

## BETRIEBSORDNUNG DATENKOMMUNIKATIONSNETZ

### Inhaltsverzeichnis:

0. [Präambel](#)
1. [Technische Spezifikation des Datenkommunikationsnetzes](#)
2. [Zugang zum Datennetz](#)
3. [Aufgaben und Pflichten des Betreibers \(MRZ\)](#)
4. [Aufgaben und Pflichten der Benutzer](#)
5. [Technische Detailregelungen](#)

### 0. PRÄAMBEL

(1) Das Datennetz des Universitätsklinikums ist eine **zentrale infrastrukturelle Einrichtung** zum Zwecke der Datenkommunikation innerhalb der Hochschule. Außerdem sind technische Einrichtungen zur bedarfsweisen Kopplung zu externen Netzen vorhanden.

(2) Das Datennetz ist eine **komplexe technische Einrichtung**, die nur bei hohen Anforderungen an die Sorgfalt, die Qualifikation und die Erfahrung der zuständigen Mitarbeiter des Betreibers geplant, installiert, betrieben, gewartet und repariert werden kann. Der reibungslose Betrieb des Datennetzes setzt außerdem einen verantwortungsvollen Umgang der Nutzer von Netzdiensten mit der leistungsfähigen Ressource Datennetz und eine **optimale Koordinierung von Betreiber und Nutzer** voraus. Deshalb wird diese Betriebsordnung erlassen.

(3) **Betreiber** des Datennetzes ist das Medizinische Rechenzentrum (MRZ).

(4) **Benutzer** des Datennetzes sind im wesentlichen die Angehörigen der Medizinischen Fakultät (Universitätsklinikum).

(5) Das Datennetz umfasst alle **Übertragungseinrichtungen** (Kabel, Koppelleinheiten, Verteilerschränke/Netzwerkelektronik) einschließlich der Anschlusspunkte für die Endgeräte. Ausgenommen sind Übertragungseinrichtungen in der Zuständigkeit anderer Stellen (z.B. Telefonnetz, Brandmeldeanlage, Elektroanlage). Bezüglich der Schnittstellen zu anderen Übertragungseinrichtungen (Telefon, Elektro, Nutzung vorhandener Trassen für die Geländeverkabelung) arbeitet das MRZ mit den zuständigen Abteilungen zusammen.

### 1. TECHNISCHE SPEZIFIKATION DES DATENKOMMUNIKATIONSNETZES

(1) Das Datennetz besteht aus einem **Glasfaser-Backbone-Ring zwischen den Gebietsverteilern (GV)**, einer sternförmigen Anbindung der **Hausverteiler (HV)** sowie einer weiteren sternförmigen Anbindung der **Etagenverteiler (EV)** über Lichtwellenleiter (LWL). Zugangseinrichtungen zum Datennetz sind spezielle **Rechneranschlussdosen**, die über die Tertiärverkabelung (strukturierte Verkabelung nach Class D/E/F oder LWL) auf Etageebene an das Lichtleiternetz angeschlossen sind. Ein EV bedient in der Regel mehrere lokale Netzsegmente in z.T. mehreren Gebäudeebenen. Die Datenübertragungsgeschwindigkeit im Glasfaser-Backbone beträgt n-mal 1000 Mbit/s (Gigabit-Ethernet), die aller übrigen peripheren Bereiche 10/100/1000 MBit/s (Ethernet). Für spezielle mobile Netzanwendungen kommen **Funknetze** mit 11 oder 51 MBit/s zur Anwendung.

(2) Alle Verbindungen werden durch technisch hochwertige **Netzwerkelektronik** (Router, Switches, Terminalserver u.a.) in den Verteilerschränken geschaltet, so dass dem Nutzer ein Datennetz hoher **Leistungsfähigkeit und Verfügbarkeit** bereitgestellt wird. Das Datennetz erlaubt durch den Einsatz geeigneter Vermittlungs- und Kopplungseinrichtungen eine universelle **Strukturierung** und bietet dabei eine **transparente, wahlfreie und leistungsfähige Kommunikation** aller Teilnehmer untereinander. Für sensible Anwendungsbereiche können mit der Netzwerkelektronik Zugriffssperren auf der Netzebene zusätzlich zu den anwendungsspezifischen Zugangsschutzeinrichtungen eingesetzt werden.

(3) Das Datennetz beruht auf den aktuellen technischen **Standards**, z.B.:

- für **Ethernet**: IEEE 802.3 (10BASE-2, 10BASE-T, 10BASE-F/FOIRL)
- für **Fast-Ethernet**: 100BASE-TX, 100BASE-FX
- für **Gigabit-Ethernet**: 1000BASE-TX, 1000BASE-SX, 1000BASE-LX
- für **ATM**: diverse Spezifikationen von ITU-T, ATM-Forum und IETF
- für **Funknetze**: 802.11b, 802.11g
- für alle **Weitverkehrsverbindungen**: die CCITT-Normen wie X.25, X.21, X.21bis, X.28, X.29, X.121, X.75, X.3
- für das **Netzwerkmanagement**: RFC 1157, RFC 1158.
- für **Datenkommunikationsprotokolle**: z.B. ISO/OSI, TCP/IP, IPX u.a.

