MEDIZINISCHE UNIVERSITÄT WIEN

Klassifikation: Intern

Richtlinie betreffend IT-Services und -Endgeräte

an der Medizinischen Universität Wien

Version 2018-1.0

Inhalt

1 Zweck und Inhalt

Zur Erreichung der Geschäftsziele und zur Erfüllung der Aufgaben der Medizinischen Universität Wien (MedUni Wien) ist die elektronische Verarbeitung von Daten, und damit verbunden der Einsatz von Informationstechnologien (IT), unerlässlich.

Zweck dieser Richtlinie ist es, Regelungen für die Nutzung von IT-Endgeräten zu treffen.

Die Vorgaben in diesem Dokument verstehen sich als Maßnahmen zur Gewährleistung einer sicheren IT-Infrastruktur.

2 Geltungsbereich

Diese Richtlinie gilt verpflichtend für alle Angehörigen der Medizinischen Universität Wien im Sinne des Universitätsgesetzes.

Dritte, d.h. Personen und Unternehmen, die nicht Angehörige der Medizinischen Universität Wien sind, sind über Vereinbarungen zur Einhaltung dieser Richtlinie zu verpflichten.

Diese Richtlinie gilt ohne zeitliche und örtliche Einschränkungen.

3 Begriffsbestimmungen

Im Kontext dieses Dokuments werden folgende Begriffe definiert:

NutzerIn

Person, die eines der unten definierten IT-Endgeräte und damit in Verbindung stehende (mobile) Datenträger oder IT-Peripheriegeräte nutzt.

IT-Arbeitsmittel

Hardware, d.h. IT-Endgeräte, IT-Peripheriegeräte, IT-Zubehör, Datenträger, Telefonapparate, Funkgeräte, Mobiltelefone, Presenter etc. sowie Software auf den IT-Geräten.

IT-Endgeräte

Standgeräte (Desktops), tragbare Geräte (Notebooks, Tablet PCs, Tablets etc.), netzwerkfähige Kleingeräte (Smartphones, Mobiltelefone, Navigationsgeräte, Datenerfassungsgeräte, VoIP-Telefone etc.), Endgeräte bei Medizintechnikgeräten und Laborgeräten sowie Multifunktionsgeräte (Kombifaxe, Druck- bzw. Faxstationen etc.).

IT-Peripheriegeräte

Geräte, die an einem IT-Endgerät angeschlossen sind (Keyboard, Maus, MT-Gerät etc.)

IT-Service

Unter einem IT-Service werden IT-basierte Prozesse verstanden, (z.B. Webserver, E-Mailserver, Druckserver, Fileserver (auch Peer-to-Peer-Fileservices), Datenbankserver, DHCP-Server, Nameserver, Timeserver).

Mobiler Datenträger

Speichersticks (USB-Sticks), Speicherkarten aller Art (auch in Multimedia-Abspielgeräten, in Kameras etc.), mobile Festplatten (z.B. magnetisch und flashspeicher-basiert), CDs, DVDs, Disketten, Magnetbänder und ähnliche Speichermedien.

Passwort

eine Zeichenfolge aus Buchstaben, Ziffern und/oder Sonderzeichen, die die Überprüfung einer Identität möglich macht.

Die Begriffe Kennwort, Schlüsselwort oder Password werden als Synonyme für Passwort verwendet.

Vertrauliche Daten/Informationen

Daten und Informationen, die von der MedUni Wien für einen geschlossenen Benutzerkreis vorgesehen sind und als vertraulich eingestuft wurden bzw. offensichtlich vertraulicher Natur sind oder aufgrund gesetzlicher Vorgaben oder vertraglicher Vereinbarungen zu schützen sind.

4 Regelungen

4.1 Umgang mit Daten

1. Die automatische Weiterleitung von dienstlichen E-Mails an einen externen E-Mail-Account ist untersagt. Ausgenommen davon sind E-Mail-Accounts, mit deren Betreibern eine spezielle Vereinbarung seitens der MedUni Wien getroffen worden ist, wie z.B. mit dem AKH.
2. Für dienstliche Zwecke ist der E-Mail-Account der MedUni Wien zu verwenden.
3. Das Versenden und Weiterleiten von Kettenbriefen und das Versenden von privaten Massenmails ist verboten.
4. Zur Vermeidung von Phishing Attacken dürfen die persönlichen UserIDs und Passwörter niemals per E-Mail weitergegeben werden.
5. Die Übertragung vertraulicher und/oder personenbezogener Daten an externe IT-Systeme hat ausschließlich verschlüsselt zu erfolgen.
6. Die Speicherung von vertraulichen Daten auf mobilen IT-Endgeräten darf nur erfolgen, wenn diese dort verschlüsselt abgelegt werden.
7. Für die Sicherung von lokal auf IT-Endgeräten oder mobilen Datenträgern abgelegten Daten ist der jeweilige Benutzer des IT-Endgerätes verantwortlich.
8. Der Einsatz von Soft- und Hardware, um Informationen auszuspähen, ist untersagt.
9. Die Synchronisation dienstlicher und/oder personenbezogener Daten auf IT-Endgeräten mit öffentlichen Cloud-Diensten (Dropbox, Google etc.) ist untersagt.
10. Im Zuge des Ausscheidens aus dem Dienstverhältnis sind alle Daten an den/die Vorgesetzten/e zu übergeben und dürfen nicht gelöscht oder unkenntlich gemacht werden. Ausgenommen hiervon sind private Daten, welche von ausscheidenden MitarbeiterInnen zu löschen sind.

