Nutzungsrichtlinie

Vorgangszeichen	O-5015.01/2024.02
Titel	Nutzungsrichtlinie
Version	5.2
Basisdokument	ITS-Betriebsrichtlinie, Version 5.2
Art des Dokuments	Richtlinie
Klassifizierung	Öffentlich
Autor	Ralf Stöber
Freigabedatum	09. Januar 2024
Freigabe durch	Dr. Hans-Jörg Bauer
Dokumenteneigentümer	Dr. Hans-Jörg Bauer
Bekanntmachung	Protokoll ARB 24-01 der ARB vom 09. Januar 2024 Alle Nutzenden: im nächsten ITS-Newsletter
Historie	Version 5.0 vom 22. Februar 2022 Version 4.4 vom 30. März 2021 Version 4.3 vom 09. Februar 2021 Version 4.0 vom 11. Februar 2020 Version 3.0 vom 03. Dezember 2019 Version 2.2 vom 27. August 2019 Version 2.1 vom 16. Juli 2019 Version 1.0 vom 25. April 2019
Mitgeltende Dokumente	siehe Abschnitt 9
Überprüfung bis zum	01. Februar 2026

1 Anwendungsbereich des Informationssicherheitsmanagementsystems und der zugehörigen Richtlinien

Der Anwendungsbereich des Informationssicherheitsmanagementsystems (ISMS) umfasst das IT-Servicezentrum der Universität Bayreuth (ITS) sowie den Betrieb der informations-technischen Anlagen in der Zentralen Universitätsverwaltung (ZUV) und in der Universitätsbibliothek der Universität Bayreuth (UB) und ist in der folgenden Grafik dargestellt.

Neben der Betriebsrichtlinie für das IT-Servicezentrum (ITS-Betriebsrichtlinie) der Universität Bayreuth wird die Nutzungsrichtlinie der Universität Bayreuth von der Leiterin oder vom Leiter des ITS nach § 4 Abs. 7 Lit.a der „Ordnung für die Informationsverarbeitungs-Infrastruktur der Universität Bayreuth“ in der jeweils aktuellen Fassung (z. Zt. vom 30. November 2018) als verbindlicher Leitfaden für alle Bediensteten innerhalb des Geltungsbereichs des Informationssicherheitsmanagementsystems zur Verfügung gestellt und ergänzt die von der Hochschulleitung am 08.02.2022 beschlossene Informationssicherheitsleitlinie für die Universität Bayreuth. Für alle Bediensteten und Nutzenden außerhalb des Geltungsbereichs des Informationssicherheitsmanagementsystems gilt diese Richtlinie für die Nutzung der vom ITS zur Verfügung gestellten Dienste. In der Informationssicherheitsleitlinie als Konkretisierung der Ziele aus der digitalen Agenda bekräftigt die Hochschulleitung die Informationssicherheit als wichtige Aufgabe für den Lehr- und Wissenschaftsbetrieb an der Universität Bayreuth. Die Bekanntgabe der Nutzungsrichtlinie oder deren Speicherort für die Einsichtnahmen erfolgt über den Newsletter des ITS, welcher per Emailverteilerliste an alle IT-Nutzerinnen und IT-Nutzer der Universität Bayreuth verteilt wird.

Im Geltungsbereich dieser Richtlinie ist das ITS gemäß der IT-Ordnung der Universität der Systembetreiber der Informationsverarbeitungs-Infrastruktur. Die Dienstleistungen des ITS werden im regelmäßig erscheinenden Jahresbericht für alle Nutzer bekannt gegeben.

2 Verwaltung der Werte

Die Inventarisierung von Werten richtet sich nach den Vorschriften der Haushaltsordnung des Freistaates Bayern (Bayerische Haushaltsordnung – BayHO). Das Inventarisierungsverzeichnis wird vom Referat Bestandsverwaltung der Zentralen Universitätsverwaltung geführt.

