Rahmenordnung für die Nutzung der Rechen- und Kommunikationstechnik am Universitätsklinikum Carl Gustav Carus und der Medizinischen Fakultät an der TU Dresden

Version:2.0.8
Stand: 17.01.2011

Inhaltsverzeichnis

§ 1 - Geltungsbereich

(1) Diese Ordnung gilt für die Nutzung aller rechen- und kommunikationstechnischen Einrichtungen, sowie der zugehörigen elektronischen Informations- und Kommunikationsdienste einschließlich Software – *IT-Systeme*[1], für deren Nutzung und die Gesamtheit der Benutzer am Universitätsklinikum „Carl Gustav Carus“ an der TU Dresden, im Folgenden UKD genannt, und an der Medizinischen Fakultät der TU Dresden, im Folgenden MF genannt. Sie enthält für die Benutzer unmittelbar geltende Mindestregelungen.
(2) Die Inanspruchnahme der in § 1 Abs. 1 dieser Ordnung genannten Einrichtungen und Dienste ist ausschließlich durch Mitglieder einer geschlossenen Benutzergruppe und zum Zweck des § 3 dieser Ordnung zulässig. Zur geschlossenen Benutzergruppe gehören abschließend folgende Personen:

1. Beschäftigte des UKD und der MF
2. sonstige natürliche Personen, die die in § 1 Abs. 1 genannten Einrichtungen und Dienste zur Erfüllung Ihrer Aufgaben nach § 3 zeitlich begrenzt in Anspruch nehmen (Studenten, Praktikanten, Doktoranden, Gäste)
3. Zum Nutzerkreis gehören weiterhin Dritte, die auf Grund von vertraglich fixierten Aufgaben Zugriff auf die rechen- und kommunikationstechnischen Einrichtungen sowie die zugehörigen elektronischen Informations- und Kommunikationsdienste des UKD und der MF haben. In diesen Fällen sind Regelungen, welche in dieser Rahmenordnung Gültigkeit haben, vertraglich zu fixieren. Folgende Verträge sind im Besonderen zu berücksichtigen:
    1. Wartungsverträge
    2. Datenverarbeitung im Auftrag
    3. Kooperationsverträge

(3) Für die dienstliche Nutzung *privater* Hard- und Software gelten die Bestimmungen dieser Rahmenordnung.
(4) Regelungen in dieser Rahmenordnung werden durch Bestimmungen in der „Dienstvereinbarung über Nutzung der E-Mail-, Intranet- und Internet-Dienste“ untersetzt..
(5) Die Bestimmungen aus der „Rahmenordnung für die Rechen- und Kommunikationstechnik und die Informationssicherheit an der TU Dresden“ vom 08.01.2009 finden in dieser Rahmenordnung Berücksichtigung.

§ 2 - Gegenstand der Ordnung

Gegenstand dieser Ordnung sind die Regelung der Nutzungsmöglichkeiten und Rechte als auch die verbindlich einzuhaltenden Pflichten für die in § 1 Abs. 1 genannten Dienste und Einrichtungen, inklusive der Software.

§ 3 - Nutzung, Zulassung zur Nutzung und Betrieb von IT-Systemen

(1) Die Zulassung zur Nutzung der *IT-Systeme* nach § 1 Abs. 1 erfolgt für dienstliche Zwecke wie z. B. medizinische Betreuung, Verwaltung, Forschung, Lehre und Studium.
(2) Der Zugang zu internem Datennetz, Internet, E-Mail und Faxversand ist grundsätzlich der dienstlichen Nutzung vorbehalten.
(3) Die Nutzung der Einrichtungen, Dienste und Software nach § 1 Abs. 1 dieser Ordnung für andere Zwecke ist nur zulässig, wenn sie geringfügig ist, die Nutzung der *IT-Systeme* durch die anderen Nutzer nicht behindert oder stört und die dienstliche Aufgabenerfüllung nicht beeinträchtigt wird.
(4) Im Rahmen der privaten Nutzung dürfen keine kommerziellen oder sonstige geschäftliche Zwecke verfolgt werden. Es besteht kein Anspruch auf private Nutzung. Die Leiter der Struktureinheiten haben das Recht, die private Nutzung an einzelnen *IT-Systemen* zu

[1] Die in kursiv gehaltenen Begriffe werden in Anlage 8 definiert.

untersagen. Im Auftrag des Leiters der Struktureinheit können die *IT-Verantwortlichen IT-Systeme* auf missbräuchliche Nutzung kontrollieren. Bezüglich der Kontrollrechte von Leitern der Struktureinheiten und IT-Verantwortlichen wird auf die §§ 15 und 16 verwiesen.
(5) Alle sicherheitsrelevanten Ereignisse, wie z. B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verdacht auf Missbrauch der eigenen Benutzerkennung sind unverzüglich dem zuständigen *IT-Verantwortlichen* der Struktureinheit zu melden.
(6) Für die Nutzung von in den Struktureinheiten selbstständig verwalteten und betriebenen *IT-Systemen* sind weiterführende Bestimmungen und Hinweise für die Leiter der Struktureinheit und die *IT-Verantwortlichen* in der Anlage 1 Pkt. 2 „Netzbetrieb“ enthalten.
(7) Die Nutzung *mobiler IT-Systeme* wird im § 9.3 und § 9.4 gesondert geregelt.
(8) Öffentlich zugängliche *Netzwerkanschlüsse* sind vor unbefugten Zugriffen auf das interne Netz zu schützen.

