KATHOLISCHE UNIVERSITÄT EICHSTÄTT-INGOLSTADT

Informationssicherheitsleitlinie der KU

Präambel

Die Kernprozesse der Katholischen Universität Eichstätt-Ingolstadt (KU) in Forschung, Lehre und Verwaltung basieren in hohem Maße auf der Verfügbarkeit und Anwendung von sicherer und zuverlässiger Informations- und Kommunikationstechnik. Daher sind Informationssicherheit und Datenschutz für die KU von zentraler Bedeutung und somit wesentliche strategische Ziele.

Insbesondere müssen Integrität, Vertraulichkeit und Verfügbarkeit der Dienste der Informationstechnik (IT) und Informationen der KU in jeweils angemessenem Umfang sichergestellt werden. Dies kann nur gelingen, wenn sämtliche Einrichtungen und Angehörige der KU Informationssicherheit als gemeinsame Herausforderung begreifen.

1 Gegenstand der Leitlinie

Die vorliegende Leitlinie bildet Rahmen und Basis für einen kontinuierlichen Informationssicherheitsprozess an der KU. In ihr werden Ziele und Prioritäten in Bezug auf Informationssicherheit (IS) und die für deren Realisierung erforderlichen Organisationsstrukturen definiert. Diese Vorgaben können in untergeordneten Richtlinien weiter konkretisiert werden.

2 Geltungsbereich

Diese Leitlinie ist gültig für die gesamte Informationsverarbeitung und damit insbesondere für alle IT-gestützten Geschäftsprozesse der KU. Sie gilt für sämtliche Personen, die Informationen an der KU verarbeiten oder bereitstellen und umfasst die Nutzung von IT-Infrastruktur und IT-Diensten der KU sowie die dienstliche Nutzung von Drittanbieter-Plattformen (Clouddienste) durch KU-Angehörige.

3 Begriffe

Im Sinne dieser Leitlinie gelten an der KU folgende Definitionen:

Vertraulichkeit: Zustand, in dem nur berechtigte Personen in zulässiger Weise Zugriff auf Informationen erhalten.

Integrität: Unverfälschtheit und Vollständigkeit von Informationen und IT-Systemen (keine unbefugte Manipulation, keine Speicher- oder Übertragungsfehler).

Verfügbarkeit: Zustand, in dem Informationen, Dienste und Systeme zum erforderlichen

Zeitpunkt in vereinbarter Qualität nutzbar sind.

Informationssicherheit (IS): Schutz aller Informationswerte der KU – unabhängig von der Form (digital oder physisch). Informationssicherheit umfasst die IT-Sicherheit.

Sicherheit in der Informationstechnik (IT-Sicherheit): Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme, IT-Verfahren, IT-Dienste und Datenbestände der Universität.

Informationswerte: Alle schützenswerten Informationen, Daten, Systeme, Anwendungen, Prozesse und physischen Einrichtungen und Geräte, die für die Aufgabenerfüllung der KU relevant sind.

IT-System: Funktionelle Einheit aus Hard- und Software zur Verarbeitung, Speicherung, Übermittlung oder Darstellung von Daten (z. B. Arbeitsplatzrechner, Server, Router).

IT-Dienst: Zentral bereitgestellte IT-Anwendung, die über Weboberflächen, Clients oder Protokolle genutzt wird (z. B. E-Mail, Gruppenlaufwerke, Campusmanagementsysteme).

IT-Infrastruktur: Gesamtheit der technischen und baulichen Einrichtungen, die der Informationsverarbeitung dienen; im engeren Sinne Einrichtungen (z. B. Netzwerke), von denen andere IT-Systeme abhängen.

Informationssicherheitsprozess: Gesamtheit der organisatorischen und technischen Verfahren und Maßnahmen zur systematischen Planung, Umsetzung, Überprüfung und Weiterentwicklung der Informationssicherheit an der KU.

Risikomanagement: Strukturierter Prozess zur Identifikation, Bewertung und Behandlung von Risiken für Informationswerte.

Schutzbedarfsfeststellung: Bewertung des erforderlichen Sicherheitsniveaus eines Informationswertes hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit.

