

Antrag Netzwerkanbindung für Fremdgeräte / Spezialgeräte

DEN ANTRAG VOR DER GERÄTEBESTELLUNG EINREICHEN

GERÄTEVERANTWORTLICHE PERSON

HERR FRAU DIVERS

Familienname Vorname

Akademischer Grad Organisationseinheit

Benutzerkennung (q-Nummer) Telefonnummer
(für Rückfragen)

STANDORT

Gebäude, Straße, Nr.

Etage Raum Netzwerkdosensbezeichnung

ANZUSCHLIESSENDES GERÄT

Typ Hersteller Modellbezeichnung

Inventarnummer

Betriebssystem (inkl. Version)

UPDATES

Verantwortliche Person / Firma (Servicevertrag)

Betriebssystem-Updates werden von der verantwortlichen Person /Firma eingespielt

JA NEIN

NETZWERK

Mac Adresse Kabel gebunden

ENDPOINT SECURITY

Virenschutz JA NEIN Hersteller

- Firewall Betriebssystem-Firewall aktiv
 Hardware-Firewall durch den Hersteller
 Hardware-Firewall durch Medizinische Universität Innsbruck erwünscht

AD ANBINDUNG

Active Directory Integration möglich JA NEIN

BENÖTIGTE NETZWERKRESSOURCEN

(z.B. Gruppenlaufwerk, Wissenschaftsspeicher, Drucker ...)

INTERNETZUGANG

Internetzugang erforderlich JA NEIN

Internetzugang Begründung und notwendige Ressourcen (z.B.: IP Adresse, DNS Name, Protokolle)

GEPLANTER INSTALLATIONSTERMIN

FERNWARTUNG DURCH FIRMA

Fernwartung JA NEIN Art

Fernwartung Begründung (wenn ja)

DISCLAIMER

- 1) Es können nur Geräte im Anlagenbestand der MUI angeschlossen werden.
- 2) Es können keine Privatgeräte an das Netzwerk der MUI angeschlossen werden.
- 3) Das Gerät muss DHCP unterstützen.
- 4) Das Gerät muss mindestens 100 Mbits/s Full-duplex unterstützen, um an das Netzwerk der MUI angeschlossen werden zu können.
- 5) Betriebssysteme, die herstellerseitig keiner Wartung mehr unterliegen, können nicht an das Netzwerk der MUI angeschlossen werden.
- 6) Eine systemseitig aktivierte lokale Firewall am Gerät darf nicht deaktiviert werden.
- 7) Das Gerät muss im LAN mittels Ping erreichbar sein.
- 8) Ein Internetzugang für das Gerät kann grundsätzlich nur freigeschaltet werden, wenn dieses über eine Endpoint Security and Response Software (EDR) oder einen aktuell gehaltenen Schadsoftwarescanner verfügt. Ausgenommen davon sind Systemplattformen, für die keine derartigen Lösungen verfügbar sind.
- 9) Ein Internetzugang für das Gerät kann nur dann freigeschaltet werden, wenn dies auf dem aktuellen Wartungsstand (Patch Level) gehalten wird. Hierfür ist die beantragende OE-Leitung bzw. die zuständige Projektleitung verantwortlich.
- 10) Ein Gerät kann nur angeschlossen werden, wenn es über einen aktivierten Zugriffsschutzmechanismus verfügt (z.B. Benutzername und Passwort).
- 11) Die beantragende OE-Leitung bzw. die zuständige Projektleitung ist für die Datensicherung auf den jeweiligen Geräten verantwortlich.

Datum

Unterschrift GeräteverantwortlicheR

Unterschrift Leitung Organisationseinheit