Universität Regensburg

Leitlinie
zu IT-Sicherheit und Datenschutz
an der Universität Regensburg

Inhaltsverzeichnis

1.0 Einleitung

1.1 Präambel

Eine Universität lebt von Wissen und dessen Produktion, Weitergabe und der Teilhabe daran. Wissen besteht aus Daten bzw. Informationen. Die Mitglieder der Universität sind bei ihrer Aufgabenwahrnehmung von sorgfältigem Umgang mit Daten bzw. Informationen, einer zuverlässigen Informationstechnik (IT) und dem angemessenen Schutz sowohl personenbezogener Daten, als auch sonstigen geistigen Eigentums und betriebssicherer datentechnischer Systeme abhängig.

Gleichzeitig müssen Daten bzw. Informationen verlässlich und komfortabel verfügbar sein. Schutz und Verfügbarkeit bilden die gleichwertigen Säulen eines leistungsfähigen Umganges mit Daten und Informationen.

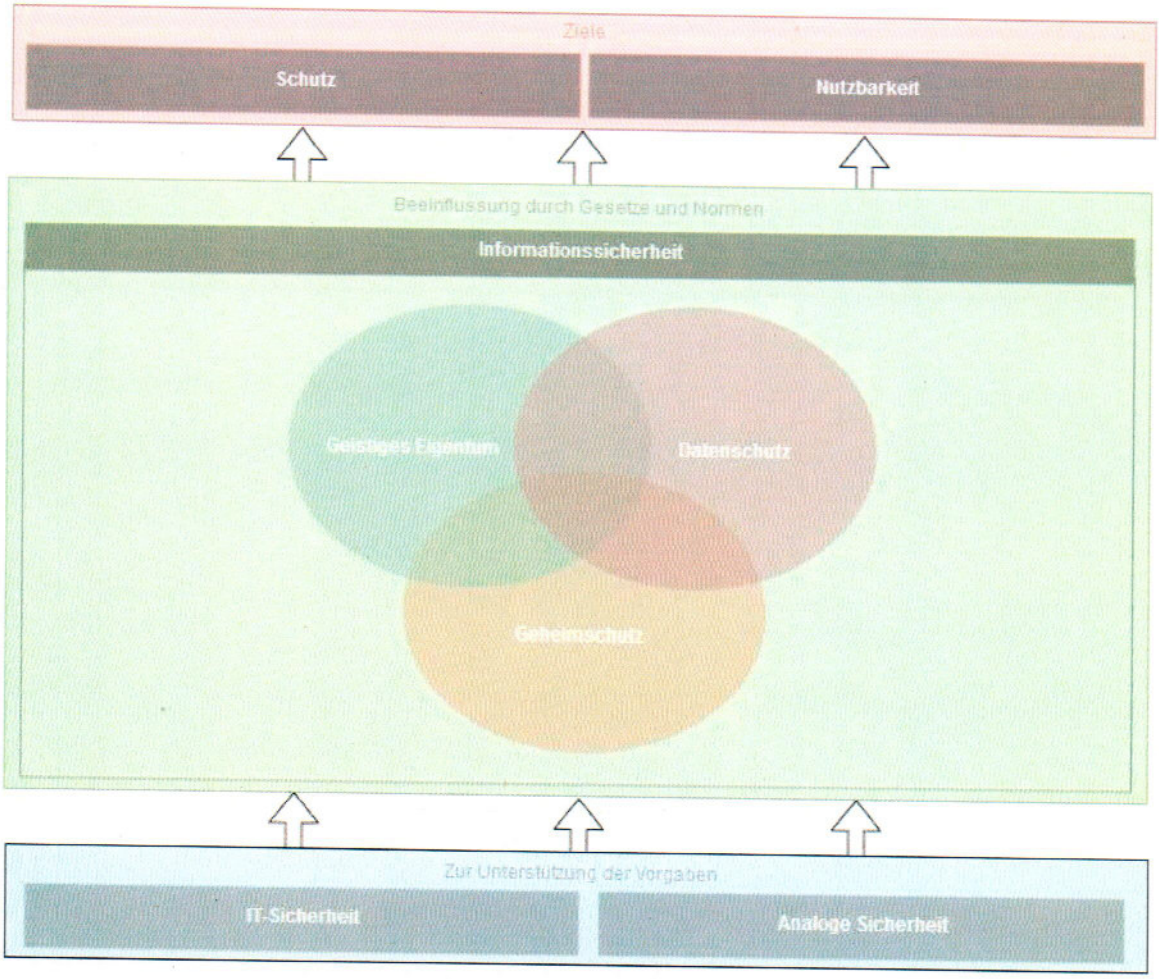
Hinzu kommen die entsprechenden Anforderungen an den sicheren und leistungsfähigen Betrieb einer öffentlichen Einrichtung und die Einhaltung zwingender gesetzlicher Vorschriften (DSGVO, EGovG) – letzteres folgend aus dem Rechtsstaatsgebot und dem Selbstwert des guten Rufes und zur Vermeidung von Schadensersatzforderungen.