Sicherheitsvorfall: Ereignis, das die Informationssicherheit beeinträchtigt oder beeinträchtigen könnte (z. B. Datenverlust, unbefugter Zugriff, Systemausfall).

Business Continuity Management (BCM): Maßnahmen zur Aufrechterhaltung oder schnellen Wiederherstellung kritischer Geschäftsprozesse im Falle eines sicherheitsrelevanten Ereignisses.

Datenschutz: Rechtlich gebotene organisatorische und technische Maßnahmen zum Schutz personenbezogener Daten und der Privatsphäre von Personen.

4 Zielsetzungen

An der KU soll ein angemessenes Informationssicherheitsniveau – dem aktuellen Stand der Technik entsprechend – gewährleistet werden. Grundlegende Voraussetzung für Informationssicherheit an der KU ist ein Risikomanagement auf Basis einer Klassifizierung aller vorhandenen und zu erhebenden Daten, Anwendungen, Dienste sowie der IT-Infrastruktur anhand ihres Schutzbedarfs.

Informationssicherheit und die zugehörigen Prozesse bilden wichtige Bausteine, um die Ziele,

Werte und Interessen der KU sowie das Ansehen der KU in der Öffentlichkeit durch die Sicherung ihrer Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit zu schützen.

Zu den Informationssicherheitszielen der KU im engeren Sinne zählen:

1. die Gewährleistung der Verfügbarkeit aller Informationswerte,
2. der Schutz der Integrität aller Informationswerte,
3. die Handhabung aller sensiblen Informationen unabhängig von der Art ihrer Aufzeichnung derart, dass ihre Vertraulichkeit jederzeit sichergestellt ist und Missbrauch durch Unbefugte verhindert wird,
4. die Einhaltung aller einschlägigen Gesetze und rechtlichen Bestimmungen,
5. die Wahrung der Persönlichkeitsrechte der von der Informationsverarbeitung betroffenen Personen.

Die Informationssicherheitspolitik der KU orientiert sich an Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Informationssicherheit. Sie folgt dem Grundsatz, dass der Aufwand für die Schutzmaßnahmen stets in Relation zum erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter zu setzen ist, weil sich nur so auf Dauer das Bedürfnis nach Sicherheit, akademischer Freiheit und praktikablen Arbeitsbedingungen miteinander vereinbaren lassen.

5 Informationssicherheitsverantwortung

Das Präsidium der KU trägt die Gesamtverantwortung für die Informationssicherheit an der KU. Das Präsidium weist in seinem Geschäftsverteilungsplan einen oder eine Chief Information Officer (CIO) aus, in dessen/deren Verantwortungsbereich auch das Informationssicherheitsmanagement an der KU fällt.

Das Präsidium benennt einschlägig qualifizierte Personen als Informationssicherheits-beauftragte/Informationssicherheitsbeauftragten (ISB) der KU sowie deren/dessen Stellvertretung (siehe 7.1).

Die Leitungen der Organisationseinheiten der KU tragen ebenfalls Verantwortung für das Informationssicherheitsmanagement in ihrem jeweiligen Zuständigkeitsbereich.

Alle KU-Angehörigen sind in ihrem Wirkungsbereich für die Einhaltung des Informations-sicherheitsniveaus der KU verantwortlich. Insbesondere leitet sich aus einer Zuständigkeit für Geschäftsprozesse, Informationen und IT-Systeme auch eine Zuständigkeit für damit verknüpfte Aspekte der Informationssicherheit ab.

6 Hauptakteure im Bereich Informationssicherheit

6.1 Informationssicherheitsbeauftragte/ Informationssicherheitsbeauftragter der KU

Die/der Informationssicherheitsbeauftragte (ISB) ist zentral für alle Aspekte von Informationssicherheit an der KU zuständig. Sie/er sowie ihre/seine Stellvertretung werden auf Vorschlag des CIOs durch das Präsidium ernannt. Dabei soll die erforderliche personelle Kontinuität berücksichtigt werden.

