CGM LAUER
Apothekenlösungen

ANLEITUNG

ABDA IT-Sicherheitsprüfliste für Apotheken

Version 1 | 15. August 2025

CompuGroup Medical

Per Klick zum gewünschten Thema

INHALTSVERZEICHNIS

Dokument	Version	Freigegeben	Geändert	Erstellt	Freigabedatum	Status
ABDA IT-Sicherheitsprüfliste für Apotheken	WAux-1	MNU		SBU/RWI	15.08.2025	Öffentlich

Disclaimer

Die in dieser Sicherheitsprüfliste bereitgestellten Informationen beziehen sich auf Sicherheitsaspekte unserer Produkte in der Standardkonfiguration und bieten allgemeine Informationen und Hinweise für das weitere Ausfüllen der Liste. Wir möchten hervorheben, dass diese Informationen keine Rechtsberatung oder individuelle sicherheitstechnische Beratung zur Erfüllung von Compliance-Kriterien darstellen und eine solche Beratung auch nicht ersetzen kann. Die Verantwortung für die Bewertung und Umsetzung angemessener Sicherheitsmaßnahmen liegt allein bei Ihnen als Kunde. Für die Erfüllung vorgegebener Sicherheitsanforderungen empfehlen wir ausdrücklich die Inanspruchnahme von qualifizierter und zertifizierter Beratung im Bereich IT-Sicherheit oder Compliance.

Bitte beachten Sie, dass wir keine Haftung für Schäden übernehmen, die aus der Nutzung oder Auslegung der in dieser Liste enthaltenen Informationen entstehen, es sei denn, diese beruhen auf Vorsatz oder grober Fahrlässigkeit oder betreffen Schäden aus der Verletzung von Leben, Körper oder Gesundheit.

Aus Gründen der Lesbarkeit wird bei Personenbezeichnungen in diesem Dokument die männliche Form gewählt. Die Angaben beziehen sich selbstverständlich auf Angehörige aller Geschlechter.

Die in den Beispielen und Screenshots verwendeten Personennamen und sonstigen Daten sind frei erfunden. Ähnlichkeiten mit realen Namen und Daten sind zufällig und nicht beabsichtigt, soweit nichts anderes angegeben ist.

Vorwort

Sofern wir in den folgenden Informationen auf einzelne Punkte der ABDA-Sicherheitsprüfliste nicht Bezug nehmen, sind die entsprechenden Informationen vollständig von Ihnen als Apotheke bereitzustellen.

2. Zugangskontrolle

2.1 Dokumentation für Zugang zu IT-Systemen

Wir empfehlen, die Passwortrichtlinien, den Anlageprozess und die Konfigurationsdaten der Benutzer zu dokumentieren. Flankierend erhalten Sie von uns eine Passwortdokumentation für Ihr System und für die Telematikinfrastruktur (sofern wir diese installiert haben).

Sie haben die Möglichkeit, die Passwörter für Server und Client zu ändern. Diese Änderung ist von Ihnen zu dokumentieren.

Die Systeme sind von uns durch eine Checkpoint-Firewall gegen unbefugte Zugriffe aus dem Internet gesichert.

2.3 Authentisierung für IT-Systeme

*In einer **WINAPO®**-Installation stehen Benutzername/Passwort oder Fingerprint als Anmeldemethode zur Verfügung. Welche Anmeldemethode Sie verwenden, wird von Ihnen definiert und ordnungsgemäß dokumentiert.*

2.5 Bildschirmsperre für alle Rechner

*Die Bildschirmsperre ist von uns standardmäßig bei automatischem Starten und Anmelden von Stationen (Wake on LAN) vorkonfiguriert, die Sie nach Ihren Bedürfnissen anpassen können. Applikationsseitig können Benutzer in **WINAPO®** automatisch abgemeldet werden; auch dies kann individuell konfiguriert werden. Die Konfiguration ist von Ihnen zu dokumentieren, und die Mitarbeiter sind entsprechend zu instruieren.*

3. Zugriffskontrolle – Maßnahme zur Verhinderung von unbefugten Zugriffen

3.1 IT-Systeme mit Rollenkonzept

Applikationsebene:

- ***WINAPO® 64** enthält eine Zugriffskontrolle über direkt dem Benutzer zugeordnete Berechtigungen.*
- ***WINAPO® ux** bietet ein Rollenkonzept mit Gruppen zur Zugriffssteuerung.*

Domänenebene: Benutzer und ihre Zugriffsrechte werden in der Domäne über Active Directory angelegt und verwaltet. Diese Benutzerkonten sind Arbeitsstationen zugeordnet und nicht personalisiert.

Sichere Passwörter: Wir empfehlen Ihnen, die Hinweise in der Dokumentation zur Passwortübergabe zu beachten und nach der Installation sichere Passwörter für die Systemkonten auf Arbeitsstationen und Servern zu vergeben, die für Updates verwendet werden. Im Rahmen der Updates muss dann beim Neustart des Systems dieses Passwort manuell eingegeben werden.

3.2 Berechtigungen auf Funktionsebene feingranular steuerbar

*In **WINAPO®** können Berechtigungen auf Funktionsebene feingranular gesteuert werden.*

4. Weitergabekontrolle – Maßnahmen zur Datenübertragung und -weitergabe

4.1 Technische Protokollierung von Datenübertragungen

*Soweit es **WINAPO®** betrifft, werden Datenübertragungen an Drittsysteme (z.B. an Abrechnungszentren) durchgängig in Logdateien bzw. in der Datenbank protokolliert.*

Für Drittsysteme oder Drittsoftware ist dies von Ihnen zu prüfen und zu dokumentieren.

