensverantwortlicher**

Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten.

**Bestandsverzeichnisse** ermöglichen einen schnellen und zielgerichteten Zugriff auf Datenträger. Bestandsverzeichnisse geben Auskunft über: Aufbewahrungsort, Aufbewahrungsdauer, berechtigte Empfänger.

Die äußerliche **Kennzeichnung** von Datenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben (z. B. die Kennzeichnung eines Magnetbandes mit dem Stichwort "Telefongebühren"), um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.

Für eine **sachgerechte Behandlung** von Datenträgern sind die Herstellerangaben, die üblicherweise auf der Verpackung zu finden sind, heranzuziehen. Hinsichtlich der **Aufbewahrung** von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

**Der Versand oder Transport** von Datenträgern muss in der Weise erfolgen, dass eine Beschädigung der Datenträger möglichst ausgeschlossen werden kann (z. B. Magnetbandversandtasche, luftgepolsterte Umschläge). Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten (z. B. mittels verschließbaren Transportbehältnissen). Versand- oder Transportarten (z. B. Kuriertransport) müssen ebenso festgelegt werden wie das Nachweisverfahren über den Versand (z. B. Begleitzettel, Versandscheine) und den Eingang beim Empfänger (z. B. Empfangsbestätigung). Der Datenträger darf über die zu versendenden Daten hinaus, keine "Restdaten" enthalten. Dies kann durch physikalisches Löschen erreicht werden. Stehen hierzu keine Werkzeuge zur Verfügung, so sollte der Datenträger zumindest formatiert werden. Dabei sollte sichergestellt werden, dass mit dem zugrunde liegenden Betriebssystem eine Umkehr des Befehls nicht möglich ist. Weiterhin ist zu beachten, dass vor Abgabe wichtiger Datenträger eine Sicherungskopie erstellt wird.

Für die interne Weitergabe von Datenträger können Regelungen getroffen werden wie Quittungsverfahren, Abhol-/Mitnahmeberechtigungen sowie das Führen von Bestandsverzeichnissen über den Verbleib der Datenträger.

Für den Fall, dass **von Dritten erhaltene Datenträger** eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel Daten für PCs übermittelt, sollte generell ein Computer-Viren-Check des Datenträgers erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von Datenträgern diese auf Computer-Viren zu überprüfen.

Eine geregelte Vorgehensweise für die **Löschung** oder **Vernichtung** von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Vor der Wiederverwendung von Datenträgern muss die Löschung der gespeicherten Daten vorgenommen werden.

## Überprüfung der Datensicherung

**Verantwortlich für Initiierung: IT-Sicherheitsmanagement**

**Verantwortlich für Umsetzung: Verantwortliche für die Datensicherung**

Um die Wiederherstellung der Daten im Bedarfsfall sicherzustellen ist es notwendig, die gesicherten Daten zu verifizieren. Dies muss auf zwei Arten erfolgen.

### Lesbarkeit der Daten

Unmittelbar nach dem Erstellen der Datensicherung ist der Inhalt des Datenträgers durch einen Lesevorgang zu Überprüfen. Dies kann in den meisten Fällen durch die eingesetzte Sicherungssoftware automatisch durchgeführt werden.

### Wiederherstellbarkeit der Daten

Die Funktionsfähigkeit der Sicherungssoftware sowie die Qualität der Datenträger muss durch regelmäßige Wiederherstellung der Daten nachgewiesen werden

Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen muss sporadisch, zumindest aber nach jeder Änderung des Datensicherungsverfahrens, getestet werden. Auf diese Weise kann zuverlässig ermittelt werden, ob

- die Datenrekonstruktion überhaupt möglich ist,
- die Verfahrensweise der Datensicherung praktikabel ist,
- eine ausreichende Dokumentation der Datensicherung vorliegt, damit ggf. auch ein Vertreter die Datenrekonstruktion vornehmen kann und
- die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entspricht

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden, dass

- die Daten ggf. auf einem Ausweich-IT-System installiert werden müssen,
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib-/Lesegeräte benutzt werden.

