CGM ALBIS

Arztinformationssystem

CGM ALBIS

Systemanforderungen

Synchronizing Healthcare

CompuGroup Medical

INHALT

1 Allgemeine Informationen für den Betrieb 5
1.1 Einzelplatzumgebung: CGM ALBIS 5
1.2 Mehrplatzumgebung: CGM ALBIS.YOU 5
2 Hardware-Anforderungen 6
2.1 Server CGM ALBIS/ CGM ALBIS.YOU 6
2.1.1 Mindestanforderungen 6
2.1.2 Empfohlene Hardware: 6
2.2 Arbeitsplatz-Computer CGM ALBIS/ CGM ALBIS.YOU 7
2.2.1 Mindestanforderungen 7
2.2.2 Empfohlene Hardware: 7
2.3 Arbeitsplatz- Monitor 8
2.3.1 Mindestanforderungen 8
2.3.2 Empfohlene Monitorunterstützung 8
2.4 Ausfallsicherheit 8
2.4.1 Unterbrechungsfreie Stromversorgung (USV) 8
2.4.2 Redundante Netzteile 8
2.4.3 RAID-Controller 8
3 Netzwerk 9
3.1 Internetanbindung (DSL) - Router 9
3.1.1 Mindestanforderungen 9
3.1.2 Empfohlene Anbindung 9
3.2 Netzwerk (LAN) 9
3.3 Verkabelung / Architektur 10
3.3.1 Terminal-Server-Betrieb 10
3.4 Außenstellenanbindung - Virtual Private Network (VPN) 10
3.4.1 Heimplatzanbindung 10
3.4.2 Verbindung zweier Netze (LAN-LAN-Kopplung) 10
3.5 Mobile Devices 11
3.5.1 Tablet 11
3.5.2 Smartphone 11
4 Geräte-Anbindung 12
4.1 MPG – Medizinproduktegesetz 12
4.2 Barcode-Leser für den „Bundeseinheitlichen Medikationsplan“/ Modul „CGM BMP PLUS“ 12
5 Betriebssysteme 13
5.1.1 Server 13
5.1.2 Arbeitsstationen 13
6 Konfiguration 14

6.1 Festplatten-Partitionen 14
6.1.1 Server 14
6.1.2 Arbeitsplatz 14
6.2 Virtualisierung 14
6.2.1 VmWare 14
6.2.2 Hyper-V 14
6.3 Netzwerkkonfiguration 15
6.3.1 TCP/IP Adressierung 15
6.3.2 Portfreischaltungen 15
6.3.3 Ports der Dienste & Firewall Nutzung 16
7 Installation 18
7.1 Rechnernamen 18
7.2 Domäne 18
7.3 Freigaben (Verzeichnisse) 18
7.4 Umgebungsvariablen 18
7.5 Dienste / Services 18
7.6 Datenbank 18
7.7 Virenschutz 19
7.8 Software und Betriebssystem Aktualisierungen 19
7.9 Server-Einstellungen 19
7.10 Arbeitsplatz-Einstellungen 19
7.11 Betriebssystem-Einstellungen 19
7.12 Standard-Software 20
7.13 Office-Anwendungen 20
7.14 Online Update(s) 20
7.15 Fernwartung 20
8 Datensicherung 21
9 CGM PRAXISARCHIV 21
10 Datensicherheit 21
10.1 Verschlüsselung 21
11 Einrichtung spezifischer Software 21
12 IT Sicherheit 22
12.1 Allgemeine Empfehlungen zur IT-Sicherheit 22
12.2 Betriebssysteme 23
12.3 Firewall- und Port-Einstellungen 23
12.4 Besondere Module zur IT-Sicherheit der CompuGroup 23
12.5 Externe Softwarelösungen 24
12.6 Schlussfolgerung 24

13 Hinweis zu Abweichungen von der Systemanforderungen 25
14 Änderungshistorie..... 26

1 Allgemeine Informationen für den Betrieb

Um in einer optimalen Umgebung die reibungslose Funktionalität des Arztinformationssystem CGM ALBIS zu gewährleisten sind in diesem Dokument Systemanforderungen als Empfehlung & Richtwert beschrieben.

Wir definieren eine „optimale Umgebung“ folgendermaßen: Das Netzwerk, in dem CGM ALBIS inkl. aller dazu notwendigen Komponenten betrieben wird, ist professionell und mit maximalem Datendurchsatz mit professionellen Komponenten ausgestattet und die Funktionsfähigkeit und Netzwerkgeschwindigkeit wurde durch einen Netzwerk-Fachmann schriftlich bestätigt und wird regelmäßig professionell gewartet.

Bei den Computerprogrammen CGM ALBIS und CGM ALBIS.YOU handelt es sich um Software, die stets durch einen zertifizierten CGM ALBIS Vertriebs- und Servicepartner zu installieren ist. Änderungen an der Infrastruktur werden ausschließlich vom Fachmann vorgenommen. Ebenfalls wird professionelle Hardware und professionell eingerichtete Betriebssystem verwendet und regelmäßig gewartet. Liegen diese Voraussetzungen nicht vor, so kann durch die im Folgenden beschriebenen Systemvoraussetzungen die reibungslose Funktionalität nicht gewährleistet werden.

