AMTLICHE MITTEILUNG

Nr.: 800

Veröffentlicht am 02.12.2022

IT-Nutzungsordnung der Hochschule RheinMain

BEKANNTMACHUNG

Nach § 1 der Satzung der Hochschule RheinMain zur Bekanntmachung ihrer Satzungen vom 04. Juni 2013 (StAnz. vom 29.7.2013, S. 929) wird die IT-Nutzungsordnung der Hochschule RheinMain hiermit bekanntgegeben.

Wiesbaden, 02.12.2022

Prof. Dr. Eva Waller
Präsidentin

Herausgeber:

Präsidentin

Hochschule RheinMain

Postfach 3251

65022 Wiesbaden

Redaktion:

Abteilung VIII

Rainer Scholl

E-Mail: rainer.scholl@hs-rm.de

IT-NUTZUNGSORDNUNG

Das Präsidium der Hochschule RheinMain hat am 19.09.2022 im Benehmen mit dem Senat die folgende IT-Nutzungsordnung für die HSRM beschlossen:

PRÄAMBEL

Die Hochschule RheinMain, ihre Fachbereiche und Einrichtungen betreiben eine Informationsverarbeitungs- und Kommunikations (IuK)-Infrastruktur, bestehend aus Informationsverarbeitungssystemen (Rechenanlagen) und einem Multiservice-Kommunikationsnetz zur Übertragung von Daten und Sprache (darunter fallen auch Bild- und Videoübertragungen). Diese IuK-Infrastruktur ist an das weltweite Internet angeschlossen.

§ 1 GELTUNGSBEREICH

Diese Nutzungsordnung gilt für die Mitglieder und Angehörigen der Hochschule RheinMain und für die von der Hochschule RheinMain betriebene IuK-Infrastruktur, bestehend aus Informationsverarbeitungssystemen, Kommunikationssystemen und weiteren Hilfseinrichtungen.

§ 2 SYSTEMBETREIBER

Systembetreiber sind:

1. für das Hochschulnetz, zentrale Systeme und Dienste das IT- und Medienzentrum (ITMZ) der Hochschule RheinMain. Das ITMZ regelt den Zugang der einzelnen Systeme zum zentralen Hochschulnetz. Dies betrifft insbesondere die Vergabe der hierzu benötigten Ressourcen (Netzzugänge, IP-Adressen, DNS- Domänen-Namen, Firewall-Freigaben).

2. für dezentrale Systeme oder Netze die jeweils zuständige Organisationseinheit der Hochschule (Fachbereich, Arbeitsgruppe, Einrichtung oder andere Untereinheit der Hochschule).

BEDINUNGEN DER (PRIVATEN) IUK-NUTZUNG

§ 3 INTERNET-NUTZUNG UND E-MAIL-NUTZUNG

1. Die in § 1 genannten IuK-Ressourcen der Hochschule RheinMain stehen den Mitgliedern und Angehörigen der Hochschule RheinMain zur Erfüllung ihrer Aufgaben gemäß §§ 3 und 4 des Hessischen Hochschulgesetzes (HHG) bzw. zur Durchführung ihres Studiums zur Verfügung.

2. E-Mail- und Internetnutzung sollen grundsätzlich nur zu dienstlichen oder Hochschulzwecken erfolgen.

3. Die private Internetnutzung ist nur in geringfügigem Umfang zulässig, wenn Hochschulbelange dem nicht entgegenstehen. Hochschulbelangen steht insbesondere entgegen, wenn die Nutzung geeignet ist den Dienstbetrieb zu beeinträchtigen, den Interessen und dem Ansehen der Hochschule zu schaden, die Verfügbarkeit der IT-Systeme zu beeinträchtigen oder die Nutzung gegen geltendes Recht, insbesondere gegen persönlichkeitsrechtliche, datenschutzrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt.

