Benutzungsordnung Für IT-Systeme der Technischen Universität Darmstadt

TECHNISCHE UNIVERSITÄT DARMSTADT

Aufgrund der Genehmigung des Präsidiums der Technischen Universität Darmstadt vom 01.10.2019, wird die Benutzungsordnung für IT-Systeme der Technischen Universität Darmstadt, nachstehend bekannt gemacht.

Darmstadt, den 01.10.2019

Die Präsidentin der TU Darmstadt
Prof. Dr. Tanja Brühl

Benutzungsordnung für IT-Systeme der TU Darmstadt

Inhalt

Satzungsbeilage 2019-V, Seite 13-33

Präambel

Die Universität, ihre Fachbereiche und Einrichtungen betreiben eine Informationstechnologie (IT)-Infrastruktur, bestehend aus physischen und virtuellen Informationsverarbeitungssystemen und einem Multiservice-Kommunikationsnetz zur Übertragung von Daten, Bildern und Sprache. Diese IT-Infrastruktur ist an das weltweite Internet angeschlossen.

Die vorliegende Benutzungsordnung regelt die Bedingungen, unter denen das Leistungsangebot dieser Infrastruktur genutzt werden kann; sie

- stellt Grundregeln für einen ordnungsgemäßen Betrieb der IT-Infrastruktur auf;
- verpflichtet die Betreiber_innen zum korrekten Systembetrieb und zur Einhaltung der IT-Sicherheitsstandards gemäß den Informationssicherheitsleitlinien des Landes;
- weist auf die zu wahrenden Rechte Dritter hin (z.B. bzgl. der Softwarelizenzen, der Auflagen von Netzbetreiber_innen oder der Datenschutzaspekte);
- verpflichtet Nutzer_innen zu korrektem Verhalten und zum ökonomischen Gebrauch der angebotenen Ressourcen;
- orientiert sich an den gesetzlich festgelegten Aufgaben der Universität sowie an ihrem Mandat zur Wahrung der akademischen Freiheit;
- klärt über eventuelle Maßnahmen bei Verstößen gegen diese Benutzungsordnung auf.
- verpflichtet die jeweiligen Führungskräfte, in ihrem Verantwortungsbereich für die nötige Sachkunde bei Nutzern / Nutzerinnen und Betreibern / Betreiberinnen zu sorgen.

§ 1 Geltungsbereich

- Diese Benutzungsordnung gilt für die von der Technischen Universität (TU) Darmstadt betriebene IT-Infrastruktur, bestehend aus Informationsverarbeitungssystemen, Kommunikationssystemen und weiteren Hilfseinrichtungen sowie die Beauftragung von Subunternehmen im Bereich IT-Infrastruktur.
- Zur Aufrechterhaltung des ordnungsgemäßen Betriebes der IT-Infrastrukturen und Services kann die Leitung der jeweiligen Organisationseinheiten weitere spezifische Regelungen und Richtlinien für die einzelnen Services als Nutzungsbedingungen festlegen. Diese sind zu dokumentieren und den betroffenen Nutzer_innen auf adäquate Weise zur Verfügung zu stellen.
- Diese Benutzungsordnung ist für alle Nutzer_innen und Betreiber_innen von IT-Infrastruktur der TU Darmstadt bindend.

§ 2 Kreis der Nutzerinnen und Nutzer und Aufgaben

1. Die in § 1 genannten IT-Ressourcen stehen den Mitgliedern der TU Darmstadt zur Erfüllung ihrer Aufgaben aus Forschung, Lehre, Studium, Transfer, Verwaltung, Aus- und Weiterbildung und Öffentlichkeitsarbeit im Rahmen der TU Darmstadt zur Verfügung.

2. Anderen Personen und Institutionen kann die Nutzung gestattet werden, sofern diese sich zur Einhaltung der Benutzungsordnung, der Datenschutzbestimmungen und der geltenden Regeln verpflichten.