Die unmittelbare Zuständigkeit für einen Wert liegt bei derjenigen oder demjenigen Bediensteten, der den Wert gewöhnlicherweise zur Ausübung von dienstlichen Aufgaben verwendet. Die übergeordnete Zuständigkeit liegt bei der Leiterin oder beim Leiter der Abteilung oder Institution, auf die der jeweilige Wert inventarisiert ist. Der Gebrauch und die Rückgabe von Werten ist in § 4 der IT-Ordnung der Universität Bayreuth geregelt.

2.1 Klassifizierung von Informationen

Die Klassifizierung von Informationen ist in der Richtlinie Klassifizierung geregelt.

2.2 Handhabung von Datenträgern

Als Datenträger gelten alle technischen Geräte, auf denen Informationen in direkt maschinenlesbarer Form abgespeichert werden können wie Festplatten, USB-Sticks oder Magnetbänder. Bei der Entsorgung von Datenträgern oder Systemen, welche Datenträger enthalten, ist sicherzustellen, dass keine Daten, Anwendungsprogramme und Betriebssysteme an unbefugte Dritte gelangen, z. B. durch Entsorgung über ein geeignetes Unternehmen oder Löschung in nicht wiederherstellbarer Weise. Für den weiteren Entsorgungsprozess gilt die Entsorgungsrichtlinie der Universität Bayreuth.

Der Einsatz von Wechseldatenträgern ist auf das erforderliche Maß zu beschränken. Jede Nutzerin und jeder Nutzer hat bei der Verwendung von Wechseldatenträgern durch geeignete Maßnahmen sicherzustellen, dass durch diese keine Schadsoftware auf Systeme der Universität Bayreuth gelangt sowie die Sicherheit, Integrität und Verfügbarkeit von Daten und Systemen nicht beeinträchtigt wird.

Für den Transport von Datenträgern gelten analog die Richtlinien für den Aktentransport in der Handlungsempfehlung zur Arbeit an anderen Orten und die mit den Beschäftigten individuell abgeschlossenen Vereinbarungen.

3 Zugangssteuerung

3.1 Zugang zu Informationen

Der Zugang zur IT-Infrastruktur der Universität Bayreuth erfolgt gemäß § 2, § 3 und § 5 Abs. 1 der IT-Ordnung der Universität Bayreuth über das IDM, Näheres ist in der Prozessbeschreibung Zugangssteuerung geregelt. Der Zugang zu Netzwerkdiensten der Universität Bayreuth erfolgt gemäß der IT-Ordnung der Universität Bayreuth und Regelungen übergeordneter Systembetreiber wie des DFN-Vereins. Der physische Zugang zu den Räumen der Universität ist in der Hausordnung der Universität Bayreuth geregelt.

Privilegierte Zugangsrechte erhalten Nutzerinnen oder Nutzer auf den vom ITS betreuten Systemen nur, wenn dies zur Erfüllung von Aufgaben erforderlich ist. Die Überprüfung der privilegierten Zugangsrechte erfolgt mindestens einmal je Semester durch die für das System verantwortliche Person.

Die Anmeldung an vom ITS betreuten Systemen erfolgt in der Regel mit Hilfe der Benutzerkennung (bt-Kennung) und des zugehörigen Passworts. Für administrative Aufgaben können lokale Benutzerkennungen eingerichtet werden, für deren Verwaltung der jeweilige Systembetreuer zuständig ist. Für den Zugang zu anderen IT-Systemen wie beispielsweise des Freistaats Bayern erfolgt der Einsatz zusätzlicher Maßnahmen beim Anmeldeverfahren nur, wenn der externe Systembetreiber dies vorschreibt.

Der Gebrauch von Benutzerkennungen und der zugehörigen Passwörter ist in der IT-Ordnung in § 4 Abs. 3 geregelt. Der/Die Leiter*in des ITS legt in der Passwortrichtlinie die aktuellen Anforderungen an Passwörter für alle Nutzenden fest. In den Medien des ITS (Newsletter) werden die Nutzenden auf Änderungen in der Passwortrichtlinie hingewiesen. Der/Die Systembetreuer*in des IDMs des ITS stellt durch technische Maßnahmen sicher, dass neu vergebene Passwörter die Anforderungen aus der Passwortrichtlinie erfüllen.