4.2 Firewall-Richtlinie

***WINAPO®**-Systeme werden standardmäßig ohne Portfreigaben geliefert. Individuelle Portfreigaben (z.B. für zusätzliche Software) werden auf Wunsch eingerichtet und von Ihnen entsprechend dokumentiert sowie kontinuierlich gepflegt.*

4.3 Zugangsbeschränkung für Fernzugriffe

***WINAPO®**-Systeme werden so konfiguriert, dass jede Fernwartung von Ihnen aktiv freigegeben werden muss.*

Der Fernzugriff aus dem Home-Office erfolgt geschützt über VPN und wird durch eine Passwortfreigabe authentifiziert.

5. Eingabekontrolle – Maßnahmen für Datenkorrektheit und -herkunft

5.1 Löschkonzept

*Alle für ein DSGVO-konformes Löschkonzept erforderlichen Aktivitäten sind in **WINAPO®** implementiert und dokumentiert (z.B. Löschung von Kunden, Wiedervorlage, die Berücksichtigung gesetzlicher vorgeschriebener Aufbewahrungsfristen usw.).*

Soweit nach einem Backup oder Datenexport der Schutz von Daten in die Verantwortung an Sie übergeht (z.B. hinsichtlich der Medien, der Aufbewahrungsorte, des Zugangs zu den Medien usw.), sind entsprechende Vorgaben durch Sie festzulegen, zu dokumentieren und entsprechend zu beachten.

7. Verfügbarkeitskontrolle und Wiederherstellbarkeit – Maßnahmen zur Geschäftsfortführung nach Sicherheitsvorfall

7.1 Kontrolle der Datenträger und Datensicherungen

*Die im Rahmen einer **WINAPO®**-Systeminstallation mitgelieferte Datensicherung wird kontinuierlich im Rahmen der hausinternen Qualitätssicherung auf ihre Funktionsfähigkeit zur Wiederherstellung der gesicherten Daten geprüft.*

7.2 Kontrolle bzw. Monitoring der technischen Einrichtungen

Nach Beauftragung liefern wir auch eine USV. Die Kontrolle bzw. das Monitoring dieser sowie anderer technischer Einrichtungen ist jedoch von Ihnen selbst durchzuführen und zu dokumentieren.

7.5 Datensicherungskonzept

***WINAPO®** stellt Ihnen im Kundenportal ein Konzept zur Datensicherung bereit, das beschreibt, wie die Sicherung von Daten aus **WINAPO®** wiederholbar durchgeführt werden kann und wie die Daten wiederhergestellt werden können. Die Funktionsfähigkeit der Datensicherung inklusive Wiederherstellungstests wird im Rahmen der technischen Qualitätssicherung vor dem Release einer neuen **WINAPO®**-Version überprüft.*

Nicht enthalten sind Empfehlungen oder Anweisungen, wie Daten aus Drittsoftware gesichert werden sollten und wie die Datensicherungsmedien zu schützen und zu lagern sind. Diese Angaben und Festlegungen (z.B. wo die Medien aufbewahrt werden, wer Zugang hat usw.) sind von Ihnen zu treffen und entsprechend zu dokumentieren.

7.7 Verfügbarkeit von Support / Reparatur-Service-Techniker

***CGM Lauer** stellt Ihnen eine Technik-Hotline zur Verfügung. Der Umfang des technischen Supports ergibt sich aus den vertraglichen Vereinbarungen.*

7.8 Schadensoftwareerkennung und -bewältigung

Nach Beauftragung liefern wir einen Virenschutz in Form von Symantec Endpoint Protection.

8. Datenträgerkontrolle – Maßnahmen zur Verhinderung von Datenverlust auf physischer Ebene

8.1 Verschlüsselung für mobile Datenträger

Mit der Datensicherung geht die Verantwortung für die Sicherheit der Daten auf Sie über. Sie sind somit selbst verantwortlich für die eventuelle Verschlüsselung und sichere Aufbewahrung mobiler Datenträger (z.B. von USB-Festplatten oder Sticks).

8.2 Verschlüsselung für Geräte

*Die Datensicherung von **WINAPO®** ist standardmäßig verschlüsselt. **CGM Lauer** bietet auch die optionale Einrichtung einer Verschlüsselung für Geräte an, die von Ihnen beauftragt werden kann.*

9. System- und Datenintegrität

9.1 Updates Betriebssystem und Firmware

*System-Updates werden regelmäßig von **CGM Lauer** als Systemanbieter durchgeführt. Firmware-Updates erfolgen im Wartungsfall.*

9.2 Updates Software

*Updates werden regelmäßig durch **CGM Lauer** als Systemanbieter durchgeführt. Für Drittsoftware, die nicht von **CGM Lauer** geliefert wird, sind Sie selbst für die Pflege der Updates verantwortlich.*

ÄNDERUNGSHISTORIE

Version:	Durchgeführte Änderungen:	Erstellt/Geändert:	Freigegeben:	Freigabedatum:
1	Ersterstellung	SBU/RWI	MNU	15.08.2025
2				
3				
4				
5				
6				

CGM LAUER

Apothekenlösungen

LAUER-FISCHER GmbH
Dr.-Mack-Straße 95
90762 Fürth
T +49 (0) 911 7432-0
F +49 (0) 911 7432-100
info.lauer@cgm.com

cgm.com/lauer

Überreicht durch:

CompuGroup Medical