09/20

13. März 2020

Amtliches Mitteilungsblatt

Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

Herausgeberin

Die Hochschulleitung der HTW Berlin

Treskowallee 8

10318 Berlin

Redaktion

Rechtsstelle

Tel. +49 30 5019-2813

Fax +49 30 5019-2815

Benutzungsordnung Informationsverarbeitungsinfrastruktur (IVI) der HTW Berlin

Aufgrund von § 12 Abs. 1 Satz 1 Nr. 5 HTW-Satzung (AMBl. HTW Berlin Nr. 29/09), zuletzt geändert am 14. Oktober 2019 (AMBl. HTW Berlin Nr. 26/19), in Verbindung mit § 6 Abs. 2 der Satzung zur Organisation und Nutzung der Zentraleinrichtung (ZE) Hochschulrechenzentrum (HRZ) der Hochschule für Technik und Wirtschaft Berlin (HTW Berlin) hat der Akademische Senat der HTW Berlin am 9. Dezember 2019 folgende Benutzungsordnung erlassen[1]:

Präambel

Diese Benutzungsordnung soll die möglichst störungsfreie, ungehinderte und sichere Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur der HTW Berlin gewährleisten. Die Benutzungsordnung richtet sich nach den gesetzlich festgelegten Aufgaben der HTW Berlin sowie ihrem Mandat zur Wahrung der akademischen Freiheit. Sie stellt Grundregeln für einen ordnungsgemäßen Betrieb der Informationsverarbeitungsinfrastruktur auf und regelt so das Nutzungsverhältnis zwischen den einzelnen Nutzer_innen und den Systembetreibern.

I. Geltungsbereich

Diese Benutzungsordnung gilt für die Nutzung der von der HTW Berlin und ihren Einrichtungen (im Folgenden „**Systembetreiber**“) bereitgestellten Informationsverarbeitungsinfrastruktur (kurz **IVI**), bestehend aus Datenverarbeitungsanlagen (Rechnern), Kommunikationssystemen (Netzen), IT-Diensten (Services) und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung, die den Systembetreibern unterstellt sind. Die IVI der HTW Berlin ist in regionale, überregionale und Netzwerke der Forschung und Lehre („Wissenschaftsnetze“) sowie das globale Internet eingebunden.

II. Nutzungsberechtigung und Zulassung zur Nutzung

(1) Die Zulassung von Nutzer_innen erfolgt ausschließlich zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, zu Zwecken der Bibliothek und der Hochschulverwaltung, zur Aus- und Weiterbildung sowie zur Erfüllung sonstiger Aufgaben der HTW Berlin. Eine hiervon abweichende Nutzung bedarf der ausdrücklichen Zulassung, die erteilt werden kann, wenn die abweichende Nutzung geringfügig ist, sie keinen gesetzlichen oder vertraglichen Verpflichtungen der HTW Berlin zuwiderläuft und die Zweckbestimmung der Systembetreiber sowie die Belange der anderen Nutzer_innen nicht beeinträchtigt werden. Nutzungen, die die Infrastruktur unnötig belasten, sind ausdrücklich untersagt.

[1] Bestätigt durch die Hochschulleitung der Hochschule für Technik und Wirtschaft Berlin am 26. Februar 2020.

(2) Zur Nutzung der Dienste der Systembetreiber können, soweit nicht spezielle Regelungen für einzelne Dienste oder Datenverarbeitungsressourcen oder vertragliche Verpflichtungen der HTW Berlin dem entgegenstehen, zugelassen werden:

a) Mitglieder, Angehörige und Einrichtungen einschließlich der Verwaltung der HTW Berlin gemäß BerlHG (z.B. Professor_innen, Lehrbeauftragte, sonstige Mitarbeiter_innen, Studierende),

b) Beauftragte der HTW Berlin zur Erfüllung ihrer Dienstaufgaben,

c) Mitglieder und Angehörige anderer Hochschulen des Landes oder staatlicher Hochschulen außerhalb des Landes aufgrund besonderer Vereinbarungen,

d) sonstige staatliche Forschungs- und Bildungseinrichtungen und Behörden des Landes aufgrund besonderer Vereinbarungen,

e) Studierendenwerke im Land Berlin,

f) Ehemalige Professor_innen der HTW Berlin,

g) andere Personen und Einrichtungen, denen die Nutzung der IVI von den Systembetreibern auf Antrag gestattet werden kann.

(3) Systembetreiber sind:

a) Das HRZ für die zentrale IVI des Hochschulnetzes (Forschung- und Lehre-Netzwerk) und des geschützten/internen Netzes.

b) Die Fachbereiche für die dezentrale IVI des jeweiligen Fachbereichs sowie für dessen Fachbereichsprojekte.

c) Die zentralen, interdisziplinären und sonstigen Einrichtungen für ihre jeweilige dezentrale IVI sowie für deren Projekte.