## Datensicherung bei mobiler Nutzung des IT-Systems

**Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team, Leiter IT**

**Verantwortlich für Umsetzung: Administrator, IT-Benutzer**

IT-Systeme im mobilen Einsatz (z. B. Laptops, Notebooks) sind in aller Regel nicht permanent in ein Netz eingebunden. Der Datenaustausch mit anderen IT-Systemen erfolgt üblicherweise über Datenträger oder über temporäre Netzanbindungen. Letztere können beispielsweise durch Remote Access oder direkten Anschluss an ein LAN nach Rückkehr zum Arbeitsplatz realisiert sein. Anders als bei stationären Clients ist es daher bei mobilen IT-Systemen meist unvermeidbar, dass Daten zumindest zeitweise lokal anstatt auf einem zentralen Server gespeichert werden. Dem Verlust dieser Daten muss durch geeignete Datensicherungsmaßnahmen vorgebeugt werden.

Generell bieten sich folgende Verfahren zur Datensicherung an:

### Datensicherung auf externen Datenträgern

Der Vorteil dieses Verfahrens ist, dass die Datensicherung an nahezu jedem Ort und zu jeder Zeit erfolgen kann. Nachteilig ist, dass ein geeignetes Laufwerk mitgeführt werden müssen und dass für den Benutzer zusätzlicher Aufwand für die ordnungsgemäße Handhabung der Datenträger entsteht. Bei unverschlüsselter Datenhaltung ergibt sich außerdem die Gefahr, dass Datenträger abhanden kommen und dadurch sensitive Daten kompromittiert werden können. Die Datenträger und das mobile IT-System sollten möglichst getrennt voneinander aufbewahrt werden, damit bei Verlust oder Diebstahl des IT-Systems die Datenträger nicht ebenfalls abhanden kommen.

Die Speicherung auf externen Datenträgern zur Datensicherung bietet sich insbesondere an, wenn auch der Datenaustausch mit anderen IT-Systemen über externe Datenträger erfolgt. Diese beiden Prozesse können u. U. kombiniert werden. Nach Rückkehr zum Arbeitsplatz müssen die Datensicherungen auf den Datenträgern in das Backup-System oder in das Produktivsystem bzw. die zentrale Datenhaltung der Institution eingepflegt werden.

### Datensicherung über temporäre Netzverbindungen

Wenn die Möglichkeit besteht, das IT-System regelmäßig an ein Netz anzuschließen, beispielsweise über Remote Access, kann die Sicherung der lokalen Daten auch über die Netzanbindung erfolgen. Vorteilhaft ist hier, dass der Benutzer keine Datenträger verwalten und auch kein entsprechendes Laufwerk mitführen muss. Weiterhin lässt sich das Verfahren weitgehend automatisieren, beispielsweise kann die Datensicherung beim Einsatz von Remote Access nach jedem Einwahlvorgang automatisch gestartet werden.

Entscheidend bei der Datensicherung über eine temporäre Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichen muss. Die Datenübertragung darf nicht zu lange dauern und nicht zu übermäßigen Verzögerungen führen, wenn der Benutzer gleichzeitig auf entfernte Ressourcen zugreifen muss. Bei gängigen Zugangstechnologien (z. B. VPN, ISDN) bedeutet dies, dass nur geringe Datenmengen pro Sicherungsvorgang transportiert werden können. Einige Datensicherungsprogramme bieten daher die Möglichkeit an, lediglich Informationen über die Änderungen des Datenbestands seit der letzten Datensicherung über die Netzverbindung zu übertragen. In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.

Eine wichtige Anforderung an die zur Datensicherung verwendete Software ist, dass unerwartete Verbindungsabbrüche erkannt und ordnungsgemäß behandelt werden. Die Konsistenz der gesicherten Daten darf durch Verbindungsabbrüche nicht beeinträchtigt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben dem Einsatz verlustfreier Kompressionsverfahren, die in viele Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differentielle Sicherungsverfahren zum Einsatz kommen.

