KATHOLISCHE UNIVERSITÄT EICHSTÄTT-INGOLSTADT

Informationssicherheitsleitlinie der KU

Vom 10. August 2018

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 Daten in jeweils angemessenem Umfang sichergestellt werden. Angesichts zunehmender Bedrohungen bei gleichzeitig begrenzter personeller und finanzieller Ausstattung kann dies nur gelingen, wenn sämtliche Einrichtungen und Verantwortliche der KU Informationssicherheit als gemeinsame Herausforderung begreifen. Die Mitwirkung von KU-Angehörigen außerhalb des Rechenzentrums ist dabei in der Regel schon bei der Festlegung des jeweils angemessenen Schutzniveaus und der für dessen Erreichen akzeptablen Kosten und Einschränkungen essentiell. Letztlich impliziert Informationssicherheit eine persönliche Verantwortung und entsprechende Pflichten jedes einzelnen KU-Angehörigen bzw. aller Nutzerinnen und Nutzer von KU-Diensten.

1. Gegenstand der Leitlinie

Die vorliegende Leitlinie bildet die Basis zur Etablierung eines kontinuierlichen Informationssicherheitsprozesses an der KU. In ihr werden Ziele und Prioritäten in Bezug auf Informationssicherheit (IS) und die für deren Realisierung erforderlichen Organisationsstrukturen definiert. Außerdem werden Zuständigkeiten, Pflichten und Aufgaben in diesem Bereich festgelegt. Die Leitlinie dient als Grundlage für ein Informationssicherheitskonzept und als Rahmen für den Informationssicherheitsprozess.

Die Informationssicherheitspolitik der KU orientiert sich an Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur IT-Sicherheit. 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.

Diese Leitlinie bildet die Grundlage für zukünftige IT-Sicherheitsrichtlinien, in denen ihre Vorgaben konkretisiert werden. Sie ergänzt die Benutzungsrichtlinien für Informationsverarbeitungssysteme der Katholischen Universität Eichstätt-Ingolstadt in der jeweils aktuell gültigen Fassung.

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 IT an der KU einsetzen oder bereitstellen und ist damit für alle Organisationseinheiten der Universität verbindlich, insbesondere für alle Fakultäten, die Zentralverwaltung sowie die wissenschaftlichen, zentralen, Forschungs- und sonstigen Einrichtungen an allen Standorten der KU. Sie gilt ebenso für die gesamte IT-Infrastruktur der KU einschließlich aller am KU-weiten Netzwerk angeschlossenen Geräte.

3. Begriffsbestimmungen

Im Sinne dieser Leitlinie ist

Sicherheit in der Informationstechnik (IT-Sicherheit):

Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme der Universität, der IT-Verfahren, der IT-Dienste sowie der Datenbestände.

Informationssicherheit:

Schutz aller Informationswerte der KU inklusive physischer Dokumente. In diesem Sinne beinhaltet Informationssicherheit auch und insbesondere die (technische) IT-Sicherheit.

Verfügbarkeit:

Ein Zustand, in dem Daten, Dienste und Funktionen eines IT-Systems und seiner Komponenten von den berechtigten Personen zum geforderten Zeitpunkt in der vorgesehenen Zeit sowie in der vorgesehenen Form und Qualität nutzbar sind.

Integrität:

Ein unverfälschter Zustand von Daten und IT-Systemen (unmanipuliert und ohne Speicher- oder Übertragungsfehler).

Vertraulichkeit:

Ein Zustand, in dem der Zugriff auf Daten nur berechtigen Personen und nur in zulässiger Weise möglich ist.

IT-Infrastruktur:

Gesamtheit der Hardware, Anwendungen und baulichen Einrichtungen der Universität, die der Informationsverarbeitung dienen. Bei IT-Infrastruktur im engeren Sinne handelt es sich um Einrichtungen (wie z.B. Netzwerke), von deren Funktionieren andere IT-Systeme abhängen.

IT-System:

Die funktionelle Einheit aus Hard-und Software, die Daten erhebt, erfasst, aufbereitet, nutzt, speichert, übermittelt, programmgesteuert verarbeitet, intern darstellt, ausgibt und wiedergewinnt. Beispiele sind Arbeitsplatzrechner, Server und Router.