(4) Die Zulassung zur Nutzung der Einrichtungen und Dienste eines Systembetreibers erfolgt durch dessen Erteilung einer Nutzungserlaubnis (z.B. in Form eines Accounts mit Nutzername und Passwort/Aktivierungscode). Ausgenommen sind Dienste, die für anonymen Zugang eingerichtet sind (z.B. Informationsdienste, Bibliotheksdienste, kurzfristige Gastkennungen bei Tagungen). Der jeweilige Systembetreiber regelt die Antragsbearbeitung sowie die Ausgabe der Accounts selbst. Er entscheidet über den Antrag und kann die Erteilung der Nutzungsberechtigung vom Nachweis bestimmter Kenntnisse über die Benutzung der Anlage abhängig machen.

a) Nutzer_innen gemäß Abschnitt II(2)a) sind auf der Grundlage ihrer Mitgliedschaft in der HTW Berlin automatisch zur Nutzung der IVI berechtigt, die vom Systembetreiber gemäß Abschnitt II(3)a) zur Verfügung gestellt wird.

b) Die Nutzung der IVI anderer Systembetreiber gemäß II(3)b) und II(3)c) ist gesondert vom jeweiligen Systembetreiber zu regeln.

c) Für Nutzer_innen gemäß Abschnitt II(2)g) entscheiden die Betreiber nach Einzelfallprüfung auf der Basis der im Antragsverfahren benannten Nutzungsbegründung.

(5) Bei der Antragstellung sind die vom jeweiligen Systembetreiber in geeigneter Weise bereitzustellenden (Online-) Formulare zu nutzen.

(6) Der Antrag auf eine formale Nutzungsberechtigung sollte, sofern für die Zwecke der Verarbeitung erforderlich, folgende Angaben enthalten:

a) Betreiber/Institut oder organisatorische Einheit (OE), bei der die Nutzungsberechtigung beantragt wird

b) IT-Dienste/System bzw. DV-Ressourcen, für die die Nutzungsberechtigung beantragt wird

c) Personenbezogene Daten der Antragsteller_in nur, soweit diese zwingend erforderlich, dem Zweck angemessen und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind: Geschlecht (m/w/d[2]), Vorname, Nachname, Adresse, Status als Studierende, Mitarbeiter_in, Einrichtung oder sonstiger Benutzer_in im Sinne von Abschnitt II(1), Geburtsdatum, Telefonnummer, Matrikelnummer (bei Studierenden), elektronische Kontaktdaten, Vertragsdaten (Beginn/Dauer) und Zugehörigkeit zu einer organisatorischen Einheit der Hochschule. Personenbezogene Daten der Antragsteller_in dürfen grundsätzlich nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

d) Beschreibung des Nutzungszwecks bzw. des geplanten Vorhabens

e) Gesetzlich geforderte schriftliche oder elektronische Einverständniserklärung der Nutzer_innen nach und II(2)g) zur Verarbeitung ihrer personenbezogenen Daten als Anhang zum Nutzungsantrag.

f) Hinweis auf Möglichkeiten einer Dokumentation des Nutzerverhaltens und der Einsichtnahme in die Nutzerdateien nach Maßgabe dieser Benutzungsordnung (Abschnitt VI).

Weitere Angaben dürfen aus datenschutzrechtlichen Gründen nur erhoben werden, soweit dies zur Entscheidung über den Zulassungsantrag erforderlich ist.

(7) Die Nutzungserlaubnis ist auf das beantragte Vorhaben beschränkt und kann zeitlich befristet werden.

(8) Zur Gewährleistung eines ordnungsgemäßen und störungsfreien Betriebs kann die Nutzungserlaubnis mit einer Begrenzung zur Rechen- und Onlinezeit sowie mit anderen nutzungsbezogenen Bedingungen und Auflagen verbunden werden.

(9) Wenn die Kapazitäten der Datenverarbeitungsressourcen nicht ausreichen, um allen Nutzungsberechtigten gerecht zu werden, können die Betriebsmittel für die einzelnen Nutzer_innen entsprechend der Reihenfolge in Abschnitt II(2) kontingentiert werden, da die Zulassung nur im Rahmen der verfügbaren Kapazitäten erfolgen kann.

(10) Die Nutzungserlaubnis kann ganz oder teilweise versagt, widerrufen oder nachträglich beschränkt werden, insbesondere wenn

a) kein ordnungsgemäßer Antrag gemäß Abschnitt II(6) vorliegt oder die Angaben im Antrag nicht oder nicht mehr zutreffen

b) die Voraussetzungen für eine ordnungsgemäße Nutzung der IVI nicht oder nicht mehr gegeben sind

[2] männlich, weiblich, divers

c) die nutzungsberechtigte Person nach Abschnitt V von der Nutzung ausgeschlossen worden ist

d) das geplante Vorhaben der Nutzer_in nicht mit den Aufgaben des Systembetreibers vereinbar ist

e) die vorhandenen IT-Ressourcen für die beantragte Nutzung ungeeignet oder für besondere Zwecke reserviert sind

f) die Kapazität der Ressourcen, deren Nutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die geplante Nutzung nicht ausreicht

g) die zu benutzenden IT-Komponenten an ein Netz angeschlossen sind, das besonderen Datenschutzerfordernissen genügen muss und kein sachlicher Grund für die geplante Nutzung ersichtlich ist

h) zu erwarten ist, dass durch die beantragte Nutzung andere berechtigte Vorhaben in unangemessener Weise beeinträchtigt werden.