„Informationssicherheit" und „Datenschutz" sind dabei parallele Ziele des überwiegend selben Regelungsbedarfes. Die „IT-Sicherheit" unterstützt und gewährleistet diese Ziele auf der technischen und organisatorischen Ebene.

Anlässlich des zunehmenden Vernetzungsgrades, der vermehrt steigenden Informationsverteilung, bei gleichzeitiger Integration der IT-Dienste, sowie der dazu parallel rapiden wachsenden Anzahl von Cybercrime Delikten und Wissenschafts- und Industriespionage der letzten Jahre ist die Gefahrenlage für eingesetzte Informationstechnik gestiegen. Diese führt zu einer Bedrohung für die Aufgabenerfüllung und für die Wahrung der verfassungsrechtlich geschützten Rechte auf freie Wissenschaft und Forschung sowie auf informationelle Selbstbestimmung der betroffenen Personen. Weiterhin können die Begründung, Bewahrung, Mehrung und Verwertung geistigen Eigentums empfindlich gestört werden.

Die Informationen und die für die Informationsverarbeitung benutzten IT-Systeme sind daher in einer Universität in besonderem Maße wertvoll und schützenswert.

Gleichzeitig soll eine Universität eine für ihre Mitglieder, Partner und Eingeladene offene öffentliche Einrichtung sein, die einen möglichst freien und barrierefreien Wissensaustausch gewährleistet. Zur Barrierefreiheit gehört dabei insbesondere ein Vermeiden nicht erforderlicher technischer, organisatorischer und bürokratischer Hürden und die stets verhältnismäßige Abwägung von Sicherheitsbedürfnissen und Offenheit.

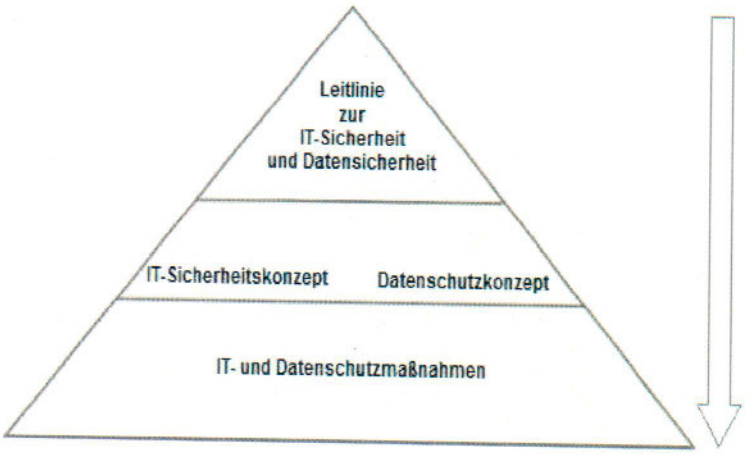


Damit die Organisation der Universität dieser Verantwortung angesichts einer wachsenden Bedrohung der sich rasch weiterentwickelnden Technik bei gleichzeitig begrenzter personeller und finanzieller Ausstattung nachkommen kann, müssen sämtliche Einrichtungen den Schutz der Informationstechnik und personenbezogener Daten als gemeinsame Herausforderung begreifen.

1.2 Ziel der Leitlinie

Die vorliegende Leitlinie ist der grundlegende Baustein des IT-Sicherheits- und Datenschutzkonzeptes der Universität und bildet den Rahmen für Richtlinien und Prozesse. Das übergeordnete Ziel ist ein angemessener Schutz der kritischen Infrastrukturen, Systeme, Anwendungen, Informationen und personenbezogene Daten an der Universität. Mit dieser Leitlinie sollen einheitliche Standards für die IT-Sicherheit und den Datenschutz geschaffen werden.

Die Beachtung dieser Leitlinie ist Voraussetzung für den sicheren Umgang mit informationstechnischen Systemen und mit personenbezogenen Daten innerhalb der UR. Im IT-Sicherheits- und Datenschutzkonzept werden die notwendigen Sicherheitsziele, Grundsätze sowie spezifische Regeln erfasst. Dort findet eine ausreichende Detaillierung der Anforderungen dieser Leitlinie und des Sicherheitsniveaus in Form von Sicherheitsrichtlinien statt. Diese sind dann Basis für die notwendigen IT- und Datenschutzmaßnahmen.



1.3 Geltungsbereich

Diese Leitlinie umfasst verbindlich die gesamte Informationstechnik und auch entsprechende nicht digitale Prozesse und gilt für sämtliche Mitglieder der Universität, die diese nutzen oder bereitstellen. Es sind alle Verfahren, Prozesse und Tätigkeiten dem Maßnahmenkatalog von ISIS12 2.0 und der DSGVO entsprechend zu organisieren.

