Otto-Friedrich-Universität Bamberg

Nutzungsrichtlinien
für Informationsverarbeitungssysteme
der Otto-Friedrich-Universität Bamberg
Vom 1. April 2020

- Beschlossen vom Senat der Otto-Friedrich-Universität Bamberg
in seiner Sitzung am 5. Februar 2020 -

Inhaltsverzeichnis

Präambel

[1]Die Otto-Friedrich-Universität Bamberg und ihre Einrichtungen („Betreiber“ oder „Systembetreiber“) betreiben eine Informationsverarbeitungs-Infrastruktur (IV-Infrastruktur), bestehend aus Hardware- und Softwaresystemen (Rechnern), Kommunikationssystemen (Netzen) und weiteren Hilfseinrichtungen der Informationsverarbeitung. [2]Die IV-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 IV-Infrastruktur auf,
- weisen hin auf zu wahrende Rechte Dritter (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.

§ 1
Geltungsbereich

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

§ 2
Nutzerinnen- oder Nutzerkreis und Aufgaben

(1) Die in § 1 genannten IV-Ressourcen stehen den Mitgliedern der Otto-Friedrich-Universität Bamberg zur Erfüllung ihrer in Art. 2 des Bayerischen Hochschulgesetzes vom 23. Mai 2006 (GVBl. S. 245, BayRS 2210-1-1-WK), das zuletzt durch § 1 Abs. 186 der Verordnung vom 26. März 2019 (GVBl. S. 98) geändert worden ist, beschriebenen Aufgaben zur Verfügung, insbesondere für Forschung, Lehre, Förderung des wissenschaftlichen Nachwuchses, Aus- und Weiterbildung, Öffentlichkeitsarbeit, Verwaltung und Bibliothek.

(2) 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.

§ 3
Formale Nutzungsberechtigung

(1) [1]Wer IV-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.

(2) Systembetreiber sind für

a) zentrale Systeme das Rechenzentrum sowie das Dezernat Informationssysteme (Z/IS),

b) dezentrale Systeme die zuständigen organisatorischen Einheiten (Fakultäten, zentrale Einrichtungen, Betriebseinheiten, Lehrstühle und weitere Untereinheiten) der Otto-Friedrich-Universität Bamberg.

(3) [1]Der Antrag auf eine formale Nutzungsberechtigung soll folgende Angaben enthalten:

- Systembetreiber, bei dem die Nutzungsberechtigung beantragt wird;
- Systeme, für welche die Nutzungsberechtigung beantragt wird;

- Antragstellerin oder Antragsteller: Name, Adresse, Geburtstag, Geburtsort, Telefonnummer (bei Studierenden auch Matrikelnummer) und eventuelle Zugehörigkeit zu einer organisatorischen Einheit der Otto-Friedrich-Universität Bamberg;
- überschlägige Angaben zum Zweck der Nutzung, beispielsweise Forschung, Ausbildung/Lehre, Verwaltung;
- die Erklärung, dass die Nutzerin oder der Nutzer die Nutzungsrichtlinien anerkennt;
- Einträge für Informationsdienste der Otto-Friedrich-Universität Bamberg;
- Einverständniserklärung der Nutzerin oder des Nutzers zur Verarbeitung ihrer oder seiner personenbezogenen Daten;
- 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 (§ 5).

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

(4) [1]Über den Antrag entscheidet der zuständige Systembetreiber. [2]Er kann die Erteilung der Nutzungsberechtigung vom Nachweis bestimmter Kenntnisse über die Nutzung der Anlage abhängig machen.

(5) [1]Die Nutzungsberechtigung darf ganz oder teilweise versagt, widerrufen oder nachträglich beschränkt werden, insbesondere wenn

a) kein ordnungsgemäßer Antrag vorliegt oder die Angaben im Antrag nicht oder nicht mehr zutreffen,

b) nicht gewährleistet erscheint, dass die Antragstellerin oder der Antragsteller ihren oder seinen Pflichten als Nutzerin oder Nutzer nachkommen wird,

c) die Kapazität der IV-Ressourcen, deren Nutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die beabsichtigten Arbeiten nicht ausreicht,

d) das Vorhaben nicht mit den Zwecken nach § 4 Abs. 1 vereinbar ist,

e) die IV-Ressourcen für die beabsichtigte Nutzung offensichtlich ungeeignet oder für spezielle Zwecke reserviert sind,

f) die zu benutzenden IV-Ressourcen an ein Netz angeschlossen sind, das besonderen Datenschutzanforderungen genügen muss und kein sachlicher Grund für diesen Zugriffswunsch ersichtlich ist,

g) 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.