11. Bei Beendigung des Dienstverhältnisses bzw. eines Vertragsverhältnisses sind im Eigentum/Verfügungsbefugnis der Medizinischen Universität Wien stehende IT-Arbeitsmittel an den/die jeweilige/n Vorgesetzte/n zu retournieren.

4.2 Sicherheitstechnische Aspekte

Folgende Punkte beziehen sich auf jene IT-Endgeräte, die Zugang zum wissenschaftlichen Datennetz der Medizinischen Universität Wien haben.

1. Die Störung von IT-Services und der ihnen zugrundeliegenden IT-Infrastruktur der Medizinischen Universität Wien ist verboten.
2. Erlaubt ist nur die Verwendung von IT-Endgeräten, die von der Medizinischen Universität Wien frei gegeben / registriert wurden[1].
3. Der Anschluss von IT-Endgeräten an die internen Netzwerke der Medizinischen Universität Wien erfolgt ausschließlich auf Basis der Autorisierung durch die Organisationseinheitsleitung.
4. Erlaubt ist nur die Verwendung von Software, für die die Medizinischen Universität Wien oder MitarbeiterInnen der Medizinischen Universität Wien ordnungsgemäße Lizenzen besitzt. Der Einsatz von Software wird vom ITSC untersagt, wenn sicherheits- und betriebstechnische Bedenken vorliegen.
5. Das Betriebssystem von IT-Endgeräten ist in Bezug auf Sicherheits-Updates aktuell zu halten.
6. Die jeweils auf IT-Endgeräten installierten Anwendungen sind in Bezug auf Sicherheits-Updates aktuell zu halten.
7. Wenn technisch möglich, ist beim Aufsetzen des PCs das Bios-Passwort des jeweiligen IT-Endgerätes zu aktivieren.
8. Das Neustarten (Booten) von öffentlich zugänglichen IT-Endgeräten der Medizinischen Universität Wien über externe Datenträger ist untersagt.
9. Das Starten (Booten) von IT-Endgeräten der Medizinischen Universität Wien über mobile Datenträger ist untersagt, ausgenommen zu Wartungszwecken.
10. Das Einschränken von Netzwerkprotokollen für die Netzüberwachung (z.B. Ping, SNMP) ist nicht zulässig.
11. Das jeweilige IT-Endgerät ist bei Verlassen des Arbeitsplatzes manuell zu sperren (z.B. passwortgeschützter Bildschirmschoner oder Ruhezustand).
12. Die/der NutzerIn hat dafür Sorge zu tragen, dass die automatische Gerätesperre spätestens nach 10 Minuten Inaktivität erfolgt (z.B. passwortgeschützter Bildschirmschoner oder Ruhezustand).
13. Auf IT-Endgeräten darf, außer zu Wartungszwecken, nicht als Benutzer mit Administrator- oder Root-Rechten gearbeitet werden.
14. Der Schadsoftwarescanner/Virenscanner darf nicht deaktiviert werden.

[1] Dazu muss das Formular „Antrag auf Nutzung des Datennetzes der MedUni Wien“ vollständig ausgefüllt und vomITSC genehmigt werden. Nur Geräte mit registrierter Netzwerkkartennummer werden ins Netz gelassen.

