IBE
Institut für medizinische Informationsverarbeitung, Biometrie und Epidemiologie

LMU

Direktor: Prof. Dr. Ulrich Mansmann
Stellvertreter: Prof. Dr. Dieter Hölzel

Benutzungsordnung

für IBE-Kommunikationsnetze und -anlagen

Stand: 24. Mai 2006

Inhalt

1. Allgemeines

1.1 Die Anlagen und Geräte des IBE sowie das Kommunikationsnetz sind nach Maßgabe dieser Benutzungsordnung entsprechend den Aufgaben des IBE in Forschung und Lehre zu verwenden.

1.2 Dienstanweisungen übergeordneter Stellen und Anweisungen des Datenschutzbeauftragten sind Teil dieser Benutzungsordnung und entsprechend zu beachten.

1.3 Diese Benutzungsordnung behält auch dann ihre Gültigkeit, wenn einzelne Punkte daraus nichtig sind oder werden.

2. Benutzung der Anlagen

2.1 Die vorhandenen Endgeräte und Einrichtungen dürfen ohne Absprache mit der Systemverwaltung weder entfernt noch technisch modifiziert werden. Jeder Benutzer ist zu pfleglichem Umgang mit den Geräten verpflichtet.

2.2 Zugeteilte Benutzerkennungen und Passwörter sind gegen Missbrauch zu schützen. Die Weitergabe von Benutzerkennungen und Passwörtern an Dritte ist nicht gestattet, kann ggf. zu disziplinarischen bzw. arbeitsrechtlichen Maßnahmen führen und Schadensersatzansprüche zur Folge haben.

2.3 Beantragte Studentenkennungen gelten für jeweils ein Semester und müssen bis spätestens zwei Wochen nach Beginn des Folgesemesters verlängert worden sein. Bei der Verlängerung ist der Nachweis einer gültigen Immatrikulation vorzulegen.
Nicht verlängerte Kennungen und darunter gespeicherte Daten können nach Beginn des neuen Semesters gelöscht werden. Sie werden in jedem Fall gelöscht, wenn eine Verlängerung zweimal hintereinander nicht erfolgt ist. Für Folgen, die sich aus dieser Maßnahme ergeben übernimmt das IBE keine Haftung.
Kurskennungen stehen nur für die Dauer des Kurses zur Verfügung. Die dort abgelegten Daten werden nicht gesichert. Sie können jederzeit gelöscht werden.

2.4 Die Bereithaltung, Verarbeitung, Speicherung und Übermittlung personenbezogener Daten (z. B. nach Bayerischem Krankenhausgesetz, den Datenschutzgesetzen usw.) ist im wissenschaftlichen Subnetz des IBE nicht zulässig.

2.5 Jeder Benutzer ist grundsätzlich selbst für eine ausreichende Sicherung seines Datenbestandes zuständig. Die den Benutzern von der Systemverwaltung zugewiesenen Server-Speicherplätze werden täglich gesichert. Monatlich wird eine Duplikat-Bandsicherung angelegt. Eine lückenlose Sicherung kann nicht garantiert werden.

3. Maßnahmen bei Ressourcenverknappung

3.1 Bei Ressourcenverknappung behält sich die Systemverwaltung vor, geeignete Maßnahmen zur Beschränkung einzelner, oder auch aller Nutzer einzuleiten.
Grundsätzlich wird jeder Benutzer dazu aufgefordert, nicht mehr benötigten Speicherplatz freizugeben.