§ 4 - Umgang mit schutzwürdigen Daten

§ 4.1 - Verarbeitung schutzwürdiger Daten

(1) Der Aufwand für *Datenschutz-* und Datensicherungsmaßnahmen muss in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Für die Beurteilung der Schutzwürdigkeit (Sensibilität) personenbezogener Daten gilt das in Anlage 1 “Definition von Schutzklassen“ beschriebene Schutzstufenkonzept. Als Grundlage für die Beurteilung der Zulässigkeit der Verarbeitung solcher Daten und des zu betreibenden Schutzaufwandes dient die Gesamtschutzstufe.
(2) Die Verarbeitung von schutzwürdigen Daten ist nur an *vertrauenswürdigen Systemen* oder am UKD und MF befindlichen *Standalone-Systemen* zulässig. Die Speicherung von schutzwürdigen Daten außerhalb des UKD bzw. MF wird in verschlüsselter Form empfohlen und ist nur solange zulässig wie für die Zweckerfüllung nach § 3 Abs. 1 notwendig. Die Verarbeitung von Daten der Gesamtschutzstufe C und D auf *privaten IT-Systemen, für die keine vertragliche Regelung besteht,* ist untersagt. Weiterführende Bestimmungen sind im § 9 enthalten.
(3) Für personenbezogene Daten, die ausschließlich zur Sicherstellung eines ordnungsgemäßen Betriebs von *IT-Systemen* dienen (z. B. Kennwörter), und für Daten, die nicht dem *Datenschutz* unterliegen, gilt § 4.1 Abs. 1 bis 2 nicht. Hier können gesonderte Regelungen existieren, die z. B. zur Wahrung des Betriebsgeheimnisses erforderlich sind.
(4) Für die Veröffentlichung personenbezogener Mitarbeiterdaten auf elektronischem Wege (z. B. Telefonverzeichnis) finden die einschlägigen Bestimmungen des Sächsischen Datenschutzgesetzes (SächsDSG) in der jeweils gültigen Fassung Anwendung. Andernfalls ist eine schriftliche Einwilligung des Betroffenen notwendig.

§ 4.2 - Übertragung schutzwürdiger Daten über das Internet

(1) Bei der E-Mailkommunikation über das Internet ist im Besonderen der §203 StGB „Verletzung von Privatgeheimnissen“ zu beachten.
(2) Die Übertragung von schutzwürdigen Daten der Gesamtschutzstufe C und D über das Internet (z. B. E-Mail) ist nur in verschlüsselter Form zulässig. Für andere schutzwürdige, nicht dem *Datenschutz* unterliegende, Daten (z,B. Betriebs- und Forschungsdaten) kann jede Struktureinheit eigene Festlegungen treffen. Zur Einrichtung der Verschlüsselung ist sich an den jeweiligen *IT-Verantwortlichen* der Struktureinheit zu wenden.
(3) Unverschlüsselter E-Mail-Versand von schutzwürdigen Daten ist nur gestattet, wenn sich die Mailkonten von Absender und Empfänger innerhalb des UKD-Netzes befinden, also auf @uniklinikum-dresden.de enden.
(4) Der externe Zugriff auf Mailkonten des UKD hat ausschließlich mit dem vom MRZ zur Verfügung gestellten OutlookWebAccess (OWA) zu erfolgen. Ausnahmeregelungen sind vom Geschäftsbereichsleiter des MRZ zu genehmigen.

(5) Die automatische Weiterleitung von Mailkonten, die auf @uniklinikum-dresden.de enden, nach externen E-Mailkonten ist nicht zulässig. Als externe Mailkonten werden alle Mailkonten betrachtet, welche nicht auf @uniklinikum-dresden.de enden.
(6) Mit Ausnahme der TU-Mailkonten ist jeglicher Zugriff auf externe E-Mailkonten nur WEB-basiert erlaubt.
(7) Weiterführende Bestimmungen zur Verschlüsselung sind für *IT-Verantwortliche* in Anlage 1 Pkt. 5 „Datenverschlüsselung und -transfer“ enthalten.

§ 4.3 - Übertragung schutzwürdiger Daten über Telefax

(1) Die Übertragung von personenbezogenen Daten der Datenschutzstufen B, C und D (entsprechend Anlage 1) per Telefax an externe Empfänger darf nur in Notfällen erfolgen, wobei zusätzlich folgende Sicherheitsvorkehrungen zu treffen sind:

1. Deckblatt mit Absender- und Empfängeranschrift sowie Anzahl der zu übertragenden Seiten verwenden
2. Abstimmung des Sendezeitpunkts mit dem Empfänger
3. sorgfältige Wahl der Anschlussnummer des Empfängers
4. Speichern wichtiger Faxnummern im Gerät
5. unverzüglicher Abbruch bei Wählfehlern
6. Registrierung und Archivierung der übertragenen Dokumente sowie der Übertragungsprotokolle.

(2) Für andere schutzwürdige, nicht dem *Datenschutz* unterliegende, Daten kann jede Struktureinheit eigene Festlegungen treffen.
(3) Für den Faxbetrieb sind grundsätzlich vom MRZ angebotene und zugelassene Lösungen zu nutzen.
(4) Die Bestimmungen im „Merkblatt zur Nutzung von Telefaxgeräten am UKD“ (siehe Intranet UKD und MF) sind zu beachten.

§ 5 - Benutzerkennung

(1) Für alle im § 1 Abs. 2 Pkt. 1 und 2 benannten Benutzer werden für zentrale *IT-Systeme* vom Medizinischen Rechenzentrum und für dezentrale *IT-Systeme* vom jeweiligen *IT-Verantwortlichen* Benutzerkennungen vergeben und verwaltet.
(2) Alle Benutzer haben persönliche Anmeldenamen und Kennwörter zu verwenden. Struktur- bzw. Funktionslogins sind nur zulässig, wenn es die Arbeitsabläufe erfordern. Benutzerkonten dürfen nur mit den minimal notwendigen Rechten ausgestattet werden. Benutzerkonten mit administrativen Rechten sind nur zum Zwecke der Administration zu verwenden. Die Benutzer sind verpflichtet, ausschließlich mit den Benutzerkennungen (Anmeldename, Kennwort) zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde. Die Weitergabe von personalisierten Benutzerkennungen, d. h. an Personen gebundene Logins, ist nicht gestattet. Jeder Nutzer hat dafür Sorge zu tragen, dass unberechtigten Personen die Verwendung seiner Benutzerkennung verwehrt wird. Dazu gehört die sorgfältige Wahl eines nicht einfach zu erratenden Kennwortes.
(3) Bei der Vergabe von Kennwörtern sollte auf die Einzigartigkeit der Kennwörter geachtet werden. Unter Berücksichtigung der technischen, strukturellen und organisatorischen Machbarkeit werden folgende Regelungen für die Kennwortvergabe empfohlen:

1. Verwendung von mindestens 8 Zeichen
2. nur zwei aufeinanderfolgende Zeichen dürfen gleich sein
3. Verwendung von mindestens einem Buchstaben, einer Ziffer und einem Sonderzeichen (z.B. „A%gh29§k“ - Bitte dieses Kennwort nicht verwenden!).

(4) Dem Nutzer ist es untersagt, fremde Kennwörter zu ermitteln und zu nutzen. Für *IT-Verantwortliche* gelten die Regelungen in § 15.
(5) Es ist eine regelmäßige Änderung der Kennwörter aller 180 Tage anzustreben.

