CGM Clinical Deutschland GmbH

Systeminformationen

Edition 2025-1

Synchronizing Healthcare

CompuGroup Medical

Inhaltsverzeichnis

Updateinformationen

Die Edition 2025-1 umfasst die in der folgenden Tabelle genannten Versionen. Beachten Sie bitte, dass die in der Spalte **Voraussetzungen** genannte Version bzw. Edition installiert sein muss, bevor Sie das Update auf die Edition 2025-1 durchführen können. **Support** und **Fehlerbehebungen** werden ausschließlich in den **Editionen 2024-1** und **2025-1** gewährleistet. Alle anderen Editionen werden nicht unterstützt.

Produkt	Versionen Edition 2025-1	Voraussetzungen
MACH RECHNUNGSWESEN	6.1.1	ab Edition 2024-1
MACH DMS FAME	6.1.1	ab Edition 2024-1
MACH RECHNUNGSEINGANG	6.1.1	ab Edition 2024-1
CGM SOZIAL TOPSOZ	9.12	ab Edition 2015-1
CGM SOZIAL DP	11.1	ab Edition 2015-1
CGM SOZIAL PEP	2.21	ab Edition 2015-1
CGM SOZIAL P&D	5.2	ab Edition 2015-1 (ab V4.0)
CGM SOZIAL P&D Mobile	2.7	Keine Einschränkung
CGM SOZIAL SIC	ab 4.0	ab Edition 2015-1
CGM SOZIAL SIC Mobile	2.6	Keine Einschränkung
CGM SOZIAL Datenschutz-Cockpit	1.26	ab Edition 2017-2
CGM SOZIAL InfoDesk	Ist mit allen freigegebenen Editionen der CGM SOZIAL Suite kompatibel.	
factis ambulant	3.18	Keine Einschränkung
factis für soziale Teilhabe	3.18	Keine Einschränkung

Mit der Edition 2025-1 sind folgende Partnerprodukte kompatibel:

Produkt	Version	Kommunikation mit/Verwendet von
mps All for public	6.1.1	MACH RECHNUNGSWESEN
WIN-EV	Version 2023 R7	MACH RECHNUNGSWESEN
DAKOTA	7.4 Build 2	CGM SOZIAL TOPSOZ
SD Worx fidelis.Personal	unabhängig	CGM SOZIAL DP CGM SOZIAL TOPSOZ MACH RECHNUNGSWESEN

Systemanforderungen

Hardwarevoraussetzungen 32/64 Bit

> **Hinweis:** Die in den Spalten **Empfohlen** genannten Hardwareanforderungen sind abhängig von der Anzahl der Clients sowie vom Datenvolumen.

Client

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp	**Thin Client:** Intel® Atom® oder AMD G-Serie **Fat Client:** Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7 oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher	mind. 4 GB	>= 6 GB
Netzwerkanbindung	1 Gbit/s	1 Gbit/s oder 10 Gbit/s
Bildschirmauflösung	1280x1024	1920x1080 (Full HD)

Anwendungsserver

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp	Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7, Xeon oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher	4 GB	>= 6 GB
Netzwerkanbindung	1 Gbit/s	1 Gbit/s oder 10 Gbit/s

Datenbank-Sizing

Bezeichnung	User-Anzahl
klein	Bis zu 20 User
mittel	Bis zu 100 User
groß	Ab 100 User

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

Datenbankserver (klein) (1- 20 User)

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp	Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7, Xeon oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher mit BI-Datenbank	8 GB 12 GB	16 GB 24 GB
Netzwerkanbindung	1 Gbit/s	1 Gbit/s oder 10 Gbit/s
Raid-Controller	Ja	Ja
Festplattenart	SAS mit 10K U/min	SAS mit 10K U/min oder SSD

Datenbankserver (mittel) (bis 100 User)

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp mit BI-Datenbank	Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7, Xeon oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher	24 GB	mind. 32 GB
Netzwerkanbindung	1 Gbit/s	10 Gbit/s
Festplattenart	SAS mit 10K U/min	SAS mit mind. 10K U/min oder SSD

Datenbankserver (groß) (ab 100 User)

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp mit BI-Datenbank	Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7, Xeon oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher	32 GB	mind. 48 GB
Netzwerkanbindung	1 Gbit/s	10 Gbit/s
Festplattenart	SAS mit 15k U/min	SSD

Datenbankserver Festplatten - Sizing

Die angegebenen Größen sind Richtwerte für Neuinstallationen. Bei Umzug eines Bestandssystems dürfen die Größen des Neusystems **nicht unter** denen des Altsystems liegen (Richtwert: jeweilige Partitionsgröße + 20%).

Laufwerksbuchstaben	Größe in GB	Virtuelle SCSI/SCSI ID
C:\ (System)	50	0:0
D:\ (App)	50	1:0
R:\ (SQL Recovery)	100	0:2
Q:\ (SQL TempDB)	50 - 100	1:0
S:\ (SQL Data)	50 - 100	2:0
T:\ (SQL T-Log)	76 - 150	3:0
P:\ (SQL OLAP) / nur BI	50	1:1

Laufwerk P:\ mit 32K Blockgröße formatieren

Laufwerke Q:\, R:\, S:\ und T:\ mit 64k Blockgröße formatieren

Webserver

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp	Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7, Xeon oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher	mind. 4 GB	>= 6 GB
Netzwerkanbindung	1 Gbit/s	1 Gbit/s oder 10 Gbit/s