4. Die private E-Mailnutzung ist in geringfügigem Umfang zulässig. Die Hochschule ist jedoch keine Telekommunikationsdiensteanbieterin im Sinne des §3 TTDSG und weist deshalb darauf hin, dass sie nicht die Verantwortung für die ständige Verfügbarkeit des Postfachzugangs übernimmt und dieses den Mitgliedern und Angehörigen privat nur für eine gelegentliche Mitnutzung zur Verfügung steht.

5. Es ist die Aufgabe der Nutzerinnen und Nutzer private E- Mailkorrespondenz, insbesondere privilegierte Korrespondenz mit

    - inner- und außerbehördlichen Interessenvertretungen (z.B. Gewerkschaften),
    - der Frauen- und Gleichstellungsbeauftragten
    - der/dem behördlichen Datenschutzbeauftragten,
    - der/dem Suchtbeauftragten,
    - den Konfliktbeauftragten,
    - den BEM-Ansprechpartner*innen,
    - den Mitgliedern der Personalräte und
    - ggf. weiteren Institutionen,

in einem als ‚privat' gekennzeichneten Ordner abzulegen, wenn eine Kenntnisnahme durch die Hochschule verhindert werden soll.

6. Zur Sicherstellung eines ordnungsgemäßen Betriebs des Systems und der Kapazitätsplanung erfolgt eine Überwachung gemäß § 8 IT-Richtlinie für Systembetreiber.

EINSICHTNAHME IN E-MAIL-POSTFÄCHER

§ 4 ZULÄSSIGKEIT DER EINSICHTNAHME

1. Eine Einsichtnahme in die Nachrichten- und E-Mail-Postfächer ist nur zulässig, soweit dies zur Behebung aktueller Störungen im jeweiligen Dienst oder zur Sicherstellung des Hochschulbetriebs (z.B. bei längerer ungeplanter Abwesenheit der Nutzerin oder des Nutzers) unerlässlich ist.

2. Zu prüfen ist vorher, ob die Schaltung einer Abwesenheitsnotiz ausreichend ist.

§ 5 VORGEHEN BEI EINSICHTNAHME IN EIN E-MAIL-POSTFACH VON BESCHÄFTIGTEN

1. Bei Einsichtnahme dürfen nur E-Mails eingesehen werden, die für einen konkreten, dringenden, dienstlichen Anlass benötigt werden.

2. In jedem Fall ist die Einsichtnahme zu dokumentieren, und der / die betroffene Beschäftigte ist spätestens nach Zweckerreichung unverzüglich zu benachrichtigen.

3. Die Einsichtnahme kann bei Beschäftigten nur in Anwesenheit eines Personalratsmitgliedes , bei anderen Nutzerinnen und Nutzern nur in Anwesenheit eines neutralen Dritten erfolgen.

WEITERE REGELUNGEN ZUR INTERNET- UND E-MAIL-NUTZUNG

§ 6 BESONDERHEITEN BEI DER NUTZUNG VON E-MAILS

1. Bei der Weiterleitung von E-Mails ist darauf zu achten, dass damit ein zulässiger Verarbeitungszweck verfolgt wird und nur die dafür erforderlichen personenbezogenen Daten übermittelt werden. Die generelle Weiterleitung aller E-Mails an eine externe Adresse (z.B. durch Eintrag einer entsprechenden Weiterleitungsadresse) ist nicht zulässig.

2. Für dienstliche Angelegenheiten ist ausschließlich der dienstliche E-Mail-Account zu verwenden.

§ 7 LÖSCHUNG VON HDS- UND E-MAIL-ACCOUNTS

1. Nach Beendigung des Rechtsverhältnisses mit der Hochschule Rhein-Main, sei es durch Ausscheiden aus dem Beschäftigungsverhältnis oder durch Exmatrikulation, werden die E-Mail-Postfächer der Nutzerin bzw. des Nutzers - vorbehaltlich besonderer Aufbewahrungs- oder Archivierungspflichten, die persönlichen Accounts und die darin gespeicherten Daten (z.B. das Home Verzeichnis) nach zwölf Monaten gelöscht.