Informationssicherheitsprozess:

Die Gesamtheit der Verfahren, die das Ziel haben, Informationssicherheit in alle relevanten Abläufe der Universität zu integrieren und weiterzuentwickeln sowie diese Vorgänge zu evaluieren.

Dienst:

Eine zentral bereitgestellte IT-Anwendung, die in der Regel über eine webbasierte Oberfläche oder spezifische Clients oder Protokolle verwendet wird. Beispiele sind Gruppenlaufwerke, E-Mail und Campusmanagementsysteme.

Datenschutz:

Organisatorische und technische Maßnahmen gegen Missbrauch von Daten innerhalb des Verantwortungsbereichs der KU, um insbesondere die Privatsphäre natürlicher Personen bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten sicherzustellen.

4. Zielsetzungen

Die Zielsetzungen in Bezug auf Informationssicherheit an der KU leiten sich, im Rahmen gesetzlicher Vorgaben und generischer Anforderungen an informationsverarbeitende Organisationen, von den primären Zielen und Aufgaben der KU („Geschäftsprozesse“) ab. Zu letzteren gehören nach Art. 2 Abs. 1 Satz 1 BayHSchG

- der **Lehr- und Weiterbildungsbetrieb** mit Vorlesungen, Seminaren sowie E-Learning-Angeboten nebst zugehörigen Prüfungen
- die **Forschung** samt fachgebietsadäquater Veröffentlichung der Ergebnisse.

Im weiteren Sinne umfassen die Ziele und Aufgaben der KU

- die Förderung von wissenschaftlichem und gesellschaftlichem **Diskurs**,
- die umfassende **Förderung und Betreuung** der Studierenden und Nachwuchswissenschaftler
- sowie eine gesellschaftlich und für die Mitarbeiter förderliche **Selbstorganisation.**

Diese Aufgaben und Ziele setzen jeweils u.a. die Erfassung bzw. Erstellung, Aufbewahrung, Aufbereitung und Verbreitung von Daten sowie vielfältige Kommunikationsmöglichkeiten voraus, mit unterschiedlichen Toleranzen für Verluste oder Verfälschungen von Daten sowie Unterbrechungen der Verfügbarkeit von Daten oder Diensten. Grundlegende Voraussetzung für Informationssicherheit an der KU ist also ein Risikomanagement auf Basis einer Klassifizierung aller vorhandenen und zu erhebenden Daten, Anwendungen, Dienste sowie der IT-Infrastruktur in Bezug auf ihre primären Ziele, Aufgaben und Werte. Insbesondere die essentiellen Werte der KU in Forschung, Lehre, Verwaltung und zentralen Einrichtungen müssen identifiziert und besonders geschützt werden.

In diesem Sinn bilden Informationssicherheit und die zugehörigen Prozesse wichtige Bausteine, um die Interessen und das Ansehen der KU in der Öffentlichkeit durch die Sicherung ihrer Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit für Studierende, Mitarbeiterinnen und Mitarbeiter sowie Kooperationspartner zu schützen.

Zu den **Informationssicherheitszielen der KU im engeren Sinne** zählen:

- die **Gewährleistung der Verfügbarkeit** der IT-Systeme, Programme und Daten,
- der **Schutz der Integrität** der IT-Systeme, Programme und Daten,
- die **Verhinderung des Missbrauchs** der IT-Systeme, Programme und Daten (zweckwidrige Nutzung, Nutzung durch Unbefugte), sowohl aus Gründen des Selbstschutzes als auch zum Schutz Dritter,
- die Handhabung der vertraulichen Informationen unabhängig von der Art ihrer Aufzeichnung derart, dass ihre **Vertraulichkeit** jederzeit sichergestellt ist,
- die Sicherstellung der Integrität, Funktionsfähigkeit und Vertraulichkeit von Arbeitsergebnissen und von Projektdaten,
- die Einhaltung der einschlägigen Gesetze und sonstigen rechtlichen Bestimmungen,
- die Wahrung der **Datenschutz- und Persönlichkeitsrechte** der Mitarbeiter, Studierenden und ggf. der Angehörigen.