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

(7) [1]Der Systembetreiber kann, falls erforderlich, Dienstanweisungen erlassen. [2]Dienstanweisungen für zentrale Systeme bedürfen der Zustimmung des Senats.

§ 4
Pflichten der Nutzerin oder des Nutzers

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

(2) [1]Die Nutzerin oder der Nutzer ist verpflichtet, darauf zu achten, dass sie oder er die vorhandenen IV-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 IV-Infrastruktur oder bei anderen Nutzerinnen oder Nutzern verursachen oder den ordnungsgemäßen Betrieb der IV-Ressourcen beeinträchtigen kann. [3]Zuwiderhandlungen können Schadenersatzansprüche begründen (§ 7).

(3) 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, und zwar auch dann, wenn diese Aktionen durch Dritte vorgenommen werden, denen sie oder er fahrlässig oder vorsätzlich schuldhaft den Zugang ermöglicht hat.

a) [1]Die Weitergabe von Kennungen, Schlüsseln und Passwörtern ist grundsätzlich nicht gestattet. [2]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.

b) Der Zugang zu den IV-Ressourcen ist durch ein geheim zu haltendes Passwort oder ein gleichwertiges Verfahren zu schützen.

c) Die Nutzerin oder der Nutzer hat Vorkehrungen zu treffen, um unberechtigten Dritten den Zugang zu den IV-Ressourcen zu verwehren; dazu gehört es insbesondere, einfache, naheliegende Passwörter zu meiden, die Passwörter regelmäßig zu ändern und das Logout nicht zu vergessen.

(4) [1]Die Nutzerin oder der Nutzer hat jegliche Art der missbräuchlichen Nutzung der IV- Infrastruktur zu unterlassen. [2]Sie bzw. er ist insbesondere dazu verpflichtet,

a) ausschließlich mit Nutzerinnen- oder Nutzerkennungen, Schlüsseln und Passwörtern zu arbeiten, deren Nutzung ihr oder ihm gestattet wurde,

b) bei der Nutzung von Software (Quellen, Objekte), Dokumentationen und anderen Daten die gesetzlichen Regelungen (Urheberrechtsschutz, Copyright) einzuhalten,

c) 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,

d) 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,

e) 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,

f) 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.

g) keine privaten Datenträger und Software ohne Virenschutzprogramm auf universitätseigenen Datenverarbeitungsgeräten (DV-Geräten) zu verwenden.

[3]Zuwiderhandlungen können Schadenersatzansprüche begründen (§ 7). [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.

(5) [1]Die IV-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:

a) Ausforschen fremder Passwörter, Ausspähen von Daten (§ 202a – Strafgesetzbuch – StGB – in der Fassung der Bekanntmachung vom 13. November 1998 – BGBl. I S. 3322),

b) Abfangen von Daten (§ 202b StGB),

c) Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB),

d) Datenhehlerei (202d StGB),

e) unbefugtes Verändern, Löschen, Unterdrücken oder Unbrauchbarmachen von Daten (§ 303a StGB),

f) Computersabotage (§ 303b StGB) und Computerbetrug (§ 263a StGB),

g) die Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB), die Verwendung von Kennzeichen verfassungswidriger Organisationen (§ 86a StGB) und Volksverhetzung (§ 130 StGB),

h) die Verbreitung pornographischer Schriften (§ 184 StGB) und gewalt- oder tierpornographischer Schriften (§ 184a StGB),

i) die Verbreitung, Erwerb und Besitz kinderpornographischer Schriften (§ 184b StGB) und jugendpornografischer Schriften (§ 184c StGB),

j) 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. § 7).

(6) [1]Der Nutzerin oder dem Nutzer 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.

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

(7) [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 des Datenschutzgesetzes ergeben.