III. Allgemeine Rechte und Pflichten der Nutzer_innen

(1) Nutzer_innen haben das Recht, die vom Systembetreiber zur Verfügung gestellte IVI im zeitlichen und inhaltlichen Umfang, der durch diese Benutzungsordnung in ihrer jeweiligen Fassung gewährt wird, zu nutzen.

(2) Nutzer_innen sind verpflichtet:

a) Die Vorgaben dieser Benutzungsordnung zu beachten, die Grenzen der Nutzungserlaubnis einzuhalten und insbesondere die Nutzungszwecke nach Abschnitt II(1) zu beachten,

b) alles zu unterlassen, was den ordnungsgemäßen Betrieb der Datenverarbeitungseinrichtungen des Betreibers stört und die vorhandenen Datenverarbeitungsanlagen, Informations- und Kommunikationssysteme und sonstigen Einrichtungen und Ressourcen (z.B. Arbeitsplätze, CPU-Kapazität, Plattenspeicherplatz, Leitungskapazitäten, Peripheriegeräte und Verbrauchsmaterial) sorgfältig und schonend zu behandeln,

c) ausschließlich mit den Nutzungskennungen zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde,

d) Benutzerpasswörter nicht an Dritte weiterzugeben und dafür Sorge zu tragen, dass keine anderen Personen Kenntnis von den Nutzerpasswörtern erlangen, sowie Vorkehrungen zu treffen, damit unberechtigten Personen der Zugang zu den Datenverarbeitungsressourcen des Betreibers verwehrt wird; dazu gehört auch der Schutz des Zugangs durch ein geheim zu haltendes und geeignetes, d.h. nicht einfach zu erratendes Passwort, das möglichst regelmäßig geändert werden sollte,

e) fremde Nutzerkennungen und Passwörter weder zu ermitteln noch zu nutzen,

f) keinen unberechtigten Zugriff auf Informationen anderer Nutzer_innen zu nehmen,

g) bekannt gewordene Informationen anderer Nutzer_innen nicht ohne deren explizite Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern,

h) bei Bekanntwerden von o.g. Informationen unverzüglich die HTW-Beauftragten für Informationssicherheit und/oder Datenschutz zu informieren,

i) bei der Nutzung von Software, Dokumentationen und anderen Daten die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten von Betreibern zur Verfügung gestellt werden, zu beachten,

j) die nationalen und internationalen Urheber-, Marken-, Patent-, Namens- und Kennzeichenrechte sowie sonstige gewerbliche Schutzrechte und Persönlichkeitsrechte Dritter bei der Nutzung der Dienste zu wahren. Das Abrufen, Anbieten, Hochladen oder Verbreiten von rechtswidrigen Inhalten, insbesondere solchen, die gegen strafrechtliche, datenschutzrechtliche, persönlichkeitsrechtliche, lizenzrechtliche oder urheberrechtliche Bestimmungen verstoßen, ist unzulässig,

k) vom Betreiber bereitgestellte Software sowie die Software, die zum Betrieb der Dienste dient, Dokumentationen und Daten weder zu kopieren noch an Dritte weiterzugeben, sofern dies nicht ausdrücklich erlaubt ist, noch zu anderen als den erlaubten Zwecken zu nutzen,

l) in den Räumen des Systembetreibers den Weisungen des Personals Folge zu leisten und die Hausordnung des Systembetreibers zu beachten,

m) Störungen, Beschädigungen und Fehler an Datenverarbeitungseinrichtungen und Datenträgern des Systembetreibers nicht selbst zu beheben, sondern unverzüglich dem Betreiber zu melden,

n) ohne ausdrückliche Einwilligung des Systembetreibers keine Eingriffe in die Hardwareinstallation des Betreibers vorzunehmen und die Konfiguration der Betriebssysteme, der Systemdateien, der systemrelevanten Nutzerdateien und des Netzwerks nicht zu verändern,

o) dem Betreiber auf Verlangen in begründeten Einzelfällen, insbesondere bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu erteilen sowie Einsicht in die Programme zu gewähren,

p) ein Vorhaben zur Verarbeitung personenbezogener Daten vor Beginn mit dem Systembetreiber und dem bzw. der Datenschutzbeauftragten der HTW Berlin abzustimmen und – unbeschadet der eigenen datenschutzrechtlichen Verpflichtungen der Nutzer_innen – die vom Betreiber vorgeschlagenen Datenschutz- und Datensicherheitsvorkehrungen zu berücksichtigen. Verpflichtungen und Bestimmungen aus geltenden Gesetzen, Verordnungen und Verwaltungsvorschriften, die im Hochschulbetrieb Datenschutz-Relevanz haben, sind stets zu beachten. So besteht u.a. eine gesetzliche Verpflichtung zur schriftlichen Beschreibung der Verarbeitungstätigkeit, die unter anderem benennen muss, welche Datenkategorien zu welchem Zweck aufgenommen und verarbeitet werden sollen. Die gespeicherten Daten dürfen nur für diesen bestimmungsgemäßen Gebrauch verwendet werden. Diese Beschreibungen der Verarbeitungstätigkeiten werden dem bzw. der Datenschutzbeauftragten zur Abnahme

vorgelegt und durch die Verfahrensverantwortlichen verwaltet. Bei wesentlichen Änderungen der Verfahren (z.B. hinsichtlich der Zwecke und gesetzlichen Grundlagen, Speicher-/Aufbewahrungs- sowie Löschfristen) hat eine entsprechende Änderungsmeldung und damit eine Anpassung der Beschreibung inkl. erneuter Vorlage bei dem bzw. der Datenschutzbeauftragten zu erfolgen.

