HOCHSCHULE ANHALT

LEITLINIE

zur Informationssicherheit

vom 22.06.2022

Im Interesse der Lesbarkeit wurde auf eine unterschiedliche Darstellung von Personen-, Amts- und Funktionsbezeichnungen verzichtet, entsprechende Formulierungen gelten für alle Geschlechter gleichermaßen.

Inhaltsverzeichnis

1 Einleitung 2

1.1 Intention des Dokuments 2

1.2 Geltungsbereich der Leitlinie 2

2 Definition und Erläuterungen 2

2.1 Sicherheitsbegriffe 2

2.1 Dokumente der Informationssicherheit 4

2.2 Grundwerte der Informationssicherheit 4

2.3 Absicherungsvarianten gemäß BSI-Grundschutz 4

2.4 Informationssicherheitsniveau allgemein 5

3 Informationssicherheit an der Hochschule Anhalt 5

3.1 Stellenwert der Informationssicherheit 6

3.2 Informationssicherheitsziel 6

3.3 Absicherungsvariante 6

3.4 Informationssicherheitsniveau 6

3.5 Informationssicherheitsprozess 6

3.6 Rollen im Informationssicherheitsprozess 7

3.7 Vorgehensweise bei Verstößen gegen die Informationssicherheit 7

3.8 Vorgehensweise bei Verstößen gegen die Leitlinie zur Informationssicherheit 8

3.9 Schlussbemerkungen 8

4 Verteiler 8

5 Inkrafttreten 8

A. Anhang – Rechtliche Grundlagen 9

B. Anhang – Rollenverteilung im Informationssicherheitsprozess 11

C. Anhang – Rollenmatrix 13

Präambel

Die Die Hochschule Anhalt ist eine der forschungsstärksten Hochschulen des Landes. Im Herzen Mitteldeutschlands bietet sie als eine der innovativsten Hochschulen des Landes Sachsen-Anhalts Lehre und Forschung auf internationalem Niveau sowie beste Studien- und Lebensbedingungen. Insbesondere in den Forschungsschwerpunkten der Hochschule sowie im Rahmen der Kooperation mit anderen wissenschaftlichen Einrichtungen sichert sie ein enges Zusammenwirken mit Unternehmen und Institutionen der Region und schafft damit neue zukunftsorientierte Arbeitsplätze für gut ausgebildete und hochmotivierte Absolventen in Sachsen-Anhalt.
Die Hochschule steht Ideen, Menschen, Lehr- und Lernmethoden und Traditionen zur Förderung von Kreativität, Innovation und Lernbereitschaft offen gegenüber, muss aber auch einen Schutz der erzeugten, gespeicherten, übertragenen und verarbeiteten Informationen gewährleisten. Die Freiheit von Forschung und Lehre sowie die persönliche Freiheit sollen dabei im Einklang stehen mit den drei wichtigsten Schutzzielen eines Informationssicherheitsmanagementsystems - Vertraulichkeit, Verfügbarkeit und Integrität.
Um alle Hochschulangehörigen gleichermaßen vor dem unberechtigten Zugriff auf persönlichen Daten zu schützen und Ergebnisse wichtiger Forschungsprojekte für nicht berechtigte Dritte geheim zu halten, ist es notwendig, ein System zum Management schutzbedürftiger Informationen zu betreiben.
Über organisatorische Maßnahmen und mittels moderner und richtig eingesetzter Informationstechnik können Informationsverluste, ungewollte Informationsveränderungen oder Informationsoffenlegungen eingedämmt und beobachtet werden. Hieran haben auch alle Mitglieder einer Hochschule einzuführen.
In einem kontinuierlichen Verbesserungsprozess wird zukünftig eine Gruppe von IT-Spezialisten daran arbeiten, Bedrohungen durch Schwachstellen zu erkennen und über die Umsetzung von zuvor definierten Maßnahmen die in diesem Zusammenhang bewerteten Risiken zu minimieren oder auszuschließen.
Das Präsidium hat daher die folgende Leitlinie zur Informationssicherheit erlassen und fordert alle Beteiligten auf, sich aktiv in den Prozess der ständigen Verbesserung der Informationssicherheit einzubringen.

1 Einleitung

1.1 Intention des Dokuments

Diese Sicherheitsleitlinie ist ein übergeordnetes zentrales Instrument zur Zielbestimmung eines Informationssicherheitsmanagementsystems.

Neben den technisch notwendigen Komponenten sollen auch tiefgreifende organisatorische Eingriffe in Prozesse, Verhaltensregeln und Arbeitsweisen erfolgen um die notwendige Informationssicherheit herzustellen.

1.2 Geltungsbereich der Leitlinie

Diese Sicherheitsleitlinie richtet sich an alle Mitglieder und Angehörige der Hochschule und alle anderen Nutzer der Infrastruktur der Hochschule Anhalt.