2.0 Rahmenbedingungen und Ziele der IT-Sicherheit und des Datenschutzes

2.1 Bewusstsein für IT-Sicherheit und Datenschutz

Wegen der vielen und mitunter sehr großen Risiken wird ein hohes Bewusstsein für die IT-Sicherheit und den Datenschutz von jedem Mitglied der Universität erwartet. Das geforderte Maß an Sicherheitsbewusstsein kann nur erreicht werden, wenn insbesondere die beschäftigten Personen für Herausforderungen hinsichtlich der IT-Sicherheit und des Datenschutzes sensibilisiert sind, die eigenen Kompetenzen und Pflichten kennen und sich verantwortungsbewusst verhalten.

IT-Sicherheit und Datenschutz werden insbesondere durch folgendes Verhalten gefördert:

- Sicherheitsbewusstsein bei allen Arbeiten,
- Persönliche Verantwortlichkeit für proaktive sowie effektive reaktive Maßnahmen fördern ein bewusstes Handeln in Bezug auf sämtliche Risiken, Schwachstellen, Vorfälle, Informationen und Vermögenswerte
- Fortführung des Universitätsbetriebes im Notfall, während die beauftragten Personen für die IT-Sicherheit und den Datenschutz bei Unregelmäßigkeiten umgehend informiert werden.

Um dieses Sicherheitsbewusstsein zu erreichen, werden insbesondere die beschäftigten Personen zu sicherheitsrelevanten Themen regelmäßig informiert und fortlaufend Schulungseinheiten angeboten.

2.2 Sicherheitsziele

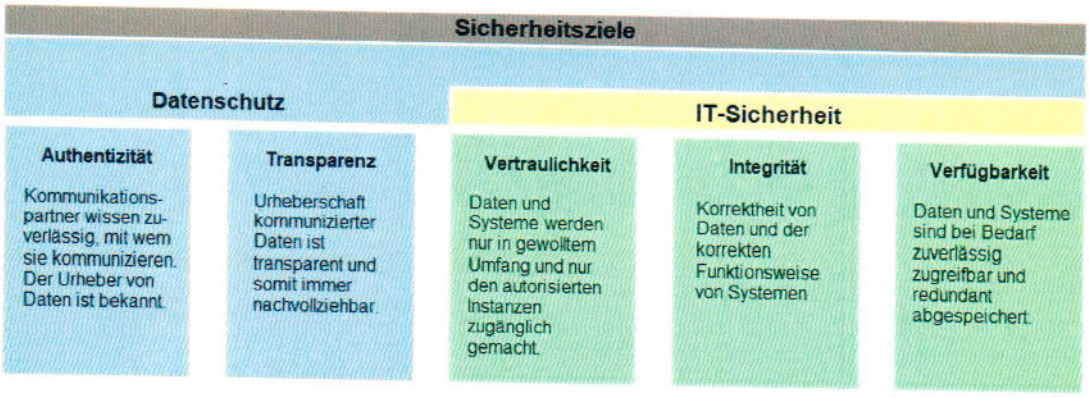
Rechnersysteme, IT-Dienstleistungen und das hochschulinterne Rechnernetz sind zur Unterstützung der universitären Aufgaben in den Bereichen Forschung, Lehre, Lernen und Administration bestimmt. Daraus ergeben sich folgende strategische Ziele:

- Sicherstellung eines reibungslosen Forschungs- und Lehrbetriebs
- Ressourceneffizienter Einsatz
- Einführung eines kontinuierlichen Verbesserungsprozesses (KVP)

Da die Bedeutung der IT-Sicherheit und des Datenschutzes für die Durchführung des Universitätsbetriebes wichtig ist, ergeben sich folgende weitere Ziele, welche von der Universitätsleitung vorgegeben werden:

Die folgenden Sicherheitsziele sind durch die gesetzlichen Vorgaben (DSGVO, EGovG) definiert.

- Datenschutz umfasst fünf Sicherheitsziele: Authentizität, Transparenz, Vertraulichkeit, Integrität und Verfügbarkeit
- IT-Sicherheit konzentriert sich auf drei Sicherheitsziele: Vertraulichkeit, Integrität und Verfügbarkeit



2.3 Verantwortlichkeiten & Organisationsrahmen

Die *Universitätsleitung* trägt die Gesamtverantwortung für IT-Sicherheit und Datenschutz. Im Rahmen dieser Gesamtverantwortung delegiert die Universitätsleitung Entscheidungsbefugnisse an die Kommission für die IT-Architektur für strategische Maßnahmen und an die Fakultäten sowie die Leitungen der zentralen Einrichtungen für die operative Umsetzung.

In der *Kommission für die IT-Architektur* (vgl. IT-Ordnung vom 05.07.2019) ist die kontinuierliche Weiterentwicklung der Leitlinie und abhängiger Dokumente der IT-Sicherheit und des Datenschutzes ein fester Bestandteil der Agenda der regelmäßigen Treffen. Der/die IT-Sicherheitsbeauftragte des Rechenzentrums berät bei IT-sicherheitsrelevanten Themen die Kommission. Er/sie berichtet der Kommission über den aktuellen Stand, um eine ordnungsmäßige Erfüllung der Pflichten zu gewährleisten und erhält seine/ihre Aufgaben basierend auf deren Entscheidungen. Die Kommission für die IT-Architektur wiederum berichtet an die Universitätsleitung.

