UNIVERSITÄT SIEGEN

Amtliche Mitteilungen

Datum **17. November 2020** **Nr. 83/2020**

I n h a l t :

Leitlinie
zur Informationssicherheit

der
Universität Siegen

Vom 16. November 2020

Herausgeber: Rektorat der Universität Siegen
Redaktion: Dezernat 3, Adolf-Reichwein-Straße 2 a, 57076 Siegen, Tel. 0271/740-4813

Leitlinie
zur Informationssicherheit

der
Universität Siegen

Vom 16. November 2020

1.
Präambel

Leistungsfähige Forschung, Lehre und Verwaltung an der Universität Siegen stützen sich auf Verfügbarkeit, Integrität und Vertraulichkeit von digitalen und analogen Informationen sowie auf funktionierende, sichere Prozesse und Dienstleistungen und bedingen somit einen kontinuierlichen Informationssicherheitsprozess.

Zur Aufrechterhaltung des Informationssicherheitsprozesses sehen die Hochschulleitung sowie alle Mitglieder und Angehörige der Universität Siegen die Informationssicherheit als gemeinsame Herausforderung und fördern die Umsetzung der Informationssicherheitsziele. Damit kommt der Informationssicherheit eine grundsätzliche und strategische Bedeutung zu, die die Entwicklung und Umsetzung eines hochschulweiten Informationssicherheitsmanagementsystems (ISMS) erforderlich macht.

Diese Leitlinie beschreibt den Informationssicherheitsprozess an der Universität Siegen, den Geltungsbereich, die Verantwortungsebenen, die Informationssicherheitsstrategie und die allgemeinen Schutzziele der Universität Siegen.

Sie wird ergänzt durch ein Rahmenkonzept, in dem u.a. die Gesamtorganisationsstruktur konkretisiert wird und sowohl risikobezogen dienste-spezifische als auch zielgruppenbezogene Maßnahmen definiert werden. Für spezielle Themenfelder werden verbindliche Richtlinien und Regelungen zur Informationssicherheit verabschiedet.

2.
Geltungsbereich

Die Leitlinie zur Informationssicherheit gilt für alle Mitglieder, Angehörige und Gäste der Universität Siegen.

Sie gilt für die gesamte Verarbeitung von digitalen und analogen Informationen an der Universität Siegen und damit insbesondere

- für alle Nutzenden von Systemen, Diensten oder Prozessen zur Informationsverarbeitung,
- für alle für die Verarbeitung von Informationen verantwortlichen Personen sowie
- für die Einheiten, die technische IT-Infrastruktur, IT-Systeme und IT-Dienste betreiben.

Externe, die Systeme, Dienste oder Prozesse der Universität Siegen zur Informationsverarbeitung nutzen und insbesondere alle, die Informationen im Auftrag der Universität Siegen verarbeiten, werden bei der Vergabe von Aufträgen auf die Einhaltung des Regelwerks zur Informationssicherheit verpflichtet.

3.
Verantwortlichkeit

Die **Universitätsleitung** trägt die Gesamtverantwortung für die Informationssicherheit an der Universität Siegen. Sie bekennt sich zu den in dieser Leitlinie formulierten Zielen, steht in vollem Umfang hinter den daraus abzuleitenden Konzepten und Maßnahmen und stellt, unter Berücksichtigung der Wirtschaftlichkeit, personelle und finanzielle Ressourcen zur Umsetzung dieser zur Verfügung.

Die **Leitungen der Einrichtungen** an der Universität Siegen tragen die Verantwortung für die Informationssicherheit für ihre Bereiche. Die **Führungskräfte** auf allen Ebenen der Universität Siegen sind dafür verantwortlich, sich aktuelle Informationen bzgl. der Informationssicherheit zu beschaffen, Maßnahmen zur Informationssicherheit entsprechend des Regelwerks zu initiieren und deren Umsetzung zu überwachen. Sie übernehmen eine Vorbildfunktion und schaffen die technischen und organisatorischen Voraussetzungen für die Informationssicherheit in ihren Bereichen.

Alle **Mitglieder, Angehörige und Gäste** der Universität Siegen sind eigenständig für die Einhaltung und Umsetzung des Regelwerks zur Informationssicherheit der Universität Siegen verantwortlich und haben dies beim Umgang mit Informationen zu beachten. Sie melden Sicherheitsvorfälle bei den entsprechenden Stellen und nehmen Informations- und Schulungsangebote der Universität Siegen wahr. Dies gilt ebenso für **Dritte**, wie beispielsweise externe Dienstleister und Kooperationspartner, die im Rahmen der Informationsverarbeitung für die Universität Siegen tätig sind (z.B. Entwicklung, Support etc.).