Bestehende Rechtsgrundlagen zur Informationssicherheit entnehmen Sie bitte dem Anhang [A].

2 Definition und Erläuterungen

Bei der Gestaltung der Informationssicherheit orientiert sich die Hochschule Anhalt an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und dessen Vorgehensweise zum IT-Grundschutz. Deshalb werden die Begriffe analog zum BSI genutzt.

2.1 Sicherheitsbegriffe

Wesentliche Grundbegriffe der Sicherheitsrichtlinie sind:

- Informationssicherheit
- IT-Sicherheit
- Cybersicherheit
- Datensicherheit
- Datenschutz
- Organisationssicherheit.

Teilgebiete der Informationssicherheit sind IT-Sicherheit, Cybersicherheit, Datensicherheit und Datenschutz. Der Schutz von Personen und ihren persönlichen Daten wird ebenfalls zur Informationssicherheit gezählt, ist aber inhaltlich darüber hinaus definiert.

Die Organisationssicherheit ist Teil der Informationssicherheit, wenn der Personenschutz und das Notfallmanagement betroffen sind.

Sicherheitsbegriffe im Zusammenhang:

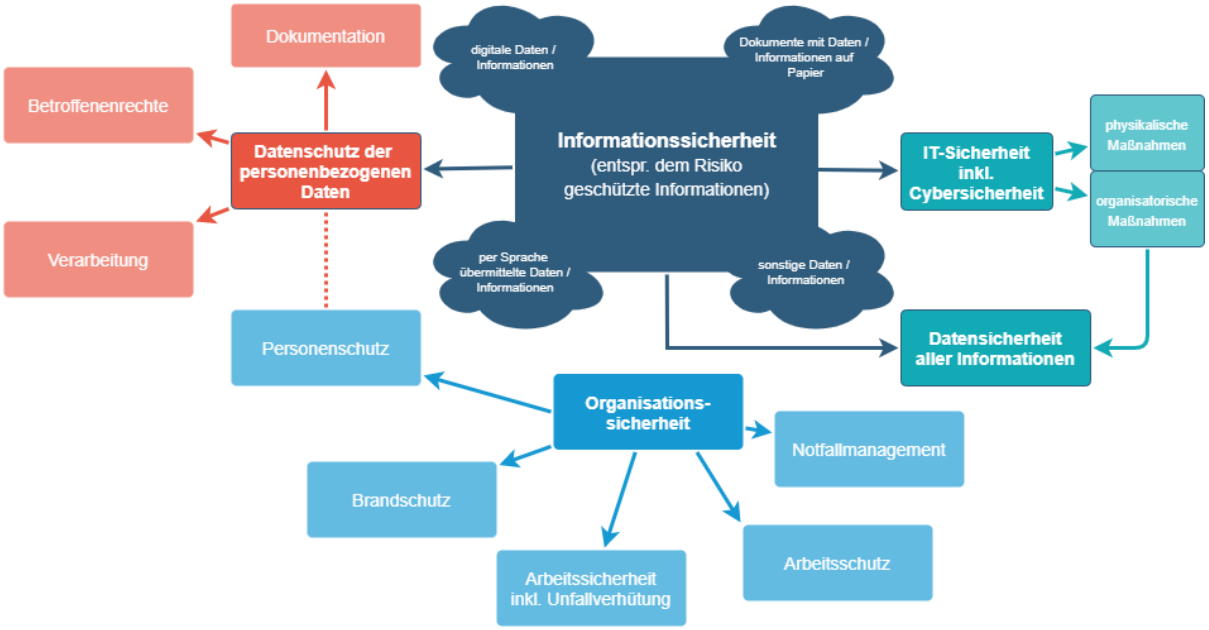


Abbildung 1: Einordnung der Sicherheitsbegriffe

Die Informationssicherheit beachtet den Schutz aller unabhängig von der Erscheinungsform und umfasst Teilgebiete der IT-Sicherheit, der Datensicherheit und des Datenschutzes.

Unter IT-Sicherheit ist die Absicherung der gespeicherten digitalen Informationen in IT-Systemen, Kommunikationsverbindungen und auf Speichergeräten zu verstehen.

Die IT-Sicherheit kann durch physikalische Maßnahmen wie Zutrittsschutz zu Gebäuden oder Räumen und durch organisatorische Maßnahmen wie die Erstellung von Richtlinien zum Gebrauch privater Technik ergänzt werden.

Als Cyber-Sicherheit oder auch Cyber-Security werden alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik verstanden. Es umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechniken und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.1

Datenschutz ist der Schutz von personenbezogenen Daten und wird zur Informationssicherheit gezählt.