5. Grundpflichten

1. Alle Nutzer der mit der IT-Infrastruktur der KU verbundenen IT-Systeme sind verpflichtet, auf Informationssicherheit hinzuwirken und die dazu erforderlichen Maßnahmen zu treffen.
2. Die Verantwortlichkeit für Informationssicherheit folgt grundsätzlich den Zuständigkeiten für IT-Systeme.
3. Alle Nutzer haben die Pflicht, Ereignisse, die die IT-Sicherheit beeinträchtigen, unverzüglich nach Kenntniserlangung zu melden. In der Regel erfolgt diese Meldung über den KU.ServiceDesk-IT, welcher den zuständigen (dezentralen oder zentralen) IT-Sicherheitsbeauftragten (ITSB) und ggf. das IT-Sicherheitsmanagementteam (ISMT) in Kenntnis setzt.
4. Verstöße oder Gefährdungen in Bezug auf nichttechnische Informationssicherheit sind auf dem hierarchischen Dienstweg zu melden.
5. Informationssicherheitsprobleme in Bezug auf Datenschutz (insbesondere Vertraulichkeit personenbezogener Daten) sind dem oder der Datenschutzbeauftragten (DSB) sowie dem ITSB zu melden.

6. ITSB und DSB arbeiten eng zusammen. Sie tauschen sich regelmäßig über relevante Vorfälle und Neuerungen aus den gemeinsamen Tätigkeitsbereichen aus.

6. Beteiligte am Informationssicherheitsprozess

Die Gesamtverantwortung für die Gewährleistung der Informationssicherheit und die Einhaltung des Informationssicherheitsprozesses an der KU liegt bei der Hochschulleitung. Durch diese werden folgende Beteiligte am Informationssicherheitsprozess bestimmt:

1. die Hochschulleitung
2. das CIO-Gremium
3. der/die IT-Sicherheitsbeauftragte (ITSB) sowie dessen/deren Stellvertreter(in)
4. das Informationssicherheits-Management-Team (ISMT)
5. der IT-Beirat
6. das Universitätsrechenzentrum (URZ)
7. alle Fakultäten und Einrichtungen der KU
8. dezentrale IT-Sicherheitsbeauftragte

7. Einsetzung der Beteiligten

1. Die Hochschulleitung (ggfs. delegiert über den Leiter des URZ) benennt einschlägig qualifizierte KU-Mitarbeiter(innen) als den/die IT-Sicherheitsbeauftragte(n) der KU (ITSB) bzw. den/die Stellvertreter(in). Dabei soll die erforderliche personelle Kontinuität berücksichtigt werden.
2. Die Hochschulleitung setzt ein **Informationsicherheitsmanagementteam (ISMT)** ein. Ständige Mitglieder dieses Gremiums sind:
    a. ein Mitglied des CIO-Gremiums
    b. der/die IT-Sicherheitsbeauftragte der KU (ITSB) sowie dessen/deren Stellvertreter(in)
    c. der/die Koordinator(in) für Datenschutz an der KU,
    d. ein Mitglied der Zentralen Universitätsverwaltung der KU,
    e. ein Mitglied der Leitungsebene des Universitätsrechenzentrums,
    f. ein Mitglied der URZ-Abteilung für IT-Infrastruktur,
    g. ein(e) Vertreter(in) des wissenschaftlichen Personals.
3. Das ISMT wird im operativen Geschäft vom **Universitätsrechenzentrum** unterstützt.
4. Das ISMT und das Universitätsrechenzentrum greifen bei Bedarf auf Rat und Unterstützung von **externen Beratern** zurück (z. B. von Spezialisten für Teilbereiche der Informationssicherheit).
5. Die/der ITSB hat den Vorsitz über das ISMT inne. Er wird vom stellvertretenden ITSB gemäß den üblichen Regelungen vertreten.
6. Alle Fakultäten und Einrichtungen, die selbst IT-Services betreiben bzw. Arbeitsplatzrechner administrieren, benennen nach Vorgabe des ISMT **dezentrale IT-Sicherheitsbeauftragte** und Stellvertreter. Durch die Benennung müssen alle IT-Services im Geltungsbereich sowie die für den Betrieb vor Ort verantwortlichen Personen einem/ einer IT-Sicherheitsbeauftragten zugeordnet sein.
7. Beteiligung der Nutzer: Das ISMT arbeitet mit dem **IT-Beirat** zusammen.
8. Die Einsetzung von dezentralen IT-Sicherheitsbeauftragten sowie von Vertretern im IT-Beirat entbindet die **Leitung der Einrichtungen und Fakultäten** nicht von ihrer Verantwortung (auch) für die Informationssicherheit in ihrem Zuständigkeitsbereich.