(8) Die Nutzerin oder der Nutzer ist verpflichtet,

a) die vom Systembetreiber zur Verfügung gestellten Leitfäden zur Nutzung zu beachten,

b) bei elektronischen Veröffentlichungen Folgendes zu beachten:

- die Pflichten zur Anbieterkennzeichnung (Impressum) nach § 5 Telemediengesetz (TMG) vom 26. Februar 2007 (BGBl. I S. 179),
- die Pflichten zur Vorab-Information (Datenschutz-Erklärung, Online-Datenschutz Prinzipien, privacy policy) nach § 13 Abs. 1 TMG wie zum Beispiel Angaben zur Speicherung von Zugriffsdaten, zur Verwendung von Cookies und aktiven Elementen,
- die Sicherstellungspflichten nach § 13 Abs. 4 TMG wie zum Beispiel Angebot von Verschlüsselungsmethoden und
- die Anzeigepflicht für externe Links nach § 13 Abs. 5 TMG,

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

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

a) 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, das Ausschalten der Beleuchtung und das Schließen der Fenster und Türen beim Verlassen der Räume.

b) Papierdokumente mit vertraulichen oder personenbezogenen Daten, die nicht mehr benötigt werden oder einer Löschpflicht unterliegen, sind fachgerecht zu schreddern.

c) An Druckern, Kopier- und Faxgeräten sollen keine vertraulichen Informationen hinterlassen werden.

d) Passwörter und Zugangsinformationen sind nicht am Arbeitsplatz aufzubewahren.

e) Rechner sind zu sperren, wenn der Arbeitsplatz für längere Zeit verlassen wird.

(10) Sorgfaltspflicht bei der Verarbeitung sensibler Daten (siehe Anlage)

a) 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.

b) 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 hat besondere Vorsicht zu walten.

(11) [1]Eine die Sicherheit der Informationstechnologie-Systeme (IT-Systeme) gefährdende Nutzung der IT-Infrastruktur ist untersagt. [2]Insbesondere dürfen

a) sicherheitsrelevante Einstellungen oder Systemkomponenten wie Firewalls, Virenschutzprogramme oder Aktualisierungsmechanismen nicht deaktiviert oder umgangen werden,

b) keine Software-Produkte, Apps oder Plugins installiert werden, die aus unsicheren Quellen stammen oder bei denen eine Sicherheitsgefährdung nicht auszuschließen ist, im Zweifel ist der zuständige Systembetreiber hinzuziehen.

(12) Anwendungsspezifische Regeln und Pflichten

a) Drucker, Kopierer- und Multifunktionsgeräte

- Wireless-Local-Area-Network-Schnittstellen (WLAN-Schnittstellen) sind zu deaktivieren, um Beeinträchtigungen auf das universitäre WLAN zu vermeiden.
- Nicht benötigte Schnittstellen und Protokolle sind zu deaktivieren.
- Beim Drucken oder Kopieren von Daten gemäß Abs. 10 lit. b ist besonders darauf zu achten, dass die Daten nicht versehentlich Unbefugten zugänglich werden.

b) Cloud-Nutzung, Nutzung externer Dienstleister

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

- Vorrangig sind für die Speicherung und Verarbeitung von dienstlichen Daten die von der Otto-Friedrich-Universität Bamberg bereitgestellten Systeme zu nutzen.
- Eine Speicherung und Verarbeitung von Informationen gemäß Abs. 10 lit. b ist in nicht von der Otto-Friedrich-Universität Bamberg freigegebenen Cloud-Speicher-Diensten grundsätzlich nicht gestattet.
- Die dienstlichen Zugangsdaten dürfen nicht bei Dritten verwendet oder hinterlegt werden.

- Die automatisierte Weiterleitung von dienstlichen Daten (beispielsweise als E-Mail-Weiterleitung an eine private Adresse) ist untersagt.