Bitte beachten Sie, dass sich die Systemanforderungen lediglich auf CGM ALBIS, CGM ALBIS.YOU und alle mit CGM ALBIS und CGM ALBIS.YOU mitgelieferten Komponenten (inkl. Betriebssystem) bezieht.

Jede weitere installierte Software erhöht die Systemanforderungen des gesamten Systems.

Bitte beachten Sie, dass Software einen stetigen Wandel unterliegt und somit eine ständige Wartung notwendig macht. Siehe dazu Kapitel: 7.8.

1.1 Einzelplatzumgebung: CGM ALBIS

In Einzelplatzumgebungen stellen wir Ihnen CGM ALBIS zur Verfügung, dass für den Einsatz auf dedizierten Rechnern programmiert und optimiert wurde.

1.2 Mehrplatzumgebung: CGM ALBIS.YOU

In Mehrplatzumgebungen/Netzwerkumgebungen stellen wir Ihnen die „Client-Server (CS)“ Variante /Netzwerkversion zur Verfügung. Diese Funktionalität wurde unter den Handelsnamen „Client-Server (CS)“ und „XXL“ vertrieben. Die Netzwerkversion ist zudem Bestandteil von CGM ALBIS.YOU.

CGM ALBIS.YOU verfügt über einen Datenbankserver, der alle Zugriffe koordiniert und verwaltet. Der Datenbankserver (CS) sorgt für die notwendige Datenintegrität innerhalb der Netzwerkumgebung des Betriebssystems und sorgt für eine sichere Verbindung.

In einer Mehrplatzumgebung, welche aus mindestens einem Server und mehr als einem Arbeitsplatz besteht, ist die hier beschriebene Installationsvariante zu wählen.

2 Hardware-Anforderungen

In dem Dokument sind jeweils minimale und empfohlene Systemanforderungen beschrieben.

Die minimale Systemanforderungen stellt die untere Grenze für ein lauffähiges System dar. Die Systemanforderungen unterliegen stark dem Nutzungsgrad in der jeweiligen Installationsumgebung und sind demnach anzupassen und zu dimensionieren.

Aus diesem Grund verweisen wir hier auf die empfohlenen Systemanforderungen, und raten Ihnen diese Variante einzusetzen, damit ein performantes Arbeiten in der Praxis mit CGM ALBIS ermöglicht wird.

Ebenfalls empfehlen wir das der Server nicht zusätzlich als Arbeitsplatz verwendet wird.

2.1 Server CGM ALBIS/ CGM ALBIS.YOU

2.1.1 Mindestanforderungen

- *Prozessor (CPU): Quad Core 2,5 GHz vergleichbarer Serverprozessor*
- *Arbeitsspeicher (RAM): 8 GB*
- *Festplatte (HD): 500 GB, SATA 600*
- *Grafikkarte/Monitor: Grafikkarte/Monitor: keine Anforderungen, wenn nicht am Server gearbeitet wird. Siehe Arbeitsplatz, falls am Server gearbeitet wird.*
- *Netzwerkverbindung mit 1 Gbit/s*

WICHTIG: Ausgeschlossen sind folgende Prozessoren: Intel Atom, Intel Celeron und vergleichbare AMD-Prozessoren, wie z.B. Sempron oder vergleichbare Prozessoren.

WICHTIG: Bei Terminal-Server-Betrieb sind der RAM-Speicher und das Gesamtsystem entsprechend größer zu dimensionieren. Bitte beachten sie hierzu die Details im Kapitel 3.3.1

2.1.2 Empfohlene Hardware:

- *Prozessor (CPU): Intel Xeon Quad Core 3GHz oder vergleichbarer Serverprozessor*
- *Arbeitsspeicher (RAM): 16 GB*
- *Festplatte (HD): 1 TB SSD, SAS- oder SSD-Festplatten mit automatischer Spiegelung Empfehlung Anbindung min. PCIe x16*
- *Grafikkarte/Monitor: Grafikkarte/Monitor: keine Anforderungen, wenn nicht am Server gearbeitet wird. Siehe Arbeitsplatz, falls am Server gearbeitet wird.*
- *Netzwerkverbindung mit 1 Gbit/s*
- *DVD-Laufwerk (optional)*

WICHTIG: Bei Terminal-Server-Betrieb sind der RAM-Speicher und das Gesamtsystem entsprechend größer zu dimensionieren. Bitte beachten sie hierzu die Details im Kapitel 3.3.1

Installations-/Update-Empfehlung:

- Freie Festplattenkapazität von mindestens 40 GB

2.2 Arbeitsplatz-Computer CGM ALBIS/ CGM ALBIS.YOU

2.2.1 Mindestanforderungen

- *Prozessor (CPU): Intel Core i3 3 GHz oder vergleichbar*
- *Arbeitsspeicher (RAM): 8 GB*
- *Festplatte (HD): 100 GB*
- *Grafikkarte (GPU): Intel HD 4000 mit 512 MB*
- *Monitor: Auflösung 1024x768 mit 60Hz oder höhere Auflösung (min. 17 Zoll)*
- *Netzwerkverbindung mit 100 Mbit/s*

WICHTIG: Ausgeschlossen sind folgende Prozessoren: Intel Atom, Intel Celeron und vergleichbare AMD Prozessoren, wie z.B. Sempron oder vergleichbare Prozessoren.