(3) Auf die folgenden Straftatbestände wird besonders hingewiesen:

a) Ausspähen von Daten (§ 202a StGB), Abfangen von Daten (§ 202b StGB), Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB), Datenhehlerei (§ 202d StGB)

b) Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB),

c) Computerbetrug (§ 263a StGB),

d) Verbreitung pornographischer Darstellungen (§§ 184 ff. StGB), insbesondere Verbreitung, Erwerb und Besitz kinderpornographischer Schriften (§ 184 b StGB) und die Verbreitung pornographischer Darbietungen durch Rundfunk und Telemedien (§ 184d StGB),

e) Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB),

f) Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB),

g) Strafbare Urheberrechtsverletzungen, z.B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG).

(4) Ein Anspruch auf ununterbrochenen und störungsfreien Zugang zu den Einrichtungen, Datenverarbeitungsanlagen und Informations- und Kommunikationssystemen der Systembetreiber sowie auf unveränderte Fortführung des Leistungsangebots besteht nicht.

IV. Besondere Rechte und Pflichten der Nutzer_innen

(1) **Aktivierung des HTW-Accounts und Nutzung des zentralen HTW-E-Mail-Dienstes**

Alle Nutzer_innen sind verpflichtet, ihren HTW-Account zu aktivieren und das damit verbundene E-Mail-Postfach für die studienrelevante bzw. dienstliche Kommunikation zu nutzen. An diesen Account gerichtete E-Mails sind regelmäßig zu lesen. Die dienstliche bzw. studienrelevante Kommunikation innerhalb der HTW Berlin erfolgt soweit möglich per E-Mail. Dies gilt z.B. auch für offizielle Mitteilungen (z.B. der Hochschulleitung), gebührenpflichtige Mahnungen der Bibliothek sowie für Mitteilungen aus den Verwaltungs-, Buchhaltungs-, Dokumenten- und Lernmanagementsystemen. Diese Mitteilungen werden - sofern gesetzlich zulässig - ausschließlich per E-Mail übermittelt und gelten mit Bereitstellung im HTW-E-Mail-Account als zugestellt und bekannt. Nutzer_innen sollen im Falle einer (geplanten) Abwesenheit eine Abwesenheitsnotiz einrichten.

Mit der Nutzung Ihres HTW-Mail-Accounts zur externen Kommunikation agieren Nutzer_innen als Angehörige der HTW Berlin und sind daher angehalten, die Nutzung im Sinne des Leitbildes der Hochschule verantwortungsvoll zu gestalten. Insbesondere E-Mails mit rassistischen, sexistischen, diskriminierenden sowie beleidigenden Inhalten sind nicht gestattet.

(2) **Verbot automatischer E-Mail-Weiterleitungen an externe Mailadressen für Beschäftigte**

Automatische E-Mail-Weiterleitungen ohne jegliche menschliche Kontrolle der Mailinhalte an externe Mail-Adressen, insbesondere automatische Weiterleitungen von E-Mails im Rahmen des Beschäftigungsverhältnisses sind nicht gestattet, da hier erhebliche Risiken im Bereich Datenschutzrecht, strafrechtlicher Geheimnisschutz, Arbeitsrecht und Informationsfreiheitsrecht bestehen. Personen, die in einem Beschäftigungsverhältnis mit der HTW Berlin stehen, sind datenschutzrechtlich Teil der „öffentlichen Stelle“ Hochschule. Ihre dienstlichen Tätigkeiten werden direkt der HTW Berlin zugerechnet und nach dem für die HTW Berlin geltenden Datenschutzrecht beurteilt.

Durch automatische Weiterleitungen werden ausnahmslos alle E-Mails an einen externen E-Mail-Provider weitergereicht (der u.U. außerhalb der EU sitzt). Das führt dazu, dass kritische Informationen und Daten die Einflusssphäre der HTW Berlin verlassen und auf Servern landen, die der Kontrolle der Hochschule nicht mehr unterliegen. Dabei gelangen die Daten aus allen dienstlichen E-Mails in den Machtbereich des externen Mail-Providers und können theoretisch von diesem eingesehen und weiterverwendet werden. Für diese potentielle Datenübermittlung an Dritte bzw. datenschutzrechtlich relevante Nutzung von Daten bedarf es entweder einer Einwilligung der Betroffenen oder einer gesetzlichen Vorschrift, die diese Nutzung erlaubt. Dies kann bei einer automatischen Weiterleitung nicht pauschal sichergestellt werden. Darüber hinaus hat die HTW Berlin keine Kontroll- und Einflussmöglichkeiten und ist nicht in der Lage, ihren gesetzlichen Auskunfts- und Löschverpflichtungen nachzukommen, wenn dienstliche Mails auf externen Servern weiterverarbeitet werden. Darüber hinaus kann die Nutzung einer automatischen E-Mail-Weiterleitung auch zu einer strafrechtlich relevanten Offenbarung von Privat- oder Dienstgeheimnissen führen. Im Einzelfall kann die Nutzung einer automatischen E-Mail-Weiterleitung auch eine arbeitsrechtlich relevante Pflichtverletzung der Beschäftigten darstellen, da die E-Mails den Einflussbereich der HTW Berlin verlassen und die Verfügbarkeit wichtiger Verwaltungsunterlagen nicht sichergestellt werden kann. Dadurch werden dienstliche Vorgänge der Steuerungsmöglichkeit durch den Dienstherrn entzogen. Ferner ist nicht auszuschließen, dass vom Informationsfreiheitgesetz erfasste Informationen an einen externen Mail-Provider weitergereicht werden, wenn Beschäftigte automatische Weiterleitungen nutzen, was dazu führt, dass der gesetzliche Zugangsanspruch zu diesen Informationen nicht mehr gewährleistet werden kann.