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

- Für dienstliche Telefonie und Fax-Nachrichten sind grundsätzlich ausschließlich die von der Otto-Friedrich-Universität Bamberg bereitgestellten Systeme zu nutzen.
- Internettelefonie-Software darf nur für Zwecke verwendet werden, bei denen keine Informationen gemäß Abs. 10 lit. b ausgetauscht werden.

d) Arbeit an anderen Orten/Telearbeit

- Arbeitsplätze an Orten außerhalb der Otto-Friedrich-Universität Bamberg müssen den arbeitsschutzrechtlichen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen genügen.
- Dokumente und Daten dürfen nur mitgeführt oder außerhalb der Otto-Friedrich-Universität Bamberg aufbewahrt werden, wenn sie vor dem Zugriff Dritter geschützt sind.
- Der elektronische Austausch von Daten zwischen Beschäftigungsstelle und Telearbeitsplatz darf nur über eine von der Otto-Friedrich-Universität Bamberg freigegebene Schnittstelle erfolgen.

e) Server

- Verbindungen zu Servern (z. B. zu Terminalservern) dürfen nur nach Aktivierung eines aktuellen Virenschutzprogramms auf dem Client aufgebaut werden.
- Betriebssysteme müssen auf aktuellem Stand sein. Alle Sicherheitsupdates und Patches von Herstellern müssen installiert sein.
- Die Firewall des Betriebssystems muss aktiviert sein.

f) Zugriff auf Intranet vom Internet

- [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 Rechenzentrum angebotene oder genehmigte Dienste genutzt werden. [3]Das Rechenzentrum veröffentlicht zulässige Dienste in seinem Dienstleistungskatalog. [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 das Rechenzentrum genehmigt hat.
- [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.

g) WLAN

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

- 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.
- Installation und Betrieb der WLAN-Komponenten liegen in der Verantwortung des Rechenzentrums.
- Bei Verwendung von öffentlichen unverschlüsselten Zugangspunkten (WLAN-Hotspots) muss der Übertragungsweg über geeignete Maßnahmen anderweitig geschützt werden (Virtual Private Network – VPN, Verschlüsselung auf Anwendungsebene).
- Die WLAN-Einwahl in das universitäre WLAN darf nur nach Aktivierung eines aktuellen Virenschutzprogramms auf dem Client aufgebaut werden.

h) Mobile IT-Nutzung

- [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), die zuletzt durch Bekanntmachung vom 24. April 2018 (GVBl. S. 281) geändert worden ist, ist zu beachten.
- [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.
- Die Weitergabe von dienstlich genutzten Geräten an Dritte oder Fremde ist nicht zulässig.
- Mobile Geräte sind permanent zu beaufsichtigen oder physisch zu sichern.
- Der Verlust eines dienstlich genutzten Geräts ist umgehend zu melden (vgl. Abs. 13 lit. a).
- Die Zugangsdaten zu den Diensten der Otto-Friedrich-Universität sind bei Verlust eines Geräts umgehend zu ändern.
- [1]Es ist sicherzustellen, dass bei Verlust keine dienstlichen Daten ausgelesen werden können. [2]Daten gemäß Abs. 10 lit. b sind angemessen zu schützen.

- Sämtliche unbenötigten Schnittstellen (WLAN, Universal Serial Bus – USB, Bluetooth, Infrarot etc.) sind permanent bzw. nach einer erforderlichen Nutzung zu deaktivieren.
- Die Übermittlung von Telemetrie-Daten an Cloud-Dienste ist auf das notwendige Maß zu beschränken.

(13) Sicherheits- und Datenschutzvorfälle („Datenschutzverletzungen“)

Die Richtlinie zur Behandlung von Sicherheitsvorfällen ist zu beachten.

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

b) Gegenmaßnahmen dürfen erst nach Aufforderung durch Berechtigte ergriffen werden.

c) Alle Begleitumstände sind durch die Betroffenen ungeschönt, offen und transparent zu erläutern, um damit zur Schadensminderung beizutragen.

d) Informationen über den Sicherheitsvorfall dürfen nicht unautorisiert an Dritte weitergegeben werden.

§ 5
Aufgaben, Rechte und Pflichten der Systembetreiber

(1) [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 22. Juni 2004 (BGBl. I S. 1190) zu vermerken. [3]Die Unterlagen sind nach Auslaufen der Berechtigung mindestens zwei Jahre aufzubewahren.

(2) 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.

(3) [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.

(4) 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.

(5) [1]Der Systembetreiber und das Rechenzentrum sind berechtigt, die Sicherheit der System-/Benutzerpasswörter und der von Nutzerinnen oder Nutzern gespeicherten Daten durch regelmäßige manuelle und automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen, zum Beispiel Änderungen leicht zu erratender Passwörter, durchzuführen, um die DV-Ressourcen und die von Nutzerinnen oder Nutzern gespeicherten Daten vor unberechtigten Zugriffen Dritter zu schützen. [2]Die betroffenen Nutzerinnen oder Nutzer sind hiervon unverzüglich in Kenntnis zu setzen.