2.2.2 Empfohlene Hardware:

- *Prozessor (CPU): Intel Core i5/i7 3 GHz oder vergleichbar*
- *Arbeitsspeicher (RAM): 16 GB*
- *Festplatte (HD): 200 GB SSD*
- *Grafikkarte: dedizierte Grafikkarte mit mind. 1GB RAM*
- *Monitor: 22“ 1920x1080, 60Hz, im Format 16:10 oder 16:9*
- *Netzwerkverbindung mit 1 Gbit/s*
- *DVD-Laufwerk*

Installations-/Update-Empfehlung:

- Freie Festplattenkapazität von mindestens 20 GB

2.3 Arbeitsplatz- Monitor

2.3.1 Mindestanforderungen

Gemäß der derzeit gültigen Bildschirmarbeitsverordnung (BildscharbV) sind für Arbeitsplätze eine Bildschirmgröße (Diagonale) von mindestens 17" (Bildschirmauflösung 1024 x 768) vorgegeben. Monitore mit einer größeren Bildschirmdiagonale sowie einer höheren Bildschirmauflösung sind empfehlenswert.

2.3.2 Empfohlene Monitorunterstützung

Wir empfehlen den Einsatz von 24" Monitoren mit einer Bildschirmauflösung von 1920x1080.

2.4 Ausfallsicherheit

2.4.1 Unterbrechungsfreie Stromversorgung (USV)

Für einen Server ist der Einsatz einer „Unterbrechungsfreien Stromversorgung“ dringend empfohlen. Diese Geräte schützen den Server vor Spannungsspitzen im Stromnetz und wirken einem plötzlichen Stromausfall entgegen, indem die Stromversorgung für einen begrenzten Zeitraum über Akkus sichergestellt wird. Die Steuerungsinformationen der USV müssen an den Server weitergeleitet werden. Bei Fragen wenden Sie sich bitte an Ihren CGM ALBIS Vertriebs- und Servicepartner.

2.4.2 Redundante Netzteile

Je nach ihren Anforderungen an die Ausfallsicherheit ihr Systems kann es erforderlich sein, dass redundante Netzteile in ihrem Server verbaut sind. Diese Maßnahme ist optional und daher empfehlen wir hierzu, dass sie sich bei Fragen mit ihrem CGM ALBIS Vertriebs- und Servicepartner in Verbindung setzen.

2.4.3 RAID-Controller

Wir empfehlen auf Server Betriebssystem den Einsatz von RAID-Controllern mit einer entsprechenden Spiegelung. Bitte setzen sie sich hierzu mit ihrem CGM ALBIS Vertriebs- und Servicepartner in Verbindung.

3 Netzwerk

3.1 Internetanbindung (DSL) - Router

Für Funktionen wie z. B. Fernwartung, CGM CONNECT, ClickDoc, Online-Update, Windows- und Virenschutz-Updates sowie weitere Online-Dienste sind eine sichere Internetverbindung und ein dafür ausgelegter Router erforderlich.

Wenn individuell weitere Onlineanwendungen mit CGM ALBIS genutzt werden sollen, ist die benötigte Bandbreite von der Art und Anzahl der Onlineanwendungen abhängig.

3.1.1 Mindestanforderungen

Für das reibungslose Übertragen von Daten (Senden und Empfangen) wird eine Übertragungsrate von mindestens 6 Mbit/s benötigt.

3.1.2 Empfohlene Anbindung

Wir empfehlen für den Einsatz auch zu Zwecken des Supports eine Übertragungsrate von mindestens 16 Mbit/s.

3.2 Netzwerk (LAN)

Es wird empfohlen eine Gbit Netzwerkverkabelung zu nutzen. Von der Nutzung eines WLAN zur Anbindung von CGM ALBIS Arbeitsplätzen wird abgeraten. Sollte dies dennoch gewünscht sein, muss dies in Absprache mit dem zuständigen Vertriebs- und Servicepartner erfolgen.

3.3 Verkabelung / Architektur

3.3.1 Terminal-Server-Betrieb

CGM ALBIS ist im Terminal-Server-Betrieb funktionsfähig.

Bei der Ermittlung der passenden Server-Hardware muss der Arbeitsspeicher, die Prozessoren und die im Server vorhandene Grafikkarte ausreichend dimensioniert werden. Wir empfehlen insbesondere 6 GB RAM pro Benutzer auf dem Terminalserver einzuplanen.

Da diese Dimensionierung des Terminal-Servers stark abhängig von der zukünftig gewählten Praxis- und Arbeitsplatzkonfiguration ist, sollte die Abstimmung und Auswahl der passenden Hardware mit dem CGM ALBIS Vertriebs- und Servicepartner durchgeführt werden.

WICHTIG: Im Terminal-Server-Betrieb muss sichergestellt sein, dass die lokalen Arbeitsverzeichnisse für den CGM ALBIS Benutzer immer identisch und im Schreib- & Lesezugriff sind. Ein lokales Arbeitsverzeichnis darf nicht auf einem Netzlaufwerk liegen, da hier schnelle und auch stabile Schreib- & Lesezugriffe notwendig sind.

3.4 Außenstellenanbindung - Virtual Private Network (VPN)

3.4.1 Heimplatzanbindung

Zur stationären Heimplatzanbindung empfehlen wir einen verschlüsselten Remote Desktop-Zugang (RDP).