Der Gebrauch administrativer Hilfsprogramme darf nur auf der Ebene der dem Benutzerkonto zugeteilten Rechte erfolgen und ist auf das notwendige Maß zu beschränken. Dabei hat jede oder jeder Verwendende eines solchen Programms dafür zu sorgen, dass die Informationssicherheit nicht durch das jeweilige Hilfsprogramm gefährdet wird.

3.2 Mobilgeräte

Mobilgeräte im Sinn dieser Richtlinie sind alle informationstechnischen Geräte, die für das einfache Verbringen und Arbeiten an unterschiedlichen Orten geeignet sind. Dabei wird zwischen Geräten mit Desktopbetriebssystemen wie Laptops und Geräten mit anderen Betriebssystemen wie Tablets oder Mobiltelefonen unterschieden.

Laptops unterliegen der Zuständigkeit der oder des jeweiligen Systemverantwortlichen, für sie gelten die gleichen Maßstäbe zur Informationssicherheit wie für dienstliche Rechner im stationären Einsatz. Bei der Verwendung von Mobilgeräten ist besonders darauf zu achten, dass

keine unbefugte Person Zugang zu den Geräten und den darauf befindlichen Daten erhält. Dies gilt auch für Programme von Dienstanbietern, die beispielsweise den Zugriff auf das Telefonbuch eines Mobiltelefons voraussetzen. Die Sicherung hat durch angemessene Maßnahmen zu erfolgen, wie die Verwendung von PIN-Codes gegen unbefugten Zugriff, Einschränkung der Rechte von Programmen und die Verschlüsselung von Datenträgern. Der Verlust eines Mobilgeräts mit Desktopbetriebssystem ist der oder dem jeweiligen Vorgesetzten unverzüglich anzuzeigen.

Für die Informationssicherheit von dienstlichen Mobiltelefonen und Tablets, die über kein Desktopbetriebssystem verfügen ist, die jeweilige nutzende Person selber verantwortlich. Das Sicherheitsniveau muss mindestens dem von Desktopgeräte entsprechen. Dazu gehören der Schutz mit einem starken Passwort gemäß der Richtlinie Kryptografie, wenn möglich die Sperrung und Löschung des Geräts nach einer angemessenen (z.B. zehn) Anzahl an Fehlversuchen bei der Passworteingabe, die sichere Speicherung von Passwörtern, der Bezug von Anwendungen nur aus vertrauenswürdigen Quellen, die Einschränkung der Installation von Anwendungen auf das dienstlich unbedingt notwendige Maß, die Einschränkung der Rechte von Anwendungen auf das notwendige Mindestmaß, die Einschränkung der Rechte von Nutzenden auf das erforderliche Mindestmaß, die Einschränkung des Zugriffs Dritter wie des Betriebssystemherstellers auf das notwendige Mindestmaß, nur die Speicherung unbedingt erforderlicher Daten auf dem Gerät, die Verschlüsselung aller Datenträger mit einem starken Verfahren usw. Der Einsatz von biometrischen Merkmalen (Gesichtserkennung, Fingerabdrücke usw.) zum Zugang ist nicht zulässig, da die entsprechenden Verfahren auf Mobiltelefonen und Tablet nicht immer sicher sind. Im Zweifelsfall ist das ITS zu fragen. Der Verlust eines dienstlichen Mobiltelefons und Tablets, das über kein Desktopbetriebssystem verfügt, ist der oder dem jeweiligen Vorgesetzten unverzüglich anzuzeigen.

Private Mobilgeräte dürfen innerhalb des Datennetzes der Universität Bayreuth nur in den vom ITS zur Verfügung gestellten Funknetzen betrieben werden. Sofern auf privaten Mobilgeräten dienstliche Angelegenheiten erledigt werden, hat die Nutzerin oder der Nutzer die gleiche Höhe der Informationssicherheit zu gewährleisten wie sie im vorherigen Absatz beschrieben wird. Der Verlust eines privaten Mobilgeräts, auf dem dienstliche Daten gespeichert sind, ist der oder dem jeweiligen Vorgesetzten unverzüglich anzuzeigen.