Citrix- / Terminalserver

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp	Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7, Xeon oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher	16 GB abhängig von der Anzahl max. aktiver Benutzer	>= 24 GB abhängig von der Anzahl max. aktiver Benutzer
Netzwerkanbindung	1 Gbit/s	1 Gbit/s oder 10 Gbit/s

Hinweise zu Azure Umgebungen

Größen für virtuelle Windows Computer in Azure

Zweck	Größen	Beschreibung
Allgemeiner Zweck	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC	Ausgewogenes Verhältnis von CPU/RAM z.B. AD Server, oder Test Maschinen
Computeroptimiert	Fsv2	Hohes Verhältnis von CPU/RAM z.B. Webserver oder APP-Server
RAM-Optimiert	Esv3, Ev3, Easv4, Eav4, Mv2, M, DSv2, Dv2	Hohes Verhältnis von RAM zu CPU z.B. relationale DB Server
Speicheroptimiert	Lsv2	Hoher Datenträgerdurchsatz und E/A z.B. SQL und NoSQL DB \ Datawarehousing / Terminal Server
GPU	NC, NCv2, NCv3, ND usw.	Videobearbeitung und aufwendiges Grafikrendering
High Performance Comp.	HB, HC, H	Schnellsten und Leistungsfähigsten CPU

Konkrete Sizings und Informationen zu Azure werden gerne als DL angeboten.

G3-Anwendungsserver

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp	Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7, Xeon oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher	24 GB	32 GB
Netzwerkanbindung	1 Gbit/s	1 Gbit/s oder 10 Gbit/s

G3-Webserver

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp	Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7, Xeon oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher	8 GB	8 GB
Netzwerkanbindung	1 Gbit/s	1 Gbit/s oder 10 Gbit/s

Kommunikations-/Druckserver

Detail	Mindestvoraussetzung	Empfohlen
Prozessortyp	Intel® Celeron®, Pentium®, Core™ i3, AMD Athlon™ oder vergleichbarem Prozessor	Intel® Core™ i5, i7, Xeon oder vergleichbarem Prozessor
Taktfrequenz	2.7 GHz	3.2 GHz
Hauptspeicher	8 GB	8 GB
Netzwerkanbindung	1 Gbit/s	1 Gbit/s oder 10 Gbit/s

Die Prozessortyp-Angaben sind als Referenzwerte zu sehen. Es können auch 64bit-Prozessoren anderer Hersteller mit gleichwertigen Leistungsangaben gewählt werden. Itanium- oder Risc-Prozessoren werden nicht unterstützt.

Bei Kleinstinstallation (<= 8 Benutzer) können auch Rechner/Prozessoren mit geringerer Leistungsfähigkeit zum Einsatz kommen.

Übersicht der Betriebssystem- und Softwareanforderungen

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 unserer 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.

In der folgenden Tabelle sehen Sie die in der jeweiligen Edition gültigen Betriebssystem- bzw. Softwareanforderungen für die Produkte der Bereiche **CGM SOZIAL**, **mps Rechnungswesen** und **mps DMS**. Freigaben, Empfehlungen und Systemvoraussetzungen anderer Hersteller, deren Produkte ebenfalls auf dem Server installiert sind und die ggf. mit den CGM Clinical Produkten interagieren müssen ebenfalls beachtet werden.

Betriebssyteme / .Net-Framwork / Java

Bitte beachten Sie, dass Windows 10 und Windows 11 nicht als Anwendungs- oder Datenbankserver verwendet werden dürfen. Die Microsoft Server-Betriebssysteme sind als Anwendungs-, Datenbank- und Terminalserver wie angegeben freigegeben. Die Nutzung von Microsoft RemoteApps wird nicht unterstützt.

Betriebsystem	Edition 2023-1	Edition 2024-1	Edition 2025-1
Windows 10	freigegeben	freigegeben	abgekündigt
Windows 11	freigegeben	freigegeben	freigegeben
Windows Server 2016	freigegeben	freigegeben	freigegeben
Windows Server 2019	freigegeben	freigegeben	freigegeben
Windows Server 2022	freigegeben	freigegeben	freigegeben
Windows Server 2025	-	freigegeben	freigegeben
Android 5.0 und höher [1)]	freigegeben	freigegeben	freigegeben

[1)] Wird von CGM SOZIAL Mobile verwendet.

.Net Framework

Es wird das Microsoft .NET Framework 4.8.1 auf dem Anwendungsserver und den Clients benötigt.

Java

Oracle hat die Lizenzbedingungen für die kommerzielle Nutzung seiner Java Runtime Environment geändert. Aufgrund dieser Änderung unterstützen die Produkte der CGM Clinical Deutschland GmbH sowie die Produkte der mps solutions GmbH zukünftig auch OpenJDK.

Für den Offline-Schnittstellen-Converter wird Java Development Kit oder OpenJDK benötigt. Bei einem x64 Betriebssystem wird Java x64 SE 7 und Java x86 SE 7 benötigt.

Automatische Java-Updates können zu inkompatiblen Stammverzeichnissen und somit zu Systemstillständen führen. Eine vorherige Prüfung ist erforderlich.