Allen *Organisationsebenen* obliegt die operative Verantwortung. Die jeweilige Leitung der zentralen Einrichtung oder Fakultät kann nachgeordnete Richtlinien erlassen. In ihrem Verantwortungsbereich weist sie die Beschäftigten auf das geltende Regelwerk für IT-Sicherheit und Datenschutz und deren Verbindlichkeit hin und treibt operative Maßnahmen voran.

Die *Administratoren/innen* der IT-Infrastruktur und IT-Angebote sorgen als technische Verantwortliche in ihrem Zuständigkeitsbereich für die praktische Realisierung. Dies beinhaltet insbesondere, dass sich die Administratoren/innen laufend aktiv über bekannt gewordene Sicherheitslücken und Schwachstellen der auf ihren Systemen eingesetzten Software informieren

und ggf. zeitnah Fehlerkorrekturen ("Patches") einspielen oder Workaround-Prozeduren implementieren.

Im Gegensatz dazu sind *alle Endnutzer/innen* für die Aufrechterhaltung der IT-Sicherheit und des Datenschutzes an ihren Arbeitsplätzen und in ihren Umgebungen verantwortlich. Alle müssen die IT in ihrer täglichen Arbeit verantwortungsbewusst einsetzen, das Regelwerk zur IT-Sicherheit und Datenschutz beachten und die verantwortlichen Stellen über sicherheitsrelevante Ereignisse informieren.

Externe Dritte sind ebenso in die Vorgaben mit einzubeziehen, sofern ihre Tätigkeiten die Ziele der IT-Sicherheit und den Datenschutz in irgendeiner Art beeinflussen könnte. Alle sind bei Aufnahme der Vertragsbeziehung über das Regelwerk zur IT-Sicherheit zu informieren und schriftlich auf dessen Beachtung und Einhaltung zu verpflichten.

2.3.1 Der/die IT-Sicherheitsbeauftragte (IT-SB)

Die Universitätsleitung beauftragt den/die IT-Sicherheitsbeauftragte/n im Sinne dieser Leitlinie zu handeln. Er/sie ist für den inhaltlichen Aufbau des IT-Sicherheitskonzeptes nach dem Maßnahmenkatalog von ISIS12 2.0 verantwortlich.

Der/die IT-Sicherheitsbeauftragte hat folgende Aufgaben:

- Einführung und Fortschreibung des IT-Sicherheitskonzepts, von IT-Sicherheitsrichtlinien und -regelungen,
- Beratung und Unterstützung der Universitätsleitung und der Kommission für IT-Architektur sowie der Administratoren und Administratorinnen bei der Umsetzung von IT-Sicherheitsaufgaben,
- Koordinierung und Prüfung von IT-Sicherheitsmaßnahmen,
- Information und Sensibilisierung der Mitglieder der Universität zum Thema IT-Sicherheit,
- Ansprechperson für alle Mitglieder der zentralen Dienste der Universität im Bereich IT-Sicherheit, insbesondere bei IT-Sicherheitsvorfällen und -mängeln. Für diesen Aufgabenbereich soll eine Vertretung bei Abwesenheit vorhanden sein.
- Zusammenarbeit mit dem/der behördlichen Datenschutzbeauftragten der UR,
- Koordinierte Zusammenarbeit mit dem ISMS-Team des Universitätsklinikum Regensburg,
- Informationsaustausch mit anderen IT-/Informationssicherheitsbeauftragten bayerischer Hochschulen und Universitäten,
- Kontaktperson für zuständigen Behörden

Der/die IT-Sicherheitsbeauftragte ist im erforderlichen Umfang in IT-sicherheitsrelevanten Fragen rechtzeitig einzubinden.

Im Auftrag der Universitätsleitung darf sich der/die IT-Sicherheitsbeauftragte einen Einblick über die IT-Sicherheit in allen Bereichen der Universität verschaffen.