Verstöße gegen das Regelwerk zur Informationssicherheit

Vorsätzliche und grob fahrlässige Verstöße gegen das Regelwerk zur Informationssicherheit können nach den geltenden Regelungen und gesetzlichen Bestimmungen geahndet werden.

Beispiele für Verstöße sind:

- das mutwillige Kompromittieren der Sicherheit von IT-Systemen, Anwendungen und Prozessen,
- der vorsätzliche unberechtigte Zugriff auf Informationen und IT-Systeme,
- die unberechtigte Änderung, Nutzung, Löschung und/oder Veröffentlichung von Informationen.

4.
Informationssicherheitsstrategie und -ziele

Die Informationssicherheitsstrategie richtet sich nach den Kernaufgaben der Universität Siegen:

Lehre, Forschung, Wissenstransfer und Verwaltung, insbesondere hinsichtlich der Schutzziele der Informationssicherheit. Dies wird durch die Einführung eines universitätsweiten Informationssicherheitsmanagementsystems (ISMS), in Anlehnung an den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), etabliert.

Dazu hat die Universität Siegen die folgende Organisationsstruktur etabliert:

- **Chief Information Security Officer (CISO) und Stabsstelle Informationssicherheit**
  Die Universitätsleitung bestellt die oder den CISO der Universität Siegen; die Fach- und Dienstaufsicht obliegt der Kanzlerin oder dem Kanzler. Die oder der CISO ist zentrale Ansprechpartnerin bzw. zentraler Ansprechpartner für alle Fragen der Informationssicherheit, steuert und koordiniert den Informationssicherheitsprozess an der Universität Siegen, berät die Universitätsleitung, die Führungskräfte und alle Anwenderinnen und Anwender.

  Die oder der CISO leitet zur Erfüllung ihrer bzw. seiner Aufgaben die Stabsstelle Informationssicherheit der Universität Siegen, das Informationssicherheitsmanagement-Team sowie das Computer Emergency Response Team.

  Die oder der CISO steht in engem Austausch mit der oder dem Chief Information Officer (CIO), dem Zentrum für Informations- und Medientechnologie und der oder dem Datenschutzbeauftragten (DSB).

- **Bereichs-Informationssicherheitsbeauftragte und Informationssicherheitsmanagement-Team (ISMT)**

  Jede Fakultät sowie das Zentrum für Lehrerbildung und Bildungsforschung, die Universitätsbibliothek, das Zentrum für Informations- und Medientechnologe, und die zentrale Universitätsverwaltung benennen Bereichsinformationssicherheitsbeauftragte, die die Leitungen der Einrichtungen bzgl. der Umsetzung des universitätsweiten ISMS beraten und unterstützen. Weitere Einrichtungen können ebenso Bereichsinformationssicherheitsbeauftragte benennen.

  Sie bilden gleichzeitig das Informationssicherheitsmanagement-Team. Das ISMT berät und unterstützt die Informationssicherheitsbeauftrage oder den Informationssicherheitsbeauftragten in Fragen zur strategischen Weiterentwicklung des Informationssicherheitsprozesses und koordiniert übergreifende Maßnahmen in der Gesamtorganisation.

- **Computer Emergency Response Team (CERT)**

  Für die sicherheitsrelevanten Tätigkeiten auf operativer Ebene wird ein zentrales Computer Emergency Response Team (CERT) aufgebaut und etabliert. Das CERT agiert sowohl präventiv, beispielsweise durch die Bekanntgabe von Warnmeldungen und Sicherheitsproblemen, die Ermittlung von sicherheitsrelevanten Schwachstellen in Systemen und Netzen etc. als auch reaktiv, beispielsweise bei der Minderung der Auswirkungen von Sicherheitsvorfällen oder deren Bereinigung.

- **Projekt-Informationssicherheitsbeauftragte**

  Für große Projekte (z.B. im Rahmen der Digitalisierung) werden Projekt-Informationssicherheitsbeauftragte benannt, die die Projektleitungen hinsichtlich Informationssicherheit beraten.