Produktspezifische Anforderungen

- CGM SOZIAL
  - CGM SOZIAL P&D: Die Server- und Einzelplatzinstallation benötigt ein 64 Bit Betriebssystem. Der Client kann auf 32 und 64 Bit Betriebssystemen verwendet werden. Bei englischen bzw. nicht deutschen Serverinstallationen müssen die deutschen Sprachpakete installiert sein. Der P&D-Serverdienst muss mit einem lokalen Administratorkonto gestartet werden. Beim Benutzerkonto des P&D-Serverdienst wie auch bei allen anderen Benutzerkonten, muss Deutsch als Regionaleinstellung für Sprache und Formate verwendet wird. Falls Sie in der Schweiz oder Österreich ansässig sind, können Sie die länderspezifische Lokalisation verwenden.
    Ab dem 01.07.2025 setzt die das-pflege.de TLS 1.3 zur Übertragung der Indikatorenerhebung in der stationären Pflege voraus.
  - CGM SOZIAL P&D Mobile: Es werden die Microsoft Internet Information Services des jeweiligen Betriebssystems benötigt. Die Kommunikation von CGM Mobile und dem Synchronisierungsdienst zum Datenaustausch wird über https vorgenommen. Damit eine sichere Verbindung zustande kommt, benötigt der Server ein SSL-Zertifikat. Damit dieses ohne Probleme von der App akzeptiert wird, muss es von einer offiziellen Zertifizierungsstelle signiert sein.
  - CGM SOZIAL SIC Mobile: Es werden die Microsoft Internet Information Services des jeweiligen Betriebssystems benötigt. Die Kommunikation von SIC Mobile und dem Synchronisierungsdienst zum Datenaustausch wird über https vorgenommen. Damit eine sichere Verbindung zustande kommt, benötigt der Server ein SSL-Zertifikat. Damit dieses ohne Probleme von der App akzeptiert wird, muss es von einer offiziellen Zertifizierungsstelle signiert sein.
  - CGM SOZIAL InfoDesk: Es werden die Microsoft Internet Information Services des jeweiligen Betriebssystems benötigt.
- mps-solutions
  - mps DMS Rechnungseingang: Es werden die Microsoft Internet Information Services des jeweiligen Betriebssystems benötigt.

Datenbankmanagementsysteme

Datenbankmanagementsysteme	Edition 2023-1	Edition 2024-1	Edition 2025-1
Microsoft Datenbankmanagementsysteme			
SQL Server 2016 Standard / Enterprise	freigegeben	freigegeben	freigegeben
SQL Server 2017 Standard / Enterprise	freigegeben	freigegeben	freigegeben
SQL Server 2019 Standard / Enterprise [1)]	freigegeben	freigegeben	freigegeben
SQL Server 2022 Standard / Enterprise [1)]	freigegeben	freigegeben	freigegeben
SQL Server 2025	-	-	freigegeben
Microsoft OLEDB Treiber [3)]	freigegeben	freigegeben	freigegeben
Oracle Datenbankmanagementsysteme (Voraussetzung: Zeichensatz WE8MSWIN1252)			
Oracle 12c (12.1.0.1) [4)]	abgekündigt	-	-
Oracle 12c (12.2) [4)]	abgekündigt	-	-
Oracle 18c [4) 5)]	abgekündigt	-	-

Datenbankmanagementsysteme	Edition 2023-1	Edition 2024-1	Edition 2025-1
Oracle 19c [4) 5)]	freigegeben	freigegeben	freigegeben
Oracle 21c [4)]	freigegeben	freigegeben	freigegeben

[1)] Es wird nur die Windows Version des SQL Servers unterstützt, Linux Versionen nicht.

[2)] Wird auf dem Anwendungsserver und jedem Client benötigt.

[3)] Wird auf dem Anwendungsserver und jedem Client benötigt. Bitte verwenden Sie ab der **Edition 2020-1** den Microsoft OLEDB Treiber. Nach der Installation ist ein Neustart des Servers notwendig.

[4)] Ab der Edition 2023-1 sind die Produkte des Bereichs CGM SOZIAL nicht mehr für Oracle Datenbankmanagementsysteme freigegeben. Produkte der Bereiche mps Rechnungswesen und mps DMS sind weiterhin für Oracle freigegeben.

[5)] Oracle CDB (Containerdatenbank) wird nicht unterstützt.

Produktspezifische Anforderungen

- CGM SOZIAL
  - CGM SOZIAL TOPSOZ ist nicht für Oracle freigegeben.
  - CGM SOZIAL DP ist nicht für Oracle freigegeben.
  - CGM SOZIAL PEP ist nicht für Oracle freigegeben.
  - CGM SOZIAL SIC: Es muss der Oracle ODBC-Treiber verwendet werden.
  - CGM SOZIAL P&D ist nicht für Oracle freigegeben.
  - CGM SOZIAL OPAS ist nicht für Oracle freigegeben.
  - CGM SOZIAL InfoDesk ist nicht für Oracle freigegeben.
- mps-solutions
  - mps DMS Rechnungseingang: Für den Zugriff auf Oracle-Datenbanken muss Oracle Data Provider für .NET 4.0 (ODP.NET) installiert sein.

Citrix

Citrix	Edition 2023-1	Edition 2024-1	Edition 2025-1
Citrix XenApp 7.6	freigegeben	freigegeben	freigegeben
Citrix XenApp 7.15. / 7.18	freigegeben	freigegeben	freigegeben
Citrix Virtual Apps und Desktops 7 1912 LTSR	freigegeben	freigegeben	freigegeben
Citrix Virtual Apps und Desktops 7 2203 LTSR	freigegeben	freigegeben	freigegeben

Informationen zum Lebenszyklus der Citrix-Versionen: http://www.citrix.com/support/product-lifecycle

Microsoft Office

Microsoft Office Word bzw. Excel muss auf jedem Terminalserver bzw. Clientbetriebssystem **lokal installiert** werden. Sie können auch die lokale Installation von Office 365 nutzen. Die Onlineversion von Office 365 wird nicht unterstützt. Bitte beachten Sie, dass lediglich **32 Bit Versionen** der Office-Produkte unterstützt werden. Lediglich ab der Edition 2025-1 kann Office 2024 mit 64 Bit verwendet werden.