2. Sollte eine Einsichtnahme in die Daten und E-Mail-Postfächer erforderlich sein, so hat diese gemäß §5 zu erfolgen.

RECHTE UND PFLICHTEN DER NUTZERINNEN UND NUTZER

§ 8 NUTZUNGSBERECHTIGUNGEN

1. Zur Nutzung der IuK-Ressourcen nach § 1 bedarf es einer formalen Nutzungsberechtigung des zuständigen Systembetreibers, z.B. Nutzerkennung, Netzanschluss oder Netzzugang, die i.d.R. beim Systembetreiber zu beantragen ist. Ausgenommen sind allgemeine Informationssysteme der Hochschule, die vom Systembetreiber für eine allgemeine Nutzung bestimmt sind (z.B. Webauftritt, Bibliothekskatalog) sowie Rechner, die nur unter Aufsicht verwendet werden (z.B. in Laboren).

2. Studierende, Lehrende und Beschäftigte erhalten mit Beginn ihres Studiums bzw. ihrer Tätigkeit eine Nutzungsberechtigung zu zentralen IuK-Ressourcen der Hochschule RheinMain entsprechend ihrer Funktion und ihres Aufgabengebiets.

3. Der Anschluss von Rechnern an das Hochschulnetz kann grundsätzlich nur von Hochschulbediensteten über die Administratorinnen und Administratoren der jeweiligen Organisationseinheit beantragt werden. Diese informieren über Rechte und Pflichten (Hinweis auf diese IT-Nutzungsordnung) und nehmen die benötigten Daten (Gerätedaten und Netzwerkinformationen) zwecks Weiterleitung an das ITMZ auf. Davon ausgenommen sind Netze, bei denen der Zugang durch eine Nutzerauthentifizierung kontrolliert wird (z.B. WLAN).

§ 9 BEFRISTETE EINRICHTUNG VON NUTZUNGSBERECHTIGUNGEN

1. Anderen Personen und Institutionen kann die Nutzung zeitlich befristet gestattet werden, sofern dabei der Betrieb der Hochschule oder die Rechte Dritter nicht beeinträchtigt werden.

2. Die Nutzungsberechtigung ist in diesem Fall schriftlich oder in Textform über ein Mitglied der Hochschule zu beantragen.

3. Die Hochschule kann sich an Authentifizierungsverbünden beteiligen, die den Nutzern anderer Institutionen die Nutzung bestimmter IuK-Ressourcen ohne Genehmigung im Einzelfall zu ermöglichen (z.B. eduroam)

§ 10 DATEN, DIE BEI DER BEANTRAGUNG EINER NUTZUNGSBERECHTIGUNG ERFASST WERDEN MÜSSEN

1. Bei der Beantragung einer Nutzungsberechtigung müssen folgende Angaben erfasst werden:
   a. Systembetreiber, bei dem die Nutzungsberechtigung beantragt wird;
   b. Systeme, für welche die Nutzungsberechtigung beantragt wird;
   c. Antragstellerin oder Antragsteller: Name, Adresse, Telefon- und/oder Telefaxnummer und E-Mail-Adresse (bei Studierenden auch Matrikelnummer) sowie Zugehörigkeit zu einer Organisationseinheit der Hochschule,
   d. bei Nichthochschulangehörigen das Mitglied (Name und Organisationseinheit) der Hochschule, über das der Antrag eingereicht wurde;

e. Angaben zum Zweck der Nutzung, z. B. Forschung, Ausbildung/ Lehre, Verwaltung;
f. Ggf. die Zustimmung der oder des Verantwortlichen der betroffenen Verfahren oder Daten;
g. Die Erklärung, dass die Nutzerin oder der Nutzer diese Nutzungsordnung anerkennt
h. bei Anträgen von Personen nach § 9 die Dauer der beabsichtigten Nutzung

2. Weitere Angaben darf der Systembetreiber nur verlangen, soweit sie zur Bearbeitung des Antrags erforderlich sind. Diese weiteren Angaben werden nur für die Dauer der Bearbeitung des Antrags gespeichert.

§ 11 ENTSCHEIDUNG ÜBER DEN ANTRAG

1. Über den Antrag entscheidet der zuständige Systembetreiber.

