Otto-Friedrich-Universität Bamberg

Nutzungsrichtlinien
für Informationsverarbeitungssysteme
der Otto-Friedrich-Universität Bamberg
Vom 10. Juli 2024

- Beschlossen vom Senat der Otto-Friedrich-Universität Bamberg
in seiner Sitzung am 5. Juni 2024 -

Inhaltsverzeichnis

Präambel

[1]Die Otto-Friedrich-Universität Bamberg und ihre Einrichtungen („Betreiber“ oder „Systembetreiber“) betreiben eine Informationstechnologie-Infrastruktur (IT-Infrastruktur), bestehend aus Hardware- und Softwaresystemen (Rechnern), Kommunikationssystemen (Netzen) und weiteren Hilfseinrichtungen der Informationsverarbeitung. [2]Die IT-Infrastruktur ist in das deutsche Wissenschaftsnetz und damit in das weltweite Internet integriert. [3]Die vorliegenden Nutzungsrichtlinien regeln die Bedingungen, unter denen das Leistungsangebot genutzt werden kann. [4]Die Nutzungsrichtlinien

- 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 IT-Infrastruktur auf,
- weisen auf zu wahrende Rechte Dritter hin (zum Beispiel Softwarelizenzen, Auflagen der Netzbetreiber, Datenschutzaspekte),
- verpflichten die Nutzerin oder den Nutzer zu korrektem Verhalten und zu ökonomischem Gebrauch der angebotenen Ressourcen,
- klären auf über eventuelle Maßnahmen bei Verstößen gegen die Nutzungsrichtlinien.

Erster Abschnitt:
Allgemeine Bestimmungen

§ 1
Geltungsbereich

Diese Nutzungsrichtlinien gelten für die von der Otto-Friedrich-Universität Bamberg und ihren Einrichtungen bereitgehaltene IT-Infrastruktur, bestehend aus Hardware- und Softwaresystemen (Rechnern), Kommunikationssystemen (Netzen) und weiteren Hilfseinrichtungen der Informationsverarbeitung.

Zweiter Abschnitt:
Nutzerinnen- oder Nutzerkreis und Aufgaben

§ 2
Universitätsmitglieder

Die in § 1 genannten IT-Ressourcen stehen den Mitgliedern der Otto-Friedrich-Universität Bamberg zur Erfüllung ihrer in Art. 2 Bayerisches Hochschulinnovationsgesetz vom 12. August 2022 (GVBl. S. 414, BayRS 2210-1-3-WK) beschriebenen Aufgaben zur Verfügung, insbesondere für Forschung, Lehre, Förderung des wissenschaftlichen Nachwuchses, Aus- und Weiterbildung, Öffentlichkeitsarbeit, Verwaltung und Bibliothek.

§ 3
Andere Personen und Einrichtungen

Anderen Personen und Einrichtungen kann die Nutzung gestattet werden, wenn dies den Aufgaben der Otto-Friedrich-Universität Bamberg dient oder damit in engem Zusammenhang steht.

Dritter Abschnitt:
Formale Nutzungsberechtigung

§ 4
Grundsatz

[1]Wer IT-Ressourcen nach § 1 nutzen will, bedarf einer formalen Nutzungsberechtigung des zuständigen Systembetreibers. [2]Ausgenommen sind Dienste, die für anonymen Zugang eingerichtet sind (zum Beispiel Informationsdienste, Bibliotheksdienste, kurzfristige Gastkennungen bei Tagungen). [3]Die formale Benutzungsberechtigung kann automatisiert erteilt werden.

§ 5
Systembetreiber

Systembetreiber sind für

1. zentral bereitgestellte und betriebene Systeme und Dienste die organisatorisch zuständigen Betriebseinheiten, insb. der IT-Service sowie das Dezernat Informationssysteme (Z/IS) der Zentralen Universitätsverwaltung,
2. dezentrale Systeme die zuständigen organisatorischen Einheiten (Fakultäten, Lehreinheiten und weitere Untereinheiten) der Otto-Friedrich-Universität Bamberg.

§ 6
Antrag

[1]Der Antrag auf eine formale Nutzungsberechtigung soll folgende Angaben enthalten:

1. Systembetreiber, bei dem die Nutzungsberechtigung beantragt wird;
2. Systeme, für welche die Nutzungsberechtigung beantragt wird;
3. Antragstellerin oder Antragsteller: Name, Adresse, Geburtstag, Geburtsort, Telefonnummer (bei Studierenden auch Matrikelnummer) und eventuelle Zugehörigkeit zu einer organisatorischen Einheit der Otto-Friedrich-Universität Bamberg;
4. überschlägige Angaben zum Zweck der Nutzung, beispielsweise Forschung, Ausbildung/Lehre, Verwaltung;
5. die Erklärung, dass die Nutzerin oder der Nutzer die Nutzungsrichtlinien anerkennt;
6. Einträge für Informationsdienste der Otto-Friedrich-Universität Bamberg;
7. Einverständniserklärung der Nutzerin oder des Nutzers zur Verarbeitung ihrer oder seiner personenbezogenen Daten;
8. Hinweis der Nutzerin oder des Nutzers auf die Möglichkeiten einer Dokumentation ihres oder seines Verhaltens und der Einsichtnahme in ihre oder seine Dateien nach Maßgabe dieser Nutzungsrichtlinien (§ 36 und 37).

[2]Weitere Angaben darf der Systembetreiber nur verlangen, soweit sie zur Entscheidung über den Antrag erforderlich sind.

§ 7
Entscheidung über den Antrag

[1]Über den Antrag auf eine formale Nutzungsberechtigung entscheidet der zuständige Systembetreiber. [2]Er kann die Erteilung der Nutzungsberechtigung vom Nachweis bestimmter Kenntnisse über die Nutzung der Anlage abhängig machen.

§ 8
Versagung, Widerruf und nachträgliche Beschränkung der Nutzungsberechtigung

[1]Die Nutzungsberechtigung darf ganz oder teilweise versagt, widerrufen oder nachträglich beschränkt werden, insbesondere wenn

1. kein ordnungsgemäßer Antrag vorliegt oder die Angaben im Antrag nicht oder nicht mehr zutreffen,
2. nicht gewährleistet erscheint, dass die Antragstellerin oder der Antragsteller ihren oder seinen Pflichten als Nutzerin oder Nutzer nachkommen wird,

3. die Kapazität der IT-Ressourcen, deren Nutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die beabsichtigten Arbeiten nicht ausreicht,
4. das Vorhaben nicht mit den Zwecken nach §§ 11 und 12 vereinbar ist,
5. die IT-Ressourcen für die beabsichtigte Nutzung offensichtlich ungeeignet oder für spezielle Zwecke reserviert sind,
6. die zu benutzenden IT-Ressourcen an ein Netz angeschlossen sind, das besonderen Datenschutzanforderungen genügen muss und kein sachlicher Grund für diesen Zugriffswunsch ersichtlich ist,
7. wenn zu erwarten ist, dass durch die beantragte Nutzung andere berechtigte Nutzungen in nicht angemessener Weise gestört werden.