Um einen störungsfreien Betrieb sicherzustellen, empfehlen wir keinen Mischbetrieb bei den Office-Versionen. 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.

Microsoft Office	Edition 2023-1	Edition 2024-1	Edition 2025-1
Office 2013 32 Bit (Word / Excel)	freigegeben	abgekündigt	-
Office 2016 32 Bit (Word / Excel)	freigegeben	freigegeben	abgekündigt
Office 2019 32 Bit (Word / Excel) [1)]	freigegeben	freigegeben	abgekündigt
Office 2024 32 Bit / 64 Bit (Word / Excel)[2)]	-	-	freigegeben
Office LTSC 2021 32 Bit (Word / Excel) [1)]	freigegeben	freigegeben	freigegeben

[1)] Bitte beachten, dass Office 2019 durch Microsoft nur für Windows 10 sowie Windows Server 2019 freigegeben ist. Wir erteilen die Freigabe aktuell nur in Verbindung mit Windows 10, da unter Windows Server 2019 die Anzeige externer Ribbons im Word Menü unterdrückt wird.
[2)] In TOPSOZ kann Office 64 Bit erst nach Umstellung eines Parameters verwendet werden. Wenden Sie sich dazu bitte an unseren Support.

Browser

	Edition 2023-1	Edition 2024-1	Edition 2025-1
Microsoft Edge	freigegeben	freigegeben	freigegeben

Produktspezifische Anforderungen

- CGM SOZIAL InfoDesk: Ist nur für die Verwendung in Google Chrome freigegeben.

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 unserer 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.

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 1 Gbit/s bis zu den Arbeitsplätzen vorhanden sein. Bei der Verwendung von Terminalserverkonzepten sind je nach Ausbaustufe sog. BackBones von min. 1 Gbit/s bzw. 10 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 128Kbit pro Arbeitsplatz / Anwender des jeweiligen Standortes, 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 Server-Virtualisierung.

Beim Einsatz von virtuellen Umgebungen wie beispielsweise VMware, MS-HyperV 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

Für den Betrieb der CGM Clinical Anwendungen werden teilweise spezifische

- Dateifreigaben
- Registryeinträge
- Windowsbenutzer für COM+ bzw. Windows- Dienste
- DCOM-Einstellungen

benötigt. Die genauen Anforderungen erfahren Sie in den Installationsanleitungen des jeweiligen Produkts.

Windows-Systemberechtigungen

Allgemeine Anforderungen

Rubrik	Erläuterung
Domäne	Microsoft Windows Domäne muss im Einsatz sein
Service-User	Es muss ein Windows-Domänenuser für Windows/COM+ - Services vorhanden sein. 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 HKEY_CURRENT_USER\SOFTWARE\All for One\
Leserecht	HKEY_LOCAL_MACHINE HKEY_CLASSES_ROOT
Lese&Schreibrecht	HKEY_CURRENT_USER
Vollzugriff bei Installation	HKEY_LOCAL_MACHINE HKEY_CLASSES_ROOT

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

Securitylevel	Verzeichnis
Vollzugriff	User-Temp
Leserecht	<Freigabe>\Cobra\Resource\Forms (Anmelde-Dialog) <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$) <%systemroot%>\System32 Lokales Applikationsverzeichnis

Dateisystem/NTFS (CGM SOZIAL TOPSOZ)

Einstellungen	Verzeichnis	Benutzer	Berechtigung
Anwendungsserver			
Freigabe	TOPSOZ Installation > Custom	Jeder	Ändern / Lesen
Sicherheit	TOPSOZ Installation > Custom	Authentifizierte Benutzer	Ändern / Lesen, Ausführen / Ordnerinhalt anzeigen / Lesen / Schreiben
Terminalserver			
Sicherheit	TOPSOZ Installation > Custom	Authentifizierte Benutzer	Ändern / Lesen, Ausführen / Ordnerinhalt anzeigen / Lesen
Sicherheit	Temporäre Verzeichnisse der Windows Benutzer	Authentifizierte Benutzer	Ändern

Für eine Installation bzw. ein Update benötigt der Benutzer Administrationsrechte.

Dateisystem/NTFS (CGM SOZIAL DP)

Einstellungen	Verzeichnis	Benutzer	Berechtigung
Anwendungsserver			
Freigabe	Dienstplan Installation > VIPP	Jeder	Ändern / Lesen
Sicherheit	Dienstplan Installation > VIPP	Authentifizierte Benutzer	Ändern / Lesen, Ausführen / Ordnerinhalt anzeigen / Lesen / Schreiben

Für eine Installation bzw. ein Update benötigt der Benutzer Administrationsrechte.

Dateisystem/NTFS (CGM SOZIAL SIC)

Einstellungen	Verzeichnis	Benutzer	Berechtigung
Anwendungsserver			
Freigabe	SIC Server > SICPA	Jeder	Ändern / Lesen
Sicherheit	SIC Server > SICPA	Authentifizierte Benutzer	Ändern / Lesen, Ausführen / Ordnerinhalt anzeigen / Lesen / Schreiben
Terminalserver			
Sicherheit	SIC Client	Authentifizierte Benutzer	Ändern / Lesen, Ausführen / Ordnerinhalt anzeigen / Lesen / Schreiben
Sicherheit	Temporäre Verzeichnisse der Windows Benutzer	Authentifizierte Benutzer	Ändern

Für eine Installation bzw. ein Update benötigt der Benutzer Administrationsrechte.