## Datensicherung Windows Server

**Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement**

**Verantwortlich für Umsetzung: Benutzer**

Bei der Durchführung der Datensicherung sind die folgenden Punkte zu beachten:

- Die Sicherungssoftware ist in der Lage, wichtige Systemdateien, wie die Registrierung des lokalen Rechners, die COM+ Registrierungen sowie die Startdateien, zu sichern. Dies sollte in regelmäßigen Abständen und nach größeren Änderungen der Konfiguration durchgeführt werden. Dazu sind unter der Option *Systemstatus* die jeweiligen Auswahlboxen zu aktivieren.

- Auf Domänen-Controllern können zusätzlich auch die Active Directory Daten gesichert werden. Dies sollte bei jedem Backup durchgeführt werden. Die relevanten Optionen sind auf Domänen-Controllern ebenfalls unter der Option Systemstatus zu finden.

- Bei der Durchführung der Sicherung sollte unbedingt eine Protokolldatei angelegt werden. Nach Abschluss der Operation ist die Protokolldatei daraufhin zu überprüfen, ob alle zu sichernden Daten auch tatsächlich gesichert werden konnten oder ob während der Sicherung Fehler aufgetreten sind. Dabei ist es empfehlenswert, die Option *Details* zu aktivieren, da damit auch festgestellt werden kann, ob alle zu sichernden Daten gesichert wurden und ob überhaupt die Verzeichnisse in die Datensicherung einbezogen wurden, die gesichert werden sollten.

- Bei der Wiederherstellung gesicherter Dateien kann deren Zugriffsschutz wiederhergestellt werden, sofern dies in den Eigenschaften des Wiederherstellungsauftrages spezifiziert wurde. Standardmäßig ist diese Option aktiviert. Dabei kann dies nur für Daten erfolgen, die von einem Windows NTFS-Dateisystem stammen.

- Die Auswahl der zu sichernden Dateien und Verzeichnisse kann, im Gegensatz Windows Version des Programms, in einer Datei gespeichert werden, die später wieder geladen werden kann. Durch diesen Mechanismus ist es auch möglich, mehrere Sicherungsvarianten zu erzeugen, durch die unterschiedliche Daten erfasst werden.

- Sicherungen sollten in regelmäßigen Abständen durchgeführt werden. Damit kann die Sicherung auch automatisiert erfolgen.

Soll für umfangreichere Installationen bzw. bei hohen Verfügbarkeitsanforderungen zusätzliche Software zur Durchführung von Datensicherungen eingesetzt werden, so ist bei der Auswahl derartiger Sicherungssoftware darauf zu achten, dass sie die folgenden Anforderungen erfüllt:

- Die eingesetzten Dateisysteme, also FAT, NTFS und ggf. auch HPFS, sollten bei der Sicherung und Wiederherstellung unterstützt werden.

- Es muss möglich sein, auch Active Directory Daten sowie die Daten des SYSVOL-Ordners zu sichern.

- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.

- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren.

## Datensicherung einer Datenbank

**Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement**

**Verantwortlich für Umsetzung: Administrator**

Die Sicherung der Daten eines Datenbanksystems kann in aller Regel nicht mit den Datensicherungsprogrammen auf Betriebssystemebene vollständig abgedeckt werden. Letztere bilden in den meisten Fällen lediglich das Bindeglied, um die zu sichernden Daten auf ein Sicherungsmedium zu schreiben. Zur Sicherung des DBMS und der Daten müssen dagegen für die meisten Datenbankprodukte zusätzlich die jeweiligen Dienstprogramme des DBMS eingesetzt werden.

Die einfachste Möglichkeit einer Datenbanksicherung, die zugleich die sicherste darstellt, ist eine Komplettsicherung der Datenbank in heruntergefahrenem Zustand. Dabei werden alle zur Datenbank gehörenden Dateien auf dem Sicherungsmedium gesichert. Meist ist dieses Vorgehen allerdings aus Gründen der Verfügbarkeitsanforderungen an die Datenbank oder aufgrund des zu sichernden Datenvolumens nicht durchführbar.

