Richtlinie zur IT-Sicherheit der Hochschule Kaiserslautern vom 06.12.2024

(Hochschulanzeiger Nr. 9/2024 vom 20. Dezember 2024, S. 2)

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 eigene 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 Vorgesetzten / 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