4. Rechte und Pflichten der Systemverantwortlichen

4.1 Die Systemverantwortlichen tragen in angemessener Weise, insbesondere in Form regelmäßiger Stichproben, zum Verhindern bzw. Aufdecken von Missbrauch bei. Hierfür sind sie insbesondere dazu berechtigt:

a) die Aktivitäten der Benutzer zu dokumentieren und auszuwerten, soweit dies zu Zwecken der Abrechung, der Ressourcenplanung, der Überwachung des Betriebes oder der Verfolgung von Fehlerfällen und Verstößen gegen die Benutzungsordnung sowie gesetzlichen Bestimmungen dient;

b) bei Verdacht auf Verstöße gegen die Benutzungsordnung oder gegen strafrechtliche Bestimmungen unter Beachtung des Vieraugenprinzips und der Aufzeichnungspflicht in Benutzerdateien und Mailboxen Einsicht zu nehmen oder die Netzwerknutzung durch den Benutzer mittels z.B. Netzwerk - Sniffer detailliert zu protokollieren;

c) bei Erhärtung des Verdachts auf strafbare Handlungen beweissichernde Maßnahmen, wie z.B. Key-stroke Logging oder Netzwerk-Sniffer, einzusetzen.
Den Systemverantwortlichen ist der Zutritt und der Zugriff auf die entsprechenden Geräte und Einrichtungen zu ermöglichen. Die Systemverwaltung ist zur Vertraulichkeit verpflichtet.

4.2 Bei einem Verstoß gegen die Benutzungsordnung kann der Zugang und die Rechenberechtigung an den Rechenanlagen des IBE gesperrt werden. Bei Nichtbeachtung oder Verstoß gegen die Benutzungsordnung ist der betreffende Benutzer im Rahmen der gesetzlichen Bestimmungen schadensersatzpflichtig.

5. Benutzung von Software

5.1 Die vom IBE zur Verfügung gestellten Programme und Softwareprodukte oder Teile daraus dürfen nur an Arbeitsplätzen des IBE benutzt werden. Es dürfen keine Kopien der Programme und ihrer Beschreibungen erstellt werden.

5.2 Die Programme dürfen nur zu Arbeiten in Forschung und Lehre verwendet werden. Eine kommerzielle Nutzung der Programme ist ausgeschlossen.

5.3 Die an den Arbeitsplätzen installierte Software sowie ausliegende Dokumentationen dürfen nicht entfernt oder modifiziert werden. Weitere Software darf nur mit ausdrücklicher Genehmigung der Systemverwaltung installiert werden.

6. Haftungsausschluss

6.1 Das IBE übernimmt, soweit gesetzlich zulässig, keinerlei Haftung für Schäden, die den Benutzern aus der Benutzung der Anlagen und Geräte des IBE - Kommunikationsnetzes entstehen.

6.2 Die Systemverwaltung übernimmt insbesondere keine Garantie dafür, dass die Systemfunktionen den speziellen Anforderungen des Nutzers entsprechen oder dass das System fehlerfrei und ohne Unterbrechung läuft. Die Systemverwaltung kann nicht die Unversehrtheit (bzgl. Zerstörung, Manipulation) und Vertraulichkeit der gespeicherten Daten garantieren.

6.3 Gerichtsstand für alle aus dem Benutzerverhältnis erwachsenden Ansprüche ist, soweit gesetzlich zulässig, München.

7. Zugang zum CIP-Pool (Kursraum 5 – Raum VI K 02 630)

7.1 Bei Verstoß gegen die Benutzungsordnung kann die Zugangsberechtigung für den IBE-CIP-Pool gesperrt werden.

7.2 Automatische Zugangskontrolle

Der Zugang zum IBE-CIP-Pool wird durch einen magnetkartengesteuerten Türöffner kontrolliert. Die Anlage besteht aus zwei Magnetkartenlesegeräten, die außen vor und innen hinter der Tür des CIP-Raumes angebracht sind.

Die Anlage verfügt darüber hinaus über optische und akustische Alarmgeber, die eine fehlerhafte Bedienung der Schließanlage signalisieren (s. Bedienungsanleitung).

Das Betreten und Verlassen des Raumes (dem Gang im Bereich der Eingangstür) wird mittels Video-Kameras rund um die Uhr kontrolliert und aufgezeichnet.
Nicht ordnungsgemäßes Verhalten beim Zu- bzw. Weggang löst Alarm aus.

Der Auswertungscomputer sichert die Daten der zum Zugang erforderlichen Magnetkarte und gibt personenbezogenen Aufschluss über Zugang und Verlassen des Raumes.