§ 3 Nutzungsberechtigungen

1. Zur Nutzung der IT-Ressourcen nach § 1 bedarf es in der Regel einer formalen Nutzungsberechtigung – z.B. Nutzungskennung, Netzanschluss, Netzzugang – des jeweils zuständigen Systembetreibers[1]. Passwörter haben mindestens die Gestaltungs-Richtlinien der Passwort-Richtlinie des Hochschulrechenzentrums (HRZ) zu berücksichtigen.
2. Alle am Netz der TU Darmstadt betriebenen Rechner müssen beim HRZ angemeldet sein. Die Anmeldung von Rechnern kann in der Regel nur von Mitarbeitenden der TU Darmstadt über ihre jeweiligen Domainbeauftragten erfolgen. Bei Studentischen Gruppen können Mitglieder der TU Darmstadt die Anmeldung vornehmen. Vertretungen stellen die Erreichbarkeit sicher. Diese Personen informieren über Rechte und Pflichten und nehmen die benötigten Daten zwecks Weiterleitung an das HRZ auf.
3. Der Antrag auf eine formale Nutzungsberechtigung soll folgende Angaben enthalten:

    a) Systembetreiber, bei dem die Nutzungsberechtigung beantragt wird;

    b) Systeme, für welche die Nutzungsberechtigung beantragt wird;

    c) Antragsteller_in: Name, Adresse, Telefon- und/oder Telefaxnummer und falls vorhanden E-Mail-Adresse (bei Studierenden auch Matrikelnummer) sowie Zugehörigkeit zu einer Organisationseinheit der Universität;

    d) Angaben zum Zweck der Nutzung, z.B. Forschung, Ausbildung/Lehre, Verwaltung;

    e) die Erklärung, dass der/die Nutzer_in diese Benutzungsordnung anerkennt und in die Erfassung und Bearbeitung der eigenen personenbezogenen Daten zum Zwecke der Nutzungsverwaltung einwilligt, insbesondere gemäß § 8 Ziffer 6, 7, 8 dieser Benutzungsordnung. Verpflichtung zur Einhaltung der Benutzungsordnung, Datenschutzbestimmungen und geltenden Regeln.

4. Weitere Angaben darf der Systembetreiber nur verlangen, soweit sie zur Entscheidung über den Antrag oder den Systembetrieb erforderlich sind. Über den Antrag entscheidet der zuständige Systembetreiber. Er kann die Erteilung der Nutzungsberechtigung vom Nachweis bestimmter Kenntnisse über die Benutzung des Systems abhängig machen.
5. Die Erteilung der Nutzungsberechtigung darf versagt werden, wenn

    a) das Vorhaben nicht mit den Zwecken gemäß § 2 dieser Benutzungsordnung vereinbar ist;

    b) nicht gewährleistet ist, dass die beantragende Person seinen/ihren Pflichten als Nutzer_in nachkommen wird;

[1] Unter Systembetreiber wird in diesem Dokument die Einrichtung verstanden, die IT-Systeme betreibt oder betreiben lässt.

c) das System für die beabsichtigte Nutzung offensichtlich ungeeignet oder für spezielle Zwecke reserviert ist;

d) wenn begründete Zweifel aufgrund konkreter Anhaltspunkte bestehen, dass durch die beantragte Nutzung andere berechtigte Nutzungen in unangemessener Weise gestört werden;

e) die benötigten IT-Ressourcen an IT-Infrastrukturen angeschlossen sind, die besonderen Datenschutzerfordernissen zu genügen haben und kein sachlicher Grund für die geplante Nutzung ersichtlich ist;

f) Gründe des Außenwirtschaftsrechts eine Nutzung durch Bürger_innen bestimmter Staaten nicht zulassen.