## 2. ZUGANG ZUM DATENNETZ

(1) Der **Anschluss von Computern** oder anderen Endgeräten an das Datennetz erfolgt ausschließlich durch das MRZ auf Antrag des Benutzers. Der Nutzer muss durch das MRZ autorisiert und eingewiesen werden. Eigenständige **Änderungen** (z.B. Austausch oder Umsetzung des Rechners sowie gravierende Konfigurationsänderungen) sind unverzüglich dem MRZ mitzuteilen. Für Beantragungen und Ummeldungen von Endgeräten existiert ein Online-Formular:

<http://www.med.uni-magdeburg.de/mrz/jpget.shtml>

(2) **Anschlusspunkte** (Endgerätedosen und Koppellelemente) dürfen nur vom MRZ eingerichtet oder verändert werden. Rechner und andere Endgeräte dürfen im Datennetz nur an den vom MRZ registrierten Anschlusspunkten betrieben werden.

(3) Von den Institutionen **selbständig betriebene Datennetze** sind nicht automatisch Bestandteil des Campus-Datennetzes. In Abstimmung mit dem MRZ können solche Netze an bestimmten Übergabepunkten in das Backbone-Netz integriert werden, wenn alle technischen Standards eingehalten wurden und der Betreiber des isolierten Netzes nachweist, dass keine Hard- und Software eingesetzt wird, die geeignet wäre, den Netzbetrieb zu stören und den Informationsfluss im Datennetz zu beeinflussen.

(4) Wird der **Netzbetrieb** über einen Anschlusspunkt oder ein angeschlossenes Endgerät gefährdet, unzumutbar behindert oder gestört, kann das MRZ geeignete Auflagen machen oder Strecken stilllegen.

(5) Kommunikation ist nur möglich, wenn die eingesetzten **Datenkommunikationsprotokolle** bei Sender und Empfänger übereinstimmen. Die Protokollvielfalt ist durch Betreiber und Benutzer des Datennetzes auf das notwendige Maß zu begrenzen. Insbesondere ist die gleichzeitige Verwendung unterschiedlicher Protokolle für vergleichbare Leistungen zu vermeiden. Diese Maßnahmen garantieren eine optimale Netzbelastung und Funktionssicherheit des Datennetzes. Für den gebäudeübergreifenden Verkehr im Campusnetz werden die Netzprotokolle TCP/IP, als Ausnahme IPX, für die Weitverkehrsverbindungen ausschließlich TCP/IP verwendet.

(6) Die **eindeutige Vergabe von logischen Netzadressen** (für Subnetze und Endgeräte) ist ebenfalls unbedingte Voraussetzung für den störungsfreien Netzbetrieb. Eine doppelte Vergabe von z.B. IP-Hostadressen kann zum völligen Stillstand von Netzabschnitten und Anwendungen führen. Aus diesem Grund werden Netzadressen nur vom MRZ vergeben und dokumentiert. Sind in den Einrichtungen qualifizierte DV-Administratoren vorhanden, kann Ihnen vom MRZ ein Adressbereich zur Verfügung gestellt werden, der eigenverantwortlich auf die Endgeräte aufzuteilen ist. Bezüglich der verwendeten Hostadressen besteht gegenüber dem MRZ Meldepflicht.

(7) Bezüglich des **Anschlusses des Universitätsklinikums an das Wissenschaftsnetz** des DFN-Vereins sowie weiterer Verbindungen im Territorium (speziell im Hochschulverbund) arbeitet das MRZ eng mit dem Universitätsrechenzentrum der Otto-von-Guericke-Universität Magdeburg zusammen. Technische Detailfragen zur Hardware- und Software-Installation (z.B. Gigabit-Backbone, DFN-Kommunikationsserver, Nameserver, Electronic Mail, Filetransfer etc.) werden im gegenseitigen Einvernehmen abgestimmt. Der Datenverkehr zum Universitätsnetz, zum Wissenschaftsnetz, Internet und in andere öffentliche Netze wird durch zentrale technische Einrichtungen (z.B. Firewall, Kommunikationsserver, Proxyserver) kanalisiert, aus Sicherheitsgründen besteht keine direkte Verbindung der Endgeräte nach außen.