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

Einstellungen	Verzeichnis	Benutzer	Berechtigung
Anwendungsserver			
Sicherheit	%ProgramData%\system.SOZIAL	Authentifizierte Benutzer	Ändern / Lesen, Ausführen / Ordnerinhalt anzeigen / Lesen / Schreiben
Terminalserver			
Sicherheit	P&D Client	Authentifizierte Benutzer	Ändern / Lesen, Ausführen / Ordnerinhalt anzeigen / Lesen / Schreiben
Sicherheit	C:\Users\<USER>\AppData\Local\AllForOne	Authentifizierte Benutzer	Ändern / Lesen, Ausführen / Ordnerinhalt anzeigen / Lesen / Schreiben

Für eine Installation bzw. ein Update benötigt der Benutzer Administrationsrechte.

Dienste

Rubrik	Erläuterung
mps Rechnungseingang	Der Dienst AppLink Connector Server benötigt lokale Adminrechte

Konfiguration der Datenbankmanagementsysteme

Einstellungen im MSSQL-Server

Bereich	Wert
Sprache	Deutsch
Dynamische Ports auf der Instanz	Deaktivieren, fixen Port einstellen

Sortierreihenfolge der Instanz

Die Instanz des Datenbankservers muss **German_PhoneBook_CS_AI_KS_WS** sein.

Sortierreihenfolge der Datenbanken

> **Hinweis:** Verwenden Sie **nicht** German_PhoneBook_100_CS_AI_KS_WS

Datenbank	Sortierreihenfolge
TOPSOZ[1]	German_PhoneBook_CI_AI_KS_WS
DPPEP	German_PhoneBook_CS_AI_KS_WS
EAI	German_PhoneBook_CS_AI_KS_WS
famaim	German_PhoneBook_CS_AI_KS_WS
SICPA	German_PhoneBook_CS_AI_KS_WS
cobra	German_PhoneBook_CS_AI_KS_WS
POFFICE	German_PhoneBook_CI_AI_KS_WS

[1] P&D wird in der TOPSOZ-Datenbank betrieben.

Datenbank-Benutzer

Der Datenbankname und Benutzer richtet sich nach dem jeweiligen Produkt. Der Benutzer muss immer die Rolle <db_owner> haben. Bei Einsatz von Cobra Applikationen muss ein Schema <cobra> in der Datenbank angelegt werden.

		Benutzer		
Produkt	**Name der Datenbank**	**Name**	**Standard-DB**	**Schema**
Cobra-Applikationen • mps RECHNUNGSWESEN • mps All for Public	cobra	cobra	master	cobra
mps DMS FAME in Verbindung mit anderen Cobra Applikationen	cobra	cobra	master	cobra
mps DMS FAME in Verbindung mit CGM SOZIAL TOPSOZ und/oder PO	fame	Cobra	master	cobra oder dbo
mps RECHNUNGSEINGANG	AppLink	AppLink		dbo
CGM SOZIAL DP (stationär)	DPPEP	DPPEP	DPPEP	dbo
CGM SOZIAL TOPSOZ, CGM SOZIAL PEP, CGM SOZIAL P&D und CGM SOZIAL DP	TOPSOZ	TOPSOZ	TOPSOZ	dbo
CGM SOZIAL SIC	SICPA	SICPA	master	dbo

Strukturierung der Festplatten

Laufwerksbuchstaben	Virtuelle SCSI/SCSI IDTyp	Blockgrößen
C:\ (System)	0:0	
D:\ (APP)	1:0	
R:\ (SQL Recovery)	0:2	64k
Q:\ (SQL TempDB)	1:1	64k
S:\ (SQL Data)	2:1	64k
T:\ (SQL T-Log)	3:1	64k

Überwachung der Leistungswerte

Zu dem Aufbau der Datenbankservers und der Konfiguration der Datenbank können nur Empfehlungen abgegeben werden. Nach der Inbetriebnahme liegt es in der Betreiberverantwortung den SQL-Server zu warten und für gute Leistungsdaten zu sorgen. Dafür gibt es wichtige Vitalwerte, die kontinuierlich überwacht werden sollten. Bei Abweichung sollten entsprechende Maßnahmen zur Verbesserung und zur Wiederherstellung der empfohlenen Werte durchgeführt werden.

PLE-Wert (Page-Life-Expectancy)

Der PLE-Wert ist in Bezug auf den Arbeitsspeicher einer der wichtigsten Werte. Er gibt an, wie lange eine Seite im Arbeitsspeicher der Instanz aufbewahrt werden kann. Der PLE wird in Sekunden, Minuten, Stunden und Tagen aus-

gegeben, dabei gilt, je höher dieser Wert, desto besser. Sehr gut: > 1-2 h Gut: > 30min - 1h Schlecht: < 1 - 30min Der PLE-Wert kann beispielsweise durch mehr RAM verbessert werden.

Zugriffszeiten auf Data & Logfiles

Wie lange beträgt die durchschnittliche Verzögerung von Lese- und Schreibvorgängen auf die Databzw. Logfiles. Die Empfehlung von Microsoft ist, dass bei den Datafiles ein Wert von 20 ms und bei den Logfiles ein Wert von 10 ms nicht überschritten werden sollte. In der Praxis ist es aber so, dass auch doppelt so hohe Verzögerungswerte als normal angesehen werden können.