6. Die Nutzungsberechtigung berechtigt nur zu Arbeiten, die im Zusammenhang mit der beantragten Nutzung stehen.

§ 4 Gesetzliche Einbindung und Leitlinien

Die IT-Infrastruktur darf nur in rechtlich korrekter Weise genutzt werden. Es wird ausdrücklich darauf hingewiesen, dass nach dem Strafgesetzbuch folgende Aktivitäten unter Strafe gestellt sind:

a) Ausspähen von Daten, insbesondere das unbefugte Verschaffen von Daten anderer, die gegen unberechtigten Zugang besonders gesichert sind (§§ 202a, 274 Abs. 1 Nr. 2 StGB);

b) die fälschliche Beeinflussung einer Datenverarbeitung (§§ 270, 269 StGB), das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten (§ 303a StGB);

c) Computersabotage (§ 303b StGB) und Computerbetrug durch unrichtige Gestaltung eines Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder durch unbefugte Einwirkung auf den Ablauf (§ 263a StGB);

d) die Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) oder rassistischem Gedankengut (§ 130 StGB);

e) das Anbieten oder Überlassen von pornographischen Schriften (§ 184 Abs. 1, Ziffer 3 StGB);

f) Abruf oder Besitz von Dokumenten mit Kinderpornographie (§ 184 Abs. 1, Ziffer 5 StGB);

g) Ehrdelikte wie Beleidigung oder Verleumdung (§ 185 ff StGB), Beschimpfungen von Bekenntnissen, Religionen oder Weltanschauungen (§ 166 StGB);

h) Urheberrechtsverletzungen, z.B. durch urheberrechtswidrige Vervielfältigung von Software oder die Eingabe geschützter Werke in eine Datenverarbeitungs-(DV)-Anlage (§§ 106 ff. UrhG);

i) die Verletzung von Privatgeheimnissen (§ 203 StGB);

j) die Verletzung von Fernmeldegeheimnissen (§ 206 StGB);

k) das Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers (§ 303b StGB);

l) die Verwendung personenbezogener Daten entgegen den Vorschriften des HDSG (§ 40 HDSG);

m) Beschäftigte, die die Sicherheit von Daten, Informationen, ITK-Systemen oder des Netzes gefährden und einen Schaden für die TU Darmstadt oder das Land Hessen oder einen Dritten verursachen, können zum Schadenersatz (§ 48 BeamtStG, § 3 Abs. 7 TV-H, § 823 BGB) herangezogen werden oder einem Rückgriffanspruch (Art. 34 GG in Verbindung mit § 839 BGB) ausgesetzt sein.

In einigen Fällen ist bereits der Versuch strafbar.

Bei der Verarbeitung personenbezogener Daten haben sich Nutzer_innen und Betreiber_innen über die einschlägigen Datenschutz-Bestimmungen zu informieren, um die Konformität mit der Europäischen Datenschutzgrundverordnung (EU-DSGVO) und dem Hessischen Datenschutz- und Informationsfreiheitsgesetz (HDSIG) einzuhalten.

Bei der Nutzung von IT-Infrastruktur haben sich Nutzer_innen und Betreiber_innen über die Informationssicherheitsleitlinien des Landes und die IT-Sicherheitsleitlinien der TU Darmstadt zu informieren und diese einzuhalten.

§ 5 Pflichten der Nutzerinnen und Nutzer

1. Die IT-Ressourcen nach § 1 dürfen in der Regel nur zu den in § 2 Ziffer 1 dieser Benutzungsordnung genannten Zwecken genutzt werden. Eine hiervon abweichende Nutzung bedarf einer gesonderten Zulassung.
2. Nutzer_innen sind verpflichtet, darauf zu achten, dass sie die vorhandenen Betriebsmittel (z.B. Arbeitsplätze, CPU-Kapazität, Speicherplatz, Leitungskapazitäten, Peripheriegeräte und Verbrauchsmaterial) verantwortungsvoll und ökonomisch sinnvoll nutzen. Der/die Nutzer_in ist verpflichtet, Beeinträchtigungen des Betriebs, soweit sie vorhersehbar sind, zu unterlassen und nach bestem Wissen alles zu vermeiden, was Schaden an der IT-Infrastruktur oder bei anderen Nutzer_innen verursachen kann. Zuwiderhandlungen können Schadensersatzansprüche begründen und zum Nutzungsausschluss führen (siehe auch § 11 dieser Benutzungsordnung).
3. Der/die Nutzer_in hat jegliche Art der missbräuchlichen Benutzung der IT-Infrastruktur zu unterlassen. Er/Sie ist insbesondere dazu verpflichtet,

