

# **IT-Richtlinie für den Betrieb von Hard- und Software in der Netzwerkinfrastruktur (extern)**

Version: 11

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b> .....	<b>3</b>
<b>2</b>	<b>Geltungsbereich</b> .....	<b>3</b>
<b>3</b>	<b>Zu widerhandlungen</b> .....	<b>3</b>
<b>4</b>	<b>Allgemeine Voraussetzungen</b> .....	<b>3</b>
<b>5</b>	<b>Voraussetzungen/Anforderungen an das Betriebssystem</b> .....	<b>3</b>
5.1	Windows-Betriebssysteme.....	3
5.2	VMware.....	4
5.3	Linux-/Unix-Distributionen.....	4
5.4	Apple iOS.....	4
5.5	Android OS.....	4
<b>6</b>	<b>Patchmanagement des Betriebssystems</b> .....	<b>4</b>
<b>7</b>	<b>Schutz vor Schadsoftware</b> .....	<b>4</b>
<b>8</b>	<b>Schwachstellenscanner</b> .....	<b>4</b>
<b>9</b>	<b>Härtung des Betriebssystems und der Anwendungen/Services</b> .....	<b>4</b>
<b>10</b>	<b>Anbindung per Wireless LAN</b> .....	<b>5</b>
<b>11</b>	<b>Medienanschlüsse und externe Speichermedien</b> .....	<b>5</b>
<b>12</b>	<b>Anbindung von Modalitäten</b> .....	<b>5</b>
<b>13</b>	<b>Lebensdauer Hard- und Software</b> .....	<b>5</b>
<b>14</b>	<b>Voraussetzungen/Anforderungen an Softwarekomponenten</b> .....	<b>5</b>
14.1	Java.....	5
14.2	Websocket.....	5
14.3	Microsoft SQL-Server und -Datenbanken .....	5
14.4	Dateifreigaben .....	6
14.5	Internet.....	6
14.6	IPsec-Tunnel/VPN-Tunnel.....	6
14.7	Mailrelay .....	6
<b>15</b>	<b>Voraussetzungen/Anforderungen an Virtualisierung</b> .....	<b>6</b>
15.1	Servervirtualisierung.....	6
<b>16</b>	<b>Fernwartung</b> .....	<b>6</b>
<b>17</b>	<b>BSI-Meldepflicht</b> .....	<b>6</b>

 Die aktuell gültige Dokumentenversion ist auf der MKK-Homepage unter <https://www.muehlenkreiskliniken.de/zentraleinkauf> abgelegt.

## 1 Einleitung

Um eine optimale und funktionsfähige Patientenversorgung und Unternehmensführung, sowie Forschung und Lehre in Kooperation mit der Ruhr Universität Bochum und der Ausbildungsakademie gewährleisten zu können, sind die Mühlenkreiskliniken (MKK) auf eine funktionsfähige und sichere Informationstechnologie (IT) angewiesen. Um dieses zu gewährleisten, betreiben die MKK eine komplexe IT-Infrastruktur in der viele der mittlerweile IT-gestützten Prozesse abgebildet sind.

Zum Schutz der IT-Infrastruktur sind Regeln bei der Auswahl und Inbetriebnahme von Endgeräten einzuhalten. Diese werden in dieser Richtlinie beschrieben zu deren Einhaltung der Mitarbeiter bzw. der Vertragspartner der MKK sich verpflichtet.

## 2 Geltungsbereich

Diese IT-Nutzungsrichtlinie gilt für alle Beschäftigte und Geschäftspartner des Unternehmens und Ihrer Tochterunternehmen, die einen Betrieb eines Endgerätes an der IT-Infrastruktur der MKK betreiben, betreiben wollen oder beschaffen möchten. Beschäftigte der MKK und Geschäftspartner sind verpflichtet, sich an diese Richtlinie zu halten.

## 3 Zuwiderhandlungen

Eine Zuwiderhandlung/ein Verstoß kann arbeits- oder dienstrechtliche Konsequenzen nach sich ziehen. Im Falle des Vorliegens von grober Fahrlässigkeit oder Vorsatzes können dem Unternehmen entstandene Schäden gegenüber dem Mitarbeiter ganz oder teilweise geltend gemacht werden. Als Verstöße werden Handlungen gegen das Regelwerk der IT-Sicherheit verstanden. Dazu zählen insbesondere die aus der vom Nutzer zu verantwortender Beeinträchtigung der Funktionalität der IT-Systeme hervorgerufene negative Auswirkungen auf die IT-Sicherheit.

