Richtlinien zur Nutzung der IT-Dienste der MHH

1. Allgemeines

Das Zentrum für Informationsmanagement (ZIMt) ist beauftragt in Zusammenarbeit mit den IT-Verantwortlichen der MHH-Abteilungen den gesicherten und störungsfreien IT-Betrieb aller IT-Einrichtungen der MHH zu gewährleisten. Die folgenden Richtlinien dienen dazu, dieses Ziel zu erreichen. Ihre Einhaltung ist verbindlich.

2. Netznutzung

2.1. Das ZIMt stellt für jedes IT-Gerät auf Antrag einen universellen Datennetzzugang bereit. Dabei werden die Dienste entsprechend der zu erfüllenden Aufgaben zur Verfügung gestellt.

2.2. Im MHH-Datennetz werden interne IP-Adressen verwendet, die ausschließlich das ZIMt auf Antrag vergibt. Beim Betrieb eines Abteilungsnetzes (LAN, WLAN) kann der Abteilung ein eigener IP-Adressbereich zugewiesen werden.

2.3. Jedes Gerät im MHH-Datennetz wird durch die Adresse der Netzadapterkarte ("MAC-Adresse") identifiziert. Nur Geräte mit im ZIMt registrierten MAC-Adressen dürfen am MHH-Datennetz betrieben werden.

2.4. Die IT-Geräte am MHH-Datennetz dürfen außer den mit dem ZIMt vereinbarten keine Anschlüsse zu anderen IT-Geräten oder Netzen haben (z. B. über Modems, ISDN-Einwahlmöglichkeiten oder WLANs).

2.5. Der Zugang zu öffentlichen und externen Netzen (z.B. Internet) erfolgt ausschließlich über die zentralen Netzkomponenten der MHH und wird vom ZIMt eingerichtet.

2.6. Ausnahmen, wie beispielsweise zur Fernwartung und bei Auftragsdatenverarbeitung sind zu begründen und beim ZIMt anzumelden. Mit den Auftragnehmern sind Vereinbarungen zur Sicherstellung von Datenschutz und Datensicherheit abzuschließen. Die Schutzmaßnahmen müssen die rechtlichen Vorschriften erfüllen, insbesondere:

- Eine Fernwartungsverbindung darf nicht ständig, sondern nur bei Bedarf existieren. Sie muss auf der Rechnerseite für die notwendigen Zeiträume explizit durch den Verantwortlichen freigeschaltet werden. Für diese Zeitscheibe ist ein entsprechendes personenbezogenes Passwort zu vergeben.
- Wenn möglich, ist ein automatisches Protokoll über die Aktivitäten aufzuzeichnen, zumindest muss die Möglichkeit einer Kontrolle vorgesehen werden.
- Jede Datenübertragung muss verschlüsselt werden, um ein "Abhören" auszuschließen (z.B. mit HTTPS oder VPN)
- Die Firma, d.h. jede aktive Person, muss vertraglich auf die Einhaltung des Nds. Datenschutzgesetzes und auf §5 des Bundesdatenschutzgesetzes verpflichtet werden.

2.7. So es aufgrund von funktionellen Anforderungen z.B. im Bereich der Medizintechnik oder Forschung erforderlich ist eigene Abteilungsnetze zu betreiben, bleibt davon der Grundsatz der Zuständigkeit des ZIMt für alle Netze auf dem MHH Campus unberührt. Solche Abteilungsnetze sind gemeinsam mit dem ZIMt zu konzipieren. Auf Antrag wird vom ZIMt konform dem Vernetzungskonzept der MHH die physikalische Netzstruktur eingerichtet. Hilfestellungen in Form von Beratungen und Planungen werden vom ZIMt erbracht. Für diese Abteilungsnetze ist die Abteilung verantwortlicher Nutzer und selbständiger Betreiber.