Eine Alternative zur oben beschriebenen Komplettsicherung ist eine Online-Sicherung der Datenbank. Die Sicherung erfolgt dann während des laufenden Betriebs, d. h. die Datenbank muss nicht heruntergefahren werden. Online-Sicherungen sollten aus diesem Grund nur dann durchgeführt werden, wenn eine permanente Verfügbarkeit der Datenbank gefordert ist. Auf eine Offline-Komplettsicherung, die in vertretbar großen Zeitabständen durchgeführt werden kann, sollte trotzdem nicht verzichtet werden. Hierfür ist meistens der Einsatz einer Datensicherungssoftware notwendig.

Partielle Datenbanksicherungen stellen eine weitere Möglichkeit dar. Sie sollten immer dann verwendet werden, wenn das zu sichernde Datenvolumen zu groß ist, um eine vollständige Sicherung durchführen zu können. Dies kann daraus resultieren, dass die Kapazitäten der Sicherungsmedien nicht ausreichen oder dass der zur Verfügung stehende Zeitrahmen je Sicherung nicht genügt, um eine vollständige Sicherung durchführen zu können.

Falls möglich, so sollten in jedem Fall alle Transaktionen zwischen zwei Offline-Komplettsicherungen archiviert werden. Oracle bietet dazu beispielsweise die Möglichkeit an, indem der so genannte ARCHIVE-Mode für die Datenbank aktiviert wird. Transaktionen werden bei Oracle in so genannten Log-Dateien protokolliert, von denen es mehrere gibt. Diese werden nacheinander beschrieben und sobald alle Log-Dateien voll sind, so wird wieder die erste Log-Datei überschrieben. Der ARCHIVE-Mode erstellt von diesen Log-Dateien eine Sicherungskopie, bevor sie wieder überschrieben werden. Auf diese Art und Weise können bei einer Zerstörung der Datenbank alle Transaktionen komplett rekonstruiert werden. Auch hierfür ist allerdings die Existenz einer Komplettsicherung der Datenbank die Voraussetzung. Die Dauer eines solchen Recovery wächst mit der Anzahl der zurückzuspielenden Archiv-Log-Dateien an.

Für die Datensicherung eines Datenbanksystems muss ein eigenes Datensicherungskonzept erstellt werden. Einflussfaktoren für ein solches Konzept sind:

### Verfügbarkeitsanforderungen an die Datenbank

Wenn beispielsweise eine Datenbank werktags rund um die Uhr zur Verfügung stehen muss, so kann eine Komplettsicherung nur am Wochenende durchgeführt werden, da dies im allgemeinen ein Herunterfahren der Datenbank erfordert.

### Datenvolumen

Das gesamte zu sichernde Datenvolumen muss mit den zur Verfügung stehenden Sicherungskapazitäten verglichen werden. Dabei muss festgestellt werden, ob die Sicherungskapazitäten für das entsprechende Datenvolumen der Datenbank ausreichend dimensioniert sind. Falls dies nicht der Fall ist, muss ein Konzept zur Teilsicherung des Datenvolumens erstellt werden. Dies kann z. B. bedeuten, dass die Daten einzelner Anwendungen oder einzelner Bereiche der Datenbank immer im Wechsel gesichert werden bzw. nur die aktuellen Änderungen. Die Möglichkeiten einer Teilsicherung hängen von der verwendeten Datenbank-Software ab.

### Maximal verkraftbarer Datenverlust

Hier muss festgelegt werden, ob bei einer Zerstörung der Datenbank der Datenverlust eines Tages verkraftbar ist, oder ob die Datenbank bis zur letzten Transaktion wiederherstellbar sein muss. Dies ist im Allgemeinen bei einer hohen Anforderung an die Verfügbarkeit bzw. Integrität der Daten der Fall.

