Department of
Information Technology

In House

MEDIZINISCHE UNIVERSITÄT
INNSBRUCK

Application for network connection for third-party devices / special devices

SUBMIT THE APPLICATION BEFORE ORDERING THE DEVICE

PERSON RESPONSIBLE FOR THE DEVICE

☐ MR. ☐ MRS. ☐ DIVERSE

Last Name ..... First Name .....

Academic degree ..... Organisational Unit .....

User ID ..... Phone Number .....
(q-Number) *(for queries)*

LOCATION

Building, Street, No. .....

Floor ..... Room ..... Network outlet designation .....

DEVICE TO CONNECT

Type ..... Manufacturer ..... Model description .....

Inventory Number .....

Operating system (incl. version) .....

UPDATES

Responsible person / company (service contract)

Operating system updates can be installed ☐ YES ☐ NO

NETWORK

Mac Adress Lan .....

ENDPOINT SECURITY

Virus protection ☐ YES ☐ NO Manufacturer .....

Firewall ☐ Operating system firewall active

☐ Hardware firewall by the manufacturer

☐ Hardware firewall by the Medical University of Innsbruck requested

AD CONNECTION

Active Directory integration possible ☐ YES ☐ NO

REQUIRED NETWORK RESOURCES

(e.g. Group drive, scientific storage, printer...)

.....

.....

.....

INTERNET ACCESS

Internet access required ☐ YES ☐ NO

Internet access justification and necessary resources (e.g.: IP address, DNS name, protocols)

.....

.....

.....

PLANNED INSTALLATION DATE

.....

REMOTE MAINTENANCE

Remote maintenance ☐ JA ☐ NEIN Type .....

Remote maintenance justification (if yes)

.....

.....

.....

DISCLAIMER

- Devices that process or store patient data cannot be connected to the network.
- Only devices in the system inventory of the Medical University of Innsbruck can be connected.
- Private devices cannot be connected to the Innsbruck Medical University data network.
- The device must support DHCP.
- The special device must support at least 100 Mbits/s full-duplex in order to be connected to the data network of the Medical University of Innsbruck.
- Operating systems that have already reached end-of-life can no longer be connected to the data network of the Medical University of Innsbruck.
- The local firewall must be activated on the end device.
- The special device must be pingable in the LAN.
- Internet access for the special device can only be enabled if the device has endpoint security (EDR) or a virus programme.
- Internet access for the special device can only be enabled if it is kept up to date. The respective OU is responsible for this.
- Internet access for the specialised device without user administration is not possible.
- If the special device requires a large number of activations, a network sketch is necessary.
- The OU or the contact person is responsible for the backup of the respective devices and the special software.
- Full Disk Encryption (FDE) must be configured on mobile devices.

.....

Date

.....

Signature of the person responsible for the device

.....

Signature Head of organisational unit