2. Er kann die Erteilung der Nutzungsberechtigung vom Nachweis bestimmter Kenntnisse über die Nutzung des Systems abhängig machen.

3. Die Erteilung der Nutzungsberechtigung darf insbesondere versagt werden, wenn

a. die beabsichtigte Nutzung nicht mit den Zwecken gemäß § 2 Ziffer 1 dieser Nutzungsordnung vereinbar ist;
b. nicht gewährleistet erscheint, dass die Antragstellerin oder der Antragsteller ihren oder seinen Pflichten als Nutzerin oder Nutzer nachkommen wird;
c. das System für die beabsichtigte Nutzung offensichtlich ungeeignet oder für andere Zwecke reserviert ist;
d. die Kapazität des Systems, dessen Nutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die beabsichtigten Arbeiten nicht ausreicht;
e. zu erwarten ist, dass durch die beantragte Nutzung andere berechtigte Nutzungen in unangemessener Weise gestört werden.

§ 12 WIDERRUF BESTEHENDER NUTZUNGSBERECHTIGUNGEN

1. Die Nutzerinnen und Nutzer können aufgrund rechtlicher Vorgaben in der Nutzung der Rechenanlagen eingeschränkt werden.

2. Die Nutzungsberechtigung berechtigt nur zu Arbeiten im Rahmen der gewährten Nutzungsberechtigung.

3. Nutzungsberechtigungen werden regelmäßig überprüft und widerrufen, wenn
   a. die Grundlage der Nutzungsberechtigung nicht mehr besteht oder
   b. die Nutzungsberechtigung nicht mehr erforderlich ist.

§ 13 VERANTWORTLICHKEITEN DER NUTZINNEN UND NUTZER

1. Die Nutzerinnen und Nutzer sind verpflichtet, auf die IT-Sicherheit zu achten und

   a. ausschließlich mit Nutzerkennungen zu arbeiten, deren Nutzung ihnen gestattet wurde;
   b. Vorkehrungen zu treffen, damit unberechtigten Dritten der Zugang zu den IuK-Ressourcen verwehrt wird; dazu gehört es insbesondere, Passwörter und andere Zugangsdaten geheim zu halten, sichere Passwörter zu verwenden, den Rechner beim Verlassen des Arbeitsplatzes zu sperren und sich nach Nutzung vom System abzumelden;
   c. fremde Nutzerkennungen und Passwörter weder zu ermitteln noch zu nutzen;
   d. die Hinweise der Hochschule zur IT-Sicherheit zu beachten.

Verboten ist:

   e. das eigene Passwort weiterzugeben

Nur mit Genehmigung des Systembetreibers[1] ist erlaubt,

   f. Eingriffe in die Hardware-Installation vorzunehmen;
   g. Software auf den Systemen zu installieren zu deinstallieren oder
   h. die Konfiguration der Systeme oder des Netzwerks zu verändern:

§ 14 VERHALTEN BEI STÖRUNGEN ODER SICHERHEITSVORFÄLLEN

Die Nutzerinnen und Nutzer sind verpflichtet,

1. die vom Systembetreiber zur Verfügung gestellten Leitfäden zur Nutzung zu beachten
2. Sicherheitsmängel und Störungen des Betriebs der Systemadministratorin oder dem Systemadministrator zu melden. Sicherheitsvorfälle sind dem Chief Information Security Officer (CISO) und

[1] Als Systembetreiber gilt die Organisationseinheit, die den Betrieb der IT-Systeme verantwortet. Die künftige Systembetreiberrichtlinie wird aktuell erarbeitet (Stand: Januar 2023)

dem Datenschutzbeauftragten (DSB) unverzüglich zu melden.

3. Hierbei gilt insbesondere, dass Nutzerinnen und Nutzer der Systemadministratorin oder dem Systemadministrator auf Verlangen in begründeten Einzelfällen - insbesondere bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung - zu Kontrollzwecken Auskünfte über Programme und genutzte Methoden zu gewähren.
4. Von dieser Regelung werden nicht die Nutzerdaten erfasst, die durch das Telekommunikationsgeheimnis oder das Datengeheimnis geschützt sind, z.B. persönliche Dateien oder personenbezogene Daten Dritter.