(6) Beim Ausscheiden eines Nutzers nach § 1 Abs. 2 Pkt. 1 und 2 sind dessen Benutzerkennungen und E-Mail-Adresse spätestens zum Ende des 1. Quartals des folgenden Kalenderjahres zu löschen.

§ 6 - E-Mail

(1) Die E-Mail-Kommunikation sollte grundsätzlich auf *vertrauenswürdigen Systemen* erfolgen.
(2) Für alle ein- und ausgehenden E-Mails am Mailsystem des UKD findet eine Prüfung auf *Schadsoftware* (z. B. Viren) statt. Eingehende E-Mails werden vor ihrer Weiterverarbeitung auf SPAM überprüft (siehe weiterführende Regelungen in § 11 Abs. 5 und § 15 Abs. 10. Da Fehlbewertungen nicht vollständig ausgeschlossen werden können, übernimmt das MRZ keine Haftung dafür, dass ausschließlich SPAM-Mails als solche erkannt werden.
(3) Am UKD werden E-Mail-Adressen für im § 1 Abs. 2 Pkt. 1 und 2 benannte Benutzer grundsätzlich mit Vorname.Nachname@uniklinikum-dresden.de gebildet.
(4) Bei Bedarf können personenunabhängige E-Mail-Adressen nach Anlage 1 Pkt. 3 „Rechte und Pflichten von IT-Verantwortlichen“ vergeben werden.
(5) Vertreterregelungen werden in der „Dienstvereinbarung zur Nutzung der E-Mail-, Intranet- und Internetdienste am Universitätsklinikum und an der Medizinischen Fakultät“ festgelegt.
(6) Für die Zweckerfüllung nach § 3 Abs. 1 sind ausschließlich die Mailadressen nach § 6 Abs. 3 und 4 dieser Rahmenordnung bzw. nach § 7 Abs. 9 der „Rahmenordnung für Rechen- und Kommunikationstechnik und die Informationssicherheit an der TU Dresden“ zu nutzen.
(7) Die Bildung und Nutzung von E-Mail-Verteilerlisten ist nur zulässig soweit dies zur Durchführung des Dienst- oder Arbeitsverhältnisses, zur Durchführung organisatorischer Maßnahmen sowie für Ausbildungs-, Prüfungs- oder wissenschaftliche Zwecke erforderlich ist.
(8) Für die Kommunikation von UKD-Mailservern mit externen mobilen Geräten sind ausschließlich vom MRZ betriebene Lösungen zu nutzen.
(9) Für die Übermittlung von größeren Datenmengen, die nicht über das existierende E- Mail-System versendbar sind, kann das MRZ Alternativen bereitstellen, die über den *IT-Verantwortlichen* zu erfragen sind.
(10) Weiterführende Hinweise und Bestimmungen zum Umgang mit E-Mails und Schutz vor *Schadsoftware* sind in Anlage 1 Pkt. 4.2 „Hinweise für Mitarbeiter“ enthalten.

§ 7 - Telekommunikation

Es gelten die Festlegungen der jeweils gültigen Fassung der Dienstvereinbarung zwischen dem UKD und dem Personalrat des UKD sowie der TU-Dresden und dem Personalrat der TU Dresden zur Nutzung der Telekommunikationsanlage am Universitätsklinikum und an der Medizinischen Fakultät.

§ 8 - Externe Kommunikation - Fernzugang

§ 8.1 - Externe Kommunikation mit dem Campusnetz

(1) Die *externe Kommunikation* mit dem Campusnetz darf ausschließlich über die zentralen Zugangssysteme des Medizinischen Rechenzentrums erfolgen. Siehe dazu die Anlage 1 Pkt. 7 „Externe Kommunikation“.
(2) Voraussetzung für die Einrichtung und Aktivierung eines Fernzuganges für Fremdfirmen zum Zwecke der Fernwartung ist ein gültiger EVB-IT-Vertrag oder ein „Fernwartungsvertrag“ (siehe Intranet UKD und MF) mit der Datenschutzvereinbarung auf der Grundlage der existierenden Mustervereinbarung „Muster Datenschutzvereinbarung zu einem IT-Vertrag (HW und SW)“ (siehe Intranet UKD und MF) und dem ausgefüllten Datenblatt „Zugriff auf die Netzinfrastruktur durch Fernwartungsfirmen“ (siehe Intranet UKD und MF). Die Beantragung hat über die

standardisierten Formulare vom Verantwortlichen des zu wartenden Systems an den Verantwortlichen für *externe Kommunikation*ssysteme zu erfolgen.
(3) Voraussetzung für die Einrichtung und Aktivierung eines Fernzuganges für medizinische Fremdeinrichtungen ist ein gültiger Kooperationsvertrag inklusive Datenschutzklausel mit geltenden Regelungen aus dieser Rahmenordnung und das ausgefüllte Datenblatt: „Zugriff auf die Netzinfrastruktur durch medizinische Fremdeinrichtung“ (siehe Intranet UKD und MF).
(4) Voraussetzung für die Einrichtung und Aktivierung eines Fernzuganges für medizinische Einrichtungen des UKD außerhalb des Campusnetzes ist das ausgefüllte Datenblatt: „Zugriff auf die Netzinfrastruktur durch externe UKD-Einrichtungen“ (siehe Intranet UKD und MF).
(5) Der Verantwortliche für *externe Kommunikationssysteme* ist vom *IT-Verantwortlichen* bei technischen Änderungen von Verträgen bezüglich Fernzugangs zu informieren.
(6) Verträge mit Fernzugangsvereinbarungen für Software sind ausschließlich vom Bereich Medizinisches Rechenzentrum abzuschließen.
(7) Der Abschluss eines Vertrages mit Fernzugangsvereinbarung ist stets dem Datenschutzbeauftragten am UKD zur Kenntnisnahme vorzulegen.
(8) Bei Abschluss und Verlängerung von Verträgen mit Fernzugangsvereinbarung ist der Verantwortliche für *externe Kommunikationssysteme* schriftlich über die voraussichtliche Laufzeit zu informieren. Bei Kündigungen von Verträgen mit Fernzugangsvereinbarung ist von der unterzeichnenden Stelle des Vertrages der Verantwortliche für *externe Kommunikationssysteme* schriftlich zu informieren.
(9) Bereits vorhandene Altverträge sollten den Bedingungen der Anlage „Muster Datenschutzvereinbarung zu einem IT-Vertrag (HW und SW)“ angepasst werden.
(10) Der Datenschutzbeauftragte hat bei Änderungen der gesetzlichen Regelungen die entsprechenden Anlagen anzupassen und die Vergabestelle Geschäftsbereich LOG, Bereich Kundendienstverträge Medizintechnik Geschäftsbereich LOG und die Arbeitsgruppe Security Policy zu informieren.
(11) Für die Übertragung medizinischer Informationen über das Internet ist ein *VPN-Tunnel* mit Verschlüsselung nach Anlage 1 Pkt. 5 „Datenverschlüsselung und -transfer“ erforderlich und vertraglich abzusichern.
(12) Die Kennwortübertragung bei Anmeldungen darf aus Sicherheitsgründen nur verschlüsselt erfolgen.
(13) Detaillierte Angaben sind in der Anlage 1 Pkt. 7 „Externe Kommunikation“ enthalten.