(8) **Externe Benutzer** des Datennetzes (Benutzer außerhalb des Universitätsklinikums) erhalten nur dann Zugang zum Datennetz, wenn ein förmlicher "Vertrag über den Zugang zum Datenkommunikationsnetz des Universitätsklinikums Magdeburg" oder eine gleichwertige schriftliche Vereinbarung abgeschlossen wurden, die den Zweck des Zugriffs und die Einhaltung der zutreffenden datenschutzrechtlichen Bestimmungen regelt.

Außerdem ist möglichst sicherzustellen, dass durch spezielle Zugangssperren die externen Benutzer nicht in die Lage versetzt werden, den Datenverkehr im Backbone-Netz zu beobachten sowie in irgendeiner anderen als der für ihn zur Verfügung gestellten Anwendung zu arbeiten.

## 3. AUFGABEN UND PFLICHTEN DES BETREIBERS (MRZ)

(1) Das Medizinische Rechenzentrum ist verpflichtet, einen **sicheren und ununterbrochenen Netzbetrieb** mit technischen und personellen Mitteln zu gewährleisten. Nicht vermeidbare Störungen sind auf ein Minimum zu beschränken.

(2) Das MRZ vergibt die **Netzadressen u.a. Identifikationen** (ID-Nr., IP-Adressen, Hostnamen) der Endgeräte sowie **Benutzer-Identifikationen**, installiert und konfiguriert in Zusammenarbeit mit den Nutzern die **Server und sonstigen Endgeräte**. Das MRZ berät in Fragen der Nutzung des Datennetzes und sorgt für die Bekanntmachung der Nutzungsmöglichkeiten.

(3) Das MRZ übernimmt das komplette **Netzwerkmanagement** in den Komponenten:

- Konfigurationsmanagement (Router, Switches, Fileserver, Terminalserver, Printserver, Gateways, Access-Points),
- Durchsatz-Leistungs-Management (Netzwerkoptimierung),
- Fehlermanagement (Erkennen von Fehlerursachen und deren Behebung),
- Informationssicherheitsmanagement (Zugangsschutz, technische Sicherung der Integrität und Qualität der übertragenen Daten, Verschlüsselung sensibler Übertragungstrecken),
- Nutzerverwaltung zentraler Netzdienste und Abrechnungsmanagement.

Das MRZ nutzt zu diesem Zweck ein zentrales Netzwerkmanagementsystem (Hard- und Software).

(4) Das MRZ ist verpflichtet, die **Dokumentation** über alle Komponenten des Netzes (Verkabelung, Ausstattung der Verteilerschränke, Gerätekonfiguration, Endgerätedatenbank) zu erarbeiten und ständig auf aktuellem Stand zu halten.

(5) Das MRZ ist berechtigt, durch belehrte und autorisierte Mitarbeiter Statistiken über die Belastung von Netzabschnitten, Protokollverteilungen, Fehlerhäufigkeiten etc. abzurufen und zum Zweck der **Fehlerbehebung** spezielle Messgeräte und -verfahren in den einzelnen lokalen Netzabschnitten einzusetzen (Protokollanalytiker, Time-Domain-Reflektometer etc.). In diesem Zusammenhang zur Kenntnis gelangte Informationen über Inhalte übertragener Daten sind streng vertraulich zu behandeln.

(6) Das MRZ erhält **Zugangsmöglichkeiten** zu allen Räumen mit technischen Einrichtungen des Datennetzes (Verteilerräume, Serverräume). Das MRZ sorgt für einen auf wenige kompetente Mitarbeiter beschränkten Zugang. In Räumen, in denen zentrale Netzkomponenten und entsprechende Computertechnik zur zentralen Speicherung personengebundener Daten (Patientendaten) untergebracht sind (zentrale Rechnerräume des MRZ), trifft das MRZ besondere technische und organisatorische Maßnahmen zur Gewährleistung der erhöhten Sicherheitsanforderungen. Bei vernetzten DV-Systemen, bei denen der Server nicht im zentralen Rechnerraum untergebracht ist, trägt die für die Applikation zuständige Fachabteilung die Verantwortung für die Sicherheit des Servers und der Daten. Sie wird dabei vom MRZ beraten und unterstützt.

(7) Die verfügbaren **Netzdienste und Protokolle** werden vom MRZ bekannt gegeben. Zusätzliche Anwendungen, die andersgeartete Datenkommunikationsprotokolle oder Netzdienste verwenden, sind auf Anforderung durch den Nutzer durch das MRZ auf Konformität zu testen und dürfen erst nach erfolgreicher Testung in das Datennetz integriert werden.

(8) Das MRZ sorgt in Zusammenarbeit mit dem Geschäftsbereich Technik und Bau für einen angemessenen **Ausbau des Datennetzes** nach Bedarf, technischem Fortschritt und finanziellen Realisierungsmöglichkeiten unter Beachtung der Wirtschaftlichkeit der Anlagen. Dabei wird das MRZ von den Planungsgremien des Universitätsklinikums bei Bau- und Investitionsvorhaben zu Beratungsleistungen hinsichtlich der notwendigen Datenkommunikationsinfrastruktur herangezogen.