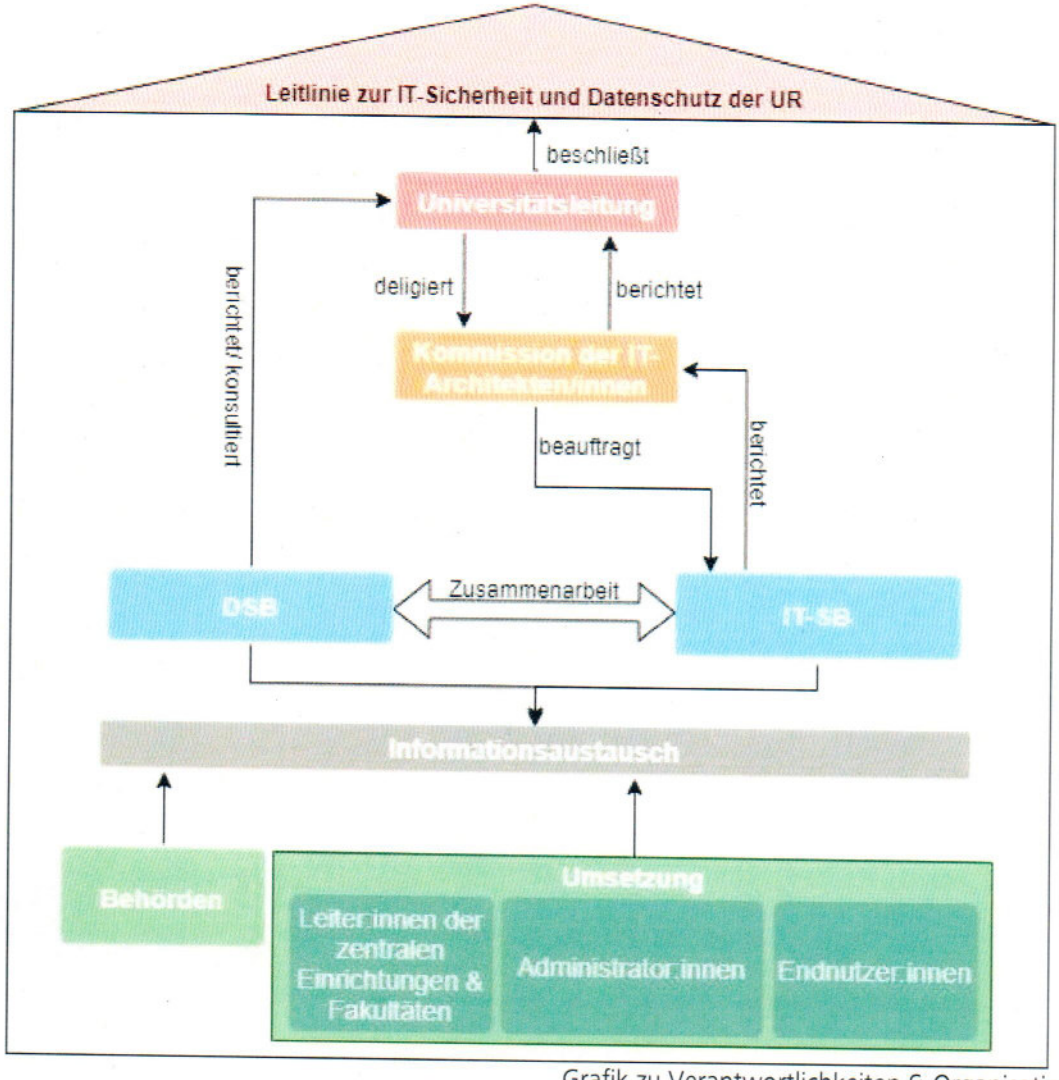
Der/die IT-Sicherheitsbeauftragte ist bei der Erfüllung seiner/ihrer Aufgaben an die Wahrung der Geheimhaltung und der Vertraulichkeit gebunden.

2.3.2 Der/die Datenschutzbeauftragte (DSB)

Der/die behördliche Datenschutzbeauftragte an der Universität Regensburg ist für den reibungslosen Ablauf des Datenschutzmanagements nach DSGVO verantwortlich.

Die Aufgaben des/der Datenschutzbeauftragten, die er/sie delegieren kann, werden in Art. 38 DSGVO beschrieben.

Seine/ihre Stellung wird gemäß Art. 39 DSGVO geregelt.



Grafik zu Verantwortlichkeiten & Organisationsrahmen

2.5 Risikomanagement

Das Risikomanagement ist die Basis des IT-Sicherheits- und Datenschutzkonzeptes. Die Universitätsleitung definiert die Risikoklassen und behält sich das Recht vor, diese bei Bedarf zu ändern. Auf Grundlage dieser Risikokategorien bewerten die zentralen Einrichtungen und Fakultäten die Sicherheitsrisiken ihrer Aufgabenbereiche und Dienste und ordnen sie einer entsprechenden Risikoklasse zu. Die Leitungen der zentralen Einrichtungen und Fakultäten sollen in enger Zusammenarbeit mit den zuständigen Administrator:innen bei Bestanderhebungen, Prozessänderungen oder neuen Projekten eine Risikoanalyse durchführen.

Es soll somit untersucht werden, wie groß die Wahrscheinlichkeit ist, dass es zur Gefährdung der informationstechnischen Systeme und bei der Verarbeitung zu einer Verletzung des Schutzes personenbezogener Daten kommt, und wie hoch der Schaden für die betroffenen Systeme und Personen in diesem Fall wäre.

Die Anwendung angemessener Sicherheitsmaßnahmen, die Verlagerung universitätsinterner Risiken und das Senken bzw. das bewusste Hinnehmen von Risiken unterhalb eines festgelegten, akzeptablen Niveaus werden in der Risikoanalyse beschrieben und von der jeweiligen Leitung der zentralen Einrichtung und Fakultät gegengezeichnet.