(3) **Automatische E-Mail-Weiterleitungen von Studierenden**

Studierende der HTW Berlin sind anders als Beschäftigte datenschutzrechtlich nicht Teil der öffentlichen Stelle Hochschule, sondern gelten einzeln als „nicht öffentliche Stelle“. Richten sich Studierende eine automatische E-Mail-Weiterleitung von ihrer HTW-Mailadresse auf eine private Mailadresse ein und nutzen diese für Zwecke des Studiums und andere ausschließlich private Angelegenheiten, ist das Datenschutzrecht für sie nicht anwendbar (Datenverarbeitung zu ausschließlich persönlichen Zwecken). Dieser Rahmen wird jedoch überschritten, sobald Studierende dienstlich für die HTW Berlin tätig werden (z.B. als studentische Hilfskräfte oder wissenschaftliche Mitarbeiter_innen) oder bestimmte Selbstverwaltungsaufgaben der HTW Berlin wahrnehmen, indem sie beispielsweise in Gremien, Ausschüssen, Fachschaften oder ähnlichem tätig werden und

dabei personenbezogene Daten verarbeiten. In diesen Einzelfällen kommen das Datenschutzrecht, die strafrechtlichen Konsequenzen laut StGB sowie die Arbeits- und informationsfreiheitsrechtlichen Aspekte auch für Studierende zur Anwendung.

Studierende, die in Hochschulgremien oder dienstlich für die HTW Berlin tätig sind, werden hiermit explizit darauf hingewiesen, dass die Nutzung einer automatischen E-Mail-Weiterleitung datenschutzrechtlich nicht risikolos und potentiell rechtswidrig ist.

Sofern Studierende eine automatische Weiterleitung von ihrer HTW-Mailadresse an eine externe Mailadresse aktivieren, verbleibt von jeder weitergeleiteten E-Mail als Zustellnachweis eine Kopie im lokalen HTW-Postfach der Nutzer_in.

(4) **Nutzung der HTW-Netzlaufwerke**

Das Hochschulrechenzentrum stellt jeder/jedem Inhaber_in eines HTW-Accounts ein persönliches Home-Laufwerk zur Verfügung. Zusätzlich stehen zur Teamarbeit Gruppen-Laufwerke für zentrale Organisationseinheiten zur Verfügung. Netzlaufwerke bieten durch eine Reihe von Sicherheitsmaßnahmen (z.B. Spiegelung und regelmäßiges Backup der Daten) einen hohen Schutz gegen Ausfall, Datenverlust und unbefugten Zugriff.

Für die Speicherung und Verarbeitung von dienstlichen und personenbezogenen Daten sind vorrangig die Netzlaufwerke der HTW Berlin zu nutzen. Dienstliche Daten und Daten, die einen sehr hohen Schutzbedarf haben, dürfen ausschließlich dort abgelegt werden.

(5) **Nutzung des Virtual-Private-Network-Dienstes (VPN-Dienst)**

Die Nutzer_innen müssen außerhalb der HTW-Netze verschlüsselte Kommunikationswege benutzen. Dazu stellt das HRZ den VPN-Dienst zur Verfügung. Dies gilt insbesondere auch bei der Nutzung von Smart-Devices (z.B. Handy, Smartphone, Tablet, etc.) sowie für die Nutzung von Remote-Desktop-Protocol-Diensten (Remote Desktop Services/Fernwartungszugriffe).

(6) **Nutzung des WLAN (Wireless Local Area Network)**

a) **Allgemeines:** Unter einem WLAN versteht man ein Funknetzwerk (drahtlos), das auf Basis von Funkverbindungen Computer und andere Endsysteme über sog. Accesspoints (AP) miteinander verbindet. Die WLAN-Nutzung ist an einen gültigen Nutzer-Account der HTW Berlin bzw. anderer Einrichtungen im Rahmen der DFN-Roaming und EDU-Roaming Infrastruktur gebunden.

b) **HTW-WLAN**: Betreiber des WLANs ist das Hochschulrechenzentrum. Teilaspekte des Betriebes für lokale Bereiche des WLANs können bei entsprechenden personellen und technischen Voraussetzungen an IT-Personal anderer Einrichtungen delegiert werden. Die Gesamtverantwortung für den Betrieb und die Gewährleistung der Sicherheit des WLANs verbleibt beim Hochschulrechenzentrum. Der Aufbau und Betrieb eigener WLANs ist nur in begründeten Einzelfällen (Forschung und Lehre) und ausschließlich nach Rücksprache mit dem Hochschulrechenzentrum statthaft. Zur Gewährleistung der Betriebssicherheit und Stabilität sind dabei die geltenden technischen und organisatorischen Festlegungen des Hochschulrechenzentrums einzuhalten. Dies beinhaltet beispielsweise zu nutzende Funkkanäle und Obergrenzen für Sendeleistungen.

