Leitlinie zur Informationssicherheit an der Universität Koblenz

Grundlage: Generische Leitlinie zur Informationssicherheit RARP/AG IT- und Informationssicherheit

Inhaltsübersicht

Präambel

Die Universität Koblenz ist die jüngste Universität Deutschlands – und fußt gleichzeitig auf einer langen akademischen Tradition. Zum Erreichen ihrer strategischen Ziele und der Erfüllung ihrer Aufgaben in Forschung, Studium und Lehre, Transfer und Verwaltung spielen Informationen eine zentrale Rolle. Informationen bilden die Grundlage fast aller universitätsweiten Abläufe. Aufgabe der Informationssicherheit ist es, diese Informationen, ob in analoger oder digitaler Form, und die zu ihrer Verarbeitung und Speicherung erforderlichen Prozesse und Systeme zu schützen. Auf diese Weise trägt sie maßgeblich dazu bei, dass die Universität Koblenz ihrem gesetzlichen Auftrag und ihren Selbstverpflichtungen gerecht werden kann.

Die Informationssicherheit an der Universität Koblenz orientiert sich an der europäischen Datenschutzgrundverordnung (DSGVO) sowie den jeweils aktuellen Richtlinien zum IT-Grundschutz, veröffentlicht im IT-Grundschutz-Kompendium[1] des Bundesamtes für Sicherheit der Informationstechnik (BSI) und dem vom ZKI e.V. daraus abgeleiteten IT-Grundschutz Profil für Hochschulen[2].

Die Universität Koblenz bekennt sich zu den Zielsetzungen der Informationssicherheit und deren verantwortungsvoller Umsetzung. Die Leitlinie zur Informationssicherheit an der Universität Koblenz dokumentiert dieses Bekenntnis und formuliert den strategisch-organisatorischen Rahmen der Informationssicherheit an der Universität Koblenz.

Geltungsbereich

Die Leitlinie zur Informationssicherheit an der Universität Koblenz gilt für alle Personen und Institutionen, die IT-Infrastruktur, Netzwerke und daran angeschlossene IT-Systeme der Universität Koblenz an beliebigen Standorten der Universität Koblenz nutzen oder selbst IT-Systeme in diesem Umfeld betreiben.

Ziele

Die Maßnahmen zur Informationssicherheit sollen ein auf einer Risikoanalyse basierendes, angemessenes Sicherheitsniveau sowie gleichzeitig die Freiheit von Forschung und Lehre gewährleisten, um Schaden von der Universität Koblenz abzuwenden. Um das angestrebte Sicherheitsniveau zu erreichen und die jeweils geltenden gesetzlichen und vertraglichen Regelungen zu erfüllen, werden folgende Ziele angestrebt:

Verfügbarkeit:

Systeme, Anwendungen und Daten müssen den Berechtigten in jeder Situation wie vorgesehen zeitgerecht zur Verfügung stehen.

Vertraulichkeit:

Der Zugriff auf und die Nutzung von Daten jeglicher Art darf ausschließlich durch berechtigte Personen in definierter und zulässiger Weise erfolgen. Diese Festlegung erfolgt durch das Kollegiale Präsidium, das Zentrum für Informations- und Medientechnologien (ZIMT) und die/den Beauftragten der Hochschulleitung für IT-Sicherheit.

[1] BSI IT-Grundschutz-Kompendium (in der jeweils aktuellen Fassung, zuletzt Edition 2023)
[2] IT-Grundschutz-Profil für Hochschulen (ZKI-Kennung erforderlich, zuletzt abgerufen am 1.12.2021)

Integrität:

Die Unversehrtheit von Daten muss jederzeit gewahrt sein. Dies umfasst auch, dass Informationen und Daten nicht unerlaubt erstellt oder verändert werden können.

Authentizität:

Daten und Informationen stammen nachweislich aus den angegebenen Quellen, wurden bei der Übertragung nicht verändert, und die Urheber der Daten lassen sich zweifelsfrei nachvollziehen.

Nichtabstreitbarkeit:

Der Versand und Empfang von Daten und Informationen soll von den an der Zusammenarbeit beteiligten Personen nicht in Abrede gestellt werden können.