Für die Telearbeit gilt die Dienstvereinbarung zur alternierenden Wohnraum-und Telearbeit t der Universität Bayreuth sowie die individuelle Vereinbarung mit jeder oder jedem Beschäftigten, die in der Personalabteilung hinterlegt ist.

4 Kryptographie

Die Regelungen für den Gebrauch von Kryptografie finden sich in der Richtlinie Kryptografie.

5 Betriebsabläufe und -verantwortlichkeiten

5.1 Schutz vor Schadsoftware

Die Grundlage für den Schutz vor Schadsoftware bildet § 6 Informationssicherheitsleitlinie der Universität Bayreuth. Alle Systeme von den zentralen Geräten zur Datenverarbeitung bis zu Arbeitsplatzrechnern sind von der oder dem Systemverantwortlichen mit einem Schutz vor Schadsoftware zu versehen, wenn dies aufgrund der Bedrohungen und des Betriebssystems

angemessen erscheint. Der Verzicht auf solche Maßnahmen ist mit dem Grund zu dokumentieren.

Alle Nutzenden haben den Schutz vor Schadsoftware zu unterstützen, indem sie mit unbekannten Dateien vorsichtig umgehen, die Dateien vor dem Öffnen mit den bereitgestellten Schutzwerkzeugen überprüfen und im Zweifelsfall eine kundige Person hinzuziehen.

5.2 Datensicherung

Bedienstete haben für den Dienstbetrieb wichtige Daten auf einem zentralen Speicherbereich abzulegen. Werden Daten aus technischen Gründen nicht auf einem zentralen Speicherbereich abgelegt, so haben die jeweiligen Beschäftigten für ein vergleichbares Maß der Datensicherheit zu sorgen.

5.3 Software im Betrieb

Die Installation von Software auf in Betrieb befindlichen Systemen erfolgt durch die jeweilige Systemverantwortliche oder den jeweiligen Systemverantwortlichen. Nutzende haben Softwareinstallationen, die das informationstechnische System gefährden könnten, zu unterlassen.

6 Kommunikationssicherheit

Die Übertragung von Informationen hat so zu erfolgen, dass die Vertraulichkeit gemäß der Klassifikation von Informationen gewahrt ist. Gewahrt ist die Vertraulichkeit bei Kommunikation innerhalb von Netzen mit gleichen Schutzanforderungen und bei Verschlüsselung zwischen Netzen mit unterschiedlichen Schutzanforderungen. Für die Übertragung von Informationen in das Bayerische Behördennetz gelten die von dessen Betreiber festgelegten Richtlinien.

Besprechungen und Telefonate sind so zu führen, soweit es die räumlichen Verhältnisse zulassen, dass keine unbefugte Person Kenntnis von internen Informationen erlangen kann, wobei ebenso die Aufzeichnung von Gesprächen mit internen Inhalten durch Sprachassistenten zu unterbinden ist. Dasselbe gilt für das Arbeiten an IT-Geräten und dienstliche Kommunikation mit Hilfe von IT-Geräten. Die automatisierte Weiterleitung von dienstlichen Emails, die an persönliche Emailadressen gesendet worden sind, ist nicht gestattet.

Besteht zwischen der Universität und externen Partnern die Notwendigkeit des Austauschs bzw. der gemeinsamen Nutzung von Informationen, so werden im Bedarfsfall Vertraulichkeits- und Geheimhaltungsvereinbarungen zwischen den beteiligten Institutionen geschlossen. In diesen Vereinbarungen wird die Klassifikation der betroffenen Informationen gemäß Abschnitt 2.1 dieser Richtlinie festgelegt.