[2]Die Ablehnung der Nutzungsberechtigung ist zu begründen.

§ 9
Umfang der Nutzungsberechtigung

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

§ 10
Dienstanweisungen

[1]Der Systembetreiber kann, falls erforderlich, Dienstanweisungen erlassen. [2]Dienstanweisungen für zentrale Systeme bedürfen der Zustimmung des Senats.

Vierter Abschnitt:
Pflichten der Nutzerin oder des Nutzers

§ 11
Zweckbindung der Nutzung

[1]Die IT-Ressourcen nach § 1 dürfen nur zu den in § 2 genannten Zwecken genutzt werden. [2]Eine Nutzung zu anderen, insbesondere zu gewerblichen Zwecken kann nur auf Antrag und gegen Entgelt gestattet werden.

§ 12
Verantwortungsvolle und ökonomisch sinnvolle Nutzung

[1]Die Nutzerin oder der Nutzer ist verpflichtet, darauf zu achten, dass sie oder er die vorhandenen IT-Ressourcen verantwortungsvoll und ökonomisch sinnvoll nutzt. [2]Die

Nutzerin oder der Nutzer ist verpflichtet, nach bestem Wissen und Gewissen alles zu vermeiden, was Schaden an der IT-Infrastruktur oder bei anderen Nutzerinnen oder Nutzern verursachen oder den ordnungsgemäßen Betrieb der IT-Ressourcen beeinträchtigen kann. [3]Zuwiderhandlungen können Schadenersatzansprüche begründen (§§ 46 und 47).

§ 13
Zugangs- und Zugriffssicherung

[1]Die Nutzerin oder der Nutzer trägt die volle Verantwortung für alle Aktionen, die unter ihrer oder seiner Nutzerin- oder Nutzerkennung oder mit ihr oder ihm zugeteilten Schlüsseln oder Passwörtern vorgenommen werden. [2]Die gilt auch für den Fall, dass diese Aktionen durch Dritte vorgenommen werden, denen sie oder er fahrlässig oder vorsätzlich schuldhaft den Zugang ermöglicht hat.

1. Die Weitergabe von Kennungen, Passwörtern, Schlüsseln, elektronischen Zertifikaten und anderen dem Nachweis der Identität dienenden Informationen, Geräten und Daten ist grundsätzlich nicht gestattet; die Nutzerin oder der Nutzer stellt sicher, dass jede Nutzung in ihrem bzw. seinem Namen identifizierbar ist und insbesondere ihre oder seine Nutzungspflichten eingehalten werden.
2. Der Zugang zu den IT-Ressourcen ist durch ein geheim zu haltendes Passwort oder ein mindestens gleichwertiges Verfahren zu schützen.
3. Die Nutzerin oder der Nutzer hat Vorkehrungen zu treffen, um unberechtigten Dritten den Zugang zu den IT-Ressourcen zu verwehren; dazu gehört es insbesondere, einfache, naheliegende Passwörter zu meiden, die Passwörter regelmäßig zu ändern, Bildschirmsperren bei Abwesenheit zu aktivieren und das Logout nicht zu vergessen.

§ 14
Einzelpflichten

[1]Die Nutzerin oder der Nutzer hat jegliche Art der missbräuchlichen Nutzung der IT-Infrastruktur zu unterlassen. [2]Sie bzw. er ist insbesondere dazu verpflichtet,

1. ausschließlich mit Nutzerinnen- oder Nutzerkennungen, Schlüsseln und Passwörtern zu arbeiten, deren Nutzung ihr oder ihm gestattet wurde,
2. bei der Nutzung von Software (Quellen, Objekte), Dokumentationen und anderen Daten die gesetzlichen Regelungen (Urheberrechtsschutz, Copyright) einzuhalten,
3. 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,

4. 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,
5. keinen unberechtigten Zugriff auf Informationen anderer Nutzerinnen oder Nutzer zu nehmen und bekannt gewordene Informationen anderer Nutzerinnen oder Nutzer nicht ohne Genehmigung weiter zu geben, selbst zu nutzen oder zu verändern,
6. dem Systembetreiber 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.
7. keine privaten Datenträger und Software ohne Virenschutzprogramm auf universitätseigenen Datenverarbeitungsgeräten (DV-Geräten) zu verwenden.

[3]Zuwiderhandlungen können Schadenersatzansprüche begründen (§§ 46 und 47). [4]Die Nutzerin oder der Nutzer trägt die volle Verantwortung für alle Aktionen, die unter ihrer oder seiner Benutzerkennung vorgenommen werden, zu denen sie oder er den Zugang ermöglicht hat.

§ 15
Strafrechtlich relevante Verhaltensweisen

[1]Die IT-Infrastruktur darf nur in rechtlich zulässiger Weise genutzt werden. [2]Es wird ausdrücklich darauf hingewiesen, dass insbesondere folgende Verhaltensweisen, die nach dem Strafgesetzbuch unter Strafe gestellt sind, einen Missbrauch darstellen:

1. Ausforschen fremder Passwörter, Ausspähen von Daten (§ 202a – Strafgesetzbuch – StGB – in der Fassung der Bekanntmachung vom 13. November 1998 – BGBl. I S. 3322),
2. Abfangen von Daten (§ 202b StGB),
3. Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB),
4. Datenhehlerei (202d StGB),
5. Fälschung beweiserheblicher Daten (§ 269 StGB),
6. Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB)
7. Datenveränderung (§ 303a StGB),
8. Computersabotage (§ 303b StGB) und Computerbetrug (§ 263a StGB),
9. Verbreiten von Propagandamitteln verfassungswidriger und terroristischer Organisationen (§ 86 StGB), Verwenden von Kennzeichen verfassungswidriger

und terroristischer Organisationen (§ 86a StGB) und Volksverhetzung (§ 130 StGB),

10. Verbreitung pornographischer Inhalte (§ 184 StGB) und Verbreitung gewalt- oder tierpornographischer Schriften (§ 184a StGB),
11. Verbreitung, Erwerb und Besitz kinderpornographischer Schriften (§ 184b StGB), Verbreitung, Erwerb und Besitz jugendpornografischer Inhalte (§ 184c StGB) und Verletzung des Intimbereichs durch Bildaufnahmen (§ 184k StGB),
12. Ehrdelikte (§§ 185 ff. StGB) wie zum Beispiel Beleidigungen, Üble Nachrede, Verleumdung.