8. Aufgabenverteilung zur Informationssicherheit

1. Das ISMT arbeitet strategisch und ist für die Erstellung der Rahmenrichtlinien verantwortlich. Es initiiert, steuert und kontrolliert die Umsetzung des Informationssicherheitsprozesses.
2. Das ISMT berichtet (i.d.R. über den zentralen ITSB) regelmäßig dem CIO-Gremium.
3. Das Universitätsrechenzentrum unterstützt das ISMT bei der Wahrnehmung seiner Aufgaben und gibt die hochschulinternen technischen Standards zur Informationssicherheit vor. Außerdem ist das URZ für die Schulung und Weiterbildung der zentralen und dezentralen IT-Sicherheitsbeauftragten zuständig und unterstützt diese bei der Umsetzung der (die hier vorliegende Leitlinie konkretisierenden) Rahmenrichtlinien.
4. Das ISMT dokumentiert mit Unterstützung des Rechenzentrums sicherheitsrelevante Vorfälle und erstellt jährlich einen Informationssicherheitsbericht.
5. Die jeweils zuständigen IT-Sicherheitsbeauftragten sind für die Überwachung der Umsetzung aller mit dem ISMT abgestimmten Sicherheitsbelange bei den IT-Systemen und -Anwendungen sowie den Mitarbeitern in ihren Bereichen verantwortlich. Sie sind verpflichtet, sich auf dem Gebiet der Informationssicherheit weiterzubilden und ihr Wissen auf einem aktuellen Stand zu halten.
6. Der IT-Beirat unterstützt den Informationssicherheitsprozess, indem er als Multiplikator die Informationen aus dem ISMT an die Nutzerschaft weitergibt und auch umgekehrt den Bedarf der Nutzerschaft an das ISMT kommuniziert.
7. Das Universitätsrechenzentrum ist für die system-, netz- und betriebstechnischen Aspekte der Informationssicherheit verantwortlich. Es arbeitet eng mit dem ISMT zusammen.
8. Die Fakultäten und Einrichtungen der Universität sind verpflichtet, bei allen relevanten Planungen, Verfahren und Entscheidungen mit Bezug zu Informationssicherheit die jeweils zuständigen IT-Sicherheitsbeauftragten sowie das ISMT zu beteiligen.
9. Die am Informationssicherheitsprozess Beteiligten arbeiten in allen Belangen der Informationssicherheit zusammen, stellen die dazu erforderlichen Informationen bereit und regeln, soweit noch nicht geschehen, die Kommunikations- und Entscheidungswege sowohl untereinander wie auch in Beziehung zu Dritten eigenverantwortlich und im Sinne der hier niedergelegten Grundsätze. Hierbei ist insbesondere der Aspekt der in Krisensituationen gebotenen Eile zu berücksichtigen.

9. Umsetzung des Informationssicherheitsprozesses

1. Das ISMT initiiert, steuert und kontrolliert die Umsetzung des Informationssicherheitsprozesses, der nach festzulegenden Prioritäten technische und organisatorische Maßnahmen sowohl präventiver als auch reaktiver Art sowie Maßnahmen zur schnellen Krisenintervention umfassen muss.
2. Die zentralen IT-Sicherheitsbeauftragten sind zuständig, im URZ den Informationssicherheitsprozess zu steuern und zu überwachen.
3. Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des Informationssicherheitsprozesses in ihrem Zuständigkeitsbereich verantwortlich. Sie informieren regelmäßig sowohl die Leitung ihrer Einrichtung als auch das ISMT und das Universitätsrechenzentrum über den Stand der Umsetzung und über aktuelle Problemfälle.
4. Der IT-Beirat bildet ein Forum, um (unter anderem) die Umsetzung des Informationssicherheitsprozesses hochschulweit abzustimmen und Erfahrungen auszutauschen.