   a) ausschließlich mit Nutzungsberechtigungen zu arbeiten, deren Nutzung ihm/ihr gestattet wurde; die Weitergabe einer Nutzungskennung zusammen mit dem dazugehörigen geheimen Passwort ist nicht gestattet. Auch das unberechtigte Weitergeben von elektronischen Zugangsmechanismen (Chipkarte) ist grundsätzlich nicht erlaubt;

   b) Vorkehrungen zu treffen, damit unberechtigten Dritten der Zugang zu den IT-Ressourcen verwehrt wird; dazu gehört es insbesondere, naheliegende Passwörter zu meiden (siehe hierzu die Gestaltungsrichtlinie der Passwort-Richtlinie der TU Darmstadt), die Passwörter öfter zu ändern und sich bei Verlassen des Arbeitsplatzes auszuloggen oder diesen zu sperren.

   c) fremde Nutzungskennungen und Passwörter weder zu ermitteln noch zu nutzen;

   d) keinen unberechtigten Zugriff auf Informationen anderer Nutzer_innen zu nehmen und bekanntgewordene Informationen anderer Nutzer_innen nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern;

   e) die Systembetreiber_innen zu informieren, falls er/sie Kenntnis über die missbräuchliche Nutzung der eigenen Nutzungskennung erhält.

Der/die Nutzer_in trägt die volle Verantwortung für alle Aktionen, die unter seiner/ihrer Nutzungskennung vorgenommen werden, und zwar auch dann, wenn diese Aktionen durch Dritte vorgenommen werden, denen er/sie zumindest fahrlässig den Zugang ermöglicht hat.

Der/die Nutzer_in ist darüber hinaus verpflichtet,

f) bei der Benutzung von Software (Quellen, Objekte), Dokumentationen und anderen Daten die gesetzlichen Regelungen (Urheberrechtsschutz, Copyright u.a.) einzuhalten;

g) sich über die Bedingungen, unter denen die zum Teil im Rahmen von Lizenzverträgen erworbene Software, Dokumentationen oder Daten zur Verfügung gestellt werden, zu informieren und diese Bedingungen zu beachten;

h) insbesondere Software, Dokumentationen und 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 (§ 11).

4. Der/die Nutzer_in ist verpflichtet, ein Vorhaben zur Verarbeitung personenbezogener Daten mit dem betrieblichen Datenschutzbeauftragten abzustimmen und entsprechende Datenschutzdokumentationen zu erstellen und zu führen. Dabei sind die von Datenschutzbeauftragten und ggf. von Systembetreibern vorgegebenen Datensicherungsvorkehrungen einzuhalten.
5. Der/die Nutzer_in ist verpflichtet,

   a) die vom Systembetreiber zur Verfügung gestellten Leitfäden zur Benutzung zu beachten;

   b) dem/der Systemverantwortlichen auf Verlangen in begründeten Einzelfällen – insbesondere bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung – zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu gewähren. Von dieser Regelung werden nicht die Nutzungsdaten erfasst, die durch das Telekommunikationsgeheimnis oder das Datengeheimnis geschützt sind, z.B. personenbezogene Daten Dritter;

   c) vor einer Installation von Software sich über die jeweiligen örtlichen und systemtechnischen Gegebenheiten und Regelungen zu informieren und diese zu befolgen.

6. Der/die Nutzer_in als Anbieter_in von Informationen im World-Wide Web (WWW)

   a) trägt die Verantwortung für die Inhalte seiner/ihrer WWW-Seiten;

   b) muss auf jeder WWW-Seite die Impressum-Angabe kenntlich machen, die Seitenverantwortliche und entsprechende Kontaktinformationen aufweist;

   c) muss auf jeder WWW-Seite eine Datenschutzerklärung bereitstellen.

   d) Die TU Darmstadt stellt für ihre zentralen Wegangebote entsprechende Vorlagen bereit.