### Wiederanlaufzeit

Auch die maximal zulässige Zeitdauer des Wiederherstellens der Datenbank nach einem Absturz muss festgelegt werden, um den Verfügbarkeitsanforderungen zu genügen.

### Datensicherungsmöglichkeiten der Datenbank-Software

Im Allgemeinen werden von einer Datenbank-Standardsoftware nicht alle denkbaren Datensicherungsmöglichkeiten unterstützt, wie z. B. eine partielle Datenbanksicherung. Im konkreten Fall gilt es also zu prüfen, ob das erstellte Datensicherungskonzept mit den zur Verfügung stehenden Mechanismen auch umgesetzt werden kann. Anhand dieser Informationen kann ein Konzept für die Datensicherung der Datenbank erstellt werden. In diesem Sicherungskonzept wird u. a. festgelegt (siehe hierzu auch Kapitel 3.4 Datensicherungskonzept)

- wer für die ordnungsgemäße Durchführung von Datensicherungen zuständig ist
- in welchen Zeitabständen eine Datenbanksicherung durchgeführt wird,
- in welcher Art und Weise die Datenbanksicherung zu erfolgen hat,
- zu welchem Zeitpunkt die Datenbanksicherung durchgeführt wird,
- die Spezifikation des zu sichernden Datenvolumens je Sicherung.
- wie die Erstellung von Datensicherungen zu dokumentieren ist, und
- wo die Datensicherungsmedien aufbewahrt werden.

## Verpflichtung der Mitarbeiter zur Datensicherung

**Verantwortlich für Initiierung: Behörden-/Unternehmensleitung**

**Verantwortlich für Umsetzung: IT-Sicherheitsmanagement**

Da die Datensicherung eine wichtige IT-Sicherheitsmaßnahmen ist, sollten die betroffenen Mitarbeiter auf die Einhaltung des Datensicherungskonzeptes bzw. des Minimaldatensicherungskonzeptes verpflichtet werden. Eine regelmäßige Erinnerung und Motivation zur Datensicherung sollte erfolgen.

## Sicheres Löschen von Datenträgern

**Verantwortlich für Initiierung: Leiter IT**

**Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher**

Eine geregelte Vorgehensweise für die **Löschung** oder **Vernichtung** von Datenträgern verhindert einen Missbrauch der gespeicherten Daten. Bevor Datenträger wieder verwendet werden, müssen die gespeicherten Daten vollständig gelöscht werden, z. B. durch vollständiges Überschreiben oder Formatieren. Dies ist insbesondere wichtig, wenn Datenträger an Dritte weitergegeben werden sollen. Auch der Empfänger des Datenträgers muss nach dem Empfang prüfen, ob der Schutzwert der Daten ein sofortiges Löschen des Datenträgers erfordert, nachdem die Daten auf ein anderes IT-System übertragen wurden.

Es gibt verschiedene Methoden um Informationen auf Datenträgern zu löschen, z. B. über Löschkommandos, durch Formatieren, durch Überschreiben oder durch Zerstörung des Datenträgers. Welche Methode gewählt werden sollte, hängt hierbei auch vom Schutzbedarf der zu löschenden Daten ab, der Schutz gegen die Restaurierung von Restdaten steigt in der genannten Reihenfolge.

### Formatieren

Um Datenträger wieder in den "Urzustand" zu versetzen und damit auch vorhandene Informationen zu löschen, können diese formatiert werden. Wie zuverlässig dabei allerdings die alten Daten gelöscht werden, ist stark abhängig vom zu Grunde liegenden Betriebssystem. Ein Überschreiben der alten Daten ist auf jeden Fall zuverlässiger.

### Überschreiben

Eine für den mittleren Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der komplette Datenträger oder zumindest die genutzten Bereiche mit einem bestimmten Muster überschrieben werden. Es werden einige handelsübliche Produkte angeboten, die sogar die physikalische Löschung einzelner Dateien gewährleisten.