10. Gefahrenintervention/Notfallvorsorge

1. Für akute Störfälle sowie für eine möglichst schnelle Wiederherstellung der Verfügbarkeit der IT-Ressourcen nach Eintritt von Schadensereignissen sind **Notfallpläne** für wichtige Dienste in allen Einrichtungen der Hochschulen, insbesondere für zentrale Dienste im Universitätsrechenzentrum, von den jeweiligen Dienstverantwortlichen zu erarbeiten, durch Notfallübungen zu überprüfen und regelmäßig fortzuschreiben. Einzelheiten bestimmt das ISMT.
2. **Bei Gefahr im Verzuge** veranlassen die zuständigen IT-Sicherheitsbeauftragten (dezentral oder zentral) in Abstimmung mit mindestens einem (weiteren) ISMT-Mitglied die sofortige vorübergehende **Stilllegung** betroffener IT-Systeme, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden nicht anders abzuwenden ist. Die URZ-Leitung und der zentrale ITSB sind unverzüglich zu informieren.
3. Die **Wiederinbetriebnahme** erfolgt erst nach der Durchführung hinreichender Sicherheitsmaßnahmen in Abstimmung mit dem zuständigen ITSB und dem Universitätsrechenzentrum. Der zentrale ITSB wird darüber informiert.

11. Vorbeugende Maßnahmen

Für die Sicherstellung der Informationssicherheit sind vorbeugende Maßnahmen notwendig. Mit geeigneten technischen und organisatorischen Maßnahmen sollen Gefährdungsrisiken erfasst und eingedämmt sowie Angriffe auf die IT-Sicherheit frühzeitig erkannt werden. Bereichsübergreifende Maßnahmen werden im ISMT koordiniert. Die Durchführung vorbeugender Maßnahmen obliegt dem jeweils zuständigen IT-Systembetreiber.

12. Finanzierung

Die Hochschulleitung ist grundsätzlich für die Finanzierung aller für die Erreichung eines angemessenen Niveaus der Informationssicherheit erforderlichen Maßnahmen verantwortlich. Insbesondere stellt sie (in der Regel über das URZ) personelle und finanzielle Ressourcen für zentrale Informationssicherheitsmaßnahmen bereit und finanziert kontinuierliche Fortbildungsmaßnahmen für alle IT-Sicherheitsbeauftragten.

Weiterführende Informationsicherheitsmaßnahmen finanziert zunächst der Teilbereich, der diese Maßnahmen initiiert und verantwortet; auf Empfehlung des ISMT oder des CIO-Gremium kann abweichend eine zentrale Finanzierung erfolgen.

13. Kontinuierliche Weiterentwicklung des Informationssicherheitsprozesses

Das ISMT hat die Aufgabe, die IT-Sicherheitsstrategie und die Wirksamkeit der bisherigen Organisationsform, Maßnahmen und Prozesse für Informationssicherheit kontinuierlich zu überprüfen und weiterzuentwickeln und der Hochschulleitung mindestens alle zwei Jahre darüber zu berichten.

14. Inkrafttreten

Diese IT-Sicherheitsleitlinie für die Katholische Universität Eichstätt-Ingolstadt tritt am Tag der Bekanntmachung in Kraft.

Ausgefertigt aufgrund des Beschlusses des Präsidiums vom 3. Juli 2018.

Eichstätt/Ingolstadt, den 10. August 2018

Prof. Dr. Gabriele Gien
Präsidentin

Diese Richtlinie wurde am 10. August 2018 in der Katholischen Universität Eichstätt-Ingolstadt niedergelegt. Die Niederlegung wurde am gleichen Tag in der Katholischen Universität Eichstätt-Ingolstadt bekannt gemacht. Tag der Bekanntmachung ist daher der 10. August 2018.