7. Der/die Nutzer_in ist verpflichtet, die ihm/ihr zugewiesene Universitäts-E-Mailadresse regelmäßig zu nutzen, um Kenntnis über administrative Mitteilungen der Universität zu erlangen.
8. IT-Sicherheitsvorfälle und -notfälle jeder Art sind meldepflichtig unter security@hrz.tu-darmstadt.de oder TU-intern unter Tel. 27777. Die Mitglieder des TU Darmstadt Computer

Emergency Response Teams (TUDA-CERT) sind vom Präsidium benannt. Den Weisungen der TUDA-CERT-Mitglieder ist im IT-Sicherheitsvorfall oder -notfall Folge zu leisten.

§ 6 Haftung der Nutzerinnen und Nutzer

1. Der/die Nutzer_in haftet für alle Nachteile, die der Universität durch missbräuchliche oder rechtswidrige Verwendung der IT-Ressourcen und Nutzungsberechtigung oder dadurch entstehen, dass der/die Nutzer_in schuldhaft seinen Pflichten aus dieser Benutzungsordnung nicht nachkommt. Die Universität kann verlangen, dass missbräuchlich genutzte Ressourcen und hieraus entstehende weitere Kosten zu erstatten sind.
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 Nutzungskennung an Dritte.
3. Der/die Nutzer_in hat die Universität von allen Ansprüchen freizustellen, wenn Dritte die Universität wegen eines missbräuchlichen oder rechtswidrigen Verhaltens der Nutzer_innen auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch genommen wird.

§ 7 Ende des Nutzungsverhältnisses

1. Die Zulassung zur Nutzung endet mit Verlust des Status (§ 2) oder Wegfall der Gründe, auf deren Basis die Zulassung erfolgte.
2. Das HRZ setzt zur Verwaltung und Organisation der Zugehörigkeit von Mitgliedern und Angehörigen der TU Darmstadt und weiteren Nutzungsberechtigten im Sinne des § 2 hierzu ein automatisiert arbeitendes System zur Identitäten-Verwaltung ein.
3. Der/Die Betreiber_in kann die Daten der Nutzer_innen bis zu sechs Monate speichern und dann löschen, sofern nicht dienstliche oder rechtliche Belange oder sonstige Vereinbarungen dem entgegenstehen

   Die dienst- und arbeitsrechtlichen Verpflichtungen der Nutzer_innen nach Ende des Nutzungsverhältnisses in Bezug auf die Datenübergabe und Datensicherung und die Vorgaben aus den Leitlinien zum Umgang mit digitalen Forschungsdaten an der TU Darmstadt in der jeweils gültigen Fassung bleiben unberührt.

§ 8 Aufgaben, Rechte und Pflichten der Systembetreiber

1. Der Systembetreiber darf über die erteilten Nutzungsberechtigungen eine Datei der Nutzenden mit den persönlichen Daten der Nutzer_innen führen. Hierzu muss ein Verzeichnis der Verarbeitungstätigkeiten (VVT) erstellt und geführt werden.
2. Der Systembetreiber gibt den/die Systemverantwortlichen für die Betreuung seiner Systeme bekannt. Der Systembetreiber und die Systemverantwortlichen sind zur Vertraulichkeit verpflichtet.