Die Organisationssicherheit beschäftigt sich mit der Abwehr von Gefahren zur Gewährleistung der Sicherheit der Beschäftigten und der Umwelt (Arbeitsschutz, Personenschutz, Brandschutz, Arbeitssicherheit inkl. Unfallverhütung und Notfallmanagement).

1 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?nn=522504&cms_lv2=132798

2.1 Dokumente der Informationssicherheit

Ein Informationssicherheitsmanagementsystem unterscheidet Dokumente nach Dokumentenklasse, Vertraulichkeitseinstufung und Zielgruppe.

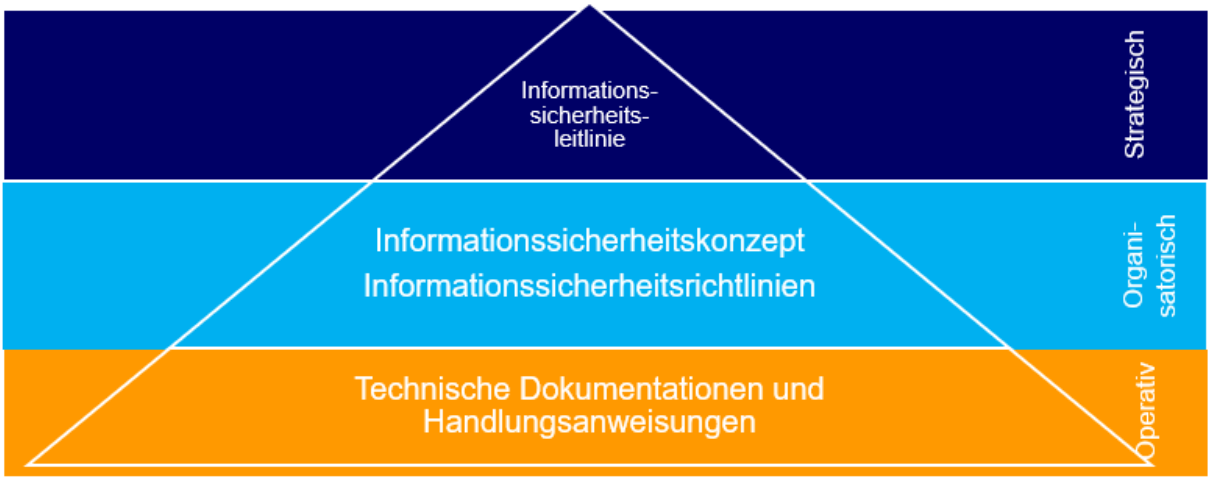


Abbildung 2: Aufbau der Dokumentation im Informationssicherheitsmanagementsystem

Die Informationssicherheitsleitlinie (ISLL) enthält die Grundsätze zur Informationssicherheit, zum Informationssicherheitsziel, zum Informationssicherheitsniveau und zum Informationssicherheitsprozess.

In der Informationssicherheitsrichtlinien werden die konkreten Anweisungen zur Absicherung konkreter Zielobjekte formuliert, die in den Bereichen umzusetzen sind. Zielobjekte können IT-Anwendungen, IT-Systeme, IT-Netze, Objekte der Infrastruktur und Objekte mit übergreifenden Funktionalitäten sein.

Technische Dokumentationen und Handlungsanweisungen beziehen sich auf ein spezifisches technisches Produkt mit seinen Eigenschaften und wie dieses sicherheitstechnisch individuell zu konfigurieren ist.

Das Informationssicherheitskonzept entsteht nach der Verabschiedung der Informationssicherheitsleitlinie enthält den Umsetzungsplan mit entsprechender Bestimmung Reihenfolge für die notwendigen generellen Erstmaßnahmen.

2.2 Grundwerte der Informationssicherheit

Die Informationssicherheit formuliert drei Grundwerte: Vertraulichkeit, Verfügbarkeit und Integrität. Die Vertraulichkeit von Informationen besteht, wenn diese nur für berechtigte Dritte zugänglich sind. Die Verfügbarkeit ist gegeben, wenn die Informationen vom berechtigten Anwender zum gewünschten Zeitpunkt genutzt werden können und als Integrität sind die Unversehrtheit und Korrektheit der Daten zu verstehen.

2.3 Absicherungsvarianten gemäß BSI-Grundschutz

Zur Absicherung der Informationssicherheit unterscheidet das BSI die Basis-, die Kern- und die Standardabsicherung. Die ersten beiden Varianten stellen die Einstiegsmöglichkeiten in ein Informationssicherheitsmanagementsystem dar. Eine Kernabsicherung wird für besonders sicherheitskritische einzelne Bereiche durchgeführt mit erhöhtem Schutzbedarf, bei denen ein Verstoß gegen die Informationssicherheit zu einer existenzbedrohenden Situation für die Organisation führen würde. Möchte man mit einer breiten Erstabsicherung beginnen, wählt man die Basis-Absicherung. Darüber hinaus kann eine Organisation mit den „SOLL-Bausteinen“ des BSI die Standardabsicherung anvisieren.

