

# Ihre Rechnerkennung am Institut für Informatik der TU München

Mit Ihrer Unterschrift auf diesem Dokument bestätigen Sie im Folgenden:

1. den Erhalt der Zugangsdaten (Login und Passwort) für Ihre Rechnerkennung an der Fakultät für Informatik
2. den Erhalt einer Kopie der *Benutzungsrichtlinien für Informationsverarbeitungssysteme der Technischen Universität München*
3. dass Sie den *Benutzungsrichtlinien für Informationsverarbeitungssysteme der Technischen Universität München*, die auf der Rückseite dieses Dokuments abgedruckt sind Folge, leisten werden
4. den Erhalt der Passphrase für Ihr Benutzerzertifikat der DFN-PKI
5. dass Sie die Regelungen der unter [https://info.pca.dfn.de/doc/Info\\_Zertifikatinhaber.pdf](https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf) veröffentlichten *Informationen für Zertifikatinhaber* einhalten werden. Das heißt insbesondere:
  - Sie dürfen den privaten Schlüssel zu Ihrem Zertifikat nicht anderen Personen zugänglich machen. Eine Weitergabe ist nicht erlaubt.
  - Jedes Gerät, auf dem Sie den privaten Schlüssel speichern bzw. einsetzen, muss angemessen geschützt, also z.B. frei von Schadsoftware wie Viren sein und regelmäßig mit Sicherheits-Patches versehen werden.
  - Sie sind unter den folgenden Bedingungen verpflichtet, das Zertifikat sperren zu lassen:
    - Das Zertifikat enthält Angaben, die nicht mehr gültig sind, beispielsweise nach einer Namensänderung.
    - Der private Schlüssel oder die dazugehörige Passphrase/PIN wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert bzw. missbraucht.
    - Sie sind nicht mehr berechtigt, das Zertifikat zu nutzen.

Sie erklären sich mit der Verarbeitung und Nutzung der erhobenen Daten zum Zweck der Zertifikaterstellung einverstanden. Die Daten dürfen an den DFN-Verein übermittelt und dort beschränkt auf diesen Zweck verarbeitet und genutzt werden.

Vorname \_\_\_\_\_

Nachname \_\_\_\_\_

Geburtsdatum  
(DD.MM.YYYY) \_\_\_\_\_

\_\_\_\_\_  
Ort

\_\_\_\_\_  
Datum

\_\_\_\_\_  
Unterschrift

**Benutzungsrichtlinien**  
**für Informationsverarbeitungssysteme der**  
**Technischen Universität München**  
Stand: 1.11.2014

**Präambel**

Die Technische Universität München und ihre Einrichtungen ("Betreiber" oder "Systembetreiber") betreiben eine Informationsverarbeitungs-Infrastruktur (IV-Infrastruktur) bestehend aus Datenverarbeitungsanlagen (Rechnern), Kommunikationssystemen (Netzen) und weiteren Hilfseinrichtungen der Informationsverarbeitung.

Die IV-Infrastruktur ist in das vom Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ) betriebene Münchener Wissenschaftsnetz und damit in das deutsche Wissenschaftsnetz (WiN) und in das weltweite Internet integriert. Für vom LRZ angebotene Dienste wie Netzanbindung, E-Mail, File-Storage, Backup, Archivierung und Hosting gelten zusätzlich die Benutzungsrichtlinien des LRZ (<http://www.lrz.de/wir/regelwerk/benutzungsrichtlinien.pdf>).

Die vorliegenden Benutzungsrichtlinien regeln die Bedingungen, unter denen das Leistungsangebot genutzt werden kann.

**Die Benutzungsrichtlinien**

- orientieren sich an den gesetzlich festgelegten Aufgaben der Hochschulen sowie an ihrem Mandat zur Wahrung der akademischen Freiheit,
- stellen Grundregeln für einen ordnungsgemäßen Betrieb der IV-Infrastruktur auf,
- weisen hin auf die zu wahren Rechte Dritter (z.B. bei Softwarelizenzen, Auflagen der Netzbetreiber, Datenschutzaspekte),
- verpflichten den/die Benutzer/in zu korrektem Verhalten und zum ökonomischen Gebrauch der - angebotenen Ressourcen,
- klären auf über eventuelle Maßnahmen des Betreibers bei Verstößen gegen die Benutzungsrichtlinien.