2.8. Bei erheblichen Störungen oder Gefahren behält sich das ZIMt vor, die verursachenden Geräte vom MHH-Datennetz zu trennen.

3. Gerätenutzung

3.1. Die eingesetzten IT-Geräte (Arbeitsplatzcomputer, Drucker etc.) müssen nach MHH-Standard beschafft und konform der IT-Strategie der MHH an das MHH-Datennetz angeschlossen werden. Die verwendeten Programme und Dienste sind mit dem ZIMt abzustimmen.

3.2. Jedes Gerät im MHH-Datennetz ist mit der vom ZIMt vorgegebenen Management- und Sicherheitssoftware bzgl. Betriebssystem und Virenschutzprogramm auszustatten und kontinuierlich zu aktualisieren. Den entsprechenden Service (WSUS, Updateserver für Virenmuster) hält das ZIMt vor.

3.3. Für jedes Gerät im MHH-Datennetz ist ein administrativer Zugang für ZIMt Mitarbeiter einzurichten. Ist dies aus technischen oder organisatorischen Gründen nicht möglich, ist eine Not-Zugangskennung mit Administrationsberechtigung schriftlich im ZIMt-Sekretariat zu hinterlegen.

3.4. Die IT-Geräte sind durch geeignete Maßnahmen gegen Manipulationen, unberechtigte Nutzung und Diebstahl zu sichern. Die IT-Geräte oder Teile dürfen ohne ausdrückliche Vereinbarung mit dem ZIMt nicht vom Aufstellungsort oder bei transportablen Geräten aus der festgelegten Einsatzumgebung entfernt werden (auch nicht kurzfristig!). Ebenso ist es nicht gestattet, die Geräte zu öffnen, irgendwelche Modifikationen an ihnen vorzunehmen oder andere Geräte anzuschließen.

3.5. Die IT-Geräte dürfen nicht unbeaufsichtigt in frei zugänglichen Räumen stehen. Grundsätzlich ist das Gerät beim Verlassen zu sperren, indem ein passwortgeschützter Bildschirmschoner aktiviert wird, der Anwender das Gerät sperrt (Windowstaste-L), der Anwender sich abmeldet oder das Gerät ausgeschaltet wird.

3.6. Die auf einem IT-Gerät installierten Programme dürfen nur zu ihrem bestimmungsgemäßen dienstlichen Zweck genutzt werden. Die Installation, Erweiterung oder Änderung von Programmen ist ausschließlich vom ZIMt autorisierten Mitarbeitern gestattet. Aus urheberrechtlichen Gründen dürfen alle Programme und diejenigen Dateien, die nicht vom Benutzer erstellt worden sind, weder kopiert noch geändert werden. Die Softwarelizenzen der installierten Programme werden im ZIMt verwaltet.

3.7. Die Ausstattung eines IT-Gerätes ermöglicht in der Regel sowohl die Benutzung von lokalen Programmen als auch von zentral verfügbaren Programmen und Diensten. Die Nutzung sämtlicher Funktionen erfordert Zugriffsberechtigungen (Passworte), die bei der ZIMt Benutzerverwaltung zu beantragen sind.

3.8. Auf Geräten am MHH-Datennetz sind grundsätzlich keine Daten lokal abzulegen, sondern entsprechende Serverlaufwerke zu nutzen, die vom ZIMt für jeden Benutzer bereitgestellt werden. Nur hierfür wird Datensicherheit und –verfügbarkeit vom ZIMt gewährleistet. Vom Benutzer gelöschte bzw. veränderte Netzwerk-Daten werden 21 Tage zur Wiederherstellung in täglichen Sicherungen vom ZIMt bereitgehalten. Wichtige Daten, die in einer alten Version vorgehalten werden sollen, sind unter einem geänderten Namen abzuspeichern.

