Hochschule Kaiserslautern
University of Applied Sciences

Hochschulanzeiger

der Hochschule Kaiserslautern

Freitag, den 20. Dezember 2024 **Nr. 9/2024**

INHALT **Seite**

Richtlinie zur IT-Sicherheit der Hochschule Kaiserslautern vom 06.12.2024

1. Einleitung

Diese IT-Richtlinie enthält grundlegende Informationen im Hinblick auf den Einsatz von und den Umgang mit IT-Geräten und Applikationen innerhalb der IT-Infrastruktur der Hochschule Kaiserslautern. Weiterhin enthält sie ergänzend zu den technischen Maßnahmen der IT-Verantwortlichen Anweisungen in Bezug auf Datenschutz, IT- und Informationssicherheit.

2. Geltungsbereich

Diese IT-Richtlinie gilt für alle Angehörigen der Hochschule Kaiserslautern. Dazu gehören alle Professorinnen und Professoren und Mitarbeiterinnen und Mitarbeiter (auch Teilzeitangestellte, Auszubildende sowie studentische Hilfs- und Aushilfskräfte). Ebenso gilt sie für Studierende und externe Personen, die regelmäßig die IT-Infrastruktur der Hochschule Kaiserslautern nutzen. Sie sind verpflichtet, sich an diese Richtlinie zu halten.

3. Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme und Applikationen der Hochschule Kaiserslautern sind die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit, Urheberrecht und Copyright sowie die Hochschulregelungen (insbesondere die Benutzungsordnung des Rechenzentrums[1]) einzuhalten. Sollte diesbezüglich Unsicherheit bestehen, ist der oder die Vorgesetzte zur Klärung heranzuziehen.

4. Schulung

Die Hochschule trägt Sorge dafür, dass die Beschäftigten die erforderlichen Schulungen und Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen und/oder Applikationen erforderlich sind. Die regelmäßige Teilnahme an einer Schulung zur Informationssicherheit und zum Datenschutz im Abstand von höchstens drei Jahren ist verpflichtend. Neue Beschäftigte erhalten mit der Vertragsunterzeichnung ein Informationsblatt mit entsprechenden Hinweisen. Es ist Aufgabe der Vorgesetzten, dafür Sorge zu tragen, dass die Beschäftigten aus ihrem Verantwortungsbereich die Schulungen regelmäßig absolvieren.

5. Allgemeine Regelungen

Die Hochschule Kaiserslautern stellt ihren Beschäftigten IT-Systeme und Applikationen zur Erledigung ihrer dienstlichen Aufgaben zur Verfügung. Die Installation von Software auf dienstlichen Geräten zu privaten Zwecken ist untersagt. Im Übrigen sind bei der Installation von Software auf dienstlichen Rechnern die allgemeinen Sicherheitsrichtlinien und die entsprechenden Lizenzverträge einzuhalten.

Die Benutzung privater Hard- oder Software zu dienstlichen Zwecken geschieht auf ei-

gene Verantwortung. Auch hier sind die allgemeinen Sicherheitsrichtlinien und die entsprechenden Lizenzverträge einzuhalten.

6. Arbeitsplatz

Der Arbeitsplatz ist so zu gestalten, dass Dritte ohne Berechtigung keinen Zugang haben. Büros sind, nachdem die letzte Person ihren Arbeitsplatz verlassen hat, grundsätzlich zu verschließen. Beim Verlassen des Arbeitsplatz-PCs muss der jeweilige Benutzer / die jeweilige Benutzerin den Arbeitsplatz sperren, so dass vor der erneuten Nutzung des IT- Systems und/oder der Applikation(en) eine Authentifizierung (Anmeldename / Passwort) erforderlich wird.

In Bereichen mit Publikumsverkehr sind die IT-Systeme - insbesondere die Bildschirme - so auszurichten, dass das Risiko der ungewollten Einsichtnahme durch Dritte nach Möglichkeit ausgeschlossen wird.

Informationen in Papierform sind so abzulegen, dass Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

Kann die / der Beschäftigte die zu treffenden Maßnahmen nicht eigenständig durchführen (z.B. aufgrund baulicher Restriktionen), so ist dies über die Vorgesetzte / den Vorgesetzten zu veranlassen.