[3]Die Otto-Friedrich-Universität Bamberg behält sich die Einleitung strafrechtlicher Schritte sowie die Geltendmachung zivilrechtlicher Ansprüche vor (vgl. §§ 46 unf 47).

§ 16
Hardware und Software

[1]Der Nutzerin oder dem Nutzer ist es untersagt, ohne Einwilligung des zuständigen Systembetreibers

1. Eingriffe in die Hardware-Installation vorzunehmen,
2. die Konfiguration der Betriebssysteme oder des Netzwerkes zu verändern.

[2]Die Berechtigung zur Installation von Software ist in Abhängigkeit von den jeweiligen örtlichen und systemtechnischen Gegebenheiten gesondert geregelt.

§ 17
Umgang mit personenbezogenen Daten

[1]Die Nutzerin oder der Nutzer ist verpflichtet, ein Vorhaben zur Bearbeitung personenbezogener Daten vor Beginn mit dem Systembetreiber abzustimmen. [2]Davon unberührt sind die Verpflichtungen, die sich aus Bestimmungen der Datenschutzgesetze ergeben.

§ 18
Besondere Pflichten

Die Nutzerin oder der Nutzer ist verpflichtet,

1. die vom Systembetreiber zur Verfügung gestellten Leitfäden zur Nutzung zu beachten,
2. bei elektronischen Veröffentlichungen Folgendes zu beachten:

a) die Pflichten zur Anbieterkennzeichnung (Impressum) nach § 5 Telemediengesetz (TMG) vom 26. Februar 2007 (BGBl. I S. 179),

b) die Sicherstellungspflichten nach § 19 Abs. 1 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG) vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045) wie zum Beispiel Angebot von Verschlüsselungsmethoden und

c) die Anzeigepflicht für externe Links nach § 19 Abs. 3 TDDDG,

3. im Umgang mit Rechnern und Netzen anderer Betreiber deren Nutzungs- und Zugriffsrichtlinien einzuhalten.

§ 19
„Clean desk policy“

Maßnahmen zur physischen Sicherung von Daten sind umzusetzen („Clean desk policy“):

1. Für das Verschließen insbesondere der Dienstzimmer, Schränke und Schreibtische sowie für das sichere Aufbewahren von Unterlagen, Datenträgern und Wertgegenständen sind die jeweiligen Berechtigten verantwortlich, ebenso für das Sichern informationstechnischer Geräte und das Schließen der Fenster und Türen beim Verlassen der Räume.
2. Papierdokumente mit vertraulichen oder personenbezogenen Daten, die nicht mehr benötigt werden oder einer Löschpflicht unterliegen, sind fachgerecht zu schreddern.
3. An Druckern, Kopier- und Faxgeräten sollen keine vertraulichen Informationen hinterlassen werden.
4. Passwörter und Zugangsinformationen dürfen am Arbeitsplatz nur mit ausreichendem Schutz vor dem Zugriff Dritter aufbewahrt werden.
5. Rechner sind zu sperren, wenn der Arbeitsplatz für längere Zeit verlassen wird.

§ 20
Sensible Daten

Die Sorgfaltspflicht besteht insbesondere bei der Verarbeitung sensibler Daten (siehe Anlage):

1. Informationen werden an der Otto-Friedrich-Universität Bamberg nach ihrer Vertraulichkeit als „öffentlich”, „nur für den Dienstgebrauch bzw. intern“, „vertraulich bzw. persönlich“ oder „geheim” klassifiziert.

2. Bei der Verarbeitung von Informationen der Klassen „vertraulich bzw. persönlich“ und „geheim”, bei der Nutzung von Diensten mit erhöhtem Schutzbedarf sowie bei der Verarbeitung sensibler Daten im Sinne des Datenschutzes, insbesondere besonderer Kategorien personenbezogener Daten im Sinn von Art. 9 Abs. 1 Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), hat besondere Vorsicht zu walten.

§ 21
Sicherheitsgefährdungen

[1]Eine die Sicherheit der Informationstechnologie-Systeme (IT-Systeme) gefährdende Nutzung der IT-Infrastruktur ist untersagt. [2]Insbesondere dürfen

1. sicherheitsrelevante Einstellungen oder Systemkomponenten wie Firewalls, Virenschutzprogramme oder Aktualisierungsmechanismen nicht deaktiviert oder umgangen werden,
2. keine Software-Produkte, Apps oder Plug-Ins installiert werden, die aus unsicheren Quellen stammen oder bei denen eine Sicherheitsgefährdung nicht auszuschließen ist; im Zweifel ist der zuständige Systembetreiber hinzuziehen.

Fünfter Abschnitt:
Anwendungsspezifische Regeln und Pflichten der Nutzerin oder des Nutzers

§ 22
Drucker, Kopierer und Multifunktionsgeräte

Bei der Nutzung von Druckern, Kopierern und Multifunktionsgeräten ist Folgendes zu beachten:

1. Wireless-Local-Area-Network-Schnittstellen (WLAN-Schnittstellen) sind zu deaktivieren, um Beeinträchtigungen auf das universitäre WLAN zu vermeiden.
2. Nicht benötigte Schnittstellen und Protokolle sind zu deaktivieren.
3. Beim Drucken oder Kopieren von Daten gemäß § 20 Nr. 2 ist besonders darauf zu achten, dass die Daten nicht versehentlich Unbefugten zugänglich werden.

§ 23
Cloud-Nutzung, Nutzung externer Dienstleister

Die Cloud-Nutzungs-Strategie der Otto-Friedrich-Universität Bamberg ist zu beachten.

1. Vorrangig sind für die Speicherung und Verarbeitung von dienstlichen Daten die von der Otto-Friedrich-Universität Bamberg bereitgestellten Systeme zu nutzen.
2. Eine Speicherung und Verarbeitung von Informationen gemäß § 20 Nr. 2 ist in nicht von der Otto-Friedrich-Universität Bamberg freigegebenen Cloud-Speicher-Diensten grundsätzlich nicht gestattet.
3. Die dienstlichen Zugangsdaten dürfen nicht bei Dritten verwendet oder hinterlegt werden.
4. Die automatisierte Weiterleitung von dienstlichen Daten (beispielsweise als E-Mail-Weiterleitung an eine private Adresse) ist untersagt.