**§1 Geltungsbereich**

Diese Benutzungsrichtlinien gelten für die von der Technischen Universität München und ihren Einrichtungen sowie dem LRZ bereitgehaltene IV-Infrastruktur, bestehend aus Rechenanlagen (Rechner), Kommunikationsnetzen (Netze), Diensten, Anwendungen und weiteren Hilfseinrichtungen der Informationsverarbeitung.

**§2 Benutzerkreis und Aufgaben**

1. Die in §1 genannten IV-Ressourcen stehen den Mitgliedern der Technischen Universität München zur Erfüllung ihrer Aufgaben aus Forschung, Lehre, Verwaltung, Aus- und Weiterbildung, Öffentlichkeitsarbeit und Außendarstellung der Hochschule und für sonstige in Art. 2 des Bayerischen Hochschulgesetzes beschriebene Aufgaben zur Verfügung.
2. Anderen Personen und Einrichtungen kann die Nutzung gestattet werden.
3. Mitglieder der Technischen Universität München wenden sich an die für sie zuständige Organisationseinheit (vgl. §3 (1)).

**§3 Formale Benutzungsrechte**

1. Wer IV-Ressourcen nach §1 benutzen will, bedarf einer formalen Benutzungsrechte des zuständigen Systembetreibers. Ausgenommen sind Dienste, die für anonymen Zugang eingerichtet sind (z.B. Informationsdienste, Bibliotheksdienste, kurzfristige Gastkennungen bei Tagungen).
2. Systembetreiber sind für ihre Systeme die zuständigen organisatorischen Einheiten der Technischen Universität München wie Fakultäten, Institute, Betriebseinheiten, Lehrstühle und weitere Untereinheiten.
3. Der Antrag auf eine formale Benutzungsrechte soll folgende Angaben enthalten:
  - a. Betreiber/Institut oder organisatorische Einheit, bei der die Benutzungsrechte beantragt wird;
  - b. Systeme, für welche die Benutzungsrechte beantragt wird;
  - c. Antragsteller/in: Name, Adresse, Telefonnummer, E-Mail-Adresse und evtl. Zugehörigkeit zu einer organisatorischen Einheit der Universität;
  - d. Überschlüssige Angaben zum Zweck der Nutzung, beispielsweise Forschung, Ausbildung/Lehre, Verwaltung;
  - e. Einverständniserklärung, dass der Betreiber Nutzerrechte und Benutzerdaten wie Passwörter zum Schutz des Betriebs ändern darf. Der/die Nutzer/in ist darüber unverzüglich in Kenntnis zu setzen;
  - f. Erklärung, dass der/die Benutzer/in die Benutzungsrichtlinien anerkennt; Der/die Nutzer/in erteilt seine/ihre Zustimmung entweder schriftlich per Unterschrift oder auf digitale Weg. Dabei muss der/die Nutzer/in über ein Ankreuzverfahren (Opt-in- Einwilligungserklärung) seine/ihre Zustimmung aktiv erteilen.
4. Die einschlägigen Datenschutzbestimmungen sind zu beachten. Weitere Angaben darf der Systembetreiber nur verlangen, soweit sie zur Entscheidung über den Antrag erforderlich sind. Über den Antrag entscheidet der zuständige Systembetreiber. Er kann die Erteilung der Benutzungsrechte vom Nachweis bestimmter Kenntnisse über die Benutzung der Anlage abhängig machen.
5. Die Benutzungsrechte darf versagt werden, wenn
  - a. nicht gewährleistet erscheint, dass der/die Antragsteller/in seinen/ihren Pflichten als Nutzer/in nachkommen wird;
  - b. die Kapazität der Anlage, deren Benutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die beabsichtigten Arbeiten nicht ausreicht;
  - c. das Vorhaben nicht mit den Zwecken nach §2 (1) und §4 (1) vereinbar ist;
  - d. die Anlage für die beabsichtigte Nutzung offensichtlich ungeeignet oder für spezielle Zwecke reserviert ist; e. die zu benutzende Anlage an ein Netz angeschlossen ist, das besonderen Datenschutzanforderungen genügen muss und kein sachlicher Grund für diesen Zugriffswunsch ersichtlich ist;
  - e. zu erwarten ist, dass durch die beantragte Nutzung andere berechnete Nutzungen in nicht angemessener Weise gestört werden.
6. Die Benutzungsrechte berechtigt nur zu Arbeiten, die im Zusammenhang mit der beantragten Nutzung stehen.