2.6 Sicherheitsniveau

Das Sicherheitsniveau für alle IT-Systeme der Universität orientiert sich am Maßnahmenkatalog von ISIS12 2.0.

Es bezieht sich auf Systeme mit normalem Schutzbedarf. Ein System hat einen normalen Schutzbedarf, wenn durch den Verlust an Vertraulichkeit, Verfügbarkeit oder Unversehrtheit des Systems

- nur ein geringfügiger Verstoß gegen Vorschriften und Gesetze möglich ist,
- eine Beeinträchtigung des informationellen Selbstbestimmungsrechts des bzw. der Einzelnen nicht möglich ist oder für diesen bzw. diese tolerabel bleibt,
- eine Beeinträchtigung der persönlichen Unversehrtheit des bzw. der Einzelnen nicht möglich ist,
- die Aufgabenerfüllung nur geringfügig beeinträchtigt ist,
- nur eine geringe Ansehens- und Vertrauensbeeinträchtigung zu befürchten ist und
- der finanzielle Schaden tolerabel bleibt.

Für Systeme mit hohem oder sehr hohem Schutzbedarf müssen Maßnahmen auf Basis der Risikoanalyse unter Beteiligung des/der IT-Sicherheitsbeauftragten und des/der Datenschutzbeauftragten ergriffen werden.

Der/die IT-Sicherheitsbeauftragte und der/die Datenschutzbeauftragte sind bei der Einführung neuer IT-Verfahren oder bei grundlegenden Änderungen bestehender IT-Verfahren mit hohem oder sehr hohem Schutzbedarf zu beteiligen.

2.7 Sicherheitsvorfälle

Ein Sicherheitsvorfall ist eine im Geltungsbereich dieser Leitlinie tatsächlich eingetretene Gefährdung eines der aufgeführten Sicherheitsziele der IT-Sicherheit und des Datenschutzes (s. Abschnitt 2.2).

Bei Verletzung der IT-Sicherheit kritischer Systeme der Universität Regensburg können ein/e Serviceverantwortliche/r des Rechenzentrums oder der betroffenen zentralen Einrichtung (Verwaltungs-IT, Bibliothek) gemeinsam mit der Rechenzentrumsleitung Maßnahmen bis zur sofortigen, vorübergehenden Stilllegung des betroffenen IT-Systems anordnen, sowie die verantwortlichen Anwendenden vorübergehend von der Nutzung der Informationstechnik ausschließen. Des Weiteren ist der/die IT-Sicherheitsbeauftragte über den Vorfall zu informieren, sowie bei Verletzung des Datenschutzes der/die Datenschutzbeauftragte.

Die Kommission für die IT-Architektur bestimmt die IT-Dienste, für die der/die IT-Sicherheitsbeauftragte des Rechenzentrums Notfallpläne erstellt und überwacht. Sie enthalten Handlungsanweisungen in Gefahrensituationen und bei Störfällen und unterteilen sich in einen allgemein zugänglichen Benachrichtigungsplan und in ein detailliertes Notfallkonzept für den Dienstgebrauch.

Der Umgang mit Sicherheitsvorfällen erfolgt entsprechend einem dokumentierten Prozess zur Behandlung von IT-Sicherheits- und Datenschutzvorfällen. Dieser enthält alle notwendigen Maßnahmen, Verantwortlichkeiten, Berichtswege und Eskalationsschritte, die vor, während bzw. nach einem derartigen Vorfall maßgeblich sind.

2.8 Kontinuierlicher Verbesserungsprozess (KVP)

Die Universitätsleitung implementiert einen kontinuierlichen Verbesserungsprozess und somit ein IT-Sicherheits- und Datenschutzkonzept auf Basis des PDCA (Plan-Do-Check-Act)-Zyklus.

Der PDCA-Kreislauf beginnt mit der Planung und Zielsetzung. Dafür bedarf es zunächst einer systematischen Analyse des Status Quo, also einer genauen Bestandsaufnahme der aktuellen Situation. Im Hintergrund stehen hierbei immer die Fragen, welche Optimierungspotenziale es gibt und wo die Ursachen für mögliche Probleme liegen. Im zweiten Schritt der ersten Phase legen die Kommission für die IT-Architektur auf Grundlage von Soll-Ist-Vergleichen und Kennzahlen klare und erreichbare Ziele fest.

In der zweiten Phase geht es darum, die Methoden und identifizierten Strategien umzusetzen. Hierbei handelt es sich um die Testphase, auf der das weitere Vorgehen basiert. Dabei kann auch festgestellt werden, wo eventuelle Probleme auftreten und worauf unbedingt geachtet werden muss, wenn die Umsetzung im größeren Rahmen stattfindet.