c) **Sicherheit:** Die Netznutzung ist nur für Zwecke im Rahmen von Forschung, Lehre und Verwaltung zulässig. Da das WLAN-Funkmedium geteilt genutzt wird und da die Schutzmechanismen (z.B. WPA2/WPA3) durch verbesserte Angriffsverfahren potentiell kompromittiert werden können, kann ein Missbrauch des WLANs nicht absolut ausgeschlossen werden. Sofern ein über die Betreibermaßnahmen hinausgehender Schutz von Daten erforderlich ist, muss dieser durch geeignete Verfahren (z.B. VPN), die vom WLAN-Client bis zur Gegenstelle im LAN bzw. im Internet wirken, selbst realisiert werden.

(7) **Nutzung von Cloud-Speicherdiensten**

a) **Allgemeines**: Der Begriff Cloud-Speicher beschreibt die Möglichkeit, Datenspeicher unabhängig von Zeit und Ort aus dem Internet mit den meisten gängigen IT-Geräten zu verarbeiten und über verschiedene (mobile) Geräte hinweg zu synchronisieren sowie selbstverwaltet mit Dritten zu teilen. Insbesondere die Nutzung von kommerziellen Cloud-Speicher-Diensten ist mit einer Reihe von Risiken verbunden. Der unklare Speicherort, die unbekannte Anzahl der zugreifenden Personen, Synchronisationsfehler sowie die ungeregelten Zuständigkeiten in Problemfällen gefährden die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Die Speicherung von Daten in einer Cloud ersetzt in keinem Fall ein Backup-Verfahren. Nutzer_innen, die Daten initial in eine Cloud einstellen (hochladen), sind damit weiterhin für eine eigene und korrekte Datensicherung unabhängig von der Cloud verantwortlich.

b) **HTW-Cloud**: Die HTW Berlin bietet allen Nutzer_innen einen vom Hochschulrechenzentrum betriebenen Cloud-Speicher-Dienst an. Er basiert auf einer quelloffenen Software, die vergleichbare Funktionalitäten anbietet wie andere, kommerzielle Cloud-Speicher-Anbieter (z.B. das Synchronisieren und Teilen von Daten). Sofern also Funktionalitäten benötigt werden, die über die Möglichkeiten der unter Abschnitt IV(4) beschriebenen Netzlaufwerke hinausgehen, besteht die Option, die HTW-Cloud zu nutzen. Ob die Daten in der Cloud gespeichert und verarbeitet werden dürfen, richtet sich jedoch ausschließlich nach ihrem Schutzbedarf.
Darüber hinaus ist eine Speicherung und Verarbeitung von dienstlichen und personenbezogenen Daten in Cloud-Speicher-Diensten Dritter wie z.B. Dropbox, Microsoft OneDrive, Google Drive oder Apple iCloud usw. grundsätzlich nicht gestattet.

c) **Schutzbedarf der Daten bestimmt den Umfang der Cloud-Nutzung**: Für die Entscheidung, ob und wie Daten in der HTW-Cloud verarbeitet und gespeichert werden dürfen, geben die unten aufgeführten beispielhaften Kategorien Anhaltspunkte. Sollte Unklarheit bezüglich der Schutzwürdigkeit der Daten bestehen, so ist ihr Schutzbedarf mittels einer Schutzbedarfsanalyse zu bestimmen bzw. die HTW-Beauftragten für Informationssicherheits- und/oder Datenschutz einzubeziehen. Aus dem Schutzbedarf der Daten folgt, ob ihre Speicherung und Verarbeitung in der Cloud zulässig ist. Verantwortlich für die Bestimmung des Schutzbedarfs ist stets die Daten verarbeitende Stelle selbst.

Schutzbedarf	**Nutzung der HTW-Cloud**	**Nutzung sonstiger Cloud-Dienste**
Normaler Schutzbedarf	Zulässig	Nicht zulässig[3]
Hoher Schutzbedarf	Nur verschlüsselt zulässig	Nicht zulässig
Sehr hoher Schutzbedarf	Nicht zulässig	Nicht zulässig