Der Praxis-Server benötigt dazu einen dauerhaft aktiven, leistungsfähigen DSL-Anschluss. Für die Dimensionierung setzen sie sich bitte mit unserm CGM ALBIS Vertriebs- und Servicepartner in Verbindung.

3.4.2 Verbindung zweier Netze (LAN-LAN-Kopplung)

Zur Außenstellenanbindung wird beidseitig mindestens ein DSL mit fester IP-Adresse oder einer Standleitung empfohlen. Der jeweilige Anschluss sollte mit der Option „Fast Path“ geschaltet sein, um eine möglichst geringe Latenzzeit zu erhalten.

Die tatsächlich benötigte Bandbreite ist abhängig von Größe und Nutzen der Außenstelle.

Für die Dimensionierung setzen sie sich bitte mit unserm CGM ALBIS Vertriebs- und Servicepartner in Verbindung.

3.5 Mobile Devices

3.5.1 Tablet

Für eine mobile Nutzung von CGM ALBIS wurde CGM ALBIS MOBIL entwickelt.
Diese steht in den jeweiligen App-Stores zur Verfügung. Nähere Information entnehmen Sie bitte der Beschreibung des jeweiligen Stores. Bei Fragen wenden Sie sich bitte an Ihren CGM ALBIS Vertriebs- und Servicepartner.

3.5.2 Smartphone

Für eine mobile Nutzung von CGM ALBIS wurde CGM ALBIS MOBIL entwickelt.
Diese steht in den jeweiligen App-Stores zur Verfügung. Nähere Information entnehmen Sie bitte der Beschreibung des jeweiligen Stores. Bei Fragen wenden Sie sich bitte an Ihren CGM ALBIS Vertriebs- und Servicepartner.

4 Geräte-Anbindung

4.1 MPG – Medizinproduktegesetz

Sämtliche Computerarbeitsplätze, die an ein Medizinprodukt angeschlossen sind und somit einen direkten Patientenkontakt haben (z. B. Audiometer, EKG, EEG, Lungenfunktion, Sonographie-Geräte, Endoskopie-Gerät, Perimeter, Phoropter und viele weitere), müssen der DIN-Norm EN 60601-1 entsprechen.

4.2 Barcode-Leser für den „Bundeseinheitlichen Medikationsplan“/ Modul „CGM BMP PLUS“

Für das Einlesen des Barcodes auf dem Bundeseinheitlichen Medikationsplan werden das Modul „CGM BMP Plus“ (dieses muss freigeschaltet werden) und ein sog. - speziell konfigurierter - Barcode-Leser benötigt.

Aufgrund der speziellen Anforderungen sind derzeit ausschließlich über CGM ALBIS bezogen und vorkonfigurierte Barcode-Leser der Marken Zebra und germangelematics verifiziert und zugelassen:

- *Barcode-Leser Zebra DS4801 2D USB*
- *Barcode-Leser BT Zebra DS6878-HC 2D*
- *Barcode-Leser germantelematics GT52 USB*
- *Barcode-Leser germantelematics GT62 BT*

Die Geräte von germantelematics sind über den autorisierten CGM ALBIS Vertriebs- und Servicepartner zu beziehen.

5 Betriebssysteme

CGM ALBIS ist für die unten folgenden Betriebssysteme für Windows-kompatible Computer geprüft und zugelassen.

Für erhöhte Sicherheit und optimale Leistung empfehlen wir die Verwendung eines gehärteten Betriebssystems beim Betrieb von CGM ALBIS.
Bitte beziehen Sie sich auf die offiziellen Microsoft-Richtlinien zur Betriebssystem-Härtung: Leitfaden zu Sicherheitsbaselines | Microsoft Learn

WICHTIG: In Mehrplatzanlagen/Netzwerkumgebungen empfehlen wir den Einsatz eines Server Betriebssystems.

5.1.1 Server

- *Microsoft Windows Server 2022 (Essentials, Standard, Datacenter)*
- *Microsoft Windows Server 2019 (Essentials, Standard, Datacenter)*
- *Microsoft Windows Server 2016 (Essentials, Standard, Datacenter)*

Allgemein verweisen wir bei Abkündigungen auf die offizielle Liste, der von Microsoft unterstützen Betriebssysteme. Diese finden Sie unter folgendem Link
Windows 10 - release Information | Microsoft Docs

5.1.2 Arbeitsstationen

- *Windows 11 22H2 oder neuer*
- *Windows 10 Professional 22H2, deutsche Version, 64-Bit*

Allgemein verweisen wir bei Abkündigungen auf die offizielle Liste, der von Microsoft unterstützen Betriebssysteme. Alle zugelassenen Betriebssysteme werden bis zum Ablaufen des „Extended Support“ von Microsoft unterstützt. *Siehe dazu:* http://support.microsoft.com/gp/lifeselectindex

Für den Einsatz auf vernetzten Arbeitsplätzen, insbesondere mit dem Betriebssystem ab Windows 10, ist die Netzwerkversion erforderlich. Diese Version wurde unter den Handelsnamen „Client-Server (CS)“ und „XXL“ vertrieben. Die Netzwerkversion ist zudem Bestandteil von CGM ALBIS.YOU.

Service-Pack
Anlehnend an die Aussage von Microsoft endet der Support eines Service Packs 24 Monate nach Erscheinen der nächsten Service Pack-Version.