15. Die Viren- bzw. Malware-Signaturen der Schadsoftwarescanner/Virenscanner sind zu installieren und aktuell zu halten.
16. Die automatische Installation von Sicherheitsupdates darf nicht eingeschränkt oder verhindert werden.
17. Die Personal Firewall darf nicht deaktiviert werden.
18. Die Installation sicherheitsgefährdender Programme ist untersagt. Eine Liste der untersagten Programme ist im Intranet einsehbar unter https://intranet.meduniwien.ac.at/service/informationssicherheit/richtlinien
19. Auf Internet-Seiten, deren Inhalte eine Sicherheitsgefährdung offensichtlich vermuten lassen (Hackerseiten, Darkweb etc.), darf aktiv nicht zugegriffen werden.
    Warnungen (durch den Webbrowser, die Anti-Virussoftware, udgl.) sind zu berücksichtigen.
20. Erkennbar sicherheitsrelevante Einstellungen dürfen vom Endbenutzer nicht abgeschwächt werden.
21. Erlaubt ist nur der Einsatz genehmigter Internet-Dienste. Eine Liste der unterbundenen Dienste und Protokolle aus dem und in das Netz der Medizinischen Universität Wien ist im Intranet einsehbar unter https://intranet.meduniwien.ac.at/service/informationssicherheit/richtlinien.
22. Nicht registrierte IT-Endgeräte bekommen Zugang zum Gäste-LAN und müssen in Konfiguration und Nutzung ebenfalls dieser Richtlinie entsprechen.
23. Laptops, Tablets, Smartphones, Mobiltelefone und andere Kleingeräte, die sich im Eigentum/Verfügungsbefugnis der Medizinischen Universität Wien befinden, sind sicher zu verwahren und gegen unbefugte Verwendung zu schützen.
24. Zur Betreuung/Wartung eines IT-Endgerätes können die Dienstleistungen Dritter in Anspruch genommen werden. Diese Dritten sind durch entsprechende Vereinbarungen (Auftragsverarbeitervertrag) zur Einhaltung dieser Richtlinie und des Datenschutzes zu verpflichten. Ihre Tätigkeiten sind auf den Umfang zu beschränken, der für die Erfüllung der jeweiligen Dienstleistung notwendig ist.
25. Eine Weitergabe der erteilten Berechtigungen und allfälliger Betriebsmittel ist nicht gestattet.
26. Die Weitergabe von Berechtigungen wie Zutrittskarten, Passwörtern, PIN-Codes etc. ist verboten.
27. Wird ein IT-Endgerät von mehreren Personen genutzt, so sind entsprechende Vorkehrungen zu treffen, um Missbrauch durch unautorisierte Personen zu verhindern.
28. Wird ein IT-Endgerät nicht mehr benötigt, so ist die Löschung der Netzwerkregistrierung beim ITSC zu beantragen und die Trennung der Netzanbindung vorzunehmen. Für die sichere Löschung bzw. Zerstörung der Datenträger ist Sorge zu tragen (siehe Löschungs- und Entsorgungsrichtlinie der Medizinischen Universität Wien).
29. Jede Änderung in der Person des Nutzers/der Nutzerin eines IT-Endgeräts ist dem ITSC vorab bekanntzugeben.

4.3 Rechtliche Aspekte

1. Alle anwendbaren datenschutzrechtlichen Bestimmungen, inklusive der Verpflichtung zur Gewährleistung des Datengeheimnisses, sind einzuhalten, ebenso Vertraulichkeits-vereinbarungen jeglicher Art.
2. Die Medizinische Universität Wien ist bei privaten Verstößen gegen Rechte Dritter schad- und klaglos zu halten.
3. Folgende Inhalte dürfen weder erzeugt noch verbreitet werden: Schadsoftware in jeglicher Form, Inhalte, die gegenüber anderen herabwürdigend sind, die Intoleranz gegenüber anderen propagieren, die pornographischer Natur sind, die gesetzeswidrige Aktivitäten befürworten oder in sonstiger Weise gegen Gesetze verstoßen und sonstige Inhalte, die im Allgemeinen als anstößig verstanden werden.
4. Auf folgende Inhalte darf nicht vorsätzlich zugegriffen werden, sofern es nicht der Zweck der wissenschaftlichen Forschung erfordert: Inhalte, die gegenüber anderen herabwürdigend sind, die Intoleranz gegenüber anderen propagieren, die pornographischer Natur sind, die gesetzeswidrige Aktivitäten befürworten oder in sonstiger Weise gegen Gesetze verstoßen und sonstige Inhalte, die im Allgemeinen als anstößig verstanden werden.
5. Urheberrechtliche Vorschriften sind zu wahren und Lizenzbestimmungen einzuhalten.
6. Werbeverbote sind zu beachten und „geistiges Eigentum“ (Immaterialgüterrechte wie z.B. Urheberrecht, Markenrechte etc.) sowie Persönlichkeitsrechte sind zu wahren.