7. Passwort-Gebrauch

Soweit technisch möglich, sind alle IT-Systeme und Applikationen so einzurichten, dass sie erst nach hinreichender Authentifizierung des Benutzers / der Benutzerin verwendet werden können. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Anmeldename / Passwort. Das Rechenzentrum wird, soweit keine betrieblichen oder technischen Gründe entgegen sprechen, jedem einzelnen berechtigten Nutzer / jeder einzelnen berechtigten Nutzerin einen Anmeldenamen sowie ein Passwort zuweisen.

Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben / Zahlen / erlaubte Sonderzeichen) zu gestalten. Jeder Beschäftigte/ jede Beschäftigte ist verpflichtet, sein / ihr Initial-Passwort unverzüglich zu ändern.

Die Passwörter sind so zu wählen, dass sie nicht leicht zu erraten sind. Der Anmeldename, Vor- und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345).

Bereits genutzte Passwörter dürfen bei Erneuerung eines Passworts nicht wiederverwendet werden. Das Passwort zur Hochschulkennung sollte unter keinen Umständen für weitere (insbesondere private) Dienste verwendet werden. Dies trifft auch auf administrative Zugänge per Web oder Konsole auf dienstliche Multifunktionsgeräte, Drucker, Beamer etc. zu.

Zum Management mehrerer Passwörter wird die sachgerechte Verwendung eines elektronischen verschlüsselten Passwort-Safes (beispielsweise Bitwarden, keepass oder keeweb) dringend empfohlen.

8. Schutz vor Viren und Phishing-Attacken

Zum Schutz vor Schad-Inhalten (Viren, Phishing) werden in der Hochschule Virenschutzprogramme eingesetzt. Sowohl ein- als auch ausgehende E-Mail-Kommunikation wird durch die eingesetzten Virenschutzprogramme überprüft. Einzelheiten zum Virenschutz und zur Behandlung virenbehafteter E-Mails können den Ergänzungen zur Benutzungsordnung des Rechenzentrums[2] entnommen werden.

Für den Fall, dass eine E-Mail mit einem unbekannten bzw. verdächtigen Dateianhang oder verdächtigen Links zugestellt wird, sollte der Anhang keinesfalls geöffnet oder Links aktiviert werden. Ist der Absender der Mail nicht zweifelsfrei als vertrauenswürdig einzustufen - z.B. durch eine gültige digitale Signatur - ist es ratsam das Rechenzentrum zu kontaktieren.

Um das Risiko des Eindringens von Viren über andere Kommunikationskanäle zu minimieren (bösartige Webseiten, USB-Sticks oder anderweitige Datenträger) ist jeder IT-Arbeitsplatz mit einem aktuellen Virenscanner auszustatten. Beratung sowie Lizenzen sind im Rechenzentrum erhältlich.

9. Schutz vor unverlangter Werbung („Spam“)

Zum Schutz vor unverlangter Werbung durch E-Mail werden in den Rechenzentren so genannte Spam-Filter eingesetzt. Einzelheiten zum Schutz vor SPAM-Mails können den Ergänzungen zur Benutzungsordnung des Rechenzentrums[2] entnommen werden.

10. Nutzung von E-Mail

Für dienstliche Belange ist ausschließlich das von der Hochschule zur Verfügung gestellte E-Mail-Konto zu verwenden. Eine Weiterleitung oder Anbindung an ein privates E-Mail-Konto ist nicht zulässig.

Bei der Übermittlung personenbezogener Daten per E-Mail[3] ist darauf zu achten, dass eine Offenlegung von Daten ausgeschlossen wird, insbesondere wenn diese ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.

Der Einsatz von digitalen Signaturen in dienstlichen E-Mails und die Verschlüsselung vertraulicher Inhalte wird dringend empfohlen.

Als Alternativen für die Datenübermittlung bieten sich die von der Hochschule bereitgestellten Cloud-Dienste an (siehe folgender Abschnitt).