§ 8.2 - Temporäre externe Kommunikation mit Standalone-Geräten

Die Kommunikation mit *Standalone-Geräten* ist individuell in den Struktureinheiten und in Abstimmung mit dem Datenschutzbeauftragten und dem *IT-Verantwortlichen* zu regeln.

§ 8.3 - Fernzugang für Mitarbeiter

(1) Die Einrichtung eines Fernzugangs kann in folgenden Fällen erfolgen:

1. Fernzugang zu Informationssystemen mit Patientendaten zur ärztlichen Betreuung von Notfallpatienten,
2. Fernzugang zur technischen Sicherstellung der Lauffähigkeit von *IT-Systemen*,
3. Fernzugang zu Informationssystemen im Rahmen der Medizinischen Forschung.

(2) Die Einrichtung eines Fernzugangs erfolgt auf Antrag des Direktors/Leiters der jeweiligen Struktureinheit und in Abstimmung mit dem Leiter des Medizinischen Rechenzentrums und dem Systemverantwortlichen. Wird dem Antragsteller der Fernzugang verwehrt, kann eine Vorstandsentscheidung herbeigeführt werden.
(3) Die Genehmigung zur Einrichtung eines Fernzuganges zu Informationssystemen im Rahmen der Medizinischen Forschung entscheidet der Leiter der Struktureinheit nach Antrag des Projektleiters.
(4) Zur Beantragung eines Fernzuganges ist das Formular “Antrag auf Nutzung von Fernzugängen in das Campusnetz des UKD“ und das Datenblatt „Zugriff auf die Netzinfrastruktur durch Mitarbeiter“ (siehe Intranet UKD und MF) zu verwenden.

(5) Für Daten der Gesamtschutzstufe D gilt: Der Fernzugang wird grundsätzlich nur mit UKD - eigenen *IT-Systemen* (z. B. Dienstnotebook) gestattet.
(6) Es ist untersagt, eigenmächtig jegliche Änderungen an den vom *IT-Verantwortlichen* vorgenommenen Sicherheitseinstellungen vorzunehmen.

§ 9 - Umgang mit Arbeitsplatz-Rechner, Daten und Speichermedien, mobilen Datenträgern sowie mobilen Systemen

§ 9.1 - Umgang mit Arbeitsplatz-Rechnern

(1) Bei jedem Verlassen des Arbeitsplatzes, auch kurzzeitig, ist der PC vor dem Zugriff unberechtigter Personen zu schützen.
(2) Nach Dienstende sind die Rechner herunterzufahren und abzuschalten, ausgenommen die Zweckerfüllung nach § 3 Abs. 1 wird dadurch gefährdet oder vom Leiter der Struktureinheit wurden gesonderte Festlegungen getroffen. Für Systemwartungen sind in Absprache mit dem zuständigen *IT-Verantwortlichen* Sonderregelungen möglich.

§ 9.2 - Speicherung von Daten

(1) Zur Speicherung von dienstlich relevanten Daten werden auf Servern zentrale Ablagen (Netzlaufwerke) vorgehalten. Sämtliche Daten sind insbesondere auch aus Gründen der Sicherheit vor Datenverlust in einem solchen Laufwerk abzulegen und zu nutzen. Die dauerhafte alleinige Ablage dienstlich relevanter Daten auf lokalen Festplatten oder Datenträgern ist untersagt.
(2) Speicherung von Daten der Gesamtschutzstufe D auf *privaten* Datenträgern ist nicht gestattet.
(3) Speicherung von Daten der Gesamtschutzstufe D auf mobilen Datenträgern bedarf einer *Rechtsgrundlage* oder der Zustimmung der betroffenen Personen. (z. B. Vertragsbeziehung, *SächsDSG, BDSG*)
(4) Daten sind den gesetzlichen Vorgaben entsprechend zu archivieren.

§ 9.3 - Verwendung von mobilen Datenträgern

(1) Bei Verwendung von mobilen Datenträgern (Diskette, CD, DVD, Wechseldatenträger, USB-Stick usw.) wird wegen der hohen Gefahr der Einschleppung von *Schadsoftware* auf die Regelungen § 11 Abs. 1 hingewiesen.
(2) Es liegt im Ermessen der Struktureinheiten die Verwendung mobiler Datenträger einzuschränken.

§ 9.4 - Umgang mit mobilen Systemen

(1) Bei der Überlassung von *mobilen Systemen* gelten besondere Sorgfaltspflichten seitens des Mitarbeiters. Es wird die Verwendung einer Diebstahlsicherung empfohlen.
(2) Bei der Nutzung von Fremdprovidern für die Internetkommunikation mit Dienstnotebooks ist die Aktivierung einer lokalen Firewall und eines Virenschutzes (z. B. Einbindung in den Sophos-Remote-Update-Service) verpflichtend.
(3) Die Nutzung von *privaten mobilen Systemen* ist am UKD-Netzwerk untersagt. Über alle *IT-Systeme* hat der *IT-Verantwortliche* die alleinige administrative Hoheit. In begründeten Einzelfällen kann der Leiter der Struktureinheit im Einvernehmen mit dem *IT-Verantwortlichen* Ausnahmen gestatten, welche mit dem Formular „Antrag auf Nutzung privater mobiler Systeme am UKD-Netzwerk“ (siehe Intranet UKD und MF) zu protokollieren sind.
(4) *Mobile Systeme* dürfen während der Verbindung mit dem UKD-Netzwerk keine Verbindung in andere IT-Netzwerke (z. B. via UMTS) haben.
(5) Bei der Nutzung *mobiler Systeme* wie z. B. Mobilfunktelefone oder Digitalkameras, mit denen Bild-, Audio- und Videodaten erstellt werden können, sind zusätzlich z,B. die Grundsätze

zum Persönlichkeitsrecht im Grundgesetz und die entsprechenden Regelungen zum Kunsturhebergesetz zu beachten.