§ 15 ÖKONOMISCH SINNVOLLE NUTZUNG DER VORHANDENEN RESSOURRCEN

1. Die Nutzerinnen und Nutzer sind verpflichtet, darauf zu achten, dass sie die vorhandenen Betriebsmittel (z.B. Arbeitsplätze, CPU-Kapazität, Plattenspeicherplatz, Leitungskapazitäten, Peripheriegeräte und Verbrauchsmaterial) verantwortungsvoll und ökonomisch sinnvoll nutzen.
2. Sie sind verpflichtet, Beeinträchtigungen des Betriebes, soweit sie vorhersehbar sind, zu unterlassen und nach bestem Wissen alles zu vermeiden, was Schaden an der IuK-Infrastruktur oder bei anderen Nutzerinnen und Nutzern verursachen kann.
3. Zuwiderhandlungen können Schadensersatzansprüche begründen und zum Nutzungsausschluss führen.

EINHALTUNG GESETZLICHR VORGABEN

§ 16 URHEBERRECHT

Die Nutzerinnen und Nutzer sind verpflichtet:

a. bei der Nutzung von Software (Quellen, Objekte), Dokumentationen und anderen Daten die gesetzlichen Regelungen (z.B. Urheberrechtsschutz, zu. a.) einzuhalten;
b. sich über die Bedingungen, unter denen die Software, Dokumentationen oder Daten zur Verfügung gestellt werden, zu informieren und diese Bedingungen zu beachten;
c. insbesondere Software, Dokumentationen, Zugangsdaten und

sonstige Daten, soweit nicht ausdrücklich erlaubt, weder zu kopieren noch weiterzugeben noch zu anderen als den erlaubten, insbesondere nicht zu gewerblichen Zwecken zu nutzen. Zuwiderhandlungen können Schadensersatzansprüche begründen.

§ 17 DATENSCHUTZRECHT

1. Die Nutzerinnen und Nutzer sind in ihrem Einflussbereich verpflichtet bei der Verarbeitung personenbezogener Daten die DSGVO, insbesondere die datenschutzrechtlichen Grundsätze aus Art 5 DSGVO, das HDSIG und der hochschulinternen Regelungen zu beachten.
2. Bei der Einführung neuer oder Änderung bestehender Verarbeitungstätigkeiten ist die Verarbeitung von den Beschäftigten mit dem jeweiligen Systembetreiber abzustimmen und das Verzeichnis der Verarbeitungstätigkeiten zu aktualisieren.
3. Zudem ist eine Risikoanalyse durchzuführen, um die nötigen technischen und organisatorischen Maßnahmen zu etablieren.
4. Basierend auf der Risikoanalyse ist ein Berechtigungskonzept (need to know, need to do) zu erarbeiten

§ 18 VERBOT MISSBRÄUCHLICHER NUTZUNG DER IUK-INFRASTRUKTUR

Die Nutzerinnen und Nutzer haben jegliche Art der missbräuchlichen Nutzung der IuK-Infrastruktur zu unterlassen. Dies umfasst insbesondere:

a. unberechtigten Zugriff auf Informationen anderer Nutzerinnen und Nutzer und Weitergabe, Nutzung oder Veränderung von Informationen anderer Nutzerinnen und Nutzer ohne deren Genehmigung;
b. Verbreitung oder In-Umlauf-Bringen von Informationen, die Personen beleidigen oder herabwürdigen oder die Interessen oder das Ansehen der Hochschule beeinträchtigen
c. unberechtigte Verbreitung von persönlichen oder anderen schützenswerten Informationen über eine Einzelperson oder eine Gruppe von Personen
d. Versenden von elektronischen Massensendungen (z.B. SPAM-E-Mails). (Ausnahme: Verbreitung von dienstlichen Mitteilungen in Analogie zur Hauspost.)
e. Weitersenden oder In-Umlauf-Bringen von elektronischen Kettenbriefen.
f. Abrufen, Verbreiten oder Herunterladen diskriminierender, beleidigender, verleumderischer, menschenverachtender, verfassungsfeindlicher, sexistischer oder pornographischer Inhalte.