Festgelegte Schwellwerte:

- Datafiles < 40ms
- Logfiles < 20ms

Anzahl VLF (Virtual Log Files)

Die Virtual Log Files Anzahl steigt je nachdem wie die "Auto_Growth" Werte und die Anfangsgröße der Transaktionsprotokolle konfiguriert sind. Um die Anzahl der Virtual Log Files möglichst gering zu halten, sollte man die Anfangsgröße groß wählen. Ein gut Wert für "Auto_Growth" wäre hierbei 1024MB oder 2048 MB. Eine Anfangsgröße sollte nie unter 10240 MB definiert werden.

Die Werte für VLF sollte pro Transaktionsprotokoll / je Datenbank den Wert 1000 nicht übersteigen.

I/O Latenz

Die Latenz sollte im laufenden Betrieb folgende Werte nicht überschreiten:

Typ Verbindung I/O-Latenz HDD Client-Server 15-20 ms HDD Lokal 2-5 ms SSD Client-Server 8-12 ms SSD Lokal < 1 ms Wenn diese Werte nicht erreicht beziehungsweise überschritten werden, sollte zum Beispiel der Virenscanner auf Ausnahmen geprüft werden, oder die Anzahl der Umdrehungen/min der Platte.

Typ	Verbindung	I/O-Latenz
HDD	Client-Server	15-20 ms
HDD	Lokal	2-5 ms
SSD	Client-Server	8-12 ms
SSD	Lokal	< 1 ms

Einstellungen in Oracle

Parameter & Werte

Bereich	Wert
Initialisierungsparameter	processes=300 OPEN_CURSORS=2048
Einstellungen zum Zeichensatz der Datenbank	WE8MSWIN1252
NLS_LANG	GERMAN_GERMANY. WE8MSWIN1252 zwingend notwendig am Oracle Client

Datenbankuser

Produkt	Benutzer
Cobra-Applikationen • mps RECHNUNGSWESEN • mps DMS FAME • mps All for Public	cobra
mps RECHNUNGSEINGANG	AppLink
CGM SOZIAL DP (stationär)	dppep
CGM SOZIAL TOPSOZ, CGM SOZIAL PEP und CGM SOZIAL DP	topsoz
CGM SOZIAL SIC	sicpa

Berechtigungen

Berechtigungen	Rechte
Rolle All41 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

Produktfamilienspezifische Anforderungen

mps RECHNUNGWESEN

Rechte	Hinweise
mps RECHNUNGSWESEN FS Elster-Modul	Für die Ausführung werden die „Visual C++ Redistributable Packages für Visual Studio 2017 x86 (32bit)“ benötigt. http://www.microsoft.com/de-de/download/details.aspx?id=40784 Vollzugriff auf <Freigabe>\Cobra\Apps\FS\Bin (MSAccess-DB, Temporärdateien, STADUEV0.UST, STADUEV0.UST.cry, STADUEV0.UST.cry.bes). Zusätzlich bei Terminalserverbetrieb auf dem Terminalserver: Vollzugriff auf ..\Cobra\Apps\FS\Bin (MSAccess-DB, Temporärdateien, STADUEV0.UST, STADUEV0.UST.cry, STADUEV0.UST.cry.bes).
mps RECHNUNGSWESEN FS Datei-Import	Create/Write/Read für Stammdaten, Bewegungsdaten von Vorsystemen Create/Write für Log-Dateien und –Ordner unterhalb des zu definierenden Importverzeichnisses
mps RECHNUNGSWESEN CP Datei-Import	Create/Write für Log-Dateien und –Ordner unterhalb des zu definierenden Importverzeichnisses.
mps RECHNUNGSWESEN AS Jahresabschluss	Create/Write/Read unter <Freigabe>\Cobra\Apps\AS\Database für Backup-Dateien und –Ordner
mps RECHNUNGSWESEN CP Kassenterminals	Hersteller der Kartenterminals: • Giesecke & Devrient: alle ZVT 700 - kompatiblen Geräte • Ingenico: alle ZVT 700 - kompatiblen Geräte; namentlich die ELITE - Produktreihe Provider und deren Terminals: • TeleCash: Giesecke & Devrient - Terminals. • InterCard: Inegnico - "Elite" - Terminals. Generell gilt 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.
mps RECHNUNGSWESEN CP Kassensicherung TSE (technische Sicherheitseinrichtung)	Hersteller der TSE (USB-Stick, (Mini-) SD-Karte) SWISSBIT Bitte beachten: • TSE muss an einem physikalischen Rechner eingesteckt werden / USB-Port oder entsprechender SD-Karteneinschub • TSE wird über eine Freigabe zur Verfügung gestellt, alle CP-User benötigen Schreib-/und Leserecht darauf. • Zugriff auf TSE muss dauerhaft gewährleistet sein, d.h. der Rechner mit-/incl. der Freigabe muss verfügbar sein, sobald mit CP gearbeitet wird.

mps RECHNUNGWESEN DS BI

Bereich	Hinweise
mps RECHNUNGWESEN DS BI	Für die Aufbereitung der Daten (Staging) ist mps RECHNUNGEWSEN DS erforderlich.
Benutzerberechtigung	Für die Steuerung der Berechtigungen in DS BI, wird die Windows Authentifizierung (Microsoft Active Directory) verwendet.
Voraussetzung bei Oracle Datenbanken	• Bei einer Konstellation BI-Server auf SQL Server x64 und mps RECHNUNGSWESEN DS auf einem Oracle Server ist auf dem SQL Server x64 der **32bit Oracle Client** zu installieren. • Auf dem SQL Server muss der Oracle OLE-DB Treiber installiert werden, sofern dieser nicht bereits durch eine vorhandene Oracle Clientinstallation verfügbar ist.