11. Nutzung von Cloud-Diensten

Für dienstliche Zwecke stellt die Hochschule einen persönlichen Zugang zu Hochschul-Cloud-Diensten (z.B. Seafile) bereit. Zur Speicherung personenbezogener oder sonstiger sensibler dienstlicher Daten ist die Verwendung von nicht-datenschutzkonformen Cloud-Diensten (wie z.B. Dropbox, Google Drive, Microsoft OneDrive) nicht gestattet.

12. Online Terminplaner

Zur gemeinsamen Abstimmung dienstlicher Termine per Internet ist auf Werbefreiheit und Datenschutz-Konformität zu achten. Es wird empfohlen den DFN-Terminplaner

zu verwenden (Terminplaner.dfn.de).

13. Richtlinie für soziale Medien

Die Hochschule verfügt über Auftritte bei verschiedenen soziale Medien Plattformen, die zentral vom Team der Öffentlichkeitsarbeit gepflegt werden. Weitere, eigenständige Auftritte im Namen der Hochschule sind dem Team der Öffentlichkeitsarbeit anzuzeigen. Die inhaltliche Verantwortlichkeit liegt bei der Person, die die Einrichtung dieses Auftritts veranlasst hat. Sie ist auch für die Einhaltung geltender Rechtsnormen verantwortlich und muss innerhalb des Auftritts ersichtlich sein. Bezüglich der Einrichtung und Pflege eines soziale Medien Auftritts ist der Leitfaden des „Bundesverband Hochschulkommunikation[4]“ zu beachten.

14. Verhalten bei Sicherheitsvorfällen

Sollte festgestellt werden, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte (durch Virenbefall, Kompromittierung des Passworts oder wenn anderweitige Anzeichen vorliegen), so hat unverzüglich eine Meldung an den Vor- gesetzten / die Vorgesetzte sowie an die zentrale E-Mail-Adresse sicherheitsvorfall@hs-kl.de [oder cert@hs-kl.de] zu erfolgen. Dies gilt insbesondere dann, wenn sich die Gefährdung auf personenbezogene Daten bezieht.

Allgemeine Fragen zum Thema IT-Sicherheit richten Sie bitte an informationssicherheit@hs-kl.de, Fragen zum Thema Datenschutz richten Sie bitte an datenschutz@hs-kl.de.

15. Inkrafttreten

Diese Richtlinie zur Informationssicherheit für die Hochschule Kaiserslautern wurde vom Senat am 24.5.2023 in der 161. Sitzung verabschiedet und tritt am Tag nach der Veröffentlichung im Hochschulanzeiger Kaiserslautern in Kraft.

Kaiserslautern, den 06.12.2024

Prof. Dr. Ing. Hans-Joachim Schmidt
Präsident der Hochschule Kaiserslautern

---

[1] Benutzungsordnung des Rechenzentrums
[2] Ergänzungen des Rechenzentrums zur Benutzungsordnung
[3] Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail
[4] Leitfaden des Bundesverbands Hochschulkommunikation

Leitlinie zur Informationssicherheit der Hochschule Kaiserslautern vom 06.12.2024

1. Präambel

Die Hochschule Kaiserslautern ist eine forschungsstarke Hochschule für Angewandte Wissenschaften mit fachlicher Fokussierung auf Technik, Wirtschaft, Gestaltung und Gesundheit mit der Informatik als integrierender Querschnittskompetenz. Zum Erreichen ihrer strategischen Ziele und der Erfüllung ihrer Aufgaben in Forschung, Lehre und Verwaltung spielen Informationen eine zentrale Rolle. Informationen bilden die Grundlage fast aller hochschulweiten 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 Hochschule Kaiserslautern ihrem gesetzlichen Auftrag und ihren Selbstverpflichtungen gerecht werden kann.

Die Informationssicherheit an der Hochschule Kaiserslautern orientiert sich an der 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 Leitung der Hochschule Kaiserslautern bekennt sich zu den Zielsetzungen der Informationssicherheit und deren verantwortungsvollen Umsetzung. Die Leitlinie zur Informationssicherheit dokumentiert dieses Bekenntnis und formuliert den strategisch-organisatorischen Rahmen der Informationssicherheit an der Hochschule Kaiserslautern.