6 Konfiguration

6.1 Festplatten-Partitionen

6.1.1 Server

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

6.1.2 Arbeitsplatz

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

6.2 Virtualisierung

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

6.2.1 VmWare

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

6.2.2 Hyper-V

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

6.3 Netzwerkkonfiguration

6.3.1 TCP/IP Adressierung

Der Praxis Server muss über eine korrekte Namensauflösung und via IPv4-Adresse erreichbar sein.

Alle CGM ALBIS-Arbeitsplätze müssen für den laufenden Betrieb - über Netzwerk Ports - auf dem zentralen Rechner installierte Dienste erreichen. Siehe dazu Kapitel 6.3.3 Ports der Dienste & Firewall-Nutzung. Ebenfalls sind die Netzwerkfreigaben via SMB auf den zentralen Rechner zu aktivieren.

Alle weiteren Einrichtungen sollten individuell durch den CGM ALBIS Vertriebs- und Servicepartner eingeschätzt werden.

6.3.2 Portfreischaltungen

Weitere Ports für Onlineanwendungen werden bei Bedarf individuell durch den zuständigen CGM ALBIS Vertriebs- und Servicepartner freigegeben.

6.3.3 Ports der Dienste & Firewall Nutzung

Ebenfalls müssen verschiedene Dienste auf dem Hauptrechner der Praxis zum Betrieb von ALBIS erreichbar und von jedem Arbeitsplatz der Praxis ansprechbar sein.

CGM ALBIS.YOU	**TCP/IP Port: 30004**
Codebase Server	**TCP/IP Port: 23165**
PostgreSQL	**TCP/IP Port: 5432** Der Dienst wird als *CGM_ALBIS_(xxxx)* unter den Windows-Diensten geführt. In Klammern steht die Portnummer.
ALBIS Service	**TCP/IP FrontendService Port: 5610** **TCP/IP Frontend Port: 5611** **TCP/IP Backend Port: 5612** **TCP/IP BackendService Port: 5613** Der Dienst wird als *CGM_ALBIS_BACKGROUND_SERVICE_(xxxx)* unter den Windows-Diensten geführt. In Klammern steht die Portnummer des FrontendService.
KIM Dienst	**TCP/IP Port: 8995** **TCP/IP Port: 8465** Der Dienst wird als *CGM_KIM_ClientModule_(xxxx)* unter den Windows-Diensten geführt. **HINWEIS:** In Klammern steht die ALBIS Instanz-Nummer in der Global Ini vorgegeben wird.
Smart Update Dienst	**TCP/IP Port: 47842** Der Dienst wird als *CGM_ALBIS_SMARTUPDATE_SERVICE* unter den Windows-Diensten geführt. Beim Smartupdate Service gibt es nur eine Installation pro Rechner.
EPA	**TCP/IP Port: 60120** Bei der Vergabe des Ports muss sichergestellt sein, dass dieser frei und somit für den ePA Dienst verwendet werden kann. Der Dienst wird als *CGM_ePA_Service _(xxxx)* unter den Windows-Diensten geführt. In Klammern steht die Portnummer.
eHIMI	**Praxisintern** **TCP / IP Port:** 47841 & 47843 **Internetkommunikation:** **TCP / IP Port 443 für:** URLs des Dienstleisters (CGI Deutschland B.V. & Co. KG):

	https://keycloak.health-service.cloud https://providers.health-service.cloud https://patients.health-service.cloud https://prescription.health-service.cloud https://routing.health-service.cloud

HINWEIS: Bei der Erstinstallation der Services (ALBIS Service, PostgreSQL) prüft die Setup-Routine ob der jeweilige Port frei und verwendet werden kann. Daher können die Porteinstellung abweichen und sind bei Bedarf jeweils an die Umgebung in der Praxis anzupassen.

WICHTIG: Bei den anderen Diensten müssen die Ports jeweils individuell freigegeben und dafür konfiguriert werden. Wir empfehlen den Einsatz einer Firewall am Server mit einer angemessenen Konfiguration.

7 Installation

7.1 Rechnernamen

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

7.2 Domäne

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

7.3 Freigaben (Verzeichnisse)

Die Berechtigungen der Verzeichnisfreigabe muss so eingestellt werden, dass der Windowsbenutzer, der mit CGM ALBIS arbeitet, immer Schreib- und Leserechte hat.

Dies muss für alle Verzeichnisse und Dateien des CGM ALBIS Serververzeichnisses sichergestellt sein.

WICHTIG: Auf der Netzwerkfreigabe liegt die Applikation und relevanten Anwendungsspezifische Daten durch das Betriebssystem und auch Netzwerk muss sichergestellt sein, dass diese Verbindung im laufenden Betrieb nicht unterbrochen wird.

Weitere Hinweise sind hierzu individuell durch den CGM ALBIS Vertriebs- und Servicepartner einzuschätzen.

7.4 Umgebungsvariablen

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

7.5 Dienste / Services

Für den Betrieb von CGM ALBIS YOU wird eine Codebase Dienst benötigt. Dieser Dienst wird bei der Installation von CGM ALBIS YOU auf einem Server installiert und eingerichtet. Für den Betrieb der Datenbank: PostgreSQL ist ebenfalls eine Dienstinstallation notwendig, die während der Installation der Anwendung auf dem Server eingerichtet wird.