Strategie

Informationssicherheitsmanagement

Zum Erreichen der Sicherheitsziele wird ein Informationssicherheits-Management (ISM) aufgebaut, welches Organisationsstrukturen und Prozesse definiert, die kontinuierlich überwacht, evaluiert und den aktuellen Erfordernissen angepasst werden. Hierzu sind ein lückenloses Asset-Management und geeignete Methoden des Monitorings erforderlich.

Das ISM bildet den Kern der Sicherheitsstrategie und beinhaltet insbesondere folgende Komponenten:

Sensibilisierung

Die Universitätsmitglieder und -angehörigen werden durch geeignete Maßnahmen in die Lage versetzt, den Stellenwert der Informationssicherheit im Rahmen ihrer Tätigkeit nachzuvollziehen, die Notwendigkeit von Maßnahmen zu verstehen und ihr eigenes Handeln an den allgemeinen Sicherheitszielen auszurichten.

Risikomanagement

Das operative Risikomanagement umfasst den Regelprozess aus Identifikation von Risiken, Einschätzung und Bewertung von Risiken, Behandlung von Risiken, Überwachung von Risiken und Risikokommunikation. Aus der Risikoanalyse erfolgt in Absprache mit dem nach Geschäftsverteilungsplan (GVP) zuständigen Mitglied der Universitätsleitung durch das ZIMT die Auswahl und Umsetzung geeigneter Maßnahmen zur Behandlung beziehungsweise Minimierung dieser Risiken. Diese Maßnahmen werden im Konzept zur Informationssicherheit dokumentiert, welches jährlich überprüft wird.

Besondere organisatorische Maßnahmen sind die zu veröffentlichenden Richtlinien zur Informationssicherheit, die Vorgaben zum Umgang mit bestimmten Risiken machen. Sie sind verbindlich und werden jährlich von der oder dem Beauftragten der Hochschulleitung für IT-Sicherheit, später der oder dem Informationssicherheitsbeauftragten (ISB), überprüft.

Vorfallmanagement

Für die Behandlung von sicherheitsrelevanten Vorkommnissen werden Verantwortlichkeiten und Vorgehensweisen festgelegt. Notfallkonzepte und -pläne sollen die Wiederaufnahme bzw. Weiterführung des Geschäftsbetriebs auch in Not- und Krisenfällen unter Wahrung der Informationssicherheit gewährleisten. Dazu gehört auch die Festlegung eines Krisenmanagement-Teams Informationssicherheit im Rahmen des universitären Krisenmanagements.

Beteiligte und deren Aufgaben

Universitätsleitung

Die Gesamtverantwortung für die Informationssicherheit liegt bei der Leitung der Universität Koblenz. Sie veranlasst die Überprüfung der vom Senat beschlossenen Leitlinie zur Informationssicherheit an der Universität Koblenz und der durch sie verabschiedeten Richtlinien zur Informationssicherheit nach jeweils spätestens 5 Jahren.

Die oder der Informationssicherheitsbeauftragte (ISB)

Die Universitätsleitung strebt im Laufe des Jahres 2024 die Bestellung einer oder eines Beauftragten für Informationssicherheit (ISB) an der Universität Koblenz an, die oder der als qualifizierte Expertin oder qualifizierter Experte verantwortlich für den Bereich Informationssicherheit ist, solange nimmt die oder der Beauftragte der Hochschulleitung für IT-Sicherheit diese Aufgabe wahr. Die oder der ISB ist in Fragen der Informationssicherheit nur an Weisungen der Universitätsleitung gebunden.

Die oder der ISB ist zuständig für die Konzeption, Steuerung, Dokumentation und Weiterentwicklung des ISM. Darüber hinaus ist sie oder er zuständig für die Risikoanalyse, untersucht Sicherheitsvorfälle und berichtet an die Universitätsleitung zum Stand der Informationssicherheit. Sie oder er verantwortet die Erstellung des Konzepts zur Informationssicherheit und daraus abgeleiteter Richtlinien gemeinsam mit allen am Sicherheitsprozess Beteiligten. Zur Erfüllung ihrer oder seiner Aufgaben werden ihr oder ihm die notwendigen Informationen zur Verfügung gestellt.