#### 4. AUFGABEN UND PFLICHTEN DER BENUTZER

(1) Für jeden an das Datennetz angeschlossenen Rechner ist dem MRZ ein **Verantwortlicher** zu benennen, soweit die Anlagen nicht vom MRZ selbst betrieben werden.

(2) Bei den an das Datennetz angeschlossenen Rechnern obliegt der **Schutz vor unberechtigtem Zugang und unberechtigtem Zugriff auf gespeicherte Daten** dem jeweiligen Rechner-Betreiber. Der Benutzer darf aus dem Datennetz nur diejenigen Daten auf seinen Rechner leiten, die für ihn bestimmt sind. Beschaffung und Einsatz von Geräten und Programmen, die einen Missbrauch ermöglichen, sind unzulässig.

(3) Bei der **Übermittlung von Daten** ist zu beachten, dass technische und organisatorische Maßnahmen nie einen 100%igen Schutz vor Missbrauch der Daten bieten können. Es sind für sensible Bereiche nur solche DV-Verfahren (Software) anzuwenden, die einen ausreichenden gestaffelten **Zugriffsschutz auf der Anwendungsebene** realisieren. Der Benutzer hat die geltenden Bestimmungen zum Datenschutz zu beachten. Schutzwürdige Daten sind im Sinne des Datenschutzgesetzes über öffentliche Netze nur bei absoluter Notwendigkeit und nach Möglichkeit verschlüsselt weiterzuleiten.

(4) Unberechtigtes "Mithören" und **Aufzeichnen fremder Daten** aus dem Datennetz sowie das Stören der Kommunikation sind verboten. Davon ausgenommen sind Maßnahmen der Fehlerverfolgung durch das MRZ (s. § 3 Absatz 5).

(5) Der Benutzer ist verpflichtet, dem MRZ **Unregelmäßigkeiten, Störungen oder Missbrauchsversuche** anzuzeigen.

(6) Benutzer oder Dritte dürfen keine **Modifikationen am Datennetz** vornehmen. Identifikationsmerkmale von Rechnern (Netzadressen, Namen usw.) dürfen nicht eigenmächtig verändert werden. Die Netzstruktur verändernde Geräte (Hubs, Switches, Router, Access-Points) sowie **Telefon-Wählmodems oder ISDN-Adapter** an Rechnern im Datennetz dürfen nicht eigenständig, ohne Mitwirkung oder Kenntnisnahme des MRZ installiert und in Betrieb genommen werden. Sollte ein Betrieb von Wählverbindungen an Rechnern im Datennetz unumgänglich sein, ist organisatorisch sicherzustellen, dass diese Verbindungen nur auf das unbedingt notwendige Maß beschränkt werden und von außen nicht anwählbar sind. Gleichzeitige Verbindungen von Endgeräten zum Telefon- und zum Datennetz sind i.d.R. unzulässig.

(7) **Anwendungsspezifische Benutzerveränderungen** (z.B. Neueintragung von Benutzernamen und -rechten, Konfiguration von Netzdruckern u.ä.) kann der Systemadministrator der Struktureinheit eigenverantwortlich vornehmen. Das MRZ ist über Veränderungen zu informieren.

(8) Der **Datenverkehr** eines Benutzers darf den anderer Benutzer nicht unangemessen beeinträchtigen. Der Einsatz besonders netzbelastender Übertragungen ist in Abstimmung mit dem MRZ nach Möglichkeit auf verkehrsschwache Zeiten zu verschieben.

#### 5. TECHNISCHE DETAILREGELUNGEN

(1) Die Verfahrensweise zur Installation von Endgeräten im Datenkommunikationsnetz und zur Vergabe von Netzwerkadressen für Endgeräte wird in der "Betriebsregelung zur Vergabe von Netzadressen" definiert.

(2) Spezielle Regelungen zu Netzwerkteilerräumen und Serverräumen enthält die "Betriebsordnung EDV-Räume".

(3) Weitere technische Detailregelungen werden vom Medizinischen Rechenzentrum entsprechend dem technischen Fortschritt und dem Fortgang der Arbeiten am Campusnetz sowie der installierten Netzanwendungen erstellt und bei Bedarf fortgeschrieben.

(4) Die Betriebsordnung für das Datenkommunikationsnetz betrifft sehr spezifische Verfahrensweisen, die insbesondere einen speziellen Personenkreis (DV-Personal) betreffen. Darüber hinaus gehende, alle Nutzer betreffende Fragen werden in der "Betriebsordnung für Datenverarbeitungs- und Informationssysteme (DV-Ordnung)" des Universitätsklinikums bzw. ggf. in den Betriebsregelungen und Betriebsvereinbarungen einzelner DV-Systeme geregelt.