WICHTIG: Für den Betrieb der Dienste notwendige Ports sind im Kapitel 0 beschrieben. Ebenfalls können dort die jeweiligen Dienstnamen entnommen werden.

7.6 Datenbank

Für den Betrieb von CGM ALBIS werden 2 Datenbanken benötigt. Diese sind Codebase und PostgreSQL. Die Daten werden jeweils im Datenbankverzeichnis im jeweiligen Installationsordner auf dem Server abgelegt. Für den Betrieb ist, wie unter Dienste / Services beschrieben, die Installation 2er Services notwendig, damit die Funktionalität von CGM ALBIS gewährleistet ist.

7.7 Virenschutz

Wir empfehlen den Einsatz von Virenschutz Software. Jeder Rechner, auch ohne Anbindung an das Internet/Intranet, sollte über ein Virenschutzprogramm verfügen.

WICHTIG: Die regelmäßige, am besten tägliche, Aktualisierung des Virenschutzes ist dabei essentiell.

WICHTIG: Die Konfiguration und auch Auswahl des Virenscanner - besonders des Laufzeitscanners - kann erheblich die Performance des Systems beeinträchtigen. Daher empfehlen wir hier dringend, dass Sie sich mit Ihrem CGM ALBIS Vertriebs- und Servicepartner in Verbindung setzen, um die für Sie beste Lösung für die optimale Sicherheit zu finden.

Bitte prüfen Sie ebenfalls in diesem Zusammenhang des Microsofts bordeigenen Virenscanner.

7.8 Software und Betriebssystem Aktualisierungen

Alle Hardware- & Softwaresysteme sind einem ständigen Wandel unterworfen, dies Bedarf einer regelmäßigen Wartung.

Wir empfehlen das Betriebssystem und Softwaremodule immer auf einem aktuellen Stand gehalten werden und möglichst dem letzten Patch-Level entsprechen.

WICHTIG: Bitte beachten Sie auch das Updates auf Offline-Systemen manuell oder durch Update Dienste - z. B. Windows Server Update Services (WSUS) - durchgeführt werden müssen.

7.9 Server-Einstellungen

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

7.10 Arbeitsplatz-Einstellungen

CGM ALBIS arbeitet mit lokalen Arbeitsverzeichnissen, die Berechtigungen dieses Verzeichnisses muss so eingestellt werden, dass der Windowsbenutzer, dort immer Schreib- und Leserechte hat.

Dies muss für alle Verzeichnisse und Dateien dieses Arbeitsverzeichnisses sichergestellt sein.

Weiterhin ist zu beachten, wie bei der die Betriebsart Terminalserver und die Verwendung von lokalen Arbeitsverzeichnissen betrieben werden müssen.

Weitere Hinweise sind hierzu individuell durch den CGM ALBIS Vertriebs- und Servicepartner einzuschätzen.

7.11 Betriebssystem-Einstellungen

Individuell einzuschätzen durch den CGM ALBIS Vertriebs- und Servicepartner.

7.12 Standard-Software

Neben dem Betriebssystem wird auf den Computern noch folgende Software benötigt, um CGM ALBIS zu verwenden:

- *Internet Explorer Version 10 (oder aktueller)*
- *Mit dem CGM ALBIS Update / Installation mitgelieferte CGM JAVA Version*
- *Microsoft .NET Framework 4.7*
- *Acrobat Reader Version*

7.13 Office-Anwendungen

Für die Briefschreibung oder auch für Auswertungen werden von CGM ALBIS aktuelle Microsoft Office-Anwendungen empfohlen.
Als Textverarbeitung ist eine Schnittstelle zu Microsoft Word in CGM ALBIS integriert.

Für folgende MS Word-Versionen ist CGM ALBIS freigegeben:

- *Microsoft Word 2010, deutsche Version*
- *Microsoft Word 2013, deutsche Version*
- *Microsoft Word 2016, deutsche Version*
- *Microsoft Word 2019, deutsche Version*

7.14 Online Update(s)

CGM ALBIS bietet die Möglichkeit alle CGM ALBIS Updates online zu beziehen. Bitte wenden Sie sich hierzu an Ihren CGM ALBIS Vertriebs- und Servicepartner.

7.15 Fernwartung

Für Fernwartungen durch unsere CGM ALBIS Hotline setzen wir CGM Remote Support basierend Anydesk ein. Siehe dazu: https://rs.cgm.com

Bei Fernwartungen durch die Hotline des CGM ALBIS Vertriebs- und Servicepartner verweisen wir auf deren individuell eingesetzten Produkte.

8 Datensicherung

Es ist eine tägliche Datensicherung der patientenbezogenen Daten gemäß den geltenden Datenschutzbestimmungen durchzuführen. Wir schlagen daher vor, dass sie eine vollständige Datensicherung des gesamten Server-Systems durchführen. Je nach Konfiguration des Systems schlagen wir ebenfalls eine Sicherung der Arbeitsplätze durchzuführen. Zur Abstimmung und individuellen Einschätzung ziehen Sie bitte Ihren CGM ALBIS Vertriebs- und Servicepartner hinzu.