§ 9.5 - Entsorgung und Reparatur von Datenträgern

(1) Alle Datenträger des UKD und MF (z. B. Diskette, USB-Stick, selbst erstellte CD und DVD, Magnetbänder, Festplatten, Farbbänder) sind entsprechend der aktuellen Ausgabe des „Abfallwegweiser UKD“ der Krankenhausökologie (siehe Intranet UKD und MF) zu entsorgen. Der Bereich Krankenhaushygiene und Umweltschutz nimmt gesammelte Datenträger entgegen und sorgt für eine datenschutzgerechte und/oder eine sachgerechte Entsorgung durch ein dafür autorisiertes Dienstleistungsunternehmen. Die Übergabe der Datenträger ist von der Krankenhausökologie zu quittieren.
(2) Für die Wartung bzw. Reparatur von Datenträgern, insbesondere von Festplatten, durch Fremdfirmen ist sicherzustellen, dass Unbefugten keine schutzwürdigen Daten zur Kenntnis gelangen können. Folgende Regelungen sind einzuhalten:

1. ausschließliche Auswahl von Firmen, die sich zur datenschutzgerechten Behandlung der Datenträger verpflichtet haben
2. schriftliche Auftragserteilung durch Geschäftsbereich BUT
3. Abgrenzung der Aufgaben des Auftragnehmers durch klare Weisungen zu Wartung bzw. Reparatur
4. der Auftragnehmer ist darüber zu unterrichten, dass Datenträger oder Geräte, auf denen sich s*chutzwürdige Daten* befinden, nicht an Dritte (z. B. Unterauftragnehmer) weitergegeben werden dürfen
5. der Auftragnehmer ist über die Besonderheiten beim Umgang mit personenbezogenen Daten zu unterrichten
6. ein *IT-System*, Speichersystem oder Gerät, welches *schutzwürdige Daten* der Datenschutzstufe C oder D enthält, darf den Wirkungsbereich des UKD bzw. der MF grundsätzlich nicht verlassen. Ausnahmen von dieser Grundsatzregelung sind nur in besonderen Fällen möglich, in denen eine zwingend benötigte Maßnahme oder Leistung nicht innerhalb des Wirkungsbereiches des UKD/der MF erstellbar oder erbringbar ist. Die jeweilige Einzelfallregelung ist für den konkreten Fall schriftlich nieder zu legen und muss unter Einbeziehung des Datenschutzbeauftragten, der Zustimmung des Leiters der Struktureinheit der speichernden Stelle und des Geräteverantwortlichen beinhalten. Die Verantwortung für die Herbeiführung der Einzelfallregelung und deren ordnungsgemäße Ausführung und Dokumentation trägt der Leiter der verantwortlichen Struktureinheit (der speichernden Stelle).
7. Der Geschäftsbereich BUT muss mit dem Auftrag zur Wartung bzw. Reparatur von IT-Systemen vom jeweiligen IT-Systemverantwortlichen in Kenntnis gesetzt werden, wenn sich auf diesen *IT-Systemen schutzwürdige Daten* befinden bzw. befinden könnten. Die Datenschutzstufe ist entsprechend anzugeben.
8. Wartungs- bzw. Reparaturarbeiten an Datenträgern oder Geräten, die s*chutzwürdige Daten* enthalten, sind nur im Geltungsbereich des Grundgesetzes erlaubt. Der Transport in das Ausland ist unzulässig.
9. Dem Auftragnehmer ist Punkt 8 zur Kenntnis zu geben.
10. Soweit einer der Punkte 1 bis 9 nicht erfüllt wird, sind nach Möglichkeit *schutzwürdige Daten* vor Auftragsausführung vom Datenträger/ Gerät zu löschen (s. a. Abs. 4 und 5). Sollte dies nicht möglich sein, ist auf eine Wartung oder Reparatur des Datenträgers zu verzichten.

(3) Bei dem Austausch defekter Datenträger mit *schutzwürdigen Daten* außerhalb des Zeitraumes der Verjährung von Mängelansprüchen (früher *Gewährleistung*) bzw. außerhalb der Dauer einer möglichen *Garantie* ist unbedingt die Übergabe des defekten Datenträgers an den Nutzer zu verlangen. Auf keinen Fall ist der Wartungsfirma die Entsorgung zu überlassen.
(4) Beim Austausch defekter Datenträger mit *schutzwürdigen Daten* innerhalb des Zeitraumes der Verjährung von Mängelansprüchen bzw. während der Dauer einer möglichen Garantie wird die zur Garantieleistung verpflichtete Firma im Allgemeinen die Rückgabe des defekten

Datenträgers verlangen. Es ist vom *IT-Verantwortlichen* zu versuchen, Daten der Datenschutzstufen C und D mit geeigneter Software oder geeigneten Geräten zu löschen, siehe dazu Anlage 1 Pkt. 6 „Entsorgung und Reparatur von Datenträgern“. Ist dies nicht möglich, so ist das Löschen oder Vernichten des Datenträgers als Datenverarbeitung im Auftrag gem. § 7 SächsDSG [1] durchführen zu lassen (Hinweise zur Auftragsvergabe s. a. Abs. 1). Ist die Sensibilität der Daten hoch (Datenschutzstufe D), sollte auf den Garantieanspruch verzichtet werden.
(5) Vor der Umsetzung von Datenträgern bzw. Geräten an Nutzer, die nicht berechtigt sind, die auf dem Gerät befindlichen Daten zu verarbeiten, sind die Daten durch Überschreiben mit geeigneter Software zu beseitigen, siehe dazu Anlage 1 Pkt. 6 „Entsorgung und Reparatur von Datenträgern“.
(6) Bei der Entsorgung von IT-Technik oder der Umsetzung nach Abs. 5 ist der *IT-Verantwortliche* der Struktureinheiten einzubeziehen. Der *IT-Verantwortliche* hat für die sachgerechte Löschung von Daten der Datenschutzstufen C und D zu sorgen.
(7) Die Löschung von Daten der Datenschutzstufen C und D muss in geeigneter Form protokolliert werden.