7.3 Ausgabe und Rückgabe der Magnetkarte

Die Ausgabe der Magnetkarten erfolgt bei Bedarf, normalerweise jedoch beim Einrichten der Benutzerkennung durch die Systemverwaltung (IBE, Raum IV KU1 804).

Dabei sind ein Personalausweis und gegebenenfalls der Studentenausweis und ein vollständig ausgefülltes Antragsformular (Antrag auf eine Benutzerkennung/Magnetkarte) vorzulegen.
Die Magnetkarte ist nach Ablauf der Gültigkeit bei der Systemverwaltung abzugeben.

7.4 Behandlung der Karte

Zugeteilte Magnetkarten sind gegen Missbrauch zu schützen. Aus diesem Grund ist eine weitere Beschriftung der Karte untersagt.
Die Weitergabe der Karte und/oder PIN an Dritte ist nicht gestattet. Bei Kartenverlust ist sofort die Systemverwaltung zu verständigen (Tel. 7095-4488).

7.5 Ablauf des regulären Zugangs mit Magnetkarte

Die Karte wird durch den vor der Eingangstür angebrachten Ausweisleser gezogen. Anschließend muss über die Tastatur die vierstellige PIN eingegeben werden.
Nach erfolgreicher Überprüfung durch das angeschlossene Computersystem wird der Zugang für ca. 2 Sekunden freigegeben.
Über die LCD-Anzeige am Magnetkartenleser werden situationsbezogene Hinweise oder Aufforderungen ausgegeben.

Wird das Schließen der Tür (über die normale Durchgangsdauer hinaus) verzögert, erfolgt die akustische Meldung, die Türe zu schließen. Nach einer gewissen Vorwarnzeit wird Alarm ausgelöst. Dieser Alarm umfasst den akustischen Alarm vor Ort und den optischen und akustischen Alarm im IBE bzw. bei den mit der Überwachung beauftragten Personen.
Der Zugang wird über Videokameras aufgezeichnet.

Nur Personen mit gültiger Magnetkarte haben Zugang. Es ist darauf zu achten, dass keine weiteren Personen ohne Anmeldung (Benutzung eigener Karten) mit eintreten. Absichtliche Missachtung dieser Vorschrift, hat die Sperrung der Magnetkarte zur Folge.

7.6 Ablauf des regulären Verlassens mit Magnetkarte

Die Karte wird durch den rechts vor der Ausgangstür angebrachten Kartenleser gezogen. Wie beim Zugang wird die Tür für ca. 2 Sekunden freigegeben. Die Alarmgebung erfolgt ggf. wie unter 7.5 beschrieben.
Das Verlassen des Raumes wird von Videokameras aufgezeichnet.
Benutzer, die den Raum ohne Benutzung der Magnetkarte verlassen, werden aufgefordert, die Magnetkarte durchzuziehen. Die Missachtung dieser Anweisung kann die Sperrung der Magnetkarte und Benutzerkennung zur Folge haben.

7.7 Videoaufzeichnung

Die Videoaufzeichnungen werden im Normalfall regelmäßig gelöscht.
Aufzeichnungen von unklaren Situationen, bzw. Alarmsituationen können bis zur endgültigen Klärung dieser Situation(en) gespeichert werden.
Im Bedarfsfall können die Aufzeichnungen unter Wahrung der Datenschutzvorschriften auch Dritten zugänglich gemacht werden.

7.8 Fluchtmöglichkeiten

Fluchtmöglichkeiten bestehen durch die Eingangstür und über einen Notausgang auf der anderen Raumseite. Aus Sicherheitsgründen lassen sich beide Türen ohne Hilfsmittel (Magnetkarte bzw. Schlüssel) von innen öffnen.
Im Normalfall jedoch ist das Verlassen des Raumes mittels Magnetkartendurchzug zu dokumentieren (siehe 7.6).

Die Benutzung des Notausganges ist nur im Notfall gestattet. Die widerrechtliche Nutzung des Notausganges führt seitens der Verwaltung des Klinikums zur Strafverfolgung und kann Schadensersatzansprüche nach sich ziehen.

-/-