Die/der ISB ist bei Planungen und Entscheidungen mit spezifischem Bezug zu

Informationssicherheit von Beginn an zu beteiligen. Zu ihren/seinen Aufgaben gehören insbesondere:

- Fachliche Verantwortung für das Informationssicherheitsmanagement
- Identifizierung und Bewertung von IS-Risiken
- Federführende Erarbeitung von Plänen im Bereich IT-Sicherheit (mit begründeten Vorschlägen zur Priorisierung)
- Regelmäßige Unterrichtung des CIO und relevanter Gremien zu IS
- Erstellung des jährlichen ISB-Berichts
- Organisation des Austausches zu IS innerhalb der KU (insb. Kontakt zu dezentralen ISBs) sowie von IS-Schulungen
- Mitarbeit in für Hochschul-IS relevanten überregionalen Arbeitskreisen (insb. ZKI)

6.2 CIO und CIO-Gremium

Das CIO-Gremium der KU wird durch das Präsidium eingesetzt und von der/dem CIO geleitet. Es unterstützt das Präsidium und das Universitätsrechenzentrum bei der strategischen Ausrichtung in den Bereichen IT und Digitalisierung (einschließlich KI).

Die federführende Rolle der/des CIO und des CIO-Gremiums in der IT-Governance erstreckt sich auch auf die Informationssicherheit:

- Entwicklung von Leit- und Richtlinien (mit Zuarbeit durch den ISB) auch im Bereich Informationssicherheit
- Beratung von Empfehlungen des ISB sowie Abnahme des jährlichen ISB-Berichts
- Unterstützung der/des CIO bei der Steuerung des IS-Prozesses
- Beauftragung der/des ISB durch die/den CIO mit spezifischen Planungen und Stellungnahmen

6.3 IT-Beirat

Der IT-Beirat der KU fungiert als Schnittstelle zwischen den Organisationseinheiten der Universität und dem CIO-Gremium. Er sammelt IT-Anforderungen aus den Fachbereichen, gibt Rückmeldungen und kommuniziert IT-Neuerungen in die Organisation.

Die Mitglieder des IT-Beirats unterstützen die Durchsetzung von Leit- und Richtlinien sowie die Umsetzung von Maßnahmen insbesondere auch im Bereich Informationssicherheit. In den IT-Beiratssitzungen berichtet der ISB regelmäßig und in angemessenem Umfang über IS-Themen.

6.4 Dezentrale Informationssicherheitsbeauftragte

Die dezentralen Informationssicherheitsbeauftragten (dezentrale ISB) sind lokale Ansprechpersonen für Informationssicherheit in den Fakultäten und weiteren Organisationseinheiten. Sie unterstützen den zentralen ISB und das URZ bei Sicherheitsthemen und -maßnahmen, fungieren als Multiplikatoren und sind erste Anlaufstelle bei Vorfällen mit lokalem Bezug.

Aufgaben:

- Beratung bei allgemeinen Fragen zur Informationssicherheit und Weiterleitung komplexer Themen an das URZ / die/den ISB
- Koordination und Informationsweitergabe innerhalb der Fakultät / Organisationseinheit

- Unterstützung der Dekanin bzw. des Dekans der Fakultät bzw. der Leitung der Organisationseinheit bei der Umsetzung ihrer Sicherheitsverantwortung

Vertiefte IT-Fachkenntnisse sind nicht erforderlich. Technische Aufgaben liegen (soweit nicht z.B. für selbstbetriebene Server oder Workstations anders vereinbart) grundsätzlich beim URZ. Dezentrale ISB werden vom URZ fachlich unterstützt, geschult und tauschen sich unter dem Vorsitz der/des ISB regelmäßig zu sicherheitsrelevanten Themen aus.

Die Rolle kann von IT-affinen Mitarbeitenden, Fakultätsmanagement oder IT-Beiratsmitgliedern übernommen werden. Dezentrale ISB werden von ihren Organisationseinheitsleitungen in der Regel für einen Zeitraum von mindestens 2 Jahren entsandt; eine Vertretung ist zu benennen.