WICHTIG: Für den Betrieb von ALBIS sind Dienste notwendig die auf dem zentralen Rechner in der Praxis laufen. Diese müssen für eine Datensicherung jeweils beendet werden. Dies sollte bei der Backup-Strategie berücksichtig werden. Siehe dazu der Dienstnamensaufbau im Kapitel 0.

9 CGM PRAXISARCHIV

Aufgrund geänderter gesetzlicher Vorgaben ist, die in CGM ALBIS integrierte Bild- und Dokumentenablage (-> „Karteikarte“) als alleiniges Archivsystem in den meisten Fällen nicht ausreichend. Für eine revisionssichere Archivierung der Patientendaten, wie diese vom Gesetzgeber verlangt wird, empfehlen wir daher das TÜV-geprüfte CGM PRAXISARCHIV einzusetzen.

10 Datensicherheit

10.1 Verschlüsselung

Es wird empfohlen Bitlocker zu verwenden. Diese Verschlüsselung beeinträchtigt nicht die Nutzung von CGM ALBIS. Die Systemanforderungen von Bitlocker sind bei Verwendung zu berücksichtigen.

11 Einrichtung spezifischer Software

Sollte weitere, spezifische Software auf den Systemen eingerichtet werden, ist in jedem Fall der CGM ALBIS Vertriebs- und Servicepartner einzubeziehen, um die gesonderten Systemvoraussetzungen der spezifischen Software zu berücksichtigen.

12 IT Sicherheit

Die Gewährleistung von IT-Sicherheit und Datenschutz ist in der Medizinbranche von größter Bedeutung. CGM ALBIS verpflichtet sich zu höchsten Sicherheitsstandards, um die sensiblen Daten von Patienten und Praxen zu schützen. Dieses Kapitel gibt allgemeine Empfehlungen zur IT-Sicherheit sowie spezielle Hinweise zu den Sicherheitsmodulen der CompuGroup, den PC Log-In-Funktionen, den Betriebssystemen, Firewall- und Port-Einstellungen und externen Softwarelösungen.

12.1 Allgemeine Empfehlungen zur IT-Sicherheit

- **Regelmäßige Updates**: Halten Sie sowohl Ihre CGM ALBIS-Software als auch das zugrunde liegende Betriebssystem stets auf dem neuesten Stand. Installieren Sie alle verfügbaren Updates zeitnah, um Sicherheitslücken zu schließen und neue Funktionen zu nutzen.
- **Starke Passwörter**: Verwenden Sie komplexe Passwörter mit mindestens 12 Zeichen, die aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Vermeiden Sie leicht zu erratende Passwörter und ändern Sie diese regelmäßig. Ändern Sie Standardpasswörter auf allen Geräten und Systemen unverzüglich nach der Einrichtung.]
- **Zugriffsrechte**: Weisen Sie Benutzern nur die benötigten Zugriffsrechte zu. Nutzen Sie die Möglichkeit, Rollen und Berechtigungen in CGM ALBIS zu definieren, um Datenzugriffe zu steuern.
- **Sicherheitsbewusstsein**: Schulen Sie alle Mitarbeiter regelmäßig in Bezug auf IT-Sicherheit und Datenschutz. Sensibilisieren Sie sie für Phishing-Angriffe und andere Bedrohungen.
- **Datensicherung**: Führen Sie regelmäßige Datensicherungen durch und bewahren Sie Sicherungskopien an einem separaten Ort auf. Nutzen Sie die integrierten Backup-Funktionen von CGM ALBIS.
- **Überprüfen Sie regelmäßig**, ob die Backups fehlerfrei wiederhergestellt werden können. Schützen Sie Ihre Backups zudem vor unerlaubtem Zugriff, Verlust und unbeabsichtigtem Überschreiben (z. B. durch einen Verschlüsselungstrojaner).

12.2 Betriebssysteme

- **Unterstützte Betriebssysteme**: Stellen Sie sicher, dass Sie eine unterstützte Version des Betriebssystems verwenden (z. B. Windows 10, Windows 11). Überprüfen Sie regelmäßig die Kompatibilität mit der neuesten Version von CGM ALBIS.
- **Sicherheitseinstellungen**: Aktivieren Sie die integrierten Sicherheitsfunktionen des Betriebssystems, wie Windows Defender, um zusätzlichen Schutz vor Malware und Viren zu gewährleisten.

12.3 Firewall- und Port-Einstellungen

- **Firewall-Regeln**: Aktivieren Sie die Firewall Ihres Betriebssystems und konfigurieren Sie sie so, dass verdächtige Verbindungen blockiert werden. Erstellen Sie spezifische Firewall-Regeln, um den Netzwerkzugriff auf CGM ALBIS zu kontrollieren.
- **Port-Management**: Schließen Sie alle nicht benötigten Ports, um unautorisierte Zugriffe zu verhindern. Prüfen Sie regelmäßig die offenen Ports auf Ihrem System und passen Sie die Einstellungen gegebenenfalls an.
- **Netzwerküberwachung**: Implementieren Sie Werkzeuge zur Überwachung des Netzwerkverkehrs, um ungewöhnliche Aktivitäten zu erkennen. Dies hilft, potenzielle Sicherheitsvorfälle frühzeitig zu identifizieren.
- **Incident Response Plan:** Seien Sie auf **potenzielle Sicherheitsvorfälle** vorbereitet, indem Sie einen **klaren Reaktionsplan** erstellen. Dieser Plan sollte definieren, **wie schnell und effektiv** auf Sicherheitsverletzungen reagiert wird. Legen Sie **Verantwortlichkeiten**, **Kommunikationswege** und konkrete **Maßnahmen zur Schadensbegrenzung** fest, um im Ernstfall handlungsfähig zu bleiben.