**§4 Pflichten des Benutzers/der Benutzerin**

1. Die IV-Ressourcen nach §1 dürfen nur zu den in §2 (1) genannten Zwecken genutzt werden. Eine Nutzung zu anderen, insbesondere zu gewerblichen Zwecken, kann nur auf Antrag und gegen Entgelt gestattet werden.
2. Der/die Benutzer/in ist verpflichtet, darauf zu achten, dass er/sie die vorhandenen Betriebsmittel (Arbeitsplätze, CPU-Kapazität, Plattenspeicherplatz, Leitungskapazitäten, Peripheriegeräte und Verbrauchsmaterial) verantwortungsvoll und ökonomisch sinnvoll nutzt. Der/die Benutzer/in ist verpflichtet, Beeinträchtigungen des Betriebes, soweit sie vorhersehbar sind, zu unterlassen und nach bestem Wissen alles zu vermeiden, was Schaden an der IV-Infrastruktur oder bei anderen Benutzern verursachen kann. Zuwiderhandlungen können Schadenersatzansprüche begründen (§7).
3. Der/die Benutzer/in hat jegliche Art der missbräuchlichen Benutzung der IV-Infrastruktur zu unterlassen. Er/sie ist insbesondere dazu verpflichtet,
  - a. ausschließlich mit Benutzerkennungen zu arbeiten, deren Nutzung ihm/ihr gestattet wurde; die Weitergabe von Kennungen und Passwörtern ist nicht gestattet;
  - b. den Zugang zu den IV-Ressourcen durch ein geheim zu haltendes Passwort oder ein gleichwertiges Verfahren zu schützen;
  - c. Vorkehrungen zu treffen, damit unberechtigten Dritten der Zugang zu den IV-Ressourcen verwehrt wird; dazu gehört es insbesondere, primitive, naheliegende Passwörter nicht zu verwenden, die Passwörter öfter zu ändern und sich am Ende der Benutzung ordnungsgemäß per Logout abzumelden. Der/die Benutzer/in trägt im Rahmen der gesetzlichen Vorschriften die Verantwortung für alle Aktionen, die unter seiner/ihrer Benutzerkennung vorgenommen werden, und zwar auch dann, wenn diese Aktionen durch Dritte vorgenommen werden, denen er/sie in ihm/ihr vorzuwerfender Weise den Zugang ermöglicht hat.Der/die Benutzer/in ist des Weiteren verpflichtet,
  - d. bei der Benutzung von Software (Quellen, Objekte), Dokumentationen und anderen Daten die gesetzlichen Regelungen (Urheberrechtsschutz, Copyright) einzuhalten;
  - e. 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;
  - f. 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 Schadenersatzansprüche begründen (§7)
4. Selbstverständlich darf die IV-Infrastruktur nur in rechtlich korrekter Weise genutzt werden. Es wird ausdrücklich darauf hingewiesen, dass insbesondere folgende Verhaltensweisen nach dem Strafgesetzbuch unter Strafe gestellt sind:

- a. Ausforschen fremder Passwörter, Ausspähen von Daten (§202 a StGB)
- b. unbefugtes Verändern, Löschen, Unterdrücken oder Unbrauchbarmachen von Daten (§303 a StGB). Computersabotage (§303 b StGB) und Computerbetrug (§263 a StGB)
- c. Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§86 StGB) oder rassistischem Gedankengut (§131 StGB)
- d. Verbreitung gewisser Formen von Pornographie im Netz (§184 Abs. 3 StGB)
- e. Abrufl oder Besitz von Dokumenten mit Kinderpornographie (§184 Abs. 5 StGB)
- f. Ehrdelikte wie Beleidigung, Verleumdung (§§185 ff StGB)

Der Systembetreiber behält sich die Verfolgung strafrechtlicher Schritte sowie zivilrechtlicher Ansprüche vor (§7).