§ 10 - Software

(1) Beim Einsatz von Software sind die für das Produkt gültigen Lizenzbestimmungen einzuhalten.
(2) Alle für die dienstliche Nutzung zu beschaffenden Software-Produkte, die vom Hersteller für den beabsichtigten Verwendungszweck kostenpflichtig zur Verfügung gestellt werden, sind vom *IT-Verantwortlichen* in benötigter Anzahl über das MRZ zu bestellen. Die Bestellung von Spezialsoftware kann nach Zustimmung des MRZ durch den *IT-Verantwortlichen* direkt ausgelöst werden.
(3) Die Installation von Software auf *IT-Systemen* und sonstigen im Campusnetz befindlichen Geräten hat ausschließlich in Verantwortung der zuständigen *IT-Verantwortlichen* zu erfolgen. Es ist nur erlaubt, auf dem *IT-System* oder im Campusnetz installierte Software auszuführen. Ausnahmen sind mit dem *IT-Verantwortlichen* abzustimmen.
(4) Bei der Beschaffung von Software ist Produkten der Vorrang zu geben, die die Sicherheitsphilosophie des jeweiligen Betriebssystems nicht unterlaufen. Falls die Erstellung von Software beauftragt wird, ist diese Bedingung ins Pflichtenheft aufzunehmen.
(5) Die Installation von Software auf labor- und medizintechnischen Geräten hat in Abstimmung mit dem *IT-Verantwortlichen* und dem Geräteverantwortlichen zu erfolgen.
(6) Unter Beachtung § 9.4 Abs. 3 bedarf die Installation von nicht privat erworbener Software auf *privaten IT-Systemen* der Genehmigung des Leiters der Struktureinheit, muss in den Lizenzbestimmungen gestattet sein und ist nur für dienstliche Zwecke nach § 3 Abs. 1 zulässig. Die Beantragung hat mit dem Formular „Antrag auf Installation nicht privat-finanzierter Software auf privatem Rechner“ (siehe Intranet UKD und MF) zu erfolgen.
(7) Die Nutzung von privat erworbener Software für dienstliche Zwecke muss durch die Lizenzbestimmungen abgedeckt sein und bedarf der Zustimmung des Leiters der Struktureinheit.

§ 11 - Schutz vor Schadsoftware

(1) Für den Schutz vor *Schadsoftware* der im UKD, MF und im privaten Bereich dienstlich genutzten *IT-Systeme* stehen zentrale Dienste des MRZ zur Verfügung. Die Konfiguration der Virenschutz-Software soll sicherstellen, dass keine Viren oder Malware in das UKD-LAN eingeschleust werden können. Bei Verwendung mobiler Speichermedien, wie z. B. Disketten, CD-ROM, USB-Stick, muss eine vollständige Virenprüfung durch die in § 1 Abs. 2 benannten Personen stattfinden.
(2) Für das Sicherheitsupdate-Management der im UKD und MF genutzten Windows-IT-Systeme stehen zentrale Dienste des MRZ zur Verfügung.

(3) Alle stationären und *mobilen IT-Systeme*, die eine Verbindung zum UKD-LAN haben, müssen über einen aktuellen Virenschutz und über aktuelle Sicherheitsupdates verfügen. Dies schließt auch alle *Medizingerätesysteme* ein. Bei vertraglich gebundenen *Medizingerätesystemen* ist diese Forderung im Vertrag zu fixieren. Der Vertragspartner haftet für alle mittelbaren und unmittelbaren Schäden, welche durch einen unzureichenden Virenschutz im UKD-LAN entstehen.
(4) *IT-Systeme*, die nicht den Forderungen im § 11 Abs. 3 entsprechen, müssen als *Standalone-Systeme* oder in separaten Netzen betrieben werden.
(5) Die einer E-Mail beigefügten Anhänge sind vor ihrer Versendung und (bei empfangenen E-Mails) vor ihrer Weiterverarbeitung in Verantwortung des MRZ auf Viren zu prüfen. Unabhängig davon ist der Postmaster des UKD befugt, eine Virenprüfung durchzuführen. Virenbefall wird dem Empfänger mitgeteilt. Die mit Viren oder anderer *Schadsoftware* befallenen E-Mails incl. Anlagen werden in Quarantäne gestellt.
(6) Eine Änderung der durch den zuständigen *IT-Verantwortlichen* eingerichteten bzw. vorgegebenen Konfiguration oder das Deaktivieren des Virenschutzes ist untersagt.
(7) Detaillierte Angaben sind in der Anlage 1 Pkt. 4 „Schutz vor Schadsoftware und unberechtigtem Zugriff auf Daten“ enthalten.

§ 12 - Sanktionen bei Missbrauch

(1) Nutzer können vorübergehend oder dauerhaft in der Benutzung beschränkt oder hiervon ausgeschlossen werden, wenn sie

1. schuldhaft gegen diese Ordnung verstoßen (missbräuchliches Verhalten) oder
2. die Rechen- und Kommunikationstechnik des UKD für strafbare Handlungen missbrauchen oder
3. dem UKD durch sonstiges rechtswidriges Nutzerverhalten Nachteile zufügen.

(2) Eine dauerhafte Nutzungseinschränkung oder der vollständige Ausschluss eines Nutzers von der weiteren Nutzung kommt nur bei schwerwiegenden oder wiederholten Verstößen im Sinne von Abs. 1 in Betracht und wenn auch künftig ein ordnungsgemäßes Verhalten nicht zu erwarten ist.
(3) Bei Verstößen gegen den Absatz 1 kommen gegen den Mitarbeiter arbeits- bzw. disziplinarrechtliche Maßnahmen in Betracht. Bei strafbarem Verhalten kann zusätzlich Strafanzeige erstattet werden.
(4) Eine vorübergehende oder dauerhafte Nutzungsbeschränkung soll grundsätzlich erst nach vorheriger Anhörung durch die Rechtsstelle des UKD bzw. MF und in Absprache mit dem Vorgesetzten erfolgen. Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein Verhalten nach Abs. 1 gegeben ist, kann der zuständige *IT-Verantwortliche* in dringenden Fällen vorläufig die weitere Nutzung verhindern, bis die Sach- und Rechtslage hinreichend geklärt ist.
(5) Vorübergehende Nutzungseinschränkungen sind aufzuheben, sobald eine ordnungsgemäße Benutzung wieder gewährleistet erscheint. Die dauerhafte Einschränkung bzw. der vollständige Ausschluss können auf Antrag aufgehoben werden, wenn Wiederholungsgefahr nicht mehr besteht. Dies ist vom Ausgeschlossenen glaubhaft zu machen.
(6) Auf die folgenden Straftatbestände wird besonders hingewiesen:

1. Ausspähen von Daten (§ 202a StGB)
2. Abfangen von Daten (§ 202b StGB)
3. Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB)
4. Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB)
5. Computerbetrug (§ 263a StGB)
6. Verbreitung pornographischer Darstellungen (§ 184 StGB) insbesondere Abruf oder Besitz kinderpornographischer Darstellungen (§ 184 Abs. 5 StGB)
7. Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB)
8. Ehrdelikte wie Beleidigung oder Verleumdung (§ 185 ff. StGB)
9. Strafbare Urheberrechtsverletzungen, z. B. durch urheberechtswidrige Vervielfältigung von Software (§ 106 ff. UrhG).