Schutz-bedarf	**Beispiele**
Normal	• personenbezogene Daten, deren Verarbeitung keine besondere Beeinträchtigung des informationellen Selbstbestimmungsrechts erwarten lassen (Anschrift, Geburtsjahr, öffentliche Register, Telefonverzeichnisse) • Informationen aus dem Hochschulbetrieb, sog. institutionelle oder organisationale Daten, deren Verlust, Offenlegung oder Manipulation einen begrenzten Schaden verursachen würden (z.B. konzeptionelle Dokumente)
Hoch	• personenbezogene Daten, deren Verlust, Offenlegung, Manipulation der bzw. dem Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen (Daten über Kontenstände, Zeugnisse, rassische oder ethnische Herkunft, religiöse oder weltanschauliche Überzeugungen, Studierendendaten) • institutionelle Daten, deren Verlust, Offenlegung, Manipulation einen erheblichen Schaden für die HTW Berlin verursachen würden (wissenschaftliche Daten, Forschungsergebnisse, die noch nicht publiziert wurden, wirtschaftliche Daten/Haushaltsdaten)
Sehr hoch	• personenbezogene Daten deren Missbrauch der bzw. den Betroffenen in ihrer bzw. seiner gesellschaftlichen Stellung oder in ihrer bzw. seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt (besonders sensible Daten aus der Personalakte wie Krankendaten, Sozialdaten, Steuerdaten, strafbare Handlungen) • institutionelle Daten, deren Missbrauch einen existentiellen und nicht tolerierbaren Schaden für die HTW Berlin bedeuten

Fragen zur Verschlüsselung von Daten sind an die zuständigen Ansprechpartner unter http://htw-berlin.de/it-kontakt zu richten.

d) **Sparsamer Umgang:** Bei der Nutzung von Cloud Speicher-Diensten sind die in Frage kommenden Datenmengen auf das notwendige Mindestmaß zu begrenzen. Der primäre Speicherplatz für Daten bleiben weiterhin die Netzlaufwerke der HTW Berlin.

[3] Soweit personenbezogene Daten enthalten sind.

e) **Erst prüfen, dann übertragen:** Bei der Übertragung ganzer Verzeichnisbäume in Cloud-Speicherdienste ist zu prüfen, ob nicht in den Unterverzeichnissen besonders schützenswerte Daten abgelegt wurden, die nicht in die Cloud gehören. Darüber hinaus ist durch eine Prüfung der vergebenen Berechtigungen sicherzustellen, dass die Daten ausschließlich einem berechtigten Personenkreis zugänglich gemacht werden.

V. Ausschluss von der Nutzung

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

a) sie schuldhaft gegen diese Benutzungsordnung, insbesondere gegen die in Abschnitt III und IV aufgeführten Pflichten, verstoßen (missbräuchliches Verhalten) oder

b) sie die Datenverarbeitungsressourcen der Betreiber für strafbare Handlungen missbrauchen oder

c) der HTW Berlin durch sonstiges rechtswidriges Nutzerverhalten Nachteile entstehen. Hierdurch werden alle sonstigen rechtswidrigen Verhaltensweisen auch außerhalb des Strafrechts erfasst, z.B. Urheberrechts-oder Markenrechtsverletzungen. Ein Nutzungsausschluss wegen eines entsprechenden (rein zivilrechtswidrigen) Verhaltens kommt jedoch nur in Betracht, wenn die HTW Berlin hiervon selbst betroffen ist, z.B. in Form einer Abmahnung, Unterlassungserklärung oder Schadenersatzforderung.

(2) Maßnahmen nach Abschnitt V(1) dürfen erst nach vorheriger erfolgloser schriftlicher, elektronischer oder in Textform verfasster Abmahnung erfolgen. Dies gilt nicht für Gefahr im Verzug. Hierüber sind die Betroffenen unverzüglich zu informieren. Dem bzw. der Betroffenen ist Gelegenheit zur Stellungnahme zu geben. In jedem Fall ist die Gelegenheit zur Sicherung seiner bzw. ihrer Daten einzuräumen.

(3) Vorübergehende Nutzungseinschränkungen, über die der Betreiber entscheidet, sind aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet ist.

(4) Eine dauerhafte Nutzungseinschränkung oder der vollständige Ausschluss von Nutzer_innen von der weiteren Nutzung kommt nur bei schwerwiegenden oder wiederholten Verstößen i.S.v. Abschnitt V(1) in Betracht, wenn auch künftig ein ordnungsgemäßes Verhalten nicht mehr zu erwarten ist. Die Entscheidung über einen dauerhaften Ausschluss trifft der/die Kanzler_in auf Antrag des Betreibers und nach Anhörung durch eine dafür eingerichtete Kommission durch Bescheid; bei Tarifbeschäftigten wird der Personalrat beteiligt. Mögliche Ansprüche des Betreibers aus dem Nutzungsverhältnis bleiben unberührt.

VI. Rechte und Pflichten des Systembetreibers

(1) Die Systembetreiber gemäß Abschnitt II(3) geben die jeweiligen Ansprechpartner_innen für die Betreuung ihrer Nutzer_innen bekannt z.B. durch Benennung auf den Intra- oder Internetseiten des Systembetreibers.

(2) Der Systembetreiber trägt in angemessener Weise zum Verhindern bzw. Aufdecken von Missbrauch bei.

(3) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutz der Nutzerdaten erforderlich ist, kann der Betreiber die Nutzung seiner Ressourcen vorübergehend einschränken oder einzelne Nutzerkennungen vorübergehend sperren. Sofern möglich, sind die betroffenen Nutzer_innen hierüber im Voraus zu unterrichten.

(4) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein_e Nutzer_in auf den Servern des Betreibers rechtswidrige Inhalte zur Nutzung bereithält, kann der Betreiber die weitere Nutzung (z.B. durch temporäre Sperrung) verhindern, bis die Rechtslage durch die zuständige Behörde hinreichend geklärt ist.

