Department of
Information Technology

In House

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 by responsible person /comapny

  YES   NO

NETWORK

Wired mac adress ....

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

1) Only devices that are part of the MUI's equipment inventory can be connected.

2) Private devices cannot be connected to the MUI network.

3) The device must support DHCP.

4) The device must support at least 100 Mbps full-duplex to be connected to the MUI network.

5) Operating systems that are no longer maintained by the manufacturer cannot be connected to the MUI network.

6) A locally activated firewall on the device must not be disabled.

7) The device must be reachable in the LAN via ping.

8) Internet access for the device can only be enabled if it is equipped with Endpoint Security and Response (EDR) software or an up-to-date malware scanner. System platforms for which such solutions are not available are exempt from this requirement.

9) Internet access for the device can only be enabled if it is kept up to date with the latest maintenance (patch level). The requesting organizational unit (OE) management or the responsible project management is responsible for this.

10) A device can only be connected if it has an activated access protection mechanism (e.g., username and password).

11) The requesting organizational unit (OE) management or the responsible project management is responsible for data backup on the respective devices.

....
Date

....
Signature of the person responsible for the device

....
Signature Head of organisational unit