(6) Der jeweilige Systembetreiber ist nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der IV-Systeme durch die einzelnen Nutzerinnen oder Nutzer 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 Nutzerinnen und Nutzer,

d) zu Abrechnungszwecken,

e) für das Erkennen und Beseitigen von Störungen sowie

f) zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung; sofern der Grund für die Dokumentation und Auswertung nicht mehr gegeben ist, sind diese Daten sofort zu löschen.

(7) [1]Unter den Voraussetzungen von Abs. 6 ist der Systembetreiber auch berechtigt, unter Beachtung des Datengeheimnisses Einsicht in die von Nutzerinnen oder Nutzern gespeicherten Daten zu nehmen, soweit dies erforderlich ist zur Beseitigung aktueller 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 aktueller Störungen im Nachrichtendienst unerlässlich ist. [3]In jedem Fall ist die Einsichtnahme zu dokumentieren und die betroffene Nutzerin oder der betroffene Nutzer ist nach der Zweckerreichung unverzüglich zu benachrichtigen.

(8) [1]Unter den Voraussetzungen von Abs. 6 können auch die Verbindungs- und Nutzungsdaten im Nachrichtenverkehr (insbesondere E-Mail-Nutzung) 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, soweit es sich nicht um Abrechnungsdaten handelt.

(9) [1]Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass eine Nutzerin oder ein Nutzer sich

a) strafrechtlich relevant,

b) rechtswidrig,

c) das Ansehen und das Erscheinungsbild der Otto-Friedrich-Universität Bamberg beeinträchtigend,

d) gegen diese Nutzungsrichtlinien verstoßend verhält, kann der Systembetreiber vorläufige Maßnahmen sowohl hinsichtlich des Inhalts als auch hinsichtlich der Benutzungsberechtigung zur Verhinderung weiterer rechtswidriger oder missbräuchlicher Nutzung anordnen und vollziehen, bis die Rechtslage hinreichend geklärt ist; die oder der Betroffene ist über die Maßnahmen umgehend zu informieren, sobald dies ohne Gefährdung des Zwecks der Maßnahmen möglich ist; die Universitätsleitung ist über das Vorliegen derartiger Anhaltspunkte und die Anordnung vorläufiger Maßnahmen unverzüglich zu informieren.

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

(11) Der Systembetreiber ist zur Vertraulichkeit verpflichtet.

(12) Der Systembetreiber gibt die Ansprechpartnerinnen oder Ansprechpartner und für die Betreuung seiner Nutzerinnen oder Nutzer (systembetreuende Stelle, z. B. Rechenzentrum, die für Informationssysteme zuständige Stelle der Universitätsverwaltung, HIS GmbH) bekannt.

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

(14) [1]Der Systembetreiber kann Maßnahmen ergreifen, die eine ressourcenschonende Nutzung der IV-Infrastruktur bewirken und den Schutz der Nutzerinnen oder Nutzer vor Störungen erhöhen. [2]Dazu zählen insbesondere

a) die Beschränkung des Speicherplatzes der Nutzerinnen oder Nutzer auf ein den Aufgaben angemessenes Maß,

b) die Bereitstellung oder zentrale Einführung von Verfahren zur sicheren Nutzung der IV-Infrastruktur (z. B. Anti-Viren-Software, Einschränkung oder Sperrung einzelner Dienste, Firewalling),

c) die Bereitstellung von Verfahren zur Unterscheidung zwischen einer Nutzung der IV-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),

d) 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).

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

a) [1]Systembetreiber müssen systemspezifische Aufgaben und Pflichten übernehmen und die Rechte Dritter beachten. [2]Das Rechenzentrum 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.

b) IT-Systeme, die gemäß § 4 Abs. 10 lit. b

- Informationen und Daten verarbeiten,
- einen erhöhten Schutzbedarf aufweisen,

müssen durch zusätzliche Maßnahmen geeignet geschützt werden.