3. Der Systembetreiber kann die Nutzung seiner Ressourcen vorübergehend einschränken oder einzelne Nutzungskennungen vorübergehend sperren, soweit es zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutze der Nutzungsdaten erforderlich ist. Sofern möglich, sind die betroffenen Nutzer_innen hierüber unverzüglich zu unterrichten.
4. Sofern begründete Anhaltspunkte dafür vorliegen, dass Nutzer_innen auf den Servern des Systembetreibers rechtswidrige Inhalte zur Nutzung bereithält, kann der Systembetreiber die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.
5. Der Zugang zu den IT-Ressourcen ist in der Regel zu schützen, z.B. durch ein geheim zu haltendes Passwort, Chipkarte oder ein gleichwertiges Verfahren.
6. Der Systembetreiber ist berechtigt, die Sicherheit der Passwörter und der Nutzungsdaten durch regelmäßige manuelle oder automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen, z.B. Änderungen leicht zu erratender oder veralteter Passwörter, zu veranlassen, um die DV-Ressourcen und Nutzungsdaten vor unberechtigten Zugriffen Dritter zu schützen. Bei erforderlichen Änderungen der Passwörter, der Zugriffsberechtigungen auf Nutzungsdaten und sonstigen nutzungsrelevanten Schutzmaßnahmen ist der/die Nutzer_in unverzüglich in Kenntnis zu setzen.
7. Der Systembetreiber ist berechtigt, für die nachfolgenden Zwecke die Inanspruchnahme der Datenverarbeitungssysteme durch die einzelnen Nutzer_innen zu dokumentieren und auszuwerten:

   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 Beseitigen von Störungen sowie
   f) zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

   Hierzu muss ein Verzeichnis der Verarbeitungstätigkeiten (VVT) erstellt und geführt werden.

8. Der Systembetreiber ist auch berechtigt, Einsicht in die Dateien der Nutzenden zu nehmen, soweit dies zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Verstößen gegen die Benutzungsordnung erforderlich ist und hierfür Anhaltspunkte vorliegen. Das Datengeheimnis ist dabei zu beachten.

   In jedem Fall ist die Einsichtnahme zu dokumentieren, und betroffene Nutzer_innen sind nach erfolgter Einsichtnahme unverzüglich, sobald dies nach Zweckerreichung möglich ist, zu benachrichtigen.

   Bei begründeten Hinweisen auf Straftaten handelt der Systembetreiber nach Abstimmung mit der Hochschulleitung in Absprache mit den zuständigen Behörden und wird – falls erforderlich – beweissichernde Maßnahmen einsetzen.

9. Systembetreiber, die Nutzer_innen eigenständige Homepages zur Veröffentlichung im Internet anbieten, sind berechtigt, automatisch ein Impressum auf diesen Seiten zu erzeugen, das den vollständigen Namen und die E-Mail-Adresse der Autor_innen enthält.

10. Nach Maßgabe der gesetzlichen Bestimmungen ist der Systembetreiber zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet.
11. Die korrekte Lizenzierung der in seinem/ihrem Verantwortungsbereich eingesetzten Software, liegt in der Verantwortung der Systembetreiber_innen. Dazu gehört auch das Führen hierzu benötigter Dokumentationen und die ausreichende Information von Nutzer_innen über einzuhaltende Rahmenbedingungen.
12. Systembetreiber benennen Ansprechpersonen für ihre Systeme und melden pro Bereich mindestens eine Ansprechperson an die IT-Sicherheitsbeauftragten der TU Darmstadt.
13. IT-Sicherheitsvorfälle und -notfälle jeder Art sind meldepflichtig unter security@hrz.tu-darmstadt.de oder intern Tel. 27777. Der Systembetreiber ist verantwortlich, dass diese Meldung durch die Nutzer_innen selbst oder durch den Systembetreiber erfolgt. Die Mitglieder des TU Darmstadt Computer Emergency Response Teams (TUDA-CERT) sind vom Präsidium benannt. Den Weisungen der TUDA-CERT-Mitglieder ist im IT-Sicherheitsvorfall oder -notfall Folge zu leisten. Darüber hinaus stellen Betreibende den IT-Sicherheitsbeauftragten alle angefragten Informationen zur Verfügung, die zur Meldung an übergeordnete Stellen notwendig sind.

§ 9 IT-Sicherheit

Die Leitung einer TU-Organisationseinrichtung trägt in dem Bereich, den sie zu verantworten hat, die Verantwortung für eine angemessene Informationssicherheit gemäß den Informationssicherheitsleitlinien des Landes und den IT-Sicherheitsleitlinien der TU Darmstadt.