6.5 Universitätsrechenzentrum

Als zentraler IT-Dienstleister der KU mit Zuständigkeit u.a. für den Betrieb der zentralen IT-Infrastruktur und aller zentralen IT-Dienste hat das Universitätsrechenzentrum (URZ) umfassende Zuständigkeiten auch im Bereich Informationssicherheit. Dazu gehören:

- Implementierung und Betrieb von IS-Einrichtungen wie Next-Generation-Firewalls, Detektionssystemen und Softwarelösungen
- Design und Implementierung von sicheren IT-Architekturen
- Durchführung von Projekten im Bereich IS
- Incident- und Notfallmanagement auch im Bereich IT-Sicherheit
- Abschluss von Support- und Beratungsverträgen
- Kooperation mit anderen Einrichtungen (u.a. im Digitalverbund Bayern und auf nationaler Ebene)

Insbesondere entscheidet die URZ-Leitung über Notfallmaßnahmen zur Abwehr akuter Bedrohungen der IS, etwa die Abschaltung von IT-Systemen und IT-Diensten sowie den Ausschluss von Nutzern; vertretungsweise kann auch der URZ-Abteilungsleiter IT-Infrastruktur solche Maßnahmen veranlassen sowie URZ-Abteilungsleiter jeweils in den eigenen Zuständigkeitsbereichen. Alle Entscheidungen werden (sobald und soweit möglich) mit dem ISB und CIO abgestimmt.

6.6 Datenschutzbeauftragter (DSB)

Die oder der Datenschutzbeauftragte der KU hat die Aufgabe, auf die Einhaltung des Gesetzes über den Kirchlichen Datenschutz (KDG) und anderer Vorschriften über den Datenschutz an der KU hinzuwirken. Er oder sie steht den Beschäftigten der Hochschule als Kontaktperson in Angelegenheiten des Datenschutzes zur Verfügung.

7 Grundprinzipien und zentrale Anforderungen der Informationssicherheit

7.1 Pflichten

- Nutzende der IT-Infrastruktur der KU sind verpflichtet, Informationssicherheit zu gewährleisten und erforderliche Maßnahmen im jeweiligen Zuständigkeitsbereich umzusetzen.
- Sicherheitsrelevante Ereignisse sind unverzüglich nach Kenntniserlangung zu

melden:
    - Informationssicherheitsvorfälle über den KU.ServiceDesk-IT (it-support@ku.de, Tel. 21010)
    - Gravierende Vorfälle zusätzlich über den Dienstweg
    - Datenschutzrelevante Informationssicherheitsprobleme an die/den DSB und an die/den ISB
- Bei IT-Projekten, der Einrichtung von IT-Diensten, und der Nutzung von Cloud-Plattformen hat Informationssicherheit von Beginn an eine hohe Priorität. Die/der ISB und ggf. die/der DSB sind entsprechend von Beginn an mit einzubeziehen.
- Alle KU-Angehörigen werden angemessen zu Themen der Informationssicherheit geschult.

7.2 Zugriffssteuerung

Der Zugriff auf Daten und IT-Systeme wird durch technische und organisatorische Maßnahmen gesteuert und orientiert sich an dem Schutzbedarf der jeweiligen Information. Insbesondere sind vertrauliche Daten nur nach erfolgreicher Authentisierung zugänglich. Dabei wird das Prinzip der minimalen Rechte angewendet, d. h. Berechtigungen werden nur in dem Umfang gewährt, wie dies zur Erfüllung der jeweiligen Aufgaben erforderlich ist.

7.3 Sensibilisierung und Schulung

Das geforderte Maß an Informationssicherheit kann nur erreicht werden, wenn die beschäftigten Personen auf Informationssicherheitsbedrohungen sensibilisiert sind, die eigenen Kompetenzen und Pflichten kennen und sich verantwortungsbewusst verhalten.

Sicherheitsrelevante Themen und Regeln werden den Hochschulangehörigen durch geeignete Schulungs- oder Informationskanäle zur Kenntnis gebracht.

8 Finanzierung

Die Hochschulleitung ist grundsätzlich für die Finanzierung aller für die Erreichung eines angemessenen Niveaus der Informationssicherheit erforderlichen Maßnahmen verantwortlich. Insbesondere stellt sie personelle und finanzielle Ressourcen für zentrale Informationssicherheitsmaßnahmen bereit und finanziert kontinuierliche Fortbildungsmaßnahmen.

9 Inkrafttreten

Diese Informationssicherheitsleitlinie für die Katholische Universität Eichstätt-Ingolstadt tritt am 05.05.2026 in Kraft. Die Informationssicherheitsleitlinie der KU vom 10. August 2018 tritt gleichzeitig außer Kraft.