2. Geltungsbereich

Die Leitlinie gilt für alle Personen, Institutionen sowie für die von der Hochschule versorgten An- und In-Institute, die IT-Infrastruktur, Netzwerke und daran angeschlossene IT-Systeme der Hochschule Kaiserslautern an beliebigen Standorten der Hochschule Kaiserslautern nutzen oder selbst IT-Systeme in diesem Umfeld betreiben.

3. Ziele

Die Maßnahmen zur Informationssicherheit, welche in einer IT-Richtlinie bzw. Maßnahmenkatalog festgelegt sind, sollen ein, auf einer Risikoanalyse basierendes, angemessenes Sicherheitsniveau gewährleisten, um Schaden von der Hochschule Kaiserslautern abzuwenden. Um das angestrebte Sicherheitsniveau zu erreichen und die jeweils geltenden gesetzlichen Regelungen[3] zu erfüllen, werden folgende Ziele

---

[1] BSI IT-Grundschutz-Kompendium

[2] IT-Grundschutz-Profil für Hochschulen

[3] Hochschulgesetz, Bundesdatenschutzgesetz (BDSG), Telekommunikationsgesetz (TKG), EU-Datenschutzgrundverordnung (EU DS-GVO)

angestrebt:

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

Vertraulichkeit:
: Der Zugriff und die Nutzung von Daten jeglicher Art darf ausschließlich durch berechtigte Personen in definierter und zulässiger Weise erfolgen.

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 Informationen soll von den beteiligten Personen nicht in Abrede gestellt werden können.

4. Strategie

Informationssicherheitsmanagement

Zum Erreichen der Sicherheitsziele wird ein Informationssicherheits-Managementsystem (ISMS) etabliert, 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 ISMS berücksichtigt in angemessener Weise die Belange der Fachbereiche in Lehre, Forschung und Innovation.

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

Sensibilisierung

Die Hochschulmitglieder werden durch geeignete Maßnahmen (Schulungen, Infomails) 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 der Leitung der Hochschule, des ISB, der Leitung des Rechenzentrums sowie den EDV-Verantwortlichen der Fachbereiche die Auswahl und Umsetzung geeigneter Maßnahmen zur Behandlung beziehungsweise Minimierung dieser Risiken. Diese Maßnahmen werden im Konzept zur Informationssicherheit dokumentiert, welches jährlich durch den ISB 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 überprüft.

Vorfallmanagement

Für die Behandlung von sicherheitsrelevanten Vorkommnissen werden Verantwortlichkeiten (IT-Leitung) und Vorgehensweisen mithilfe von definierten Prozessen 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 (Zusammensetzung siehe Risikomanagement).

5. Beteiligte und deren Aufgaben

Hochschulleitung

Die übergeordnete Verantwortung für die Informationssicherheit liegt bei der Leitung der Hochschule Kaiserslautern. Sie stellt notwendige Ressourcen bereit und verabschiedet die vorliegende Leitlinie zur Informationssicherheit und veranlasst deren Überprüfung nach spätestens 3 Jahren.

Informationssicherheitsbeauftragte/r (ISB)

Die Hochschulleitung bestellt eine Beauftragte / einen Beauftragten für Informationssicherheit (ISB) an der Hochschule Kaiserslautern, die / der als qualifizierte/r Expertin / Experte verantwortlich für den Bereich Informationssicherheit ist. Die / der ISB ist in Fragen der Informationssicherheit nur an Weisungen der Hochschulleitung gebunden.

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

Die / der ISB hat in Abstimmung mit der Hochschulleitung Weisungsrecht in kritischen Fragen der Informationssicherheit.

Krisenmanagement-Team Informationssicherheit

Das Krisenmanagement-Team steuert und koordiniert alle Maßnahmen im Rahmen von Sicherheitsvorfällen. Das Kernteam besteht aus ISB, DSB (Datenschutzbeauftragter) und der Leitung der zentralen IT-Abteilung. Im Krisenfall wird das Team durch Vertreter der Hochschulleitung und ggf. Vertreter betroffener Einrichtungen ergänzt. Hierzu muss jede Einrichtung (Fachbereich, Institution der Hochschule) einen IT-Verantwortlichen benennen.