Nach der Testphase steht eine ausführliche Analyse und Kontrolle an. Teil dieser Phase sind weitere Anpassungen und Optimierungen. Wurden alle Vorgaben und Erwartungen erfüllt, kann die Einwilligung für die flächendeckende Umsetzung gegeben werden.
Der letzte Schritt ist die allgemeine Einführung und Umsetzung in allen Bereichen.

Es sind weiterhin Kontrollen notwendig, um zu überprüfen, ob die Ziele kontinuierlich erreicht werden und ob alle betroffenen Mitarbeiter sich an die neuen Vorgaben halten. Darüber hinaus kann im KVP ein neuer PDCA-Zyklus angestoßen werden, der weitere Potenziale aufdeckt.

3. Schlussbestimmungen

3.1 Bekanntmachung

Diese Leitlinie ist allen Beschäftigten der Universität in geeigneter Weise zugänglich zu machen, veröffentlicht auf der „Informationssicherheit"-Webseite.

3.2 Gültigkeit und Dokumenten-Handhabung

Das Universitätsleitung behält sich das Recht vor, diese Leitlinie bei Bedarf zu ändern. Änderungen können insbesondere erforderlich werden, um gesetzlichen Vorgaben, bindenden Verordnungen, Forderungen der zuständigen Aufsichtsbehörde oder internen Verfahren der Universität Regensburg zu entsprechen.
Der/die Verantwortliche für dieses Dokument ist der/die IT-Sicherheitsbeauftragte, welche/r die Richtlinie in regelmäßigen Abständen auf inhaltliche Richtigkeit und Konsistenz mit anderen Richtlinien, Handlungsanweisungen, etc. prüft und aktualisiert. Nach Freigabe muss die nächste Überprüfung in 730 Tage erfolgen.

3.3 Inkrafttreten

Diese Leitlinie tritt am Tage nach ihrer Bekanntmachung in Kraft und ist für alle Mitglieder der Universität Regensburg verbindlich.

Regensburg, den 24.11.2021
Universität Regensburg
Der Präsident

(Prof. Dr. Udo Hebel)

Anhang

I. Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
bzw.	beziehungsweise
CERT	Computer Emergency and Response Team (Computer-Notfall-Team)
DFN	Deutsches Forschungsnetz
DSGVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
etc.	et cetera
ISIS12	Informations-Sicherheitsmanagement System in 12 Schritten
IT	Informationstechnik
KVP	Kontinuierlicher Verbesserungsprozess
PDCA	Plan-Do-Check-Act
RZ	Rechenzentrum
s.	siehe
u.a.	unter anderen/ unter anderen
UR	Universität Regenburg

II. Glossar

Aufsichtsbehörde	Eine von einem Mitgliedstaat gemäß Artikel 51 DSGVO eingerichtete unabhängige staatliche Stelle für den Datenschutz.
Authentizität	Personenbezogene Daten müssen jederzeit ihrem Ursprung zugeordnet werden können. An der richtigen Herkunft der Daten dürfen keine Zweifel bestehen und die Urheber der Daten müssen korrekt identifiziert werden können.
Daten	Durch Beobachtungen, Messungen, statistische Erhebungen u. a. gewonnene [Zahlen]werte und beruhende Angaben.
Datenschutz	Bezeichnung für den Schutz des Einzelnen davor, dass er durch die Verarbeitung seiner personenbezogenen Daten in unzulässiger Weise in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).
Datensicherheit	Alle technischen und organisatorischen Maßnahmen im Sinne des Datenschutzes, die die Funktionsfähigkeit der IT-Systeme und den Schutz von informationellen Selbstbestimmungsrechten der Betroffenen sicherstellen.
Dritter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten.
Endnutzer/innen	Eine juristische oder natürliche Person, die weder öffentliche Telekommunikationsnetze betreibt noch Telekommunikationsdienste für die Öffentlichkeit erbringt.
Informationen	Gehalt einer Nachricht, die aus Zeichen eines Codes zusammengesetzt ist, d.h. Daten aller Art in jeglichen Übertragungs- und Speichermedium (z.B. elektronisch, schriftlich, bildlich oder auch mündlich).
Informationssicherheit	Übergeordnete Begriff zur Datensicherheit, der auch den Schutz und die Verfügbarkeit sonstigen geistigen Eigentums, das kein personenbezogenes Datum ist, einschließt.