Im Falle externer Personen, Systemanbieter und Dienstleister kann eine Zuwiderhandlung/ein Verstoß vertragliche Konsequenzen und Strafzahlungen nach sich ziehen. Im Falle des Vorliegens von grober Fahrlässigkeit oder Vorsatzes können dem Unternehmen entstandene Schäden gegenüber dem externen Partner ganz oder teilweise geltend gemacht werden.

## 4 Allgemeine Voraussetzungen

- Verwalten von Apple iOS-Endgeräten im MDM (Mobile Device Management) – im speziellen [WorkspaceOne](#) und Softwarekomponente *WorkspaceOne HUB*.
- Im ADE (Apple Enrollment Program, ehemals DEP) der MKK eingebunden.
- Apple iOS-Apps werden ausschließlich über den offiziellen App-Store bezogen. Eine Lizenzierung der Apps muss über den Hersteller direkt erfolgen und nicht über den App-Store.
- Datenspeicher, wie z.B. Festplatten/SSDs und Speicherkarten sind zu verschlüsseln.
- Netzwerkkommunikation der Software/Hardware erfolgt im Grundsatz verschlüsselt, mindestens TLS 1.2.
- Ein UML-Sequenzdiagramm zur Darstellung der Kommunikation muss in einem editierbaren Format (VSDX oder DRAWIO) vorliegen.
- Das Rollen- und Rechtekonzept muss beschrieben sein.
- Eingesetzte Software muss VDI-fähig und -freigegeben sein (*Omnissa Horizon*).

## 5 Voraussetzungen/Anforderungen an das Betriebssystem

Nachfolgende Versionen werden je nach Betriebssystem für den Betrieb in der Netzwerkinfrastruktur der MKK vorausgesetzt.

Sollte es sich um ein Medizinprodukt handeln, für welches ein aktuelles Betriebssystem nicht zulässig ist, ist dies vom Hersteller/Lieferant explizit anzugeben und von den Abteilungen IT und Informationssicherheitsmanagement & Datenschutz freigeben zu lassen.

### 5.1 Windows-Betriebssysteme

Die von Microsoft veröffentlichten Produktlebenszyklen für Windows sind einzuhalten. Es ist immer das am längsten unter Support stehende und vom Servicepartner unterstützte Betriebssystem im aktuellen Versions- und Patchstand einzusetzen. Das Betriebssystem ist im Server- und Clientbereich als Enterprise-Edition zu betreiben.

## 5.2 VMware

Die von VMware eingesetzten Hypervisor sowie Infrastrukturkomponenten sind im aktuellen Versions- und Patchstand einzusetzen.

## 5.3 Linux-/Unix-Distributionen

Es ist immer das am längsten unter Support stehende und vom Servicepartner unterstützte Betriebssystem im aktuellen Versions- und Patchstand einzusetzen. Die Distributoren haben dazu die Produktlebenszyklus im Internet veröffentlicht.

## 5.4 Apple iOS

Es ist immer das am längsten unter Support stehende und vom Servicepartner unterstützte Betriebssystem im aktuellen Versions- und Patchstand einzusetzen.

## 5.5 Android OS

Der Einsatz von Android ist grundsätzlich in den MKK nicht gestattet.

# 6 Patchmanagement des Betriebssystems

Die benannten [Betriebssysteme](#) sind immer auf der aktuellen Version und Patchstand zu halten. Die Einbindung Active Directory fähiger Betriebssysteme und dem in der Domäne der MKK vorgegebenen Update- und Patchmanagement ist im Grundsatz vorgegeben.

Apple iOS und Android basierte Endgeräte werden im Grundsatz über die MKK MDM-Plattform [WorkspaceOne](#) verwaltet.

Die Einbindung von Endgeräten ohne Anbindung in das [Active Directory](#) der MKK und/oder dem Management über die MKK MDM-Plattform und somit auch dem Patchmanagement der MKK ist nur dann gestattet, wenn der Hersteller/Lieferant schriftlich zusichert, dass er das Endgerät immer auf dem aktuellen Versionsstand und Patchstand hält. Eine Überprüfung des Versionsstandes und des Patchlevels kann durch die IT-Abteilung jederzeit erfolgen. Für die Prüfung ist der aktuelle Einsatzort des Geräts der IT-Abteilung jederzeit zu nennen.

Bei Verwendung eines eigenen Updatemanagement ist vorab die technische Umsetzung darzustellen.