(7) Siehe weiterführende Anlage 2 „Rechtliche Grundlagen“.

§ 13 - Haftung Nutzer gegenüber UKD und MF

(1) Die Haftung ergibt sich aus den gesetzlichen Bestimmungen und ist beschränkt auf Vorsatz und grobe Fahrlässigkeit. Hingewiesen wird insbesondere auf zivilrechtliche Schadensersatzansprüche sowie das Urheber- und Markenrecht.
(2) Der Nutzer haftet für alle Nachteile, die dem UKD und der MF durch die missbräuchliche oder rechtswidrige Verwendung der Rechen- und Kommunikationstechnik sowie Software bzw. Nichteinhaltung seiner Verpflichtungen aus dieser Rahmenordnung entstehen.
(3) Der Nutzer haftet auch für Schäden, die im Rahmen der ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er diese Drittnutzung zu vertreten hat.
(4) Der Nutzer hat das UKD und die MF von allen Ansprüchen freizustellen, wenn Dritte das UKD wegen eines missbräuchlichen oder rechtswidrigen Verhaltens des Nutzers auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen.

§ 14 - Haftung UKD und MF gegenüber Nutzer

(1) UKD und MF übernehmen keine Garantie dafür, dass die Rechen- und Kommunikationstechnik sowie die am UKD und MF eingesetzte Software fehlerfrei und jederzeit ohne Unterbrechung verfügbar ist. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher schutzwürdiger Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.
(2) UKD und MF übernehmen keine Verantwortung für die zur Verfügung gestellte Software. Sie haften auch nicht für den Inhalt, insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang zur Nutzung vermittelt.
(3) Das UKD und die MF haften im Übrigen nur bei Vorsatz und grober Fahrlässigkeit ihrer Mitarbeiter.

§ 15 - Rechte und Pflichten des IT-Verantwortlichen

(1) Die Administration von *IT-Systemen* muss kooperativ, sachgerecht und zweckgebunden und unter Einhaltung des § 13 Abs. 3 *SächsDSG* erfolgen.
(2) Die *IT-Verantwortlichen* der Struktureinheiten sind verpflichtet, Hinweisen zu Sicherheitsproblemen nachzugehen und entsprechend darauf zu reagieren.
(3) Die Organisation von Datensicherungsmaßnahmen liegt in der Verantwortung der *IT-Verantwortlichen*.
(4) Die *IT-Verantwortlichen* verwalten die erteilten Benutzberechtigungen und Bestandsdaten der Benutzer, die zu ihrem Verantwortungsbereich gehören.
(5) Zur ausschließlichen Sicherstellung eines ordnungsgemäßen Betriebs und zum Aufdecken von Missbrauch bei bestehendem Einzelverdacht wird der Datenverkehr zum bzw. vom Internet auf dem zentralen Zugangssystem protokolliert. Als Protokolldaten können neben Datum und Uhrzeit, die Zieladressen der aufgerufenen Internetseiten sowie die Benutzerkennung und IP-Adresse des Abrufers erfasst werden. Protokollierte Daten sind spätestens nach 6 Monaten, insofern *berechtigte Stellen* keine weitere Vorhaltung festlegen, zu löschen.
(6) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -wartung oder aus Gründen der Systemsicherheit, zum Schutz der nutzereigenen Daten sowie zur Aufklärung und Unterbindung von Missbräuchen erforderlich ist, können die *IT-Verantwortlichen* die Nutzung der Ressourcen vorübergehend einschränken oder einzelne Nutzerkonten vorübergehend sperren. Die betroffenen Nutzer sind hierüber – sofern möglich – im Voraus zu unterrichten. Zur Aufklärung und Unterbindung von Missbräuchen kann, bis zur Zweckereichung nach § 12 Abs. 4 die vorherige Information des Nutzers unterbleiben. Bei Missbrauch mit zu erwartenden

Schadensfolgen sind Anhaltspunkte zu dokumentieren und zusätzlich ist in diesem Falle unverzüglich die Rechtsstelle in Kenntnis zu setzen und der zuständige Personalrat zu informieren.
(7) Der *IT-Verantwortliche* ist berechtigt, zum Zwecke der Gewährleistung der Netzwerk- und Systemsicherheit manuelle oder automatisierte Tests in seinem Verantwortungsbereich durchzuführen und Funktionen des IT-Systems einzuschränken.
(8) Der *IT-Verantwortliche* ist berechtigt, die Inanspruchnahme der *IT-Systeme* und Software durch die Nutzer zu protokollieren, jedoch nur soweit dies erforderlich ist:

1. zur Gewährleistung eines ordnungsgemäßen Systembetriebs,
2. zur Ressourcenplanung und Systemadministration,
3. zum Schutz der personenbezogenen Daten anderer Nutzer,
4. zu Abrechnungszwecken,
5. für das Erkennen und Beseitigen von Störungen sowie
6. zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

(9) Unter den Voraussetzungen von Abs. 8 Nr. 1, 5, 6 und soweit dies zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Missbräuchen unbedingt erforderlich ist, ist der *IT-Verantwortliche* berechtigt, unter Beachtung des Datengeheimnisses und vorheriger Information des Nutzers Zugriff auf die benutzereigenen *Dateien* zu nehmen. Für einen Missbrauch müssen tatsächliche und dokumentierte Anhaltspunkte vorliegen. Nur in diesem Fall kann die vorherige Information des Nutzers bis zur Zweckereichung nach § 12 Abs. 4 unterbleiben.
(10) Der Zugriff und die Einsichtnahme in *Verbindungsdaten* sind jedoch nur zulässig, soweit dies zur Vermeidung und Behebung von Störungen unerlässlich ist. Der Zugriff auf Inhaltsdaten für den Viren-Scan sowie die Untersuchung auf SPAM auf einem Mailgateway ist zulässig. Die Einsichtnahme in Inhaltsdaten ist nur mit Zustimmung des Nutzers zulässig.
(11) Alle Maßnahmen nach Abs. 5, 6, 7, 8 und 9 sind nachvollziehbar zu dokumentieren.
(12) Die Übermittlung von *Nutzungsdaten* an Dritte ist unzulässig.
(13) Nach Maßgabe der gesetzlichen Bestimmungen ist der *IT-Verantwortliche* zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet.
(14) Weitere detaillierte Angaben sind in den Anlagen 1 Pkt. 3 „Rechte und Pflichten IT-Verantwortliche“ und Anlage 1 Pkt. 2 „Netzbetrieb“ enthalten.