§ 24
Telekommunikationsanlage (TK-Anlage) und Voice-over-Internet-Protocol-Telefonie (VoIP-Telefonie)

(1) Für dienstliche Telefonie und Fax-Nachrichten sind grundsätzlich ausschließlich die von der Otto-Friedrich-Universität Bamberg bereitgestellten Systeme zu nutzen.

(2) Internettelefonie-Software darf nur für Zwecke verwendet werden, bei denen keine Informationen gemäß § 20 Nr. 2 ausgetauscht werden.

§ 25
Arbeit an anderen Orten/Telearbeit

(1) Arbeitsplätze an Orten außerhalb der Otto-Friedrich-Universität Bamberg müssen den arbeitsschutzrechtlichen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen genügen.

(2) Dokumente und Daten dürfen nur mitgeführt oder außerhalb der Otto-Friedrich-Universität Bamberg aufbewahrt werden, wenn sie vor dem Zugriff Dritter geschützt sind.

(3) Der elektronische Austausch von Daten zwischen Beschäftigungsstelle und Telearbeitsplatz darf nur über eine von der Otto-Friedrich-Universität Bamberg freigegebene Schnittstelle, in der Regel ein virtuelles privates Netzwerk (VPN), erfolgen.

§ 26
Server

(1) Verbindungen zu Servern (z. B. zu Terminalservern) dürfen nur nach Aktivierung eines aktuellen Virenschutzprogramms auf dem Client aufgebaut werden.

(2) [1]Betriebssysteme müssen auf aktuellem Stand sein. [2]Alle Sicherheitsupdates und Patches von Herstellern müssen installiert sein.

(3) Die Firewall des Betriebssystems muss aktiviert sein.

§ 27
Zugriff auf Intranet vom Internet

(1) [1]Verschiedene Datendienste sind nur innerhalb des Datennetzes der Otto-Friedrich-Universität Bamberg erreichbar. [2]Für einen Zugriff aus dem Internet auf das Datennetz der Otto-Friedrich-Universität Bamberg dürfen nur vom IT-Service angebotene oder genehmigte Dienste genutzt werden. [3]Der IT-Service veröffentlicht zulässige Dienste in seinem Dienstleistungskatalog, siehe https://www.uni-bamberg.de/its/dienstleistungen/. [4]Für Einwahl in eines einer Organisationseinheit (OE) zugeordneten Subnetzes kann auch ein von der OE betriebener Dienst verwendet werden, sofern es sich um einen Dienst handelt, den der IT-Service genehmigt hat.

(2) [1]Die Einwahl in das universitäre Datennetz darf nur nach Aktivierung eines aktuellen Virenschutzprogramms auf dem Client aufgebaut werden. [2]Vorhandene Schutzmechanismen der Betriebssysteme auf den Clients sind zu aktivieren.

§ 28
WLAN

Die WLAN-Strategie und die Dienstvereinbarung WLAN der Otto-Friedrich-Universität Bamberg sind zu beachten.

1. In den Gebäuden der Otto-Friedrich-Universität Bamberg können sich alle Universitätsangehörigen, Teilnehmerinnen und Teilnehmer von universitären Tagungen, Wissenschaftlerinnen und Wissenschaftler, Studierende und Beschäftigte per WLAN mit dem Datennetz der Otto-Friedrich-Universität Bamberg verbinden.
2. Installation und Betrieb der WLAN-Komponenten liegen in der Verantwortung des IT-Services.
3. Bei Verwendung von öffentlichen unverschlüsselten Zugangspunkten (WLAN-Hotspots) muss der Übertragungsweg über geeignete Maßnahmen anderweitig geschützt werden (Virtual Private Network – VPN, Verschlüsselung auf Anwendungsebene).
4. Die WLAN-Einwahl in das universitäre WLAN darf nur nach Aktivierung eines aktuellen Virenschutzprogramms auf dem Client aufgebaut werden.

§ 29
Mobile IT-Nutzung

(1) [1]Bei der Verwendung von mobilen Geräten für dienstliche Zwecke muss besondere Vorsicht walten. [2]§ 10 Abs. 4 der Allgemeinen Geschäftsordnung für die Behörden des Freistaates Bayern (AGO) vom 12. Dezember 2000 (GVBl. S. 873; 2001 S. 28 BayRS 200-21-I) ist zu beachten.

(2) [1]Geräte sind sicher zu betreiben. [2]Dabei ist von den technischen Möglichkeiten (z. B. Verschlüsselung von Datenspeichern, Sperrcode, Bildschirmsperre, Persönliche Identifikationsnummer – PIN – für Mailbox, PIN oder Einschaltkennwörter, PIN-Sperre nach wiederholten Fehlversuchen, Antivirensoftware, Personal Firewall) Gebrauch zu machen.

(3) Die Weitergabe von dienstlich genutzten Geräten an Dritte oder Fremde ist nicht zulässig.

(4) Mobile Geräte sind permanent zu beaufsichtigen oder physisch zu sichern.

1. Der Verlust eines dienstlich genutzten Geräts ist umgehend zu melden (vgl. § 30 Nr. 1).
2. Die Zugangsdaten zu den Diensten der Otto-Friedrich-Universität sind bei Verlust eines Geräts umgehend zu ändern.
3. [1]Es ist sicherzustellen, dass bei Verlust keine dienstlichen Daten ausgelesen werden können. [2]Daten gemäß § 20 sind angemessen zu schützen.
4. Sämtliche nicht benötigten Schnittstellen (WLAN, Universal Serial Bus – USB, Bluetooth, Infrarot etc.) sind permanent bzw. nach einer erforderlichen Nutzung zu deaktivieren.
5. Die Übermittlung von Telemetrie-Daten an Cloud-Dienste ist auf das notwendige Maß zu beschränken.

§ 30
Sicherheits- und Datenschutzvorfälle

In Bezug auf Sicherheits- und Datenschutzvorfälle („Datenschutzverletzungen“) ist die Richtlinie zur Behandlung von Sicherheitsvorfällen zu beachten:

1. [1]IT-Sicherheitsvorfälle (z. B. Phishing, Krypto-Trojaner, Missbrauch von Zugangsdaten, Identitätsdiebstahl, Urheberrechtsverletzungen, Diebstahl oder Verlust von mobilen Geräten oder Datenträgern, Beeinträchtigung der Verfügbarkeit von dienstlichen Daten, Verletzung des Schutzes personenbezogener Daten, dubiose Anrufe von extern) sind nach Kenntnisnahme umgehend zu melden. [2]Die erste Meldung eines Vorfalls kann direkt an die zuständigen Systembetreiber, über den IT-Support des IT-Services

oder im Falle eines Datenschutzvorfalls („Datenschutzverletzung“) an die Datenschutzbeauftragte oder den Datenschutzbeauftragten erfolgen.