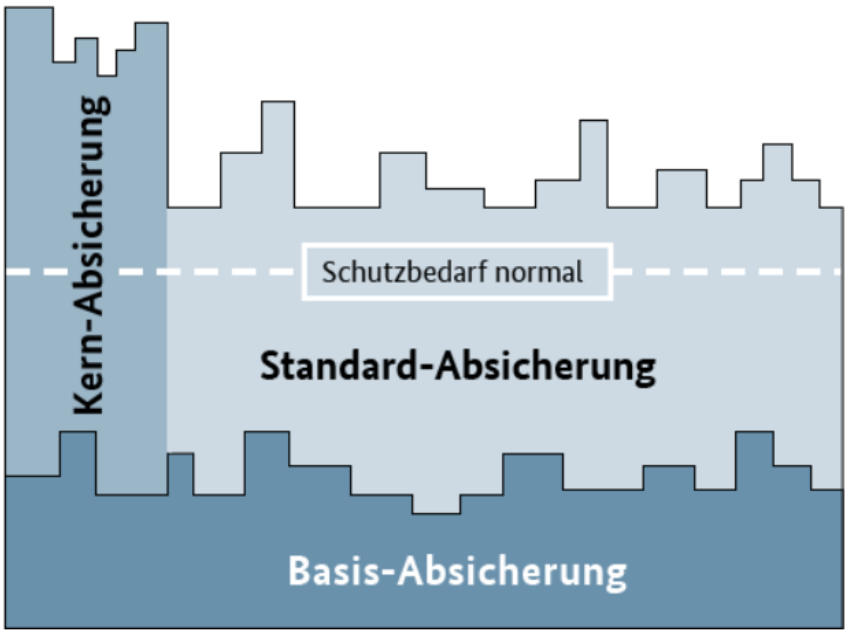


Abbildung 3: Absicherungsvarianten

2.4 Informationssicherheitsniveau allgemein

In der ersten Phase des Sicherheitsprozesses ist zu entscheiden, welches Sicherheitsniveaus angestrebt werden soll. Dabei unterscheidet man qualitativ zwischen „normal“, „hoch“ und „sehr hoch“. In der folgenden Abbildung wird dargestellt, welche Folgen bei einem Schadenseintritt in den unterschiedlichen Informationssicherheitsniveaus zu erwarten sind.

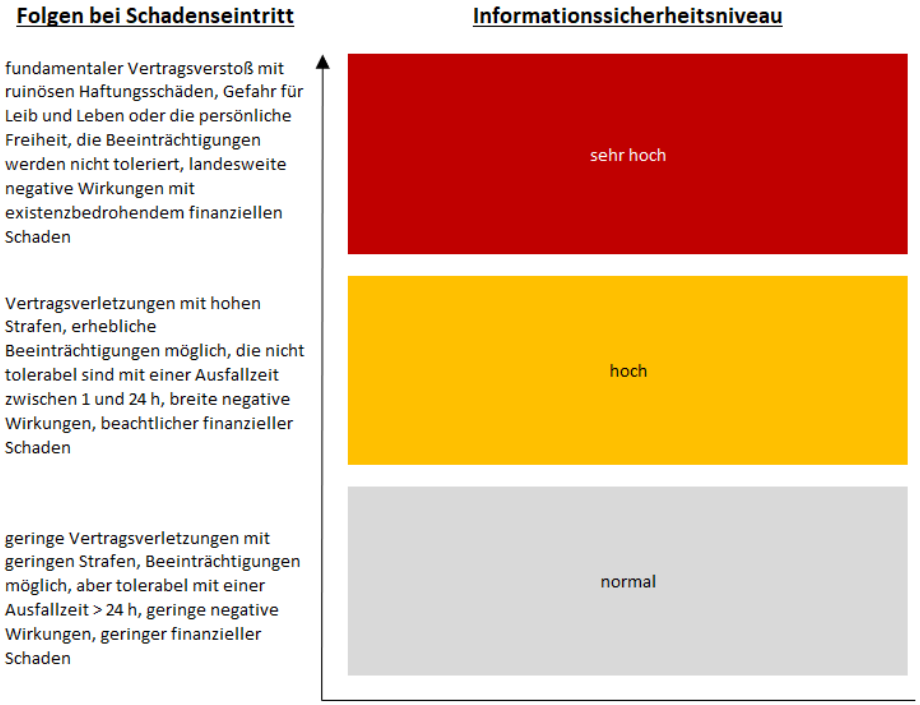


Abbildung 4: Einstufung des Informationssicherheitsniveaus

3 Informationssicherheit an der Hochschule Anhalt

Die Sicherung von Informationen ist nicht nur für solche aus IT-Systemen zu gewährleisten, sondern auch für Informationen die in analoger Form vorliegen.