(5) Der Systembetreiber ist nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme durch die einzelnen Nutzer_innen zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist:

a) zur Gewährleistung eines ordnungsgemäßen Systembetriebs,

b) zur Ressourcenplanung und Systemadministration,

c) zum Schutz der personenbezogenen Daten anderer Nutzer_innen,

d) zu Abrechnungszwecken,

e) für das Erkennen und Beseitigungen von Störungen sowie

f) zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

(6) Unter den Voraussetzungen von Abschnitt VI(5) ist der Systembetreiber auch berechtigt, unter Beachtung des Datengeheimnisses Einsicht in die Benutzerdateien zu nehmen, soweit dies erforderlich ist zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Missbräuchen, sofern hierfür tatsächliche Anhaltspunkte sowie eine Anweisung der Kanzler_in oder der Rechtsstelle der HTW Berlin vorliegen. Eine Einsichtnahme in die Nachrichten und E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung aktueller Störungen im Nachrichtendienst unerlässlich ist. In jedem Fall ist die Einsichtnahme zu dokumentieren und sowohl der bzw. die betroffene Nutzer_in als auch der bzw. die Datenschutzbeauftragte unverzüglich zu benachrichtigen.

(7) Unter den Voraussetzungen von Abschnitt VI(5) können auch die Verkehrs- und Nutzungsdaten im Nachrichtenverkehr (insb. Mail-Nutzung) dokumentiert werden. Es dürfen jedoch nur die näheren Umstände der Telekommunikation – nicht aber die nicht-öffentlichen Kommunikationsinhalte – erhoben, verarbeitet und genutzt werden. Die Verkehrs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Telemediendiensten, die das Hochschulrechenzentrum zur Nutzung bereithält oder zu denen das Hochschulrechenzentrum den Zugang zur Nutzung vermittelt, sind frühestmöglich, spätestens unmittelbar am Ende der jeweiligen Nutzung, zu löschen, soweit es sich nicht um Abrechnungsdaten handelt.

(8) Nach Maßgabe der gesetzlichen Bestimmungen ist der Systembetreiber zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet.

VII. Haftung der Nutzer_innen

(1) Der/die Nutzer_in haftet für alle Nachteile, insbesondere Schäden, die der Hochschule durch schuldhafte missbräuchliche oder rechtswidrige Verwendung der Datenverarbeitungsressourcen und der Nutzungsberechtigung oder dadurch entstehen, dass der/die Nutzer_in schuldhaft seinen/ihren Pflichten aus dieser Benutzungsordnung nicht nachkommt.

(2) Der/die Nutzer_in haftet auch für Schäden, die im Rahmen der ihm/ihr zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er/sie diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe seiner/ihrer Nutzerkennungen an Dritte. In diesem Fall kann die HTW Berlin von der/dem Nutzer_in nach Maßgabe der Entgeltordnung ein Nutzungsentgelt für die Drittnutzung verlangen. Weitergehende Schäden bleiben vorbehalten.

(3) Der/die Nutzer_in stellt die HTW Berlin von allen Ansprüchen frei, wenn Dritte die HTW Berlin wegen eines missbräuchlichen oder rechtswidrigen schuldhaften Verhaltens der Nutzer_innen auf Schadenersatz in Anspruch nehmen. Die HTW Berlin wird den Nutzer_innen den Streit verkünden, sofern Dritte aufgrund dieser Ansprüche gegen den Betreiber gerichtlich vorgehen.

VIII. Haftung der HTW Berlin

(1) Die HTW Berlin kann weder eine Gewährleistung noch eine Garantie dafür übernehmen, dass die Systeme fehlerfrei und jederzeit ohne Unterbrechung laufen und dass eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter ausgeschlossen werden können.

(2) Die HTW Berlin übernimmt keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der Informationen und Programme, zu denen sie lediglich den Zugang zur Nutzung vermittelt.

(3) Die HTW Berlin haftet ausschließlich im Rahmen gesetzlicher Vorschriften; weitergehende Haftungsansprüche bestehen nicht.

IX. Sonstige Regelungen

Für die Nutzung spezieller IT-Dienste/-Ressourcen der IVI können

(1) in gesonderten Ordnungen Gebühren festgelegt werden.

(2) bei Bedarf ergänzende Nutzungsregelungen getroffen werden.

X. Übersicht der Zuständigkeiten

Ansprechfall	**Person/Bereich (vgl. VI(1))**
Fragen zur Nutzung von Netzlaufwerken und Cloud-Speicherdiensten in den Fachbereichen und Laboren der HTW Berlin	Laboringenieure und dezentrale Informationssicherheitsbeauftragte
Fragen zur Nutzung von Netzlaufwerken und Cloud-Speicherdiensten in der zentralen Verwaltung der HTW Berlin	Hochschulrechenzentrum
Fragen zum Schutz personenbezogener Daten	Datenschutzbeauftragte_r der HTW Berlin
Fragen zum Schutz betrieblicher Daten der HTW Berlin	Zentrale und dezentrale Informationssicherheitsbeauftragte_r der Fachbereiche

XI. In-Kraft-Treten

Diese Benutzungsordnung tritt am Tage nach ihrer Veröffentlichung im Amtlichen Mitteilungsblatt der HTW Berlin in Kraft.