2. Gegenmaßnahmen dürfen erst nach Aufforderung durch Berechtigte ergriffen werden.
3. Alle Begleitumstände sind durch die Betroffenen ungeschönt, offen und transparent zu erläutern, um damit zur Schadensminderung beizutragen.
4. Informationen über den Sicherheitsvorfall dürfen nicht unautorisiert an Dritte weitergegeben werden.

Sechster Abschnitt
Aufgaben, Rechte und Pflichten der Systembetreiber

§ 31
Dokumentationspflicht

[1]Jeder Systembetreiber soll über die erteilten Nutzungsberechtigungen eine Dokumentation führen. [2]Die Vergabe von Telekommunikationsberechtigungen (E-Mails, Rufnummern) ist gemäß dem Telekommunikationsgesetz (TKG) vom 23. Juni 2021 (BGBl. I S. 1858) zu vermerken. [3]Die Unterlagen sind nach Auslaufen der Berechtigung mindestens zwei Jahre aufzubewahren.

§ 32
Prüfpflichten beim Einsatz fremder Software

Jeder Systembetreiber hat, bevor er der Installation fremder, von der Nutzerin oder dem Nutzer gewünschter Software zustimmt, zu prüfen, ob sie im Hinblick auf den Anlagenschutz unbedenklich ist und im Hinblick auf Schutzrechte von der Nutzerin oder dem Nutzer berechtigterweise genutzt werden darf.

§ 33
Vorübergehende Einschränkung der Nutzung

[1]Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutz der Nutzerinnen- oder Nutzerdaten erforderlich ist, kann der Systembetreiber die Nutzung seiner Ressourcen vorübergehend einschränken oder einzelne Nutzerinnen- oder Nutzerkennungen vorübergehend sperren. [2]Sofern möglich, sind die betroffenen Nutzerinnen oder Nutzer hierüber im Voraus zu unterrichten.

§ 34
Vorübergehende Verhinderung der Nutzung

Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass eine Nutzerin oder ein Nutzer auf IT-Systemen rechtswidrige Inhalte zur Nutzung bereithält, kann der Systembetreiber die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.

§ 35
Überprüfung der Sicherheit der System-/Benutzerpasswörter

[1]Die Systembetreiber sind berechtigt, die Sicherheit der System-/Benutzerpasswörter durch automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen, zum Beispiel die Verwendung leicht zu erratender Passwörter zu untersagen. [2]Die betroffenen Nutzerinnen oder Nutzer sind entsprechend zu informieren.

§ 36
Einsicht in Daten und Postfächer

[1]Die Systembetreiber sind berechtigt, unter Beachtung des Datengeheimnisses und der IT-Rahmendienstvereinbarung Einsicht in die von Nutzerinnen oder Nutzern gespeicherten Daten zu nehmen, soweit dies erforderlich ist zur Beseitigung akuter Störungen oder zur Aufklärung und Unterbindung von Missbräuchen, sofern hierfür tatsächliche Anhaltspunkte vorliegen. [2]Eine Einsichtnahme in die Nachrichten- und E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung akuter Störungen im betroffenen Dienst unerlässlich ist. [3]Der Systembetreiber ist berechtigt, zur Behebung oder Vermeidung von Ressourcenengpässen sowie zur Ressourcenplanung statistische Informationen über den verwendeten Speicherplatz zu erheben. [4]In den Fällen der Sätze 1 und 2 ist die Einsichtnahme zu dokumentieren und die betroffene Nutzerin oder der betroffene Nutzer ist nach der Zweckerreichung unverzüglich zu benachrichtigen und umfassend über den Grund und das Ergebnis der Einsichtnahme zu informieren, auch bei ergebnisloser Einsichtnahme.

§ 37
Verbindungs- und Nutzungsdaten

[1]Für Abrechnungszwecke können die Verbindungs- und Nutzungsdaten im Nachrichtenverkehr dokumentiert werden. [2]Es dürfen jedoch nur die näheren Umstände der Telekommunikation – nicht aber die nichtöffentlichen Kommunikationsinhalte – erhoben, verarbeitet und genutzt werden. [3]Die Verbindungs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Telediensten, die der Systembetreiber zur Nutzung bereithält oder zu denen der Systembetreiber den Zugang zur Nutzung

vermittelt, sind frühestmöglich, spätestens unmittelbar am Ende der jeweiligen Nutzung zu löschen.

§ 38
Vorläufige Maßnahmen

[1]Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass eine Nutzerin oder ein Nutzer oder ein Systembetreiber sich

1. strafrechtlich relevant,
2. rechtswidrig,
3. das Ansehen und das Erscheinungsbild der Otto-Friedrich-Universität Bamberg beeinträchtigend,
4. gegen diese Nutzungsrichtlinien verstoßend oder
5. die Sicherheit der IT-Infrastruktur oder Daten der Universität gefährdend

verhält, kann der System- oder Netzbetreiber vorläufige Maßnahmen sowohl hinsichtlich des Inhalts als auch hinsichtlich der Benutzungsberechtigung zur Verhinderung weiterer rechtswidriger, missbräuchlicher oder die IT-Sicherheit gefährdender Nutzung anordnen und vollziehen, bis die Rechtslage hinreichend geklärt ist. [2]Insbesondere kann der IT-Service als Betreiber des Datennetzes der Universität einzelne Geräte oder Netzbereiche vom Datennetz abkoppeln. [3]Die oder der Betroffene ist über die Maßnahmen umgehend zu informieren, sobald dies ohne Gefährdung des Zwecks der Maßnahmen möglich ist. [4]Die Universitätsleitung ist über das Vorliegen derartiger Anhaltspunkte und die Anordnung vorläufiger Maßnahmen unverzüglich zu informieren.

§ 39
Grundsätzliche Pflichten des Systembetreibers

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

(2) Der Systembetreiber ist zur Vertraulichkeit verpflichtet.

(3) Der Systembetreiber gibt die Ansprechpartnerinnen oder Ansprechpartner und für die Betreuung seiner Nutzerinnen oder Nutzer (systembetreuende Stelle, z. B. IT-Service, die für Informationssysteme zuständige Stelle der Universitätsverwaltung, Hochschul-Informations-System HIS eG) bekannt.