mps Rechnungseingang

Bereich	Hinweise
Spezifische Anforderungen	• Die Software wird als virtuelles Server-Image auf einer USB-Platte oder USB-Stick zur Verfügung gestellt (für VMWare, HyperV oder Citrix XenServer). • Das Image hat den Namen ´SmartDMSWF´. • Das Image muss mit einer Microsoft Standard/Enterprise oder Datacenter-Edition Lizenz aktiviert werden. • Das Image benötigt eine fixe IP-Adresse. • Für die Windows-Dienste ist ein eigener Dienste-Benutzer erforderlich. Gerne würden wir hier einen Benutzer mit dem Namen „dmsServices“ verwenden. • Für die Anbindung an den vorhandenen Oracle Datenbank-Server wird ein eigenes Schema in einer Oracle-Datenbank benötigt • 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 • IRISPowerscan9 ist unter Windows 10 nicht mehr freigegeben.
formcraft FCI Invoice (Rechnungsleser) ab Version 4.90.5	Systemvoraussetzungen, siehe Dokumentation: • EMC Captiva InputAccel Version 7.5 Release Notes • Server: mindestens Prozessor 2,4 GHz Pentium, 6 GB Arbeitsspeicher, 4 GB freier Plattenplatz • Client: unter einem 64bit System läuft der Client als 32bit Anwendung Kurzanleitung Installation FCI 5.0.22 & IA 7.6
Saperion Archivsoftware ab Version 7.5.6	Systemvoraussetzungen, siehe Dokumentation: SAPERION Technical Specifications Version 7.5.6

mps DMS FAME

Bereich	Hinweise
Verwendung von PDF-Vorlagen	Adobe PDF Reader ab Version 7
Modul Volltextdaten MODI	Microsoft Office Document Imaging (MODI) Komponente (ab Version 2007) Diese ist ab Office Version 2010 nicht mehr enthalten und muss deshalb von einer Vorgängerversion (Office 2007) installiert werden.
FAME STA Diktatplayer	Visual C++2012 Redistributable (32 bit) muss installiert sein.
Scanning	IRISPowerscan9 ist unter Windows 10 nicht mehr freigegeben.

Empfehlung für weitere Systeme (Test, Schulung, Entwicklung)

Neben dem Produktivsystem sind zusätzliche Systeme für die Schulung von Anwendern, das Testen von Aktualisierungen oder die Erarbeitung individueller Erweiterungen nützlich. Die Systemanforderungen für die zusätzlichen Systeme orientieren sich an den Systemanforderungen für das Produktivsystem. Diese sieht eine Abstufung in klein, mittel und groß vor, die der geringeren Anzahl an Benutzern, die Zugriff auf die Systeme haben und ggf. einer geringeren Menge an Daten Rechnung tragen. Konkrete Empfehlungen zum Sizing werden durch ein Feinkonzept erstellt.

Testsystem

Die CGM stellt durch umfangreiche Qualitätssicherungsmaßnahmen sicher, dass die Produkte möglichst fehlerfrei ausgeliefert werden. An vielen Stellen enthalten die Produkte allerdings kundenspezifische Inhalte und Prozesse (durch Customizing und spezielle Parametrisierung). Diese Inhalte können von der CGM nicht getestet werden und unterliegen deshalb der Verantwortung der Betreiber.

> **Hinweis:** Neue Versionen sollen in andere Systeme erst nach einer erfolgreichen Prüfung im Testsystem übernommen werden.

Aus diesem Grund, aber auch zur Risikominimierung empfehlen wir dringend den Betrieb eines Testsystems.

Ziele des Testsystems

- Test der Geschäftsprozesse anhand realer Testdaten
- Test von noch nicht beim Kunden im Einsatz befindlichen Funktionen und Modulen (Ersteinsatz)
- Integrationstests bei Schnittstellen zu externen Modulen
- Systemtests: Zwingend notwendig bei Servicepack Update und Releasewechsel des gesamten Systems gegen die kundenspezifischen Kernprozesse, um wirtschaftlichen oder Personenschaden zu verhindern. Das Einspielen von Servicepacks oder Releases im Produktivsystem darf erst nach erfolgreicher Freigabe des Testsystems erfolgen.
- Schulungen
- Fehleranalyse: Zur Reproduktion von Fehlern, um korrupte Daten zu vermeiden.

Inhalte eines Testsystems

Wir empfehlen das Testsystem inhaltlich **eng am Produktivsystem** zu halten, um die Tests mit möglichst realistischen Daten durchführen zu können. Deshalb sollte das Testsystem regelmäßig mit einer Datenbanksicherung aus dem Produktivsystem abgeglichen werden.

> **Hinweis:** Nach dem Abgleich des Testsystems aus dem Produktivsystem:
>
> - müssen ggf. Schnittstellen zu anderen Produkten angepasst werden. Es ist unbedingt zu vermeiden, dass das Testsystem mit anderen Produktivsystemen verbunden bleibt.
> - müssen ggf. Berechtigungen im Testsystem angepasst werden.