Die fortschreitende Digitalisierung in allen Arbeits- und Lebensbereichen schafft bekannte und unbekannte Schwachstellen, die eine Gefahr bedeuten. Es ist stets darauf zu achten, dass ein Mindestmaß an Informationssicherheit vorherrscht.

3.1 Stellenwert der Informationssicherheit

Mit der Sicherheitsrichtleitlinie erkennt die Hochschule ausdrücklich an, dass die Gewährleistung der drei Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität der schützenswerten Informationen eine kontinuierlich zu verfolgende Aufgabe ist und geeignete technische und organisatorische Maßnahmen erfordert.

3.2 Informationssicherheitsziel

Das übergeordnete Ziel, welches mit der Verabschiedung der Informationssicherheitssicherheitsleitlinie angestrebt wird, ist:

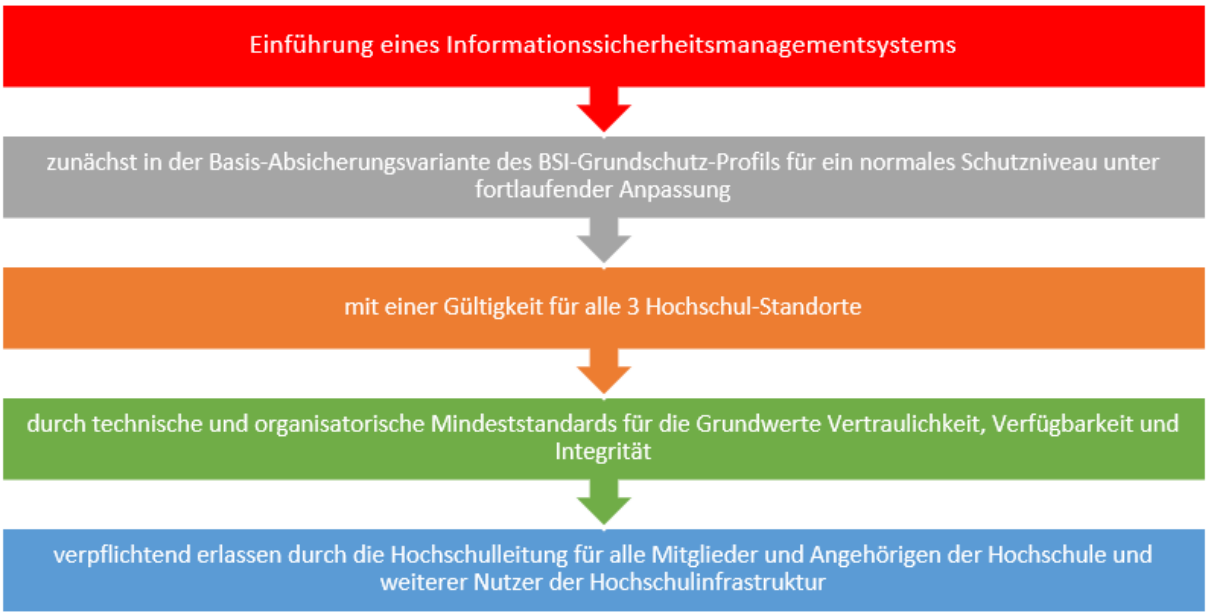


Abbildung 5: Übergeordnetes Ziel für den Informationssicherheitsprozess

3.3 Absicherungsvariante

Um eine grundlegende, breite Erstabsicherung und einen Einstieg in den IT-Grundschutz zu ermöglichen, bei der zeitnah die wichtigsten Sicherheitsanforderungen umgesetzt werden, wird für die Hochschule Anhalt die Basis-Absicherung gewählt. Danach kann bei bestehender Erforderlichkeit die sukzessive Erweiterung dieser Absicherungsvariante für spezielle einzelne kritische Prozesse erfolgen bzw. für ein höheres Sicherheitsniveau für alle Prozesse und Bereiche der Hochschule insgesamt.

3.4 Informationssicherheitsniveau

Bei einem Informationssicherheitsniveau „normal“ an der Hochschule Anhalt ist es möglich, dass auftretende Schäden zu Beeinträchtigungen der Institution führen, aber nicht zur kompletten Handlungsunfähigkeit. Es sind keine erheblichen oder schwerwiegenden Schäden zu erwarten. Durch die geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Basis-Sicherheitsmaßnahmen wird das Niveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist. Wird bei der Schutzbedarfsanalyse für ein Zielobjekt ein höherer Schutzbedarf ermittelt, erfolgt die Anpassung an dieses Schutzniveau punktuell durch Zuweisung der entsprechenden Sicherheitsmaßnahmen aus den BSI-Bausteinen für hohen und höchsten Schutzbedarf.