5. Dem/der Benutzer/in ist es untersagt, ohne Einwilligung des zuständigen Systembetreibers
  - a. Eingriffe in die Hardware-Installation vorzunehmen;
  - b. die Konfiguration der Betriebssysteme oder des Netzwerkes zu verändern.Die Berechtigung zur Installation von Software ist in Abhängigkeit von den jeweiligen örtlichen und systemtechnischen Gegebenheiten gesondert geregelt.
6. Der/die Benutzer/in ist verpflichtet, ein Vorhaben zur Bearbeitung personenbezogener Daten vor Beginn mit dem Systembetreiber abzustimmen. Davon unberührt sind die Verpflichtungen, die sich aus Bestimmungen des Bayerischen Datenschutzgesetzes ergeben. Dem/der Benutzer/in ist es untersagt, für andere Benutzer/innen bestimmte Daten und Nachrichten zur Kenntnis zu nehmen und/oder zu verwerfen.
7. Der/die Benutzer/in ist verpflichtet,
  - a. die von einem Systembetreiber zur Verfügung gestellten ergänzenden Nutzungsbedingungen, Richtlinien und Leitfäden zur Benutzung zu beachten;
  - b. im Verkehr mit Rechnern und Netzen anderer Betreiber deren Benutzungs- und Zugriffsrichtlinien einzuhalten.

**§5 Aufgaben, Rechte und Pflichten der Systembetreiber**

1. Jeder Systembetreiber muss über die erteilten Benutzungsrechte eine Dokumentation führen. Die Unterlagen sind nach Auslaufen der Berechtigung zwei Jahre aufzubewahren.
2. Der Systembetreiber trägt in angemessener Weise zum Verhindern bzw. Aufdecken von Missbrauch bei. Hierfür ist er insbesondere dazu berechtigt,
  - a. Passwörter und Nutzerdaten auf ihre Sicherheit zu prüfen und Schutzmaßnahmen wie das Ändern oder Sperren leicht zu ertastenden Passwörter zum Schutz vor unberechtigtem Zugriff durchzuführen. Der/die Nutzer/in ist hiervon unverzüglich in Kenntnis zu setzen;
  - b. Aktivitäten der Benutzer/innen zu dokumentieren und auszuwerten, soweit dies zu Zwecken der Abschreckung, der Ressourcenplanung, des Schutzes personenbezogener Daten anderer Nutzer/innen, der Überwachung des Betriebes oder der Verfolgung von Fehlerfällen und Verstößen gegen die Benutzungsrichtlinien sowie gesetzlichen Bestimmungen dient;
  - c. bei Verdacht auf Verstöße gegen die Benutzungsrichtlinie oder gegen strafrechtliche Bestimmungen unter Beachtung des Vieraugenprinzips (bei Beschäftigten gelten die Regularien der „Rahmendienstvereinbarung zur Verarbeitung systemimmanenter Daten, des Einsatzes von Fernüberwachungsmaßnahmen und der Einsichtnahme in Benutzerdaten an der Technischen Universität München“) und der Aufzeichnungspflicht in Benutzerdateien und Mailboxen Einsicht zu nehmen oder die Netzwerknutzung durch den/die Benutzer/in z.B. mittels Netzwerk-Sniffer detailliert zu protokollieren; Jede Einsichtnahme ist zu dokumentieren und der/die betroffene Nutzer/in nach Zweckerreichung unverzüglich zu benachrichtigen;
  - d. bei Erhärtung des Verdachts auf strafbare Handlungen beweisichernde Maßnahmen wie z.B. Key-stroke Logging oder Netzwerk-Sniffer einzusetzen.Unmittelbar nach Zweckerreichung sind die gewonnenen Daten zu löschen.
3. Der Systembetreiber ist zur Vertraulichkeit verpflichtet.
4. Der Systembetreiber gibt die Ansprechpartner für die Betreuung seiner Benutzer/innen bekannt.
5. Der Systembetreiber ist verpflichtet, im Verkehr mit Rechnern und Netzen anderer Betreiber deren Benutzungs- und Zugriffsrichtlinien einzuhalten.
6. Betriebsbedingt kann der Betreiber die Nutzung der IV-Infrastruktur vorübergehend einschränken oder einzelne Nutzerkennungen vorübergehend sperren. Sofern möglich, sind die betroffenen Nutzer/innen hierüber im Voraus zu unterrichten.
7. Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein/e Nutzer/in auf der IV-Infrastruktur des Betreibers rechtswidrige Inhalte zur Nutzung bereithält, kann der Betreiber die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.