Schulungssystem

Mitarbeitende, denen der Umgang mit den Produkten oder neuen Modul vermittelt werden, benötigen ein System, um anhand von Vorgaben beispielhafte Problemstellungen zu bearbeiten. Dabei kann es sein, dass sich die Schulungsinhalte auf mehrere aufeinander aufbauende Schulungstage aufteilen. Ein explizit für Schulungen ausgelegtes System bildet die beste Voraussetzung für die störungsfreie Weiterbildung Ihrer Mitarbeitenden.

Wir weisen darauf hin, dass

- das Testsystem nicht für Schulungen geeignet ist, weil nicht vollständige geprüfte Neuerungen zu Problemen führen können und eventuell Rücksicherungen der Datenbank notwendig machen. Dabei würden

bereits eingegebene Schulungsinhalte verloren gehen. Außerdem kann das Einspielen von Servicepacks im Testsystem in Konflikt zu Schulungsterminen stehen.
- im Schulungssystem keine Echtdaten von Betreuten vorhanden sein sollen, um den Datenschutz zu gewährleisten. Das Schulungssystem soll deshalb keine Kopie des Produktivsystems sein. Es ist aber darauf zu achten, dass relevante Einstellungen dem Produktivsystem entsprechen.

Entwicklungssystem

Die Produkte der CGM Clinical ermöglichen es, individuelle Prozesse durch die Erstellung eigener oder Anpassung vorhandener Masken, Berichte und Auswertungen umzusetzen. Diese Anpassungen sollten in einem abgetrennten System entwickelt werden, um sie durch Datenbanksicherungen dediziert speichern zu können und ein vom Test- bzw. Schulungssystem unabhängiges Arbeiten zu ermöglichen (insbesondere eventuelle Rücksicherungen der Datenbank).

Die Arbeitsergebnisse können durch Export- und Importfunktionen in die anderen Systeme übertragen werden.

Drucken in Terminalserver Umgebungen

Das größte Problem beim Drucken in Terminalserverumgebungen stellt die mangelnde Unterstützung der Hersteller dar. Die Druckertreiber werden hauptsächlich für die Betriebssysteme Windows 10 / 11 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.

> **Hinweis:** 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
Kyocera	bei Kyocera gibt es sogenannte Classic Mini Treiber. 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 Achtung: den Mini-Treiber gibt es nicht für alle Druckertypen

Technische Hinweise zur Fernwartung bei CGM Clinical

Nachstehende Angaben haben Gültigkeit für die Produktbereiche:

- CGM SOZIAL
- CGM IT Design & Service

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

Zugangssoftware für Fernwartung

Um Ihnen bei Problemen schnell helfen zu können, verbinden sich unsere Hotline-Mitarbeiter mit der Fernwartungssoftware AnyDesk auf Ihre Rechner. Beachten Sie bitte, dass unsere Mitarbeiter diese Möglichkeit nur nutzen können, wenn eine gültige Vereinbarung zur Auftragsverarbeitung vorliegt.

> **Hinweis:** Unsere Supportmitarbeiter können sich nur auf die in den Produkten hinterlegten bzw. unter remotesupport.cgm.com verfügbaren AnyDesk-Versionen verbinden. Eine Verbindung mit Versionen, die direkt von anydesk.com heruntergeladen werden, kann nicht hergestellt werden.

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 freigeschaltet. 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.

Betreiberverantwortung

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 unterstützen Sie natürlich auch unsere IT-Spezialisten.

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, Archive-Filesystem)
- 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 Indizes)
- (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

Virenscanner-Administration

Inzwischen kommt es durch den Einsatz von Virenscanner auf den Serversystemen selbst als auch auf Virtualisierungsebene häufig zu Performance-Engpässen und Fehler in den Anwendungen z.B. durch das Sperren von Zugriffen auf Temporär-Dateien. Sollte dies der Fall sein prüfen Sie bitte Ihre Virenscanner-Einstellungen.

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

Servertyp	Reboot empfohlen	Warum
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

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

1. **Definitionen**
   - Anwendungsdaten, Systemdaten, Software, Protokolldaten
   - Vollsicherung, inkrementelle Datensicherung
2. **Gefährdungslage**
   - Abhängigkeit der Institution vom Datenbestand
   - Typische Gefährdungen wie ungeschulte Benutzer, gemeinsam genutzte Datenbestände, Computer-Viren, Hacker, Stromausfall, Festplattenfehler
   - Institutionsrelevante Schadensursachen
   - Schadensfälle im eigenen Haus
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
    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
    2. Festlegung der Vorgehensweise bei der Datenrestaurierung
    3. Randbedingungen für das Datensicherungsarchiv
        - Vertragsgestaltung (bei externen Archiven)
        - Refresh-Zyklen der Datensicherung
        - Bestandsverzeichnis
        - Löschen von Datensicherungen
        - Vernichtung von unbrauchbaren Datenträgern
    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. Veeam Backup

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. Veeam Backup

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. Veeam Backup

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. Veeam Backup oder Oracle RMAN Backup

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. Veeam Backup oder SQL Server Wartungspläne

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. Veeam Backup

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 Systems, 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. V-oll	Wöchentl. Voll	Offline pro Quartal	Offline nach Hardware-Änderung	Datenbank	Logfiles 9 Uhr	Logfiles 12 Uhr	Logfiles 18 Uhr	Tägl. Benutzerdaten
Domain-controller	X		X	X	X				
File und Print		X	X	X					X
Exchenage	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

Kontakt

CGM Clinical Deutschland GmbH
Unixstraße 1, 88436 Oberessendorf
T +49 (0) 7355 799-0
F +49 (0) 7355 799-111

www.cgm-clinical.de
www.cgm.com/de