3.5 Informationssicherheitsprozess

Die Gesamtverantwortung für die Informationssicherheit an der Hochschule Anhalt hat der Präsident der Hochschule. Er ist verantwortlich für die Initiierung des Sicherheitsprozesses sowie für den kontinuierlichen Verbesserungsprozess zur Aufrechterhaltung der Informationssicherheit an der Hochschule Anhalt.

Trotz dieser Verantwortungszuweisung ist zu kommunizieren, dass das Thema Informationssicherheit Aufgabe aller Nutzer der Hochschulinfrastruktur ist. Oft können menschliche Anwendungsfehler zu Risiken für die Informationssicherheit führen. Aus diesem Grund sind die notwendigen Sensibilisierungs- und Schulungsmaßnahmen regelmäßig und zielgruppenspezifisch durchzuführen und nachzuweisen.

Die Hochschulleitung wird einen zentralen Informationssicherheitsbeauftragten bestellen. Dieser ist zuständig für die Bearbeitung zentraler Fragestellungen zum Thema der Informationssicherheit. Es wird ein regelmäßiger Austausch mit den am Informationssicherheitsprozess beteiligten Personen, Institutionen und Fachbereichen stattfinden und auch Zusammenkünfte unter reinen Fachspezialisten (IT-Administratoren aus den verschiedenen Fachbereichen) sind durchzuführen.

3.6 Rollen im Informationssicherheitsprozess

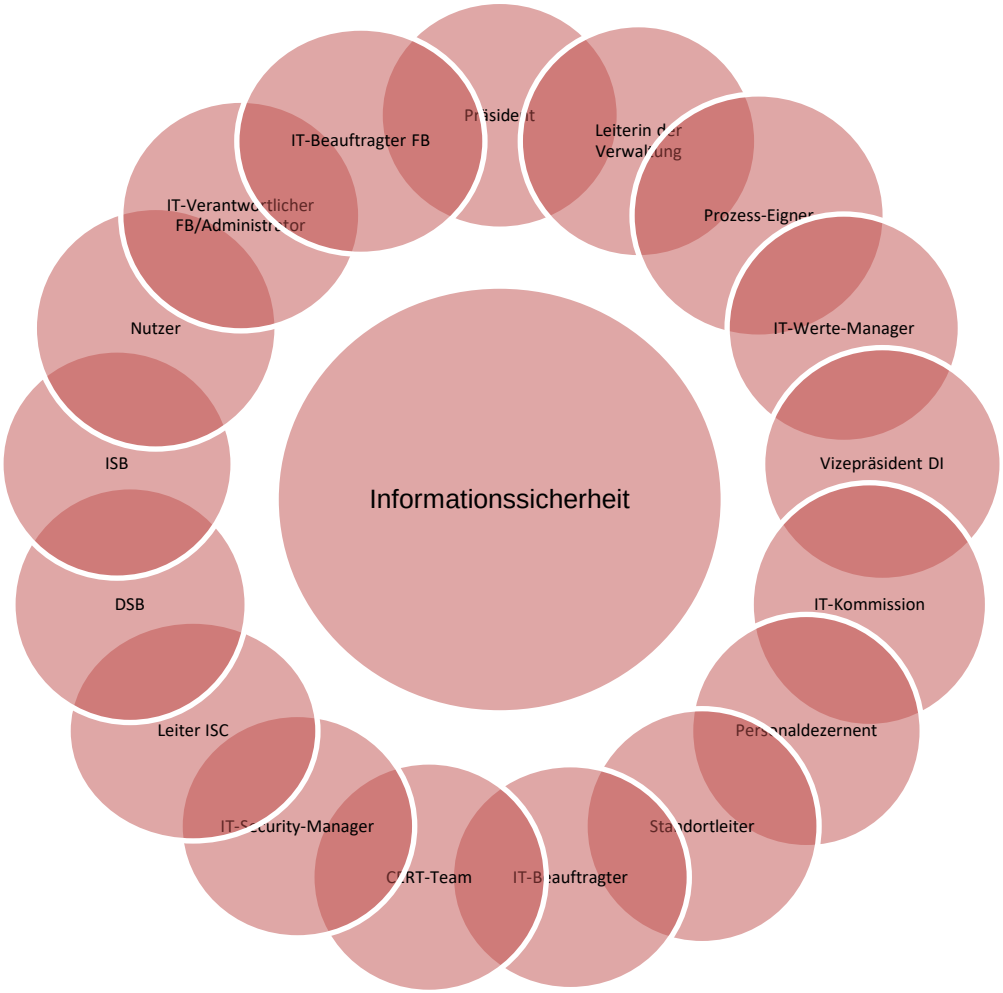
Im Informationssicherheitsprozess gibt es verschiedene relevante Rollen, die konkreten Mitarbeitern und Stellen zugewiesen werden. Sie haben die Verantwortung für bestimmte Teilbereiche im Gesamtprozess. Der Präsident kann Teile seiner Gesamtverantwortung delegieren. So werden für Mitarbeiter konkrete Verantwortungen verpflichtend festgelegt. Die Verantwortung kann somit nicht an höhere Ebenen weitergereicht oder abgelehnt werden.