Leitung der zentralen IT-Abteilung

Die Leitung der zentralen IT-Abteilung 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 Informationssicherheit folgt grundsätzlich den Zuständigkeiten für IT-Systeme, d. h. jeder der ein IT-System im Netzwerk der Hochschule Kaiserslautern betreibt, ist über die gesamte Lebenszeit des Systems für den ordnungsgemäßen und sicheren Betrieb bis zur Stilllegung und fachgerechten Entsorgung verantwortlich.

Datenschutzbeauftragte/r (DSB)

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

6. Rechte und Pflichten

Mitwirkung

Die Nutzenden der IT-Infrastruktur der Hochschule Kaiserslautern 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 ihrer Bedeutung für den Betrieb der Hochschule nach bestem Wissen und technischen Möglichkeiten.

Kommunikation

Bei Informationssicherheitsrisiken und -vorfällen[4] ist in jedem Fall die / der ISB sowie der oder die unmittelbar Vorgesetzte unverzüglich zu informieren. Die Kommunikation mit Dritten außerhalb der Hochschule erfolgt immer durch ISB, DSB oder die Hochschulleitung.

Bei der Konzeption, Einführung und Umgestaltung informationsverarbeitender Systeme und Prozesse ist die / der ISB rechtzeitig einzubinden.

[4] Risikoanalyse, Risiken und Vorfälle werden definiert im ISMS

7. Gefahrenintervention

Bei Gefahr im Verzug sind die / der ISB 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.

8. Inkrafttreten

Diese Leitlinie zur Informationssicherheit für die Hochschule Kaiserslautern wurde vom Senat am 24.5.2023 in der 161. Sitzung verabschiedet und tritt am Tag nach der Veröffentlichung im Hochschulanzeiger in Kraft.

Kaiserslautern, den 06.12.2024

Prof. Dr. Ing. Hans-Joachim Schmidt

Präsident der Hochschule Kaiserslautern

Ordnung
zur Änderung der Beitragsordnung
des Studierendenwerks Kaiserslautern
vom 15.12.2024

Aufgrund des § 112 Abs. 2 Satz 2, § 113 Abs. 1 Satz 2, Nr. 3 b und § 114 Abs. 5 Satz 1 des Hochschulgesetzes (HochSchG) in der Fassung vom 23. September 2020 (GVBl. S. 461), zuletzt geändert durch Gesetz vom 22. Juli 2021 (GVBl. S. 453), BS 223-41, hat der Verwaltungsrat des Studierendenwerks Kaiserslautern am 25. November 2024 die nachstehende Änderung der Beitragsordnung beschlossen. Diese Beitragsordnung hat das Ministerium für Wissenschaft und Gesundheit mit Schreiben vom 10. Dezember 2024 genehmigt.
Sie wird hiermit bekannt gemacht.

Artikel 1

Die Beitragsordnung des Studierendenwerks Kaiserslautern vom 29. November 1978 (StAnz. Nr. 1/1979) zuletzt geändert am 18.09.2024 (Amtliche Bekanntmachung Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau Nr. 9 vom 28. November 2024, Hochschulanzeiger Hochschule Kaiserslautern Nr. 7 vom 31. Oktober 2024) wird hiermit wie folgt geändert:

§ 3
Höhe des Sozialbeitrages

Die Sozialbeiträge werden zum Sommersemester 2025 wie folgt festgesetzt:

1.	Für die Studierenden der RPTU Campus Kaiserslautern	125,00 €
2.	Für die Studierenden der Hochschule Kaiserslautern, Standort Kaiserslautern	125,00 €
3.	Für die Studierenden der Hochschule Kaiserslautern, Standort Zweibrücken	125,00 €
4.	Für die Studierenden der Hochschule Kaiserslautern, Standort Pirmasens	125,00 €
5.	Für die Fernstudierenden und die Teilnehmer an berufsbezogenen Weiterbildungsstudiengängen	125,00 €

Artikel 2

Die Änderung der Beitragsordnung tritt mit Beginn des Sommersemesters 2025 in Kraft.

Kaiserslautern, 15.12.2024

Marlies Kohnle-Gros
Vorsitzende des Verwaltungsrates
des Studierendenwerks Kaiserslautern