(16) [1]Der Systembetreiber ist verpflichtet, die gesetzlichen Regelungen zum Datenschutz einzuhalten. [2]Dazu gehören insbesondere:

a) Erfüllung der Nachweis-, Dokumentations- und Rechenschaftspflichten, insbesondere in Form einer Datenschutzerklärung.

b) Umsetzung der Informationspflichten gegenüber Nutzerinnen oder Nutzern.

c) Erstellung einer Beschreibung aller Verarbeitungstätigkeiten und Führung eines Verzeichnisses der Verarbeitungstätigkeiten.

d) Bei Inanspruchnahme der Leistungen externer Dritter Abschluss von Auftragsverarbeitungsverträgen.

e) Meldung von Beeinträchtigungen des Schutzes personenbezogener Daten („Datenschutzverletzungen“).

f) Bei Verarbeitungstätigkeiten mit einem hohen Risiko für Rechte und Freiheiten natürlicher Personen Durchführung einer Datenschutz-Folgenabschätzung.

g) Die Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) darf nur nach Freigabe durch die Datenschutzbeauftragte oder den Datenschutzbeauftragen erfolgen.

[3]Das Datenschutzkonzept der Otto-Friedrich-Universität Bamberg ist zu beachten.

§ 6
Haftung des Systembetreibers und 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.

(3) [1]Im Übrigen haften 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.

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

§ 7
Folgen einer missbräuchlichen oder gesetzeswidrigen Nutzung

(1) [1]Bei Verstößen gegen gesetzliche Vorschriften oder gegen die Bestimmungen dieser Nutzungsrichtlinien, insbesondere des § 4 (Pflichten der Nutzerin oder des Nutzers), können 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 IV-Ressourcen nach § 1 ausgeschlossen werden.

(3) [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.

§ 8
Sonstige Regelungen

(1) Die Leistungen des Rechenzentrums können gesondert festgelegt werden.

(2) Für die Nutzung der IV-Ressourcen können in gesonderten Ordnungen Gebühren festgelegt werden.

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

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

(5) [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.

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

§ 9
Inkrafttreten

[1]Diese Richtlinien treten am 1. April 2020 in Kraft. [2]Gleichzeitig treten die Richtlinien in der Fassung des Senatsbeschlusses vom 10. September 2008 außer Kraft.

Bamberg, 1. April 2020

gez.

Prof. Dr. Dr. habil. Godehard Ruppert
Präsident

Anlage: Umgang mit Dokumenten

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“

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 Informations-verantwortliche oder den Informations-verantwortlichen 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 darauf Handzeichen anbringen Bei Risiko der Öffnung durch unbefugte	Kuvertierung doppelt ausführen Inneres Kuvert: Verschlossener Briefumschlag mit Stempelung „persönlich“ und darauf Handzeichen anbringen Äußeres Kuvert:

Was mache ich bei ...?		öffentlich	nur für den Dienst-gebrauch bzw. intern	vertraulich bzw. persönlich	geheim
				Kuvertierung doppelt ausführen	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
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

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

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
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 Geheimschutzbeauftragten 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 Geheimschutzbeauftragten möglich. In diesen Fällen ist die Verschlüsselung der Informationen erforderlich
Bereitstellung im Internet	Keine Einschränkungen	Verboten	Verboten	Verboten
Löschen von elektronischen Informationen	Keine Einschränkungen	Löschen in Filesystem	Löschen in Filesystem	Löschen in Filesystem

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

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 den Informationsverantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten	Unbefugten Zugriff durch Dritte verhindern. Eine angemessene technische Umsetzung ist durch die Informationsverantwortliche oder den Informations-verantwortlichen im Einzelfall in Abhängigkeit von den Gefährdungen zu gewährleisten	Unbefugten Zugriff durch Dritte verhindern. Eine angemessene technische Umsetzung ist durch die Informationsverantwortliche oder den Informations-verantwortlichen im Einzelfall in Abhängigkeit 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	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

Physische Aufbewahrung und Ablage von Informationen	öffentlich	nur für den Dienstgebrauch bzw. intern	vertraulich bzw. persönlich	geheim
			Bei physisch abgesicherten Bereichen sind Sonderregelungen möglich	
Unterwegs oder Zuhause	Keine Einschränkungen	Abgesperrter Raum	Vor Zugriff sicher ausbewahren (Verschlüsselung und Wegsperren)	Vor Zugriff sicher ausbewahren (Verschlüsselung und Wegsperren)