(4) Der Systembetreiber ist verpflichtet, im Umgang mit Rechnern und Netzen anderer Betreiber deren Nutzungs- und Zugriffsrichtlinien einzuhalten.

§ 40
Maßnahmen des Systembetreibers

[1]Der Systembetreiber kann Maßnahmen ergreifen, die eine ressourcenschonende Nutzung der IT-Infrastruktur bewirken und den Schutz der Nutzerinnen oder Nutzer vor Störungen erhöhen. [2]Dazu zählen insbesondere

1. die Beschränkung des Speicherplatzes der Nutzerinnen oder Nutzer auf ein den Aufgaben angemessenes Maß,
2. die Bereitstellung oder zentrale Einführung von Verfahren zur sicheren Nutzung der IT-Infrastruktur (z. B. Anti-Viren-Software, Einschränkung oder Sperrung einzelner Dienste, Firewalling),
3. die Bereitstellung von Verfahren zur Unterscheidung zwischen einer Nutzung der IT-Infrastruktur im Sinne von § 2 und einer unberechtigten Nutzung, z. B. durch Bereitstellung von Methoden zur Klassifikation unverlangt zugesandter Daten (Spam-Mail, E-Mail-Anhänge mit ungewöhnlich großem Volumen),
4. die automatische Löschung von Daten, bei denen ein hinreichender Verdacht auf ungerechtfertigte Nutzung vorliegt, sofern der Anwender nicht von selbst geeignete Maßnahmen trifft (z. B. Löschung von als virenbehaftet eingestuften E-Mails und Dateien oder als Spam klassifizierten E-Mails nach einem angemessenen Zeitintervall).

§ 41
Systemspezifische Aufgaben und Pflichten des Systembetreibers

Aufgaben und Pflichten des Systembetreibers aufgrund des Betriebs von IT-Systemen:

1. [1]Systembetreiber müssen systemspezifische Aufgaben und Pflichten übernehmen und die Rechte Dritter beachten. [2]Der IT-Service stellt hierfür Standards, Konzepte, Regelungen, Handlungsempfehlungen, Checklisten und Vorgaben für den technischen Betrieb bereit, die als Mindestmaßnahmen für IT-Systeme mit normalem Schutzbedarf angesehen werden.
2. IT-Systeme, die gemäß § 20 Nr. 2 Informationen und Daten verarbeiten, einen erhöhten Schutzbedarf aufweisen, müssen durch zusätzliche Maßnahmen geeignet geschützt werden.

§ 42
Datenschutzrechtliche Pflichten des Systembetreibers

[1]Der Systembetreiber ist verpflichtet, die gesetzlichen Regelungen zum Datenschutz einzuhalten. [2]Dazu gehören insbesondere:

1. Erfüllung der Nachweis-, Dokumentations- und Rechenschaftspflichten, insbesondere in Form einer Datenschutzerklärung.
2. Umsetzung der Informationspflichten gegenüber Nutzerinnen oder Nutzern.
3. Erstellung einer Beschreibung aller Verarbeitungstätigkeiten und Führung eines Verzeichnisses der Verarbeitungstätigkeiten.
4. Bei Inanspruchnahme der Leistungen externer Dritter Abschluss von Auftragsverarbeitungsverträgen.
5. Meldung von Beeinträchtigungen des Schutzes personenbezogener Daten („Datenschutzverletzungen“).
6. Bei Verarbeitungstätigkeiten mit einem hohen Risiko für Rechte und Freiheiten natürlicher Personen Durchführung einer Datenschutz-Folgenabschätzung.
7. Die Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) darf nur in Abstimmung mit der oder dem Datenschutzbeauftragen erfolgen.

Siebter Abschnitt:
Haftung des Systembetreibers und Haftungsausschluss

§ 43
Haftungsausschluss

(1) [1]Der Systembetreiber und die Otto-Friedrich-Universität Bamberg übernehmen keine Garantie dafür, dass die Systemfunktionen den speziellen Anforderungen der Nutzerin oder des Nutzers entsprechen oder dass das System fehlerfrei und ohne Unterbrechung läuft. [2]Der Systembetreiber und die Otto-Friedrich-Universität Bamberg können eventuelle Datenveränderungen oder -verluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter nicht ausschließen.

(2) [1]Der Systembetreiber und die Otto-Friedrich-Universität Bamberg übernehmen keine Verantwortung für die Richtigkeit der zur Verfügung gestellten Programme. [2]Der Systembetreiber und die Otto-Friedrich-Universität Bamberg haften auch nicht für den Inhalt, insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu welchen sie lediglich den Zugang zur Nutzung vermitteln.

§ 44
Haftungsbegrenzung

[1]Im Übrigen haftet der Systembetreiber bzw. die Otto-Friedrich-Universität Bamberg nur bei Vorsatz oder grober Fahrlässigkeit ihrer Mitarbeiterinnen oder Mitarbeiter, es sei denn, dass eine schuldhafte Verletzung wesentlicher Kardinalpflichten vorliegt. [2]In diesem Fall ist ihre Haftung auf typische, bei Begründung des Nutzungsverhältnisses vorhersehbare Schäden begrenzt, soweit nicht vorsätzliches oder grob fahrlässiges Handeln vorliegt.

§ 45
Amtshaftung

Mögliche Amtshaftungsansprüche gegen den Systembetreiber oder die Otto-Friedrich-Universität Bamberg bleiben von den vorstehenden Regelungen unberührt.

Achter Abschnitt:
Folgen einer missbräuchlichen oder gesetzeswidrigen Nutzung

§ 46
Grundsatz

(1) [1]Bei Verstößen gegen gesetzliche Vorschriften oder gegen die Bestimmungen dieser Nutzungsrichtlinien, insbesondere des Vierten Abschnitts (Pflichten der Nutzerin oder des Nutzers) und des Fünften Abschnitts (Anwendungsspezifische Regeln und Pflichten der Nutzerin oder des Nutzers), kann der Systembetreiber bzw. die Otto-Friedrich-Universität Bamberg die Nutzungsberechtigung einschränken, ganz oder teilweise entziehen. [2]Es ist dabei unerheblich, ob der Verstoß einen materiellen Schaden zur Folge hatte oder nicht.

(2) Bei schwerwiegenden oder wiederholten Verstößen kann eine Nutzerin oder ein Nutzer auf Dauer von der Nutzung sämtlicher IT-Ressourcen nach § 1 ausgeschlossen werden.