Sollte es sich um ein Medizinprodukt handeln, für welches ein Patchmanagement nicht zulässig ist, ist dies vom Hersteller/Lieferant explizit anzugeben und von den Abteilungen IT und Informationssicherheitsmanagement & Datenschutz freigeben zu lassen.

# 7 Schutz vor Schadsoftware

Für den Betrieb eines Endgeräts in der Netzwerkinfrastruktur wird der Einsatz und Betrieb von Sicherheitssoftware, bestehend aus *Fortinet FortiEDR* und *Microsoft Defender*, vorausgesetzt.

Sollte es sich um ein Medizinprodukt handeln, für welches eine Sicherheitssoftware nicht zulässig ist, ist dies vom Hersteller/Lieferant explizit anzugeben und von den Abteilungen IT und Informationssicherheitsmanagement & Datenschutz freigeben zu lassen.

# 8 Schwachstellenscanner

Für den Betrieb eines Endgeräts in der Netzwerkinfrastruktur wird der Einsatz und Betrieb von Schwachstellenscannern, bestehend aus *Tenable.sc* und *Asimily* vorausgesetzt.

# 9 Härtung des Betriebssystems und der Anwendungen/Services

Im Grundsatz ist eine Härtung des Betriebssystems, der Anwendungen und der Services durch den Hersteller durchzuführen. Administrative Kennwörter und Accounts sind nicht für den Betrieb und die Bereitstellung von Betriebssystemen, Anwendungen und Services zu benutzen. Zugriffsmöglichkeiten auf das Betriebssystem, die Anwendungen und die Services sind auf ein für den Betrieb notwendiges Minimum zu beschränken und zu sichern (z.B. Netzwerkports, Konsolen, Tools, Treiber, Dienste). Alle nicht benötigten Softwarebestandteile/Anwendungsprogramme und Funktionen sind zu entfernen.

- Für Windows-Clients ist der die [Empfehlung zur Härtung von Windows 10 mit Bordmitteln](#) des BSI in der aktuellen Fassung anzuwenden.
- Für Windows-Server ist der [IT-Grundschutz-Baustein SYS.1.2.3 Windows Server](#) des BSI in der aktuellen Fassung anzuwenden.
- Für Linux-Systeme ist der [IT-Grundschutz-Baustein SYS.1.3 Server unter Linux und Unix](#) des BSI in der aktuellen Fassung anzuwenden.

Eine Überprüfung der Härtung des Betriebssystems und der Anwendung kann durch die IT-Abteilung jederzeit erfolgen. Für die Prüfung ist der aktuelle Einsatzort des Geräts der IT-Abteilung jederzeit zu nennen.

Sollte es sich um ein Medizinprodukt handeln, für welches eine Härtung nach BSI nicht hergestellt werden kann, ist dies vom Hersteller/Lieferant explizit anzugeben und von den Abteilungen IT und Informationssicherheitsmanagement & Datenschutz freigeben zu lassen.

## 10 Anbindung per Wireless LAN

Die eingesetzten Endgeräte unterstützen den 2,4 und 5 GHz Wireless-Standard und sind in der Lage nach mindestens *WPA2-802.1x* mit Zertifikaten zu verschlüsseln und zu authentifizieren. Unabhängig von der Anbindung direkt an die MKK-Infrastruktur ist ein Betrieb fremder WLAN-Netzwerktechnik (nicht MKK-Infrastruktur) zum Aufbau eigener Strukturen nicht zulässig.

## 11 Medienanschlüsse und externe Speichermedien

Die Nutzung von externen Speichermedien (wie z.B. USB-Massenspeicher) ist nicht zulässig. Externe Anschlüsse an Endgeräten, wie z.B. USB sind auf ein für den Betrieb notwendiges Minimum zu beschränken und zu sichern. Ungenutzte Anschlüsse sind zu deaktivieren.

## 12 Anbindung von Modalitäten

Bildgebungsmodalitäten, die Bilder, Clips oder Videos erzeugen, müssen sicherstellen, dass sie dem DICOM-Standard 3.0 (Version 2008) entsprechen. Darüber hinaus ist die Unterstützung mindestens einer DICOM-Worklist, sowie eines DICOM-Storages zwingend erforderlich, um einen Informationsaustausch innerhalb der Systemumgebung zu gewährleisten.

Zur Absicherung administrativer Funktionen muss für die Modalität eine Nutzerverwaltung bereitgestellt werden. Diese muss gewährleisten, dass administrative Einstellungen und sicherheitsrelevante Konfigurationen vor unbefugtem Zugriff geschützt sind. Sollte das vom Hersteller/Lieferant nicht unterstützt werden, so ist dies explizit anzugeben und von den Abteilungen IT und Informationssicherheitsmanagement & Datenschutz freigeben zu lassen.