Zum Überschreiben sollten keine gleichförmigen Muster wie "0000" benutzt werden, sondern es sollten Muster wie "C1" (hexadezimal, entspricht der Bitfolge 11000001) benutzt werden. Dazu sollte bei einem zweiten Durchlauf ein dazu komplementäres Muster (also z. B. 3E, entspricht der Bitfolge 00111110) benutzt werden, damit möglichst jedes Bit einmal geändert wird.

Die Überschreibprozedur sollte daher mindestens zweimal, besser aber dreimal wiederholt werden, da hierdurch eine verbesserte Schutzwirkung erzielt wird.

Schreibgeschützte oder nicht mehrfach beschreibbare Datenträger wie DVD-Rs oder CD-Rs können selbstverständlich auch nicht gelöscht werden und sollten vernichtet werden.

### Löschgeräte

Flexible magnetische Datenträger können mit einem Löschgerät gelöscht werden. Dabei werden die Datenträger einem externen magnetischen Gleich- oder Wechselfeld ausgesetzt (Durchflutungslöschen). Geeignete Löschgeräte, die die Norm DIN 33858 erfüllen, sind in der BSI-Publikation 7500 aufgeführt.

Grundsätzlich sind die Datenträger nach dem Löschen wieder verwendbar. Es ist aber zu beachten, dass Datenträger mit einer magnetisch geschriebenen Servospur (z. B: Bandkassetten IBM 3590, Travan 4, MLR und ZIP-Disketten) nach einem Löschen unbrauchbar werden.

### Vernichtung der Datenträger

Eine einfache Möglichkeit, Datenträger zu vernichten, besteht darin, dass Disketten und Magnetbänder zerschnitten und Festplatten mechanisch zerstört werden. Dies ist allerdings zu umständlich bei größeren Mengen zu vernichtender Datenträger und auch nicht ausreichend bei höherem Schutzbedarf.

Geeignete Vernichtungsgeräte für Magnetbänder, Disketten und CD-ROMs, die der Norm DIN 32757 entsprechen, sind in der BSI-Publikation 7500 aufgeführt. Bei diesen Vernichtungsgeräten werden die Datenträger entweder zerkleinert oder eingeschmolzen. Vernichtungsgeräte für Festplatten sind nicht bekannt.

## Minimaldatensicherungskonzept

**Verantwortlich für Initiierung: IT-Sicherheitsmanagement**

**Verantwortlich für Umsetzung: IT-Sicherheitsmanagement**

Für ein Unternehmen/eine Behörde ist festzulegen, welche Minimalforderungen zur Datensicherung eingehalten werden müssen. Damit können viele Fälle, in denen eingehende Untersuchungen und die Erstellung eines Datensicherungskonzeptes zu aufwendig sind, pauschal behandelt werden. Weiterhin ist damit eine Grundlage gegeben, die generell für alle IT-Systeme gültig ist und auch für neue IT-Systeme, für die noch kein Datensicherungskonzept erarbeitet wurde.

Ein Beispiel soll dies erläutern:

## Minimaldatensicherungskonzept

**Software:**

Sämtliche Software, erworben oder selbst erstellt, ist einmalig mittels einer Vollsicherung zu sichern.

**Systemdaten:**

Systemdaten sind mindestens einmal monatlich mit einer Generation zu sichern.

**Anwendungsdaten:**

Alle Anwendungsdaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

**Protokolldaten:**

Sämtliche Protokolldaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

## Datensicherungskonzept

**Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement**

**Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen**

Der Verlust gespeicherter Daten kann erhebliche Auswirkungen auf den IT-Einsatz haben. Sind die Anwendungsdaten oder die Kundenstammdaten verloren oder verfälscht, so können privatwirtschaftliche Betriebe in ihrer Existenz bedroht sein. Der Verlust oder die Verfälschung wichtiger Dateien kann in Behörden Verwaltungs- und Fachaufgaben verzögern oder sogar ausschließen.