1. In Abwägung der Werte der zu schützenden Informationen, der Risiken sowie des Aufwands an Personal und Finanzmitteln für Informationssicherheit soll für eingesetzte und geplante IT-Systeme an der TU Darmstadt ein angemessenes Informationssicherheitsniveau angestrebt und erreicht werden. Für IT-Systeme mit normalem Schutzbedarf sind Sicherheitsmaßnahmen – ausgehend von den Grundschutz-Standards und Grundschutzkatalogen des BSI sowie von den internationalen Normen DIN ISO/IEC 27001 ff. – vorzusehen und umzusetzen. Für Bereiche, in denen ein höherer Schutzbedarf festgestellt wird, müssen ergänzende Sicherheitsmaßnahmen eingeführt und dokumentiert werden.
2. Die Leitung einer TU-Organisationseinrichtung ist dafür verantwortlich, dass die Sicherheitsmaßnahmen in dem von ihr verantworteten Bereich umgesetzt werden. Im Rahmen der jeweiligen Möglichkeiten sollen die Beschäftigten Sicherheitsvorfälle von innen und außen vermeiden sowie sicherheitsrelevante Ereignisse den Zuständigen umgehend melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können. In jeder TU-Organisationseinrichtung wird eine Ansprechperson für den/die IT-Sicherheitsbeauftragte_n benannt, der/die die erforderlichen Informationen für den jeweiligen Schutzbedarf liefert und – unter Berücksichtigung von Finanzierbarkeit und Wirtschaftlichkeit – die jeweils angemessenen Sicherheitsmaßnahmen ergreift.

§ 10 Haftung des Systembetreibers/Haftungsausschluss

1. Der Systembetreiber übernimmt keine Garantie dafür, dass die Systemfunktionen den speziellen Anforderungen der Nutzer_innen entsprechen oder dass das System fehlerfrei und ohne

Unterbrechung läuft. Die TU Darmstadt garantiert nicht die Unversehrtheit (bzgl. Zerstörung, Manipulation) und Vertraulichkeit der bei ihr gespeicherten Daten.

2. Der Systembetreiber haftet nicht für Schäden gleich welcher Art, die dem/der Nutzer_in aus der Inanspruchnahme der IT-Ressourcen gemäß § 1 dieser Benutzungsordnung entstehen, soweit sich nicht aus den gesetzlichen Bestimmungen zwingend etwas anderes ergibt.

§ 11 Folgen einer missbräuchlichen oder gesetzeswidrigen Benutzung

Bei Verstößen gegen gesetzliche Vorschriften oder gegen die Bestimmungen dieser Nutzungsordnung, insbesondere des § 5 (Rechte und Pflichten der Nutzerinnen und Nutzer), kann der Systembetreiber die Nutzungsberechtigung einschränken. Es ist dabei unerheblich, ob der Verstoß einen materiellen Schaden zur Folge hatte oder nicht.

Maßnahmen zum Entzug oder zur Einschränkung der Nutzungsberechtigung, über die die Leitung der Einrichtung entscheidet, sollen erst nach vorheriger erfolgloser Abmahnung erfolgen. Dem/der Betroffenen ist Gelegenheit zur Stellungnahme zu geben.

§ 12 Beschäftigte als Betreiber_innen und Nutzer_innen

Beschäftigte der TU Darmstadt sind zum besonders sorgfältigem Umgang im Rahmen des Betriebes und der Nutzung der IT-Systeme der TU Darmstadt verpflichtet. Im Hinblick auf die den Dienstherrn und die Arbeitgeberin sowie die jeweils verantwortlichen Führungskräfte treffende Fürsorgepflicht gelten ergänzend folgende Regelungen:

1. Die in § 4, § 5 Ziffer 3f, § 5 Ziffer 5a zitierten Gesetze und Leitlinien werden den Beschäftigten in geeigneter Weise zugänglich gemacht.