Integrität	Informationen müssen während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Schutz vor unbefugten Veränderungen, Verlust und Zerstörung).
IT-Organisation	Allgemeine Bezeichnung der aktiv am IT-Sicherheitskonzept und Datenschutzkonzept beteiligten Personen und des IT-Sicherheitsbeauftragten sowie Datenschutzbeauftragten.
IT-Sicherheit	Alle technischen und organisatorischen Maßnahmen, die die Funktionsfähigkeit der IT-Systeme gewährleisten und damit eine der notwendigen Bedingungen für Datensicherheit und Informationssicherheit sind.
IT-System	Hardware- und Software, die geeignet sind, Daten zu speichern, zu verarbeitet und zu übermitteln.
Kontinuierlicher Verbesserungsprozess	Der Begriff kam in den 80er Jahren im Rahmen von Kaizen (Automobilindustrie – Toyota) von Japan nach Deutschland. Er steht zusammenfassend für alle Maßnahmen, die geeignet sind, Produkte, Service, Prozesse und einzelne Tätigkeiten in einem Unternehmen zu verbessern. Die Informationssicherheit hat diesen Terminus übernommen und als feststehenden Begriff etabliert.
Organisationsrahmen	Allgemeine Bezeichnung der aktiv am IT-Sicherheitskonzept und Datenschutzkonzept beteiligten Personen und des IT-Sicherheitsbeauftragten sowie Datenschutzbeauftragten.
Patch	Softwareprogramm, das in bestehenden Anwendungs- oder Systemprogrammen enthaltene Fehler, Mängel oder funktionale Lücken beheben soll.
Plan-Do-Check-Act-Zyklus	Beschreibt einen iterativen vierphasigen Prozess für Lernen und Verbesserung des US-amerikanischen Physikers Walter Andrew Shewhart, s.a. Demingkreis.
Prozess	Ein gerichteter Ablauf eines Geschehens (Allg.); ein von einem Computerprogramm gesteuerter Informationsverarbeitungs-vorgang (Informatik).
Ressourcen	Gesamtheit aller zur Aufgabenerfüllung notwendiger materieller und immaterieller Mittel.
Personenbezogene Daten	Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (z.B. Name, Anschrift, Geburtsdatum, familiäre Situation, Personalnummer, Beurteilungen, Fotos, berufliche Position).

Risikoanalyse	Mittel zur Feststellung und Bewertung von Gefährdungen und Bedrohungen im Risikomanagement.
Risikomanagement	Prozess zur Behandlung von Management Risiken, wobei Maßnahmen festgelegt werden, um verbleibende Risiken zu vermeiden, zu reduzieren, auf Dritte abzuwälzen oder ggf. die damit verbunden Konsequenzen zu tragen.
Transparenz	Die Verfahrensweisen bei der Verarbeitung von personenbezogenen Daten sollen vollständig, aktuell und in einer Weise dokumentiert sein, dass sie in zumutbarer Zeit nachvollzogen werden können.
Verantwortliche/r	Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
Verfügbarkeit	Informationen sollen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.
Verletzung des Schutzes personenbezogener Daten	Eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
Vertraulichkeit	Nur Befugte dürfen Informationen zur Kenntnis nehmen können (Schutz vor unbefugtem Zugriff).
Vortragsrecht	Recht des Urhebers eines sprachlichen Werkes, dieses öffentlich zu Gehör zu bringen, vorzutragen.
Wissen	Als Wissen wird in der Regel ein für Personen oder Gruppen verfügbarer Bestand von Fakten, Theorien und Regeln verstanden, die sich durch den höchstmöglichen Grad an Gewissheit auszeichnen, so dass von ihrer Gültigkeit bzw. Wahrheit ausgegangen wird.
Workaround	Ein Workaround ist ein Umweg zur Vermeidung eines bekannten Fehlverhaltens eines technischen Systems. Es ist ein Hilfsverfahren, das das eigentliche Problem nicht behebt, sondern mit zusätzlichem Aufwand seine Symptome umgeht.

III. Dokumentenlenkung

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie_20211124.docx	2.0	08.10.2021	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
Öffentlich	Hauptversion	24.11.2021	Prof. Dr. Udo Hebel

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie_20210721.docx	1.9	21.07.2021	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
Intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie_20210721.docx	1.1	21.07.2021	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
Intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie_20190723.docx	1.0	23.07.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Hauptversion	24.07.2019	Prof. Dr. Udo Hebel

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie_20190723.docx	0.19	23.07.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.18	25.06.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.17	24.06.2019	Projektpaten
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.16	06.06.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie_20211124.docx	2.0	08.10.2021	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
Öffentlich	Hauptversion	24.11.2021	Prof. Dr. Udo Hebel

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.15	06.06.2019	Jan von Hassel
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.14	06.05.2019	Universitätsleitung
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.13	24.04.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.12	15.04.2019	Dr. Christian Blomeyer
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.11	15.04.2019	Caren Altmann
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.10	05.04.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.10	29.04.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.9	27.03.2018	Dr. Christoph Bauer
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.8	26.03.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.7	25.03.2018	Jan von Hassel
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.6	22.03.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.5	13.03.2019	Dr. Christian Blomeyer
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.4	07.03.2019	Elena Kellinghaus
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.3	28.02.2019	Dr. Susanne Leist
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.2	20.12.2018	Jan von Hassel
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Arbeitsversion	-	-

Dateiname	Version	Änderungsdatum	Autor/in
Leitlinie.docx	0.1	19.12.2018	Sylvia Kirchner-Luft
Vertraulichkeitsstufe	Bearbeitungsstatus	Freigabedatum	Freigabe durch
intern	Entwurf	-	-