Dabei können die Gründe für den Verlust gespeicherter Daten vielfältiger Art sein:

- Entmagnetisierung von magnetischen Datenträgern durch Alterung oder durch ungeeignete Umfeldbedingungen (Temperatur, Luftfeuchte),
- Störung magnetischer Datenträger durch äußere Magnetfelder,
- Zerstörung von Datenträgern durch höhere Gewalt wie Feuer oder Wasser,
- versehentliches Löschen oder Überschreiben von Dateien,
- technisches Versagen von Peripheriespeichern (Headcrash),
- fehlerhafte Datenträger,
- unkontrollierte Veränderungen gespeicherter Daten (Integritätsverlust) und
- vorsätzliche Datenzerstörung durch Computer-Viren usw.

Zur Realisierung der Datensicherung ist es notwendig das Datensicherungskonzept anhand der in den Punkten 1-12 beschriebenen Vorgaben zur Erstellen.

## Inhaltsverzeichnis Datensicherungskonzept

***3. Einflussfaktoren je IT-System***

- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer

***4. Datensicherungsplan je IT-System***

4.1 Festlegungen je Datenart

- Art der Datensicherung
- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der Generationen
- Datensicherungsmedium
- Verantwortlichkeit für die Datensicherung
- Aufbewahrungsort der Backup-Datenträger
- Anforderungen an das Datensicherungsarchiv
- Transportmodalitäten
- Rekonstruktionszeiten bei vorhandener Datensicherung

4.2 Festlegung der Vorgehensweise bei der Datenrestaurierung

4.3 Randbedingungen für das Datensicherungsarchiv

- Vertragsgestaltung (bei externen Archiven)
- Refresh-Zyklen der Datensicherung
- Bestandsverzeichnis
- Löschen von Datensicherungen
- Vernichtung von unbrauchbaren Datenträgern

4.4 Vorhalten von arbeitsfähigen Lesegeräten

5. Minimaldatensicherungskonzept

6. Verpflichtung der Mitarbeiter zur Datensicherung

7. Sporadische Restaurierungsübungen

# Empfehlungen zur Datensicherung

Die hier zusammengestellten Informationen stellen eine Empfehlung zur Datensicherung der CGM Clinical Deutschland GmbH dar. Die Durchführung und der Betrieb der Datensicherung, sowie das Restore und Recovery obliegt dem Kunden.

## Domaincontroller

### Sicherung

z.B. Symantec Backup Exec mit Active Directory Agent verwenden

tägliche Voll-Sicherung inkl. Systemstate (beinhaltet Active Directory) und Registry ab 20:00 Uhr

Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

### Restore

Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal ( Wiederherstellung des kompletten Systems, sowie einzelne Dateien und Objekte des Active Directory)

### Recovery

Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

## File und Print Server

### Sicherung

z.B. Symantec Backup Exec Agent verwenden

tägliche Sicherung der Benutzerspezifischen Daten inkl. Systemstate und Registry ab 20:00 Uhr

wöchentliche Voll-Sicherung inkl. Systemstate und Registry oder nach Hardware-Änderung ab 20:00 Uhr

Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

### Restore

Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal ( Wiederherstellung des kompletten System, sowie einzelne Dateien )

### Recovery

Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

## Exchange Server

### Sicherung

z.B. Symantec Backup Exec Agent mit Granular Restore Technology verwenden

tägliche Voll-Sicherung inkl. Systemstate ab 22:00 Uhr

tägliche Sicherung der Exchange Datenbank ab 22:00 Uhr

Sicherung der Exchange Logfiles im 3 Stunden Zyklus

Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

### Restore

Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal ( Wiederherstellung des kompletten System, der Exchange Datenbanken, einzelner Postfächer und öffentlicher Ordner, sowie einzelne Dateien )

### Recovery

Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

## Oracle Server

### Sicherung

z.B. Symantec Backup Exec Agent für Oracle-DB und Betriebssystem verwenden

wöchentliche Voll-Sicherung inkl. Systemstate oder nach Hardware-Änderung ab 22:00 Uhr

tägliche Sicherung der Oracle Datenbank ab 22:00 Uhr

tägliche Sicherung der Logfiles 09:00 /12:00 / 18:00 Uhr oder nach Anforderung

Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

### Restore

Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal ( Wiederherstellung des kompletten System, der Oracle Datenbank, einzelner Datenbankfiles, sowie einzelne Dateien )