§ 47
Weitere Maßnahmen

[1]Verstöße gegen gesetzliche Vorschriften oder gegen die Bestimmungen dieser Nutzungsrichtlinien werden auf ihre strafrechtliche Relevanz sowie auf zivilrechtliche Ansprüche hin überprüft. [2]Bedeutsam erscheinende Sachverhalte werden der jeweiligen Rechtsabteilung übergeben, die die Einleitung weiterer geeigneter Schritte prüft. [3]Die

Otto-Friedrich-Universität Bamberg behält sich die Verfolgung strafrechtliche Schritte sowie zivilrechtlicher Ansprüche ausdrücklich vor.

Neunter Abschnitt:
Sonstige Regelungen

§ 48
Leistungen des ITS

Die Leistungen des IT-Services können gesondert festgelegt werden.

§ 49
Gebührenfestsetzung

Für die Nutzung der IT-Ressourcen können durch Satzung der Universität Gebühren festgelegt werden.

§ 50
Systemspezifische Regelungen

Für bestimmte Systeme können bei Bedarf ergänzende oder abweichende Nutzungsregelungen festgelegt werden.

§ 51
Weitergehende Regelungen der Universität

Die IT-Rahmendienstvereinbarung, die Leitlinie zum Notfallmanagement, die Ordnung zum Geschäftsgang und das IT-Sicherheitskonzept der Otto-Friedrich-Universität Bamberg sind zu beachten.

§ 52
Beschwerden

[1]Bei berechtigten Beschwerden von Nutzerinnen oder Nutzern ist durch den Systembetreiber zu prüfen, ob diesen abgeholfen werden kann. [2]Soweit dies nicht der Fall ist, sind die Beschwerden zusammen mit einem Entscheidungsvorschlag des zuständigen Systembetreibers durch dessen Leitung über den Chief Information Office (CIO) der Universitätsleitung zur Beratung und Entscheidung vorzulegen.

§ 53
Gerichtsstand

Gerichtsstand für alle aus dem Nutzungsverhältnis erwachsenden rechtlichen Ansprüche ist Bamberg.

Zehnter Abschnitt:
Schlussbestimmungen

§ 54
Inkrafttreten

[1]Diese Richtlinien treten am 11. Juli 2024 in Kraft. [2]Gleichzeitig treten die Richtlinien in der Fassung des Senatsbeschlusses vom 1. April 2020 außer Kraft.

Otto-Friedrich-Universität Bamberg

Bamberg, 10. Juli 2024

gez.

Prof. Dr. Kai Fischbach
Präsident

Anlage: Umgang mit Dokumenten

Tabelle 1

Wie wird gekennzeichnet?	öffentlich	nur für den Dienstgebrauch bzw. intern	vertraulich bzw. persönlich	geheim
Kennzeichnung von Informationen in Papierform	Explizit mit „öffentlich“	Keine oder Explizit mit „nur für den Dienstgebrauch“ bzw. „intern“	Explizit mit „vertraulich“ bzw. „persönlich“	Explizit mit „geheim“
Kennzeichnung von elektronischen Informationen	Explizit mit „öffentlich“ oder durch Freigabe im Intranet	Explizit mit „nur für den Dienstgebrauch“ bzw. „intern“ oder durch Freigabe im Intranet	Explizit mit „vertraulich“ bzw. „persönlich“	Explizit mit „geheim“

Tabelle 2

Was mache ich bei ...?		öffentlich	nur für den Dienst-gebrauch bzw. intern	vertraulich bzw. persönlich	geheim
Vervielfältigung mittels Kopierer, Drucker		Keine Einschränkungen	Keine Einschränkungen	Beaufsichtigung des Vervielfältigungsvorgangs	Nur nach Freigabe durch die Informationsverantwortliche oder den Informationsverantwortlichen Beaufsichtigung des Vervielfältigungsvorgangs
Weitergabe		Keine Einschränkungen	An alle Mitglieder der Otto-Friedrich-Universität Bamberg oder an externe Stellen – sofern dienstlich benötigt	Weitergabe an von der oder von dem Informations-verantwortlichen definierte Nutzerinnen oder Nutzer (namentlich oder Rollen), sofern dienstlich benötigt Bei externen Stellen muss eine Vertraulichkeits-vereinbarung vorliegen	Weitergabe an namentlich von der oder von dem Informationsverantwortlichen definierte Nutzerinnen oder Nutzer Von der Empfängerin oder von dem Empfänger dürfen geheime Informationen nur nach expliziter Freigabe der oder des Informationsverantwortlichen weitergegeben werden Bei externen Stellen muss eine Vertraulichkeitsvereinbarung vorliegen
Übermittlung auf dem Postweg	**Intern**	Keine Einschränkungen	Umschlag für inneramtliche Dienstpost	Umschlag für inneramtliche Dienstpost mit Klebestreifen verschließen und	Kuvertierung doppelt ausführen Inneres Kuvert: Verschlossener Briefumschlag mit Stempelung „persönlich“ und darauf Handzeichen anbringen

Was mache ich bei ...?		öffentlich	nur für den Dienst-gebrauch bzw. intern	vertraulich bzw. persönlich	geheim
				darauf Handzeichen anbringen Bei Risiko der Öffnung durch unbefugte Kuvertierung doppelt ausführen	Äußeres Kuvert: Umschlag für inneramtliche Dienstpost. Dieser darf keinen Hinweis auf die Vertraulichkeit enthalten
	Extern	Keine Einschränkungen	Normaler Brief	Normaler Brief Empfängerin oder Empfänger mit Zusatz „persönlich“ benennen	Per Übergabe-Einschreiben oder Kuriersendung Empfängerin oder Empfänger mit Zusatz „persönlich“ benennen Kuvertierung doppelt ausführen Die innere ist mit der Kennzeichnung der Vertraulichkeitsklasse zu versehen, die äußere darf keinen Hinweis auf die Vertraulichkeit enthalten
Übermittlung per E-Mail	**Intern**	Keine Einschränkungen	Keine Einschränkungen	Mit der Nachrichtenoption „Vertraulich“ zu versenden	Mit der Nachrichtenoption „Vertraulich“ zu versenden
	Extern	Keine Einschränkungen	Keine Einschränkungen	Der Inhalt der E-Mail ist mit S/MIME zu verschlüsseln	Der Inhalt der E-Mail ist mit S/MIME zu verschlüsseln