Die oder der ISB trifft nach Maßgabe der Leitung der Universität Koblenz die erforderlichen Maßnahmen zur Informationssicherheit.

Krisenmanagement-Team Informationssicherheit

Das Krisenmanagement-Team Informationssicherheit steuert und koordiniert alle Maßnahmen im Rahmen von Sicherheitsvorfällen, solange kein universitäres Krisenmanagement eingerichtet ist. Das Kernteam besteht aus ISB, DSB und der Leitung des ZIMT. Im Krisenfall wird das Team um das gemäß GVP zuständige Mitglied der Universitätsleitung, die Präsidentin oder den Präsidenten und ggf. die Vertretung betroffener Organisationseinheiten ergänzt.

Leitung des Zentrums für Informations- und Medientechnologien (ZIMT)

Die Leitung des ZIMT ist verantwortlich für die Sicherheit der IT-Infrastruktur und der zentral betriebenen und betreuten IT-Systeme und sorgt für die Dokumentation der umgesetzten Sicherheitsmaßnahmen.

Verantwortliche für IT-Systeme

Die Verantwortlichkeit für die IT-Systeme und damit der Informationssicherheit folgt grundsätzlich den Zuständigkeiten für IT-Systeme, d. h. jede Person, die ein IT-System im Netzwerk der Universität Koblenz betreibt, ist über die gesamte Lebenszeit des Systems für den ordnungsgemäßen und sicheren Betrieb bis zur Stilllegung und fachgerechten Entsorgung verantwortlich. Während der gesamten Betriebsdauer ist dem ZIMT zu berichten und die Erfüllung der Anforderungen nachzuweisen. Der Betrieb von IT-Systemen außerhalb des ZIMT sollte nur in begründeten Ausnahmefällen erfolgen, z. B. für Forschungsprojekte.

Die oder der Datenschutzbeauftragte (DSB)

Die oder der Datenschutzbeauftragte beurteilt die Maßnahmen zur Informationssicherheit bezüglich des Datenschutzes. Sie oder er ist bei Sicherheitsvorfällen, die personenbezogene oder sonstige sensible Daten betreffen, auch schon unterhalb des Krisenfalles einzubeziehen.

Rechte und Pflichten

Mitwirkung

Die Nutzerinnen und Nutzer der IT-Infrastruktur der Universität Koblenz gehen täglich mit großen Mengen an Informationen um. Damit der Schutz dieser Informationen gelingen kann, ist die Mitwirkung all dieser Personen zwingend erforderlich. Sie schützen Informationen, Prozesse und Systeme entsprechend ihres Wertes nach bestem Wissen und Vermögen.

Kommunikation

Bei Informationssicherheitsrisiken und -vorfällen ist in jedem Fall die oder der ISB sowie die oder der unmittelbar Vorgesetzte unverzüglich zu informieren. Die Kommunikation mit Dritten außerhalb der Universität erfolgt immer durch ISB, DSB oder die Universitätsleitung. Bei der Konzeption, Einführung und Umgestaltung informationsverarbeitender Systeme und Prozesse ist neben dem ZIMT immer die oder der ISB rechtzeitig einzubinden.

Gefahrenintervention

Bei Gefahr im Verzug sind die oder der ISB, das ZIMT und die unmittelbar Verantwortlichen für die betroffenen IT-Systeme oder Prozesse berechtigt, unmittelbar notwendige Abwehrmaßnahmen vorzunehmen. Bei den zu treffenden Maßnahmen ist der Grundsatz der Verhältnismäßigkeit der Mittel zu wahren. Die Maßnahmen sollten so erfolgen, dass betroffene Nutzerinnen und Nutzer - wenn irgend möglich - bereits vorher in Kenntnis gesetzt werden.

Inkrafttreten

Die Leitlinie zur Informationssicherheit an der Universität Koblenz wurde am 05.07.2023 vom Senat der Universität Koblenz beschlossen und tritt am Tage nach ihrer Veröffentlichung im Mitteilungsblatt der Universität Koblenz in Kraft. Sie gilt bis auf Widerruf.

Koblenz, den 11. März 2024

Prof. Dr. Stefan Wehner
Präsident der Universität Koblenz