4. Dienste und Applikationen

4.1. Zur Nutzung der IT-Dienste der MHH wird dem Antragsteller ein Benutzername mit Erstpasswort per Hauspost persönlich zugestellt. Die Zugangskennung ist mit einem geeigneten Passwort abzusichern und geheim zu halten.

4.2. Die Beschaffung und/oder Verwendung fremder Zugangskennungen und E-Mail-Adressen ist nicht zulässig.

4.3. Zentrale Fileservices: Das ZIMt hält datengesicherten zentralen Speicherplatz für die Abteilungen (Laufwerke: P, Q) und für jeden Benutzer (Laufwerk O:) bereit. Der Zugriff auf den abteilungsspezifischen Speicherbereich wird den Abteilungsmitarbeitern nach Rücksprache mit den IT-Verantwortlichen der Abteilung gewährt. Dieser Speicherplatz steht ausschließlich für dienstliche Zwecke zur Verfügung und ist nicht als Backupmedium von lokalen Festplatten vorgesehen.

4.4. Internet-Nutzung: Das Internet wird abteilungsbezogen für dienstliche Zwecke eingerichtet.

4.5. E-Mail-Nutzung: Auf Antrag wird eine E-Mail-Adresse personenbezogen / abteilungsbezogen eingerichtet. Der Antragsteller geht hiermit die Verpflichtung ein, den Postfachinhalt zu sichten und sicherzustellen, dass die E-Mail-Adresse nicht missbraucht wird.

4.6. Jeder Internet Nutzer (Mitarbeiter, Praktikant, Student) ist auf die Einhaltung des Niedersächsischen Datenschutzgesetzes und auf § 5 des Bundesdatenschutzgesetzes zu verpflichten.

5. Rechtliche und organisatorische Rahmenbedingungen

5.1. Das Zentrum für Informationsmanagement (ZIMt) ist eine zentrale Einrichtung der MHH, deren Aufgaben sich aus §3 des Niedersächsischen Hochschulgesetzes ergeben. Dazu gehören:

- der Betrieb der Datenverarbeitungsanlagen und des Datenkommunikationsnetzes zur Erfüllung der Aufgaben der Hochschule in Forschung, Lehre und Studium sowie zur Erledigung von Verwaltungsaufgaben und Aufgaben der Patientenversorgung,
- die Beratung und Unterstützung für die Nutzung der Datenverarbeitungsanlagen, des Kommunikationsnetzes und der Rechnerprogramme,
- die Betreuung aller der Hochschule verfügbaren Datenverarbeitungskapazitäten und Datenkommunikationsnetze sowie die betriebsfachliche Aufsicht über alle Datenverarbeitungsanlagen der Hochschule,
- die Koordination der Beschaffung und Ergänzung von Datenverarbeitungsanlagen, Datenkommunikationsnetzen und Rechnerprogrammen,
- die Entwicklung, Planung und Koordination der IT-Strategie in der MHH.

5.2. Die an der MHH bearbeiteten Daten sind in der Regel personenbezogen oder aus wissenschaftlichen oder wirtschaftlichen Gründen schutzwürdig. Der Krankenhaus- und Universitätsbetrieb erfordert eine hohe Systemverfügbarkeit und Sicherheit. Alle schutzwürdigen Daten dürfen das Hochschulgelände nur gesichert (z.B. verschlüsselt) verlassen. Das Niedersächsische Datenschutzgesetz und das Bundesdatenschutzgesetz sind zu beachten. Der Landesbeauftragte für den Datenschutz (LfD) in Niedersachsen hat dazu diverse Orientierungshilfen und Prüfkonzepte herausgegeben. Diese können über den Datenschutzbeauftragten der MHH zur Verfügung gestellt werden.

5.3. Die vom Niedersächsischen Innenministerium herausgegebenen „Normen, Standards und Empfehlungen für den Einsatz der Iuk-Technik in der Landesverwaltung" sind zu beachten.