## 13 Lebensdauer Hard- und Software

Die Produktlebenszyklen der Produkte und Hersteller sind einzuhalten. Ein Betrieb des Endgerätes ist ausschließlich nur dann gestattet, wenn alle Soft- und Hardwareprodukte vom Hersteller noch nicht abgekündigt sind und ein Produktsupport (bei Software mit Updatesupport) besteht.

## 14 Voraussetzungen/Anforderungen an Softwarekomponenten

### 14.1 Java

Java ist grundsätzlich in einer lizenzkostenfreien Version einzusetzen und ausschließlich im aktuellen Versions- und Patchstand zu betreiben. Ist eine Nutzung einer lizenzpflichtigen Java-Version erforderlich, so ist die Lizenz durch den Hersteller/Anbieter zu stellen.

### 14.2 Websocket

Im Grundsatz ist die Nutzung von Websockets in den Mühlenkreiskliniken untersagt.

### 14.3 Microsoft SQL-Server und -Datenbanken

Im Grundsatz ist für MS SQL-Datenbanken der zentrale [MS SQL-Cluster](#) der MKK zu nutzen. Abweichungen hiervon bedarf einer individuellen Freigabe. Für den Betrieb der Datenbanken werden ausschließlich administrative Rechte auf der Datenbank selbst zur Verfügung gestellt. Sogenannte administrative Instanz- oder SA-Rechte werden nicht vergeben (auch nicht temporär). Es werden keine individuellen Instanzen auf dem Datenbank-Cluster der MKK vergeben.

## 14.4 Dateifreigaben

Im Grundsatz sind keinerlei Dateifreigaben oder s.g. Shares für die Bereitstellung der Softwareanwendung oder Daten gestattet. Insbesondere Freigaben mit *Jeder/Everyone*-Berechtigungen sind ausnahmslos nicht gestattet.

## 14.5 Internet

Wird eine Kommunikation in das Internet benötigt, müssen vollständig mit Quelle, Port, Ziel und Protokoll angegeben werden. Angaben wie *\*.hersteller.de* (sog. Wildcards) werden im Grundsatz nicht akzeptiert. Die Kommunikation muss nach den technischen Richtlinien des BSI [TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen](#) erfolgen.

## 14.6 IPsec-Tunnel/VPN-Tunnel

IPsec-Tunnel/VPN-Tunnel sind nicht zulässig.

## 14.7 Mailrelay

Ein sog. Mail-Relay auf die Mailserver der MKK ist ausschließlich aus den internen Netzwerkbereichen der MKK und nur als internes Relay gestattet.

# 15 Voraussetzungen/Anforderungen an Virtualisierung

## 15.1 Servervirtualisierung

Im Grundsatz kann die Server-Virtualisierungs-Infrastruktur der MKK (basierend auf VMware) genutzt werden. Voraussetzung hierfür ist eine unmittelbare und fortlaufende Unterstützung der aktuellen VMware-Versionen, sowie Treiber und Tools.

# 16 Fernwartung

Zur Fernwartung von Endgeräten in der IT-Infrastruktur der MKK wird der Einsatz des Fernwerkzeuges [BeyondTrust Privileged Access Management](#) vorausgesetzt (siehe [IT-Nutzungsrichtlinie zur Fernwartung von IT-Systemen](#)).

# 17 BSI-Meldepflicht

Die MKK betreibt eine kritische Infrastruktur gem. BSI-Gesetz und ist verpflichtet Meldung vom BSI über Schwachstellen, Gefährdungen, Vorfälle etc. entgegenzunehmen und zeitnahe zu behandeln. Sofern Produkte des Auftragnehmers im Rahmen von BSI-Meldungen thematisiert werden, behält sich die MKK vor eine Stellungnahme zu der entsprechenden BSI-Meldung von dem Auftragnehmer einzuholen. Die Stellungnahme muss u.a. eine Risikoabschätzung seitens des Auftragnehmers, einen Maßnahmenplan zur Behandlung inkl. verbindlicher zeitlicher Planung zum weiteren Vorgehen enthalten. Die Stellungnahme muss zeitnah, unter Berücksichtigung der gesetzlichen Fristen für Datenschutzvorfälle gemäß DSGVO bzw. Informationssicherheitsvorfälle, bei den MKK eingehen.