2. Die Beschäftigten werden in geeigneter Weise informiert über

   a) die verantwortungsvolle und ökonomisch sinnvolle Nutzung und die Pflicht zur Vermeidung von Schäden (§ 5, Ziffer 2);

   b) über die Bedingungen, unter denen die zum Teil im Rahmen von Lizenzverträgen erworbene Software, Dokumentationen oder Daten zur Verfügung gestellt werden (§ 5 Ziffer 3g), sofern diese bestimmte Verhaltensregeln im dienstlichen Kontext nach sich ziehen;

   c) den Umgang mit personenbezogenen Daten im Rahmen von Vorhaben zur Verarbeitung solcher Daten (§ 5 Ziffer 4);

   d) die Standards im Rahmen der Veröffentlichung von Informationen im World-Wide-Web (WWW) (§ 5, Ziffer 6 und § 11a, Ziffer 3).

3. Anbieter von Informationen im World-Wide-Web (WWW) (§ 5, Ziffer 6) ist die Präsidentin oder der Präsident der TU Darmstadt. Die Beschäftigten sind hinsichtlich der Inhalte zur Abstimmung mit sämtlichen zuständigen Stellen der TU Darmstadt und zur besonderen Sensibilität im Umgang

mit eingestellten Informationen verpflichtet. Hinsicht der Angabe des Impressums und der Datenschutzerklärung gelten die hierfür vorgegebenen Standards.

4. Für Beschäftigte der TU Darmstadt gelten die arbeits- und dienstrechtlichen Haftungsprivilegierungen, wonach sie für Vorsatz und grobe Fahrlässigkeit haften.

5. Die Einsicht in die Dateien der Nutzenden durch den Systembetreiber ist nur zulässig, soweit dies zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Verstößen gegen die Benutzungsordnung erforderlich ist und hierfür Anhaltspunkte vorliegen. In der Regel erfolgt die Einsichtnahme in Abstimmung mit der oder dem Personalverantwortlichen des Bereichs, in dem eine Einsichtnahme erforderlich ist. Nur wenn dies zur Abwendung von Gefahrenerforderlich ist, erfolgt eine Information, sobald dies im Rahmen des Zweckerreichens notwendig ist, erst nachträglich.

6. Die jeweiligen Führungskräfte tragen dafür Sorge, dass ihre Beschäftigten über die notwendige Sachkunde zur Einhaltung der vorliegenden Benutzungsordnung und damit zum Betrieb und zur Nutzung der IT-Infrastruktur der TU Darmstadt verfügen. Die TU Darmstadt bietet geeignete Schulungsveranstaltungen an.

§ 13 Sonstige Regelungen

1. Für die Nutzung von IT-Ressourcen können Entgelte oder Gebühren festgelegt werden. Es gilt dabei die Entgeltordnung des jeweiligen Systembetreibers.
2. Für einzelne Systeme können bei Bedarf ergänzende oder abweichende Nutzungsregeln festgelegt werden. Ergänzungen oder Abweichungen von § 12 bedürfen der Beteiligung durch den Personalrat der TU Darmstadt, sofern es sich um Regelungen handelt, die Beschäftigte betreffen, die gem. § 3 und § 97 Hessisches Personalvertretungsgesetz durch den Personalrat vertreten werden.
3. Über Änderungen dieser Benutzungsordnung entscheidet die zuständige Hochschulleitung.

§ 14 In-Kraft-Treten

Diese Benutzungsordnung tritt am Tage nach der Veröffentlichung in der Satzungsbeilage der Technischen Universität Darmstadt in Kraft. Die „Allgemeine Benutzungsordnung für die Informationsverarbeitungs- und Kommunikations-Infrastruktur“ vom 13. März 2000, veröffentlicht im Hessischen Staatsanzeiger 17/2000, tritt mit In-Kraft-Treten dieser Nutzungsordnung außer Kraft.

Darmstadt, 01. Oktober 2019

Prof. Dr. Tanja Brühl
Die Präsidentin der
Technischen Universität Darmstadt