g. Systematisches Ausforschen von Servern und Services (z.B. Portscans). Ausnahme: Sicherheitstests nach Absprache mit der Systemadministratorin /dem Systemadministrator und dem CISO.
h. Unerlaubte Aneignung von Ressourcen oder der Versuch einer solchen Aneignung (z. B. Cracken). Ausnahme: Sicherheitstests nach Absprache mit der Systemadministratorin /dem Systemadministrator und dem CISO.
i. Beschädigung oder Störung von elektronischen Diensten (z.B. „Denial of service attacks“).
j. Vorsätzliche Verbreitung oder In-Umlauf-Bringen von Schadsoftware (z.B. Viren, Würmer, Trojanische Pferde, Ransomware).
k. Ausspähen von Passwörtern oder der Versuch des Ausspähens (z.B. Key Logger).
l. Unberechtigte Manipulation oder Fälschung von Identitätsinformationen (z.B. Mailheader, elektronische Verzeichnisse, IP-Spoofing).
m. Ausnutzen erkannter Sicherheitsmängel bzw. administrativer Mängel.

FOLGEN EINER MISSBRÄUCHLICHEN ODER GESETZESWIDRIGEN NUTZUNG

§ 19 INTERNE FOLGEN EINER MISSBRÄICHLICHEN ODER GESETZESWIDRIGEN NUTZUNG

1. Bei schuldhaften Verstößen gegen diese Ordnung, bei der Begehung von strafbaren Handlungen oder Ordnungswidrigkeiten oder sonstigem schuldhaften rechtswidrigen Verhalten im Zusammenhang mit der Nutzung, kann der Systembetreiber Nutzungsberechtigungen unter Wahrung der Verhältnismäßigkeit zeitweise oder auf Dauer einschränken oder entziehen. Dabei ist es unerheblich, ob der Verstoß materiellen Schaden zur Folge hatte oder nicht. Vor einer solchen beschränkenden oder entziehenden Maßnahme ist der oder dem Betroffenen Gelegenheit zur Stellungnahme zu geben.
2. Dem Ausschluss soll eine Verwarnung vorausgehen, in der auf die Möglichkeit von Maßnahmen nach Ziffer 1 hingewiesen wird.
3. Bei Maßnahmen gegen Beschäftigte ist vor der Entscheidung der Personalrat zu beteiligen.
4. In dringenden Fällen können vom Systembetreiber vorläufige Maßnahmen nach Ziffer 1 auch ohne vorherige Anhörung getroffen werden. Wenn Beschäftigte betroffen sind, ist der Personalrat darüber unverzüglich zu informieren.

§ 20 WEITERE FOLGEN EINER MISSBRÄUCHLICHEN ODER GESETZESWIDRIGEN NUTZUNG

1. Die Haftung der Nutzerin oder des Nutzers für Verstöße gegen die ihr oder ihm im Rahmen der Nutzung obliegenden Pflichten (z.B. Urheberrechtsverletzungen) richtet sich nach den allgemeinen haftungsrechtlichen Regelungen.
2. Die Nutzerin oder der Nutzer hat die Hochschule RheinMain von allen Ansprüchen freizustellen, wenn Dritte die Hochschule wegen eines missbräuchlichen oder rechtswidrigen Verhaltens der Nutzerin oder des Nutzers auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen.

§ 21 IN-KRAFT-TRETEN

Diese Nutzungsordnung tritt am Tage nach der Veröffentlichung in den Amtlichen Mitteilungen der Hochschule RheinMain in Kraft. Die Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Fachhochschule Wiesbaden vom 18.08.2008 und die IT-Sicherheitsrichtlinie der Fachhochschule Wiesbaden vom 22.10.2008 werden gleichzeitig außer Kraft gesetzt.