**§6 Haftung des Systembetreibers/Haftungsausschluss**

1. Der Systembetreiber übernimmt keine Garantie dafür, dass die Systemfunktionen den speziellen Anforderungen des Nutzers/der Nutzerin entsprechen oder dass das System fehlerfrei und ohne Unterbrechung läuft. Der Systembetreiber kann nicht die Unversehrtheit (bzgl. Zerstörung, Manipulation) und Vertraulichkeit der bei ihm gespeicherten Daten garantieren.
2. Der Systembetreiber haftet nicht für Schäden gleich welcher Art, die dem/der Benutzer/in aus der Inanspruchnahme der IV-Ressourcen nach §1 entstehen; ausgenommen ist vorsätzliches Verhalten und grobe Fahrlässigkeit des Systembetreibers oder der Personen, deren er sich zur Erfüllung seiner Aufgaben bedient.

**§7 Haftung des Nutzers/der Nutzerin**

1. Der/die Nutzer/in haftet im Rahmen der gesetzlichen Vorschriften für alle Nachteile, die dem Systembetreiber durch missbräuchliche oder rechtswidrige Verwendung der IV-Ressourcen und der Nutzungsrechte und/oder dadurch entstehen, dass der/die Nutzer/in schuldhaft seinen Pflichten aus dieser Benutzungsrechte nicht nachkommt.
2. Der/die Nutzer/in haftet auch für Schäden, die im Rahmen der ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe seiner Benutzerkennung an Dritte. In diesem Fall kann der Systembetreiber von dem/der Nutzer/in ein Nutzungsentgelt für die Drittnutzung verlangen.
3. Der/die Nutzer/in hat den Systembetreiber, soweit der/die Nutzer/in dafür haftbar gemacht werden kann, von allen Ansprüchen freizustellen, wenn Dritte den Systembetreiber wegen eines missbräuchlichen oder rechtswidrigen Verhaltens des Nutzers/der Nutzerin auf Schadenersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen. Der Systembetreiber wird dem/der Nutzer/in den Streit verkünden, sofern Dritte gegen ihn gerichtlich vorgehen.

**§8 Folgen einer missbräuchlichen oder gesetzeswidrigen Benutzung**

1. Bei Verstößen gegen gesetzliche Vorschriften, gegen die Bestimmungen dieser Benutzungsrichtlinien, insbesondere des §4 (Pflichten des Benutzers/der Benutzerin) oder wenn dem Betreiber durch sonstiges rechtswidriges Nutzerverhalten Nachteile entstehen, kann der Systembetreiber die Benutzungsrechte einschränken, ganz oder teilweise entziehen. Es ist dabei unerheblich, ob der Verstoß einen Schaden zur Folge hatte oder nicht.
2. Bei schwerwiegenden oder wiederholten Verstößen kann ein/e Benutzer/in auf Dauer von der Benutzung sämtlicher IV-Ressourcen nach §1 ausgeschlossen werden.
3. Dem/der Betroffenen/en wird die Gelegenheit zur Stellungnahme und zur Sicherung seiner/ihrer Daten gegeben.
4. Verstöße gegen gesetzliche, arbeitsrechtliche oder dienstrechtliche Vorschriften oder gegen die Bestimmungen dieser Benutzungsrichtlinien werden auf ihre strafrechtliche Relevanz sowie auf zivilrechtliche Ansprüche hin überprüft. Bedeutsam erscheinende Sachverhalte werden der jeweiligen Rechtsabteilung übergeben, die die Einleitung geeigneter weiterer Schritte prüft. Der Systembetreiber behält sich die Verfolgung strafrechtlicher Schritte sowie zivilrechtlicher Ansprüche ausdrücklich vor.

**§9 Sonstige Regelungen**

1. Für die Nutzung von IV-Ressourcen können in gesonderten Ordnungen Gebühren festgelegt werden.
2. Für bestimmte Systeme können bei Bedarf ergänzende oder abweichende Nutzungsregelungen festgelegt werden.
3. Für Bedienstete können aufgrund von Dienstvereinbarungen und dienst-/tarifrechtlichen Vorschriften zum Teil ergänzende oder abweichende Nutzungsregeln gelten.
4. Sollten Teile dieser Benutzervereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der übrigen Teile nicht.
5. Gerichtsstand für alle aus dem Benutzungsverhältnis erwachsenden rechtlichen Ansprüche ist München.

**§10 In Kraft treten**

Diese Benutzungsrichtlinien treten am Tage nach der Veröffentlichung in Kraft.

München, den 1.11.2014

Herbert Vogt

Leiter IT-Servicezentrum