  Die Konkretisierung der Aufbauorganisation der Informationssicherheit wird im Rahmenkonzept zur Informationssicherheit der Universität Siegen beschrieben.

Jede Einrichtung kann für ihren Bereich über die universitätsweit geltenden Regelungen hinausgehende, angepasste Informationssicherheitsziele und -strukturen aufstellen.

Das Gesamtkonzept der Informationssicherheit wird regelmäßig auf seine Aktualität, Angemessenheit und Wirksamkeit geprüft und angepasst. Durch eine kontinuierliche Revision der Regelungen bzw. Richtlinien und deren Einhaltung wird das angestrebte Sicherheitsniveau gefestigt. Abweichungen werden mit dem Ziel analysiert, das Informationssicherheitsniveau zu verbessern und ständig auf dem aktuellen Stand der Informationssicherheitstechnik zu halten.

Die Universitätsleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Alle Mitglieder und Angehörigen der Universität Siegen sind angehalten, mögliche Verbesserungen oder Schwachstellen an die Stabsstelle Informationssicherheit weiterzugeben.

Ziele der Informationssicherheit und ihrer Realisierung in den entsprechenden Handlungskontexten der Universität Siegen

Aus den allgemeinen Schutzzielen der Informationssicherheit werden unter anderem folgende Informationssicherheitsziele für die Universität Siegen abgeleitet:

- Sicherstellung der **Vertraulichkeit** bei der Verarbeitung von Informationen
- Schutz der **Integrität** der Informationen, Systeme und Dienste
- Schutz der **Verfügbarkeit** von Informationen, Systemen und Diensten
- Schutz der Freiheit von Forschung, Lehre und Studium
- Einhaltung der einschlägigen Gesetze, vertraglichen Regelungen, Selbstverpflichtungen und sonstigen rechtlichen Bestimmungen
- Schutz vor Reputationsschäden
- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte
- Reduzierung der im Schadensfall entstehenden Kosten (sowohl durch Schadenvermeidung als auch Schadenverhütung) und Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Universität Siegen

5.
Leitsätze zur Informationssicherheit an der Universität Siegen

Folgende Leitsätze gelten für die Umsetzung des Informationssicherheitsprozesses an der Universität Siegen und werden durch die Universitätsleitung, die Leitungen der Einrichtungen, alle Mitglieder, Angehörige und Gäste sowie Dritte, wie beispielsweise externe Dienstleister und Kooperationspartner, eingehalten:

- Alle Nutzerinnen und Nutzer nehmen das **Schulungs- und Sensibilisierungsangebot** zur Informationssicherheit wahr.
- Der **Schutzbedarf** der Informationen an der Universität Siegen wird durch die informationsverarbeitenden Bereiche und Personen bestimmt und es werden entsprechende Schutzmaßnahmen umgesetzt. Bei Bedarf werden Risikoanalysen durchgeführt. Die Maßnahmen werden durch die Bereiche und Personen dokumentiert und regelmäßig auf ihre Wirksamkeit hin überprüft.
- Informationen, Daten und IT-Systeme werden durch die informationsverarbeitenden Bereiche und Personen dem Stand der Technik entsprechend **vor unberechtigtem Zugriff, vor Verlust und vor Manipulation geschützt.**
- IT-Systeme werden durch die informationsverarbeitenden Bereiche und Personen auf dem **aktuellen Stand** gehalten, in einer **sicheren Umgebung** betrieben und **adäquat vor schädlicher Software** (sog. Malware) **geschützt**.
- Regelmäßige **Überprüfung** der Wirksamkeit von Maßnahmen zur Informationssicherheit sowie der Einhaltung des Regelwerks.
- **Informationssicherheitsvorfälle** werden durch alle Beteiligten dokumentiert und an die oder den

CISO kommuniziert. Gegebenenfalls wird die Kommunikation für einen IT-Notfall eingeleitet. Detaillierte Festlegungen, IT-Notfälle betreffend, werden im Rahmen der Regelungen zum Umgang mit IT-Notfällen geregelt.

6.

Inkrafttreten

Diese Leitlinie tritt am Tag nach ihrer Veröffentlichung in dem Verkündungsblatt „Amtliche Mitteilungen der Universität Siegen" in Kraft.

Ausgefertigt aufgrund des Beschlusses des Rektorats vom 4. Juni 2020.

Siegen, den 16. November 2020

Der Rektor

gez.

(Universitätsprofessor Dr. Holger Burckhart)