§ 16 - Rechte und Pflichten des Leiters der Struktureinheit

(1) Der Leiter der Struktureinheit ist verantwortlich für die Gewährleistung des ordnungsmäßigen Betriebes der Rechen- und Kommunikationstechnik in seinem Verantwortungsbereich einschließlich der Veranlassung erforderlicher Sicherheitsmaßnahmen.
(2) Der Leiter ist verantwortlich für den ordnungsgemäßen Umgang seiner Mitarbeiter mit den genutzten Einrichtungen der Informationstechnologie sowie mit den Softwareressourcen.
(3) Der Leiter der Struktureinheit trägt die Verantwortung für die Funktion „IT-Verantwortlicher“. Er muss in seinem Verantwortungsbereich einen oder mehrere *IT-Verantwortliche* benennen und eine Vertretungsregelung sicherstellen. Für die MF gilt § 15 Abs. 3 der „Rahmenordnung für Rechen- und Kommunikationstechnik und die Informationssicherheit an der TU Dresden“.
(4) Zur Wahrnehmung dieser Verantwortung ist er befugt, entsprechende Überprüfungen anzuordnen.

§ 17 - Notfallplan
§ 17.1 - Allgemein

(1) Für den Ausfall von *IT-Systemen* sind detaillierte Notfallpläne in den Struktureinheiten des UKD und der MF vorzuhalten.
(2) Jede Struktureinheit benennt für Notfälle einen Ansprechpartner und Vertreter, der die weiteren Maßnahmen veranlasst und koordiniert.

§ 17.2 - Vorsätzlicher oder fahrlässiger Missbrauch

(1) Zur Erkennung und Bewertung eines Missbrauchs sind vom im § 17.1 Abs. 2 benannten Ansprechpartner folgende Fragen zu klären:

1. Wer hat wann den Missbrauch erkannt?
2. Welche Geräte sind betroffen?
3. Wie hoch wird das Risiko für Folgeschäden eingeschätzt?
4. Wer muss informiert werden?

(2) Zur Verhinderung weiteren Missbrauchs sind im Rahmen der Möglichkeiten folgende Maßnahmen einzuleiten:

1. Der *IT-Verantwortliche* der Struktureinheit ist schriftlich in Kenntnis zu setzen.
2. Der *IT-Verantwortliche* hat entsprechend den Regelungen im § 15 Abs. 6 und 11 zu verfahren.
3. Entscheidung über weitere Maßnahmen (z. B. Wiederzulassung oder Fortdauer der Sperre bis zur endgültigen Klärung) hat durch die Rechtsstelle des UKD bzw. MF zu erfolgen.

§ 18 - Schlussbestimmungen

(1) Sollten einzelne Klauseln oder Bestimmungen in dieser Rahmenordnung ganz oder teilweise unwirksam sein oder werden oder weist diese Rahmenordnung Lücken auf, so wird hierdurch die Wirksamkeit der Rahmenordnung im Übrigen nicht berührt.
(2) Die Anpassung dieser Rahmenordnung und ihrer Anlagen an den Stand der Technik erfolgt durch die Arbeitsgruppe „Security Policy" in Verantwortung des Geschäftsbereiches Medizinisches Rechenzentrum und in Abstimmung mit dem Datenschutzbeauftragten. Mitglieder sind in der Anlage 1 Pkt. 8 „Mitglieder Arbeitsgruppe Security Policy" benannt.
(3) Die Arbeitsgruppe tagt nach Bedarf und führt mindestens alle 2 Jahre ein Review der Rahmenordnung durch.
(4) Änderungen der Rahmenordnung bedürfen der Zustimmung des Vorstandes des UKD, des Dekans der MF und der Personalrätewährend Änderungen in den Formularen durch die Arbeitsgruppe und den Leiter des Medizinischen Rechenzentrums und den Datenschutzbeauftragten freigegeben werden.
(5(Die Rahmenordnung ist im Intranet des UKD und der MF für alle Mitarbeiter zugänglich zu publizieren.

§ 19 - Inkrafttreten

Die Ordnung tritt am Tage nach der Veröffentlichung in den Bekanntmachungen des UKD und MF in Kraft.

Dresden .2011

Wolf-Eckhard Wormser
Kanzler der
Technischen Universität
Dresden

Prof. Dr. med. D. Micheal Albrecht
Medizinischer Vorstand
des Universitätsklinikums
Carl Gustav Carus

Wilfried E. B. Winzer
Kaufmännischer Vorstand
des Universitätsklinikums
Carl Gustav Carus

Anlagenübersicht

Anlage 1: Ergänzende Informationen und Hinweise zur „Rahmenordnung für die Nutzung der Rechen- und Kommunikationstechnik am Universitätsklinikum Carl Gustav Carus und der Medizinischen Fakultät an der TU Dresden“

Anlage 2: Rechtliche Grundlagen

Anlage 3: Aktueller Stand Datenschutzrecht

Anlage 4: Datenschutzvereinbarung zu einem IT-Vertrag (HW und SW)

Anlage 5: Handlungsanweisungen für IT-Verantwortliche

Anlage 6: Handlungsanweisungen für Mitarbeiter

Anlage 7: Mustervertrag Fernwartung

Anlage 8: Begriffsbestimmung zur „Rahmenordnung für die Nutzung der Rechen- und Kommunikationstechnik am Universitätsklinikum Carl Gustav Carus und der Medizinischen Fakultät an der TU Dresden“ und deren Anlagen

Formularübersicht

Formular 1: Antrag Installation nicht privat finanzierter Software

Formular 2: Antrag auf Nutzung privater mobiler IT-Systeme am UKD-Netzwerk

Formular 3: Antrag auf Nutzung von Fernzugängen in das Campusnetz des UKD

Formular 4: Datenblatt Zugriff auf das Campusnetz durch UKD-Mitarbeiter

Formular 5: Datenblatt Zugriff auf das Campusnetz durch externe UKD-Einrichtungen

Formular 6: Datenblatt Zugriff auf das Campusnetz durch Fernwartungsfirmen

Formular 7: Datenblatt: Zugriff auf das Campusnetz durch Fremdeinrichtungen