4.4 Private Nutzung

1. Die private Nutzung von IT-Arbeitsmitteln, die im Eigentum/Verfügungsbefugnis der Medizinischen Universität Wien stehen, ist untersagt. Geduldet wird bis auf Widerruf eine in Bezug auf Zeitausmaß und Ressourcenbedarf geringfügige Nutzung, die zu keiner Beeinträchtigung des ordnungsgemäßen Unibetriebs führt und im Rahmen der sonstigen Regelungen dieser Richtlinie erfolgt. Allenfalls dabei entstandene private Daten (Dateien, E-Mails etc.) sind in als "privat" gekennzeichneten Ordnern abzulegen.
2. Jede/r NutzerIn ist für die Sicherung privater Inhalte selbst verantwortlich. Die Medizinische Universität Wien übernimmt keine Haftung für den Verlust von privaten Daten.
3. Die private Nutzung der dienstlichen E-Mail-Adresse ist untersagt. Geduldet wird bis auf Widerruf eine in Bezug auf Zeitausmaß und Ressourcenbedarf geringfügige Nutzung, die im Rahmen der sonstigen Regelungen dieser Richtlinie erfolgt. Die Verwendung der E-Mail-Signatur der Medizinischen Universität Wien ist im privaten Kontext untersagt. Die dienstliche E-Mail-Adresse darf nicht zur Registrierung von Onlinediensten für private Zwecke verwendet werden. Ausgenommen davon sind Registrierungen für Sonderkonditionen für Bedienstete der Medizinischen Universität Wien, die die dienstliche E-Mail-Adresse zum Nachweis der Firmenzugehörigkeit benötigen.
4. Die private Nutzung des Internetzugangs der Medizinischen Universität Wien ist untersagt. Geduldet wird bis auf Widerruf eine in Bezug auf Zeitausmaß und Ressourcenbedarf geringfügige Nutzung, die im Rahmen der sonstigen Regelungen dieser Richtlinie erfolgt.

5. Die Nutzung von Server-Speicherplatz für private Zwecke ist untersagt, geduldet wird bis auf Widerruf eine in Bezug auf Zeitausmaß und Ressourcenbedarf geringfügige Nutzung, die im Rahmen der sonstigen Regelungen dieser Richtlinie erfolgt. Auf Aufforderung durch das ITSC sind private Daten auf Speichern/Datenträgern, für die die Medizinische Universität Wien das uneingeschränkte Nutzungsrecht hat, von der Person, die diese Daten dort gespeichert hat, zu löschen.

5 Meldung von Sicherheitsvorfällen und -mängeln

Alle Personen, die vom Geltungsbereich dieser Richtlinie umfasst sind, haben ihnen bekannt gewordene sicherheitsrelevante Vorfälle und Sicherheitsmängel umgehend an die/den IT-SicherheitskoordinatorIn (security@meduniwien.ac.at) zu melden.

6 Folgen der Nichteinhaltung

Die Einhaltung dieser Richtlinie wird regelmäßig, aber auch anlassbezogen überprüft.

Eine Missachtung der in dieser Richtlinie getroffenen Regelungen kann neben entsprechenden disziplinären und dienstrechtlichen auch zivil- und strafrechtliche Folgen nach sich ziehen, zudem kann der Netzwerkzugang eingeschränkt oder widerrufen werden.

Eine Verletzung dieser Richtlinie durch Dritte (z.B. Wartungsfirmen) kann (neben etwaigen zivil- und strafrechtliche Folgen) zur Kündigung des bestehenden Vertragsverhältnisses oder zum Ausschluss von künftigen Aufträgen führen.

7 Ausnahmen von dieser Richtlinie

Grundsätzlich ist eine Vorgehensweise zu wählen, die die Vorgaben der geltenden Richtlinie erfüllt. Erst wenn dies aus technischen oder organisatorischen Gründen nicht möglich oder wirtschaftlich nicht zu vertreten ist, kann über eine Ausnahmeregelung entschieden werden.

Ausnahmen müssen

- zeitlich begrenzt,
- auf Zweck und Benutzerkreis eingeschränkt,
- hinsichtlich Antrag, Genehmigung/Ablehnung, Änderungen und Auslaufen dokumentiert,
- kontrolliert und im Falle des Auslaufens ohne Neuantrag nach entsprechender Frist aufgehoben und
- im Falle der Nichtbeachtung einschlägiger Richtlinien der Medizinischen Universität Wien umgehend aufgehoben werden.

Der Antrag zur Erteilung einer Ausnahme ist vorab von dem/der Universitätsangehörigen an die/den IT-SicherheitskoordinatorIn zu stellen.

Die aktuell gewährten Ausnahmen sind getrennt von dieser Richtlinie im Dokument „Ausnahmen von IT-Sicherheitsrichtlinien der Medizinischen Universität Wien“ von der InfoSec-SicherheitskoordinatorIn zu verwalten. Das Ausnahmenregister ist nicht öffentlich einsehbar.

Wien, am .....

Für die Medizinische Universität Wien:

.....

Rektor Univ.-Prof. Dr.med.univ. Markus Müller