Jeder/Jede Bedienstete muss seine Arbeitsumgebung im Büro so gestalten, dass unbefugte Personen unter normalen Umständen keine Möglichkeit haben, von internen Informationen Kenntnis zu nehmen. Unterlagen und Datenträger mit internen Informationen sind auch bei kurzer Abwesenheit entsprechend zu sichern, beispielsweise durch Wegsperren. Beim Verlassen des Arbeitsplatzes ist der Bildschirm zu sperren. Außerdem ist der Bildschirm soweit möglich mit einer automatisierten Sperre zu versehen, die diesen nach 15 Minuten Inaktivität sperrt. Zum Entsperren muss bei Rechnern ein Passwort mit entsprechender Stärke gemäß den Vorgaben des Leiters des ITS und bei mobilen Geräten außer tragbaren Rechnern ein PIN-Code, Bildschirmmuster oder ähnliches mit vergleichbarer Stärke dienen.

7 Handhabung von Informationssicherheitsvorfällen und IT-Notfällen

Die grundsätzlichen Verantwortlichkeiten und das Verfahren für die Behandlung von Informationssicherheitsvorfällen für alle Nutzenden sind in der Informationssicherheitsleitlinie der Universität Bayreuth vom 22.09.2015 sowie in der Ordnung für die Informationsverarbeitungs-Infrastruktur der Universität Bayreuth beschrieben.

Als Informationssicherheitsereignis gilt jedes Ereignis, das die Informationssicherheit im Bereich der Universität Bayreuth gefährden kann (siehe § 3 Abs. 3 der Informationssicherheitsleitlinie). Alle Bediensteten des ITS melden relevante Informationssicherheitsereignisse an die das System betreuende Person auf einem geeigneten Weg. Meldungen von Nutzenden außerhalb des ITS können an die das System betreuende Person, per Email an das ITS unter its-security@uni-bayreuth.de oder telefonisch unter der Rufnummer 3003 erfolgen. Bei der Meldung von Schademails soll – soweit möglich – der Reportmailbutton verwendet werden.

Müssen Nutzende infolge einer Störung, eines Notfalls, einer Krise oder einer Katastrophe ihren Arbeitsplatz verlassen, so sollen sie diesen so wie beim täglichen Dienstschluss verlassen, soweit dies ohne Selbstgefährdung möglich ist.

Alle Regeln der Informationssicherheit behalten grundsätzlich im Falle eines IT-Notfalls ihre Gültigkeit. Eine Abweichung ist nur zulässig, wenn dies zur Abwehr der Gefahr oder der Verringerung der Auswirkungen des Ereignisses zwingend erforderlich ist. Die Entscheidung über die Außerkraftsetzung von Regeln der Informationssicherheit obliegt der Leiterin oder dem Leiter des ITS oder der Vertretung. Anstelle der Maßnahme aus den Leitlinien und Richtlinien muss eine Ersatzmaßnahme treten, die zur Abwehr der Gefahr zweckmäßig ist und der vorgesehenen Maßnahme möglichst nahekommt. Diese Ersatzmaßnahme ist mit dem Zeitraum ihrer Gültigkeit zu dokumentieren.

8 Compliance

Anwendung finden die geltenden Gesetze der Bundesrepublik Deutschland und des Freistaats Bayern, soweit sie für die Universität Bayreuth relevant sind.

Zur Verhinderung und Bekämpfung von Korruption gilt die Richtlinie zur Verhütung und Bekämpfung von Korruption in der öffentlichen Verwaltung (Korruptionsbekämpfungsrichtlinie – KorruR, Bekanntmachung der Bayerischen Staatsregierung vom 13. April 2021).

Für geistige Eigentumsrechte gilt die Satzung der Universität Bayreuth zur Sicherung der Standards guter wissenschaftlicher Praxis und zum Umgang mit wissenschaftlichem Fehlverhalten. Für die Privatsphäre und den Schutz personenbezogener Daten gilt die Datenschutzgeschäftsordnung der Universität Bayreuth.

Aufzeichnungen in nicht elektronischer Form, welche Daten enthalten, die nach den geltenden Gesetzen nicht von Unbefugten eingesehen werden dürfen, sind so zu schützen, dass unter normalen Umständen kein Unbefugter davon Kenntnis erlangen kann. Beispielsweise können die Unterlagen in abschließbaren Schränken gelagert werden, die nur befugten Personen zugänglich sind. Führungskräfte müssen die Einhaltung dieser Vorgehensweise sicherstellen.

9 Mitgeltende Dokumente