5.4. Das ZIMt als der verantwortliche Betreiber des Datennetzes der MHH überlässt die Arbeitsplatzcomputer und die Netzinfrastruktur zur temporären Nutzung. Damit wird auch die Berechtigung erteilt, an den angeschlossenen IT-Geräten die vereinbarten Netzdienste über die vorgegebenen Leitungswege anzuwählen.

5.5. Die Netzeinrichtungen dürfen ausschließlich zum Erreichen der vereinbarten Dienste genutzt werden. Bestehender Veränderungsbedarf am MHH-Datennetz (LAN) oder drahtlosen Funknetz (WLAN) oder Neuinstallationen von Arbeitsplatzcomputern oder Servern, sowie die Einbindung bestehender Netze (z.B. Abteilungs-LANs oder Abteilungs-WLANs) sind über das ZIMt zu beantragen und durchzuführen. Jede Veränderung der Nutzung bzw. nicht mehr benötigte Anschlüsse sind dem ZIMt schriftlich bekannt zu machen, damit die äußerst knappen Ressourcen im MHH-Datennetz wirtschaftlich eingesetzt werden können.

5.6. Die gültigen gesetzlichen Regelungen, diese MHH-internen Richtlinien und die Regeln der wirtschaftlichen Haushaltsführung sind einzuhalten. Verstöße können mit Ausschluss von der Nutzung oder ggf. als Dienstvergehen personalrechtlich geahndet werden.

5.7. Von der nutzenden Abteilung ist dem ZIMt ein IT-Verantwortlicher zu benennen, der den ordnungsgemäßen Betrieb zu gewährleisten hat und als Ansprechpartner für das ZIMt verfügbar ist. Er koordiniert Anforderungen zur Installation weiterer Programme, zur Hardwareausstattung oder zur Umstellung der Geräte im Einvernehmen mit der Abteilung und dem ZIMt.

5.8. Bei Betriebsstörungen aller Art ist der IT-Service des ZIMt (Tel. 7777) unter Angabe des am Gerät angebrachten Gerätenamens bzw. der IP-Adresse zu informieren. Nach Vereinbarung wird der IT-Verantwortliche der Abteilung informiert. Jedes Gerät kann durch Anklicken des Blauen „I" auf gelben Grund unten rechts identifiziert werden.

5.9. Jede Abteilung und jeder Nutzer ist für die Einhaltung der rechtlichen Bestimmungen und Vorschriften zum Datenschutz durch die Benutzer eines Arbeitsplatzcomputers selbst verantwortlich. Insbesondere sind vor dem Anlegen und Benutzen von Datenbeständen mit personenbezogenen Inhalten (z.B. Name, Geburtsdatum, Adresse oder Identifikations-Nummer von Patienten oder Mitarbeitern) die vorgeschriebenen Genehmigungen einzuholen und Dateien anzumelden.

6. Glossar:

- Domäne: zentraler Windows Verzeichnisdienst für Benutzer und Geräte
- Fileservice: zentrale Dateiserver der MHH
- HTTPS: steht für HyperText Transfer Protocol Secure und ist ein Verfahren, um Daten im Internet abhörsicher zu übertragen
- ISDN: steht für Integrated Services Digital Network und meint das klassische Telefonnetz
- IT-Service: zentrale Hotline der MHH – Tel. 7777
- LAN: Local Area Network – kabelgebundenes Computer-Netzwerk
- MAC-Adresse: die Media-Access-Control-Adresse (auch Ethernet-ID oder Physikalische Adresse genannt) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifizierung des Geräts in einem Rechnernetz dient.

- VPN: ein Virtual Private Network ist ein Computernetz, das zum Transport privater Daten ein öffentliches Netz (zum Beispiel das Internet) nutzt. Es ermöglicht somit eine sichere Übertragung über ein unsicheres Netzwerk.
- WLAN: Wireless Local Area Network – Funk basiertes Computer-Netz
- ZIMt: Zentrum für Informationsmanagement