Bei der technischen Umsetzung der Informationssicherheit in den einzelnen Fachbereichen oder Betriebseinheiten kommen den IT-Verantwortlichen bzw. zugeordneten Administratoren eine entscheidende Bedeutung zu. Sie sind zuständig für die Einhaltung der festgelegten und zentral organisierten Maßnahmen zur Gewährleistung der Informationssicherheit. Im Rahmen dieser beratenden Zuständigkeit sind sie berechtigt, die Zugänge auf schützenswerte Objekte zu kontrollieren, und bei Notwendigkeit auch einzuschränken bzw. Sonderlösungen nur in einer auf den jeweiligen Zweck zugeschnittenen Umgebung zu realisieren und Schwachstellen zu prüfen und abzusichern. In Betriebs- und Organisationseinheiten ohne eigenen Administrator übernimmt das das IT-Service-Center diese Aufgaben.

So können die IT-Beauftragten der Sonderstellung der Forschung Rechnung tragen. Sie beachten, dass Forschungsnetze an der Hochschule für die Informationssicherheit der Hochschule insgesamt kein Risiko darstellen und verhindern Datenabflusses und Datenveränderung.

Die verschiedenen Rollen im Rahmen der Informationssicherheit sind im Anhang [B] detaillierter beschrieben. Die tatsächlichen personellen Besetzungen dieser Rollen in der Hochschule Anhalt sind im Anhang [C] zu finden.

Die nachfolgende Abbildung stellt noch einmal grafisch die Rollen im Informationssicherheitsmanagementprozess an der Hochschule Anhalt dar. Zukünftig wird sich auch eine Arbeitsgruppe „Informationssicherheit“ ausführlich mit den Themen zur Umsetzung der Informationssicherheit beschäftigen.



Eine nähere Beschreibung der Rollen befindet sich im Anhang [B] dieses Dokuments.

Abbildung 6: Rollen im Informationssicherheitsprozess

3.7 Vorgehensweise bei Verstößen gegen die Informationssicherheit

Ein Verstoß gegen die Informationssicherheit wird als Informationssicherheitsvorfall bezeichnet. Es handelt sich dabei um ein Ereignis, das die Sicherheitsziele (also Vertraulichkeit, Verfügbarkeit oder Integrität) von schützenswerten Informationen gefährdet. Dazu gehören schützenswerte Daten, Informationen, IT-Systeme, IT-Anwendungen, IT-Netze und die Hochschulinfrastruktur an sich. Dabei sei ausdrücklich darauf hingewiesen, dass auch private oder extern betriebene Systeme, die Hochschuldaten verarbeiten, mit eingeschlossen sind.

Die ungewollte Offenlegung von schützenswerten Informationen, der Verlust eines Schlüssels zu schützenswerten Räumlichkeiten, die Nicht-Nutzbarkeit des E-Mail-Dienstes oder die ungewollte Veränderung von Daten einer Datenbank sind Beispiele für Informationssicherheitsvorfälle und damit Verstöße gegen die Informationssicherheit.

Zur Meldung eines Informationssicherheitsvorfalls oder einer Datenpanne wird ein standardisierter Arbeitsablauf in einer Verfahrensanweisung an der Hochschule Anhalt geschaffen und ein CERT-Team gebildet.

Den Mitglieder und Angehörige der Hochschule, die an den mit der IT verbundenen Prozessen der Hochschule beteiligt sind, wird empfohlen, pro Jahr mindestens an einer Schulung zur Sensibilisierung für Informationssicherheit teilzunehmen, wobei die Schulungen dabei zielgruppenspezifisch sind und in verschiedenen Medienformaten angeboten werden. Der jeweilige Vorgesetzte entscheidet darüber, wer bei einem bestimmten Vorfall an einer weiteren Schulung teilnehmen sollte. Für Professoren trifft der Dekan des Fachbereiches die Entscheidung.

3.8 Vorgehensweise bei Verstößen gegen die Leitlinie zur Informationssicherheit

Bei mutwilligen Verstößen gegen die Sicherheitsleitlinie findet zunächst ein 4-Augen-Gespräch mit dem Vorgesetzten des Fachbereichs bzw. der Struktureinheit statt. Zur Vermeidung künftiger Verstöße können Schulungsmaßnahmen durchgeführt werden. Arbeitsrechtliche Konsequenzen können sich anschließen.

