

## Technische Anforderungen QUINCY

Die Anforderungen von QUINCY an die Netzwerkinfrastruktur und die Hardware finden Sie nachfolgend zusammengefasst unter Systemvoraussetzungen, Sicherheitseinstellungen, Service und Telematikinfrastruktur.

### 1 Systemvoraussetzungen

QUINCY ist eine windowsbasierte Software, kann aber auch auf Apple-Hardware (MacOS) per Parallels mit separatem Windows 11 genutzt werden.

#### 1.1 Netzwerkstruktur

- Dedizierter Server ab 5 Arbeitsplätzen
- Für den Server muss Hardware mit hoher Ausfallsicherheit wie z.B. FUJITSU Primergy verwendet werden
- Verkabelung mit 1GB mit Kat 6/7

#### 1.2 Server

Komponente	
CPU (Prozessor)	Aktuelle Mehrkernprozessoren Intel und AMD
Arbeitsspeicher	Mindestens 16GB
Speichermedium	SSD für System, SSD oder HDD für Daten
Freier Speicherplatz	Mindestens RAID mit 2x 1TB SSDs (mindestens 500 GB für Daten)
Zusätzliche Laufwerke	Nicht notwendig
Monitor/Display Auflösung	1024*768
USB-Schnittstelle	notwendig
USV (Unterbrechungsfreie Stromversorgung)	empfohlen
LAN	1Gbit, ab Kat6, empfohlen Kat7; bestehende 100Mbit-Verkabelung kann vorübergehend verwendet werden, sollte aber ausgetauscht werden
Betriebssystem	Ab Windows Server 2016-2025 (Essentials/Standard), Achtung: EoL für 2012er Version nur mit 3 Jahre extended Service im Okt. 2026); Windows Server 2016 bis Januar 2027
Datenbank PostgreSQL	Ab 15.6

#### 1.3 Arbeitsplatz

Komponente	
CPU (Prozessor)	Aktuelle Mehrkernprozessoren Intel und AMD
Arbeitsspeicher	16GB
Speichermedium	256 SSD
Freier Speicherplatz	100 GB
Zusätzliche Laufwerke	Nicht notwendig, wenn Onlineupdate
Monitor/Display Auflösung	1024*768
USB-Schnittstelle	notwendig

Betriebssystem	Ab Windows 11
MS Office	Ab Word 2021 32BIT, kein Office 365 mit Cloudanb.

## 1.4 Terminalserver

Komponente	
Terminalserver-Installation möglich	
Speicherplatz pro Benutzer	Mind. 10 GB
MS Office	u.U. Volumenlizenz
Freier Speicherplatz	pro Benutzer 5GB freier Festplattenspeicher auf Laufwerk C:

## 2 Sicherheitseinstellungen

- Anti-Virenschutz: wir empfehlen ESET; bitte halten Sie Rücksprache, welche Dateien ausgeschlossen werden müssen
- Hardware-Firewall: wir empfehlen **Sophos**
- Windowsupdate: wir empfehlen **automatisch**
- Einrichtung Benutzer Installation mit Adminrechten, Benutzer Praxis Hauptnutzer

## 3 Serviceleistungen

### 3.1 Datensicherung

Die Datensicherung sollte mindestens täglich mit eine der nachfolgenden Funktionen erfolgen:

- klassisch auf **kennwortgeschützte** USB-Platten/Flashspeicher ausgeführt werden, direkt aus QUINCY heraus. Es stehen hier 3 verschiedene Umfänge zur Verfügung (Bewegliche Daten, gesamtes QUINCY; gesamtes Laufwerk) – empfohlen auf ein Medium pro Tag (mindestens 2 pro Woche)
- Per Online-Datensicherung über die GUSbox

Für die Datensicherung müssen alle Workstation QUINCY verlassen haben.

**Datenwiederherstellungen** müssen unter Einbeziehung des QUINCY-Supports durchgeführt werden.

Es empfiehlt sich, folgende Sicherungen durchzuführen:

- eine Quartalssicherung nach der Abrechnung auf ein separates Medium durchzuführen. Die Verwendung eines nicht wiederbeschreibbaren Mediums (z.B. DVD, Blue-ray oder Tape) erhöht den Beweiswert für eventuelle nachträgliche Überprüfungen.
- den gesamten Server inkl. Betriebssystem

### 3.2 Fernwartung/Remote Service

In QUINCY ist TeamViewerQS integriert, dass den Anwender:innen ermöglicht, aktiv den Zugriff per Remote zu ermöglichen.



## 4 Telematikinfrastruktur

### 4.1 Stationäre eHealth-Kartenterminals

Es dürfen nur für die Telematikinfrastruktur zugelassene eHealth-Kartenterminals angebunden werden, wie z.B. das Cherry ST 1506 oder ORGA 6141 online.

Es wird ein eigener Netzwerkanschluss benötigt.

### 4.2 Schutz des Konnektors

Der Konnektor muss zwingend vor Zugriff geschützt werden. Das kann durch Aufstellung in einem abschließbaren Serverraum bzw. Serverschrank realisiert werden. Sollte kein Serverraum/-schrank in der Praxis vorhanden sein, empfehlen wir den Einsatz eines Konnektorschrankes.