Was mache ich bei ...?		öffentlich	nur für den Dienst-gebrauch bzw. intern	vertraulich bzw. persönlich	geheim
Übermittlung per Fax	**Intern**	Keine Einschränkungen	Keine Einschränkungen	Nur nach Vorankündigung	Nur nach Vorankündigung
	Extern	Keine Einschränkungen	Deckblatt mit Anzahl der Seiten	Nur nach Vorankündigung	Verboten
Übermittlung per Messenger	**Interner Dienst**	Keine Einschränkungen	Keine Einschränkungen	Identität der Empfängerin oder des Empfängers sicherstellen	Identität der Empfängerin oder des Empfängers sicherstellen
	Externer Dienst	Keine Einschränkungen	Der Inhalt der Nachricht ist Ende-zu-Ende zu verschlüsseln Identität des Empfängers sicherstellen	Der Inhalt der Nachricht ist Ende-zu-Ende zu verschlüsseln Identität der Empfängerin oder des Empfängers sicherstellen	Der Inhalt der Nachricht ist Ende-zu-Ende zu verschlüsseln Identität der Empfängerin oder des Empfängers sicherstellen
Verbale Weitergabe		Keine Einschränkungen	Nur erlaubt, wenn keine Unberechtigten zuhören können	Nur erlaubt, wenn keine Unberechtigten zuhören können	Nur erlaubt, wenn keine Unberechtigten zuhören können Nicht auf Anrufbeantworter oder Voicemailbox hinterlassen Identität der Gesprächspartnerin oder des Gesprächspartners sicherstellen

Was mache ich bei ...?	öffentlich	nur für den Dienst-gebrauch bzw. intern	vertraulich bzw. persönlich	geheim
Vernichtung von Informationen in Papierform	Keine Einschränkungen	Papierkörbe am Arbeitsplatz (nicht bei personenbezogenen Daten)	Schreddern	Schreddern

Tabelle 3

Informationen in IT-Systemen	öffentlich	nur für den Dienstgebrauch bzw. intern	vertraulich bzw. persönlich	geheim
Speicherung in IT-Systemen/ Anwendungen der Otto-Friedrich-Universität Bamberg	Keine Einschränkungen	Speicherung unter Berücksichtigung der Zugriffsrechte, ggf. explizite Vergabe von Zugriffsrechten	Speicherung unter Berücksichtigung der Zugriffsrechte, ggf. explizite Vergabe von Zugriffsrechten	Speicherung unter Berücksichtigung der Zugriffsrechte, ggf. explizite Vergabe von Zugriffsrechten Regelmäßige Prüfung der aktuellen Zugriffsrechte

Informationen in IT-Systemen	öffentlich	nur für den Dienstgebrauch bzw. intern	vertraulich bzw. persönlich	geheim
Mobile Geräte (z. B.: Notebooks, Smartphones, Tablets)	Keine Einschränkungen	Keine Einschränkungen	Bei Notebooks Verschlüsselung erforderlich Bei anderen mobilen Geräten Speicherung vertraulicher Daten vermeiden	Grundsätzlich verboten Ausnahmen im Einzelfall unter Mitwirkung der oder des Datenschutzbeauftragten bzw. der oder des Geheimschutz-beauftragten möglich. In diesen Fällen ist die Verschlüsselung der Informationen erforderlich
Mobile Datenträger (z .B.: CD, DVD, USB-Stick)	Keine Einschränkungen	Keine Einschränkungen	Verschlüsselung erforderlich	Grundsätzlich verboten Ausnahmen im Einzelfall unter Mitwirkung der oder des Datenschutzbeauftragten bzw. der oder des Geheimschutz-beauftragten möglich. In diesen Fällen ist die Verschlüsselung der Informationen erforderlich

Informationen in IT-Systemen	öffentlich	nur für den Dienstgebrauch bzw. intern	vertraulich bzw. persönlich	geheim
Bereitstellung im Internet	Keine Einschränkungen	Verboten	Verboten	Verboten
Löschen von elektronischen Informationen	Keine Einschränkungen	Löschen in Filesystem	Löschen in Filesystem	Löschen in Filesystem
Entsorgung/Vernichtung von Hardware und mobilen Datenträgern	Keine Einschränkungen	Abgabe bei Dezernat Z/IS oder PC-Service (IT-Service) Mobile Datenträger: physische Vernichtung	Abgabe bei Dezernat Z/IS oder PC-Service (IT-Service) zur Vernichtung	Abgabe bei Dezernat Z/IS oder PC-Service (IT-Service) zur Vernichtung

Tabelle 4

Physische Aufbewahrung und Ablage von Informationen	öffentlich	nur für den Dienstgebrauch bzw. intern	vertraulich bzw. persönlich	geheim
Allgemein	Keine Einschränkungen	Unbefugten Zugriff durch Dritte über einfache Mittel verhindern. Eine angemessene technische Umsetzung ist durch die Informations-verantwortliche oder	Unbefugten Zugriff durch Dritte verhindern. Eine angemessene technische Umsetzung ist durch die Informationsverantwortliche oder den Informations-verantwortlichen im Einzelfall in Abhängigkeit	Unbefugten Zugriff durch Dritte verhindern. Eine angemessene technische Umsetzung ist durch die Informationsverantwortliche oder den Informations-verantwortlichen im Einzelfall in Abhängigkeit

Physische Aufbewahrung und Ablage von Informationen	öffentlich	nur für den Dienstgebrauch bzw. intern	vertraulich bzw. persönlich	geheim
		den Informations-verantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten	von den Gefährdungen zu gewährleisten	von den Gefährdungen zu gewährleisten
In Gebäuden der Otto-Friedrich-Universität Bamberg	Keine Einschränkungen	Absperren des Raums wo möglich Bei physisch extra abgesicherten Bereichen sind Sonderregelungen möglich	Absperren des Raums, wo möglich Falls gewährleistet ist, dass niemand außer der Schlüsselbesitzerin oder dem Schlüsselbesitzer das Büro betreten kann, ist diese Maßnahme ausreichend Sonst: Wegsperren der Informationen Bei physisch abgesicherten Bereichen sind Sonderregelungen möglich	Absperren des Raums, wo möglich Falls gewährleistet ist, dass niemand außer der Schlüsselbesitzerin oder dem Schlüsselbesitzer das Büro betreten kann, ist diese Maßnahme ausreichend Sonst: Wegsperren der Informationen
Unterwegs oder Zuhause	Keine Einschränkungen	Abgesperrter Raum	Vor Zugriff sicher ausbewahren (Verschlüsselung und Wegsperren)	Vor Zugriff sicher ausbewahren (Verschlüsselung und Wegsperren)