12.4 Besondere Module zur IT-Sicherheit der CompuGroup

- **Security Monitoring**: Nutzen Sie das integrierte Monitoring-Tool zur Überwachung von ungewöhnlichen Aktivitäten und Sicherheitsvorfällen. Dies umfasst die Protokollierung von Zugriffen und Änderungen innerhalb der Software.
- **Verschlüsselung**: Alle sensiblen Daten werden sowohl bei der Speicherung als auch bei der Übertragung durch moderne Verschlüsselungstechniken geschützt. Stellen Sie sicher, dass die Verschlüsselungseinstellungen in den Softwareoptionen aktiviert sind.
- **Antiviren-Integration**: Integrieren Sie eine zuverlässige Antivirensoftware, die in Echtzeit Sicherheitsbedrohungen erkennt und blockiert. Halten Sie diese Software stets auf dem neuesten Stand.

12.5 Externe Softwarelösungen

- **Zuverlässige Software**: Verwenden Sie nur vertrauenswürdige externe Softwarelösungen, die den Datenschutzanforderungen entsprechen. Informieren Sie sich über die Sicherheitszertifikate und Datenschutzrichtlinien der jeweiligen Anbieter.
- **Integration von Drittanbietersoftware**: Stellen Sie sicher, dass integrierte Drittanbietersoftware (z. B. Praxisverwaltungssysteme, Abrechnungssoftware) ebenfalls sicher konfiguriert ist. Überprüfen Sie die Kompatibilität mit CGM ALBIS und halten Sie diese Software ebenfalls regelmäßig updated.
- **Datenschutzbestimmungen**: Beachten Sie stets die datenschutzrechtlichen Bestimmungen und stellen Sie sicher, dass die externe Software die notwendigen Maßnahmen zum Schutz sensibler Patientendaten umsetzt.

12.6 Schlussfolgerung

Die Implementierung der oben genannten Empfehlungen und Module ist entscheidend für die Sicherheit Ihrer Praxisdaten und die Einhaltung der gesetzlichen Vorgaben. CGM ALBIS unterstützt Sie dabei, Ihre IT-Sicherheitsstrategie zu optimieren. Bei Fragen oder Unterstützung wenden Sie sich bitte an Ihren zuständigen CGM ALBIS Vertriebs- und Servicepartner.

13 Hinweis zu Abweichungen von der Systemanforderungen

WICHTIG: Sollten die Systemanforderungen in der Praxis von den vorgenannten Systemanforderungen für den Betrieb von CGM ALBIS abweichen, kann es zu Beeinträchtigungen beim Betrieb von CGM ALBIS kommen.

Für weiterführende Fragen wenden Sie sich gerne direkt an Ihren autorisierten CGM ALBIS Vertriebs- und Servicepartner.

14 Änderungshistorie

Datum	Version	Änderung
15.02.2013	1.0	Erstellung des Dokuments
08.11.2018	1.1	Überarbeitung CGM ALBIS
26.11.2018	1.2	Kürzel herausgenommen; Formatierung geprüft; Rechtschreibfehler korrigiert. Freigabe: 26.11.2018
11.04.2019	1.3	Überarbeitung Netzwerk; CGM ALBIS.YOU - Empfohlenen Hardware; Verzeichnisberechtigung: Server & Lokale Arbeitsverzeichnisse. Freigabe: 11.04.2019
31.07.2019	1.4	Überarbeitung Freigaben; Überarbeitung Aktualisierung Software und Betriebssystemen; Layout des Dokumentes Freigabe: 31.07.2019
27.04.2020	1.5	Einzelplatz: CGM ALBIS; Mehrplatzanlagen / Netzwerkumgebung: CGM ALBIS.YOU;
25.11.2020	1.6	Betriebssystem Server 2019, sowie Office 2019 hinzugefügt. Ergänzung der notwendigen Ports und ALBIS Hintergrund Dienste.
05.04.2022	1.7	Entfernung 32-Bit / Verweis auf die Microsoft Liste der unterstützen Betriebssysteme / Erweiterung Windows Server 2022, Microsoft Windows 11 / Vereinheitlichen der Systemanforderungen für CGM ALBIS und CGM ALBIS.YOU / Ergänzung des EPA Dienstes
28.03.2024	1.8	Kapitel 5.1.2 Arbeitsstationen Ergänzung: *Windows 11 22H2 oder neuer*
01.04.2025	1.9	Kapitel 12 „IT Sicherheit“ eingefügt
07.04.2025	2.0	Kapitel 12: Anpassung der Login Regeln Kapitel 5: Verweis auf die Sicherheitsbestimmungen von Microsoft
17.04.2025	2.1	eHIMI Portfreigaben hinzugefügt

CGM ALBIS

Arztinformationssystem

CompuGroup Medical Deutschland AG
Geschäftsbereich ALBIS
Maria Trost 21, 56070 Koblenz
info.albis.de@cgm.de

cgm.com/albis

Synchronizing Healthcare

CompuGroup Medical