### Recovery

Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

## SQL Server

### Sicherung

z.B. Symantec Backup Exec Agent für SQL-DB und Betriebssystem verwenden

wöchentliche Voll-Sicherung inkl. Systemstate oder nach Hardware-Änderung ab 22:00 Uhr

tägliche Sicherung der SQL Datenbank ab 22:00 Uhr

tägliche Sicherung der Logfiles um 09:00 /12:00 / 18:00 Uhr oder nach Anforderung

Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

### Restore

Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal ( Wiederherstellung des kompletten System, der SQL Datenbank, einzelner Datenbankfiles, sowie einzelne Dateien )

### Recovery

Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

## Terminalserver

### Sicherung

z.B. Symantec Backup Exec Agent verwenden

tägliche Sicherung der Benutzerspezifischen Daten inkl. Systemstate und Registry ab 20:00 Uhr

wöchentliche Voll-Sicherung inkl. Systemstate und Registry ab 20:00 Uhr

Offline Sicherung einmal pro Quartal oder nach Hardware-Änderung

### Restore

Verifikation der Wiederherstellungsfähigkeit der Daten auf einem Testsystem einmal pro Quartal ( Wiederherstellung des kompletten System, sowie einzelne Dateien Recovery

Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

### Recovery

Verifikation der wiederhergestellten Daten auf Funktionsfähigkeit einmal pro Quartal

## Sicherungsjobs

Die Sicherungsjobs für die filebasierte Sicherung werden in einem Sicherungsjob zusammengefasst. Das heißt, alle Betriebssysteme werden in einem Job gesichert.

Für die Sicherung der Datenbanken ist jeweils ein separater Sicherungsjob zu erstellen.

Die angegebenen Zeiten stellen Empfehlungen dar und können je nach Kundensituation angepasst werden

**Werden bestimmte Server des Kunden im Outsourcing betreut wird die Sicherung dieser Server in separate Sicherungsjobs ausgegliedert. Es wird deshalb ein Sicherungsjob für die Outsourcing-Sever angelegt und ein weiterer für die Filesicherung der übrigen vom Kunden verwalteten Server.**

## Datenträgersätze

### Filesicherung

2 Wochensätze á 4 Bänder (Mo-Do)

4 Freitagsbänder

12 Monatsbänder

2 Bänder pro Server für Offline-Sicherung

### Datenbanken (Oracle, SQL)

**Datenbanksicherung + Logfilesicherung**

4 Wochensätze á 5 Bänder (Mo-Fr)

12 Monatsbänder

## Datenträgernutzung

Die Datenträger sind nach Maßgabe des Herstellers zu verwenden. Ein Austausch ist nach einem Jahr notwendig

Bitte hierzu auch die Hinweise zur Verwaltung und Nutzung der Datenträger in den Grundlagen Datensicherung der CGM Clinical Deutschland GmbH beachten.

| Server | Tägl. Voll | Wöchentl. Voll | Offline pro Quartal | Offline nach Hardware-Änderung | Datenbank | Logfiles 09:00 Uhr | Logfiles 12:00 Uhr | Logfiles 18:00 Uhr | Täglich Benutzerdaten |
|---|---|---|---|---|---|---|---|---|---|
| Domaincontroller | **X** | | **X** | **X** | **X** | | | | |
| File und Print | | **X** | **X** | **X** | | | | | **X** |
| Exchange | **X** | | **X** | **X** | **X** | | | | |
| Oracle | | **X** | **X** | **X** | **X** | **X** | **X** | **X** | |
| SQL | | **X** | **X** | **X** | **X** | **X** | **X** | **X** | |
| Terminalserver | | **X** | **X** | **X** | **X** | | | | **X** |