3.9 Schlussbemerkungen

Ein stets an den notwendigen Schutzbedarf angepasstes Informationssicherheitsmanagementsystem hängt von einem kontinuierlichen Verbesserungsprozess ab. Ziel dieses kontinuierlichen Prozesses sollte eine entsprechende erfolgreiche Zertifizierung sein. Neben der positiven Öffentlichkeitswirkung kann eine solche Zertifizierung auch bei nationalen und europäischen Forschungsanträgen und der Zusammenarbeit mit Unternehmen Vorteile haben, wenn diese zu kritischen Infrastrukturen gehören.

Bei aller Entschlossenheit für die Umsetzung von Sicherheitsmaßnahmen müssen der Bedarf und die Sichtweise der Nutzer weiterhin beachtet werden. Es besteht sonst die Gefahr, dass die Maßnahmen nicht akzeptiert, sondern eher umgangen oder gänzlich abgelehnt werden. Es gehört demnach immer auch ein Kommunikationskonzept zu einem Informationssicherheitsmanagementsystem, welches eines der Ziele in der Umsetzungsphase sein wird.

4 Verteiler

Neben der Veröffentlichung im Intranet erhalten folgende Stellenpositionen diese Leitlinie noch einmal separat:

Präsident der Hochschule, Leiterin der Verwaltung, alle Vizepräsidenten der Hochschule, Beauftragter für Informationstechnologie, Datenschutzbeauftragter, Informationssicherheits-beauftragter, IT-Verantwortlicher der Verwaltung, Leiter IT-Service-Center, IT-Security Manager, IT-Fachbereichsbeauftragter, Technischer Standortleiter, Personalratsvorsitzender, IT-Fach-bereichsverantwortlicher, Kommission für Informationstechnologien, Personaldezernent, Leiterin Studierenden-Service-Center

5 Inkrafttreten

Diese Richtlinie tritt nach Genehmigung durch den Präsidenten am 22.06.2022 in Kraft.

Die Veröffentlichung erfolgt im Amtlichen Mitteilungsblatt der Hochschule Anhalt Nr. 89/2022 und im Intranet der Hochschule Anhalt.

Köthen, 22.06.2022

Prof. Dr.-Ing. Jörg Bagdahn

Präsident der Hochschule Anhalt

A. Anhang – Rechtliche Grundlagen

E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749) zuletzt geändert durch Artikel 1 des Gesetzes vom 16. Juli 2021 (BGBl. I S. 2941)

Das E-Government-Gesetz enthält alle wichtigen Bestimmungen, die im Hinblick auf die Weiterentwicklung der Verwaltung zu einer sicheren, modernen, bürgerfreundlichen und kostensparenden E-Government-Landschaft notwendig sind. Auch wenn die Hochschulen Einrichtungen des Landes und somit für die Bürger des Landes sind, so sind sie aus dem Geltungsbereich des E-Government-Gesetz des Landes Sachsen-Anhalt aktuell ausgenommen. Das Gesetz hat somit aktuell keine Bedeutung für die Hochschulen in Sachsen-Anhalt. Es ist jedoch möglich, dass einige Paragraphen schon bald auch im Hochschulalltag Bedeutung erlangen könnten, wie der § 7 (elektronische Bezahlmöglichkeiten) und § 8 (Nachweise, z. B. Hochladen von Kopien der Hochschulzugangsberechtigung).

Onlinezugangsgesetz vom 14. August 2017 (BGBl. I S. 3122, 3138), zuletzt geändert durch Artikel 16 des Gesetzes vom 28. Juni 2021 (BGBl. I S. 2250)

Das OZG ist ein Bundesgesetz mit einer Verpflichtung für Bund und Länder bis 31.12.2022 bestimmte Verwaltungsleistungen über Verwaltungsportale digital anzubieten. Dazu zählt das im OZG-Umsetzungskatalog definierte Themenfeld „Bildung“ mit der Lebenslage „Studium“ auch dazu. Das Onlinezugangsgesetz betrifft demzufolge auch die Hochschulen.

Derzeit wird vom BMBF und dem Land Sachsen-Anhalt an einem technikneutralen Datenaustausch-Standard zwischen den Hochschulen im deutschen und europäischen Hochschulraum gearbeitet, genannt „XHochschule“. Auch die Hochschule Anhalt wird sich dieser Entwicklung anschließen müssen, um ihren Fortbestand zu sichern. Beim Austausch personenbezogener Daten müssen dabei der Informationssicherheit und auch dem Datenschutz eine besondere Bedeutung beigemessen werden.

Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179, 251), zuletzt geändert durch Artikel 24 des Gesetzes vom 25. Juni 2021 (BGBl. I S. 2099)

Mit Telemedien lassen sich fast alle Angebote im Internet zusammenfassen, welche elektronische Informations- und Kommunikationsdienste darstellen. Also Dienste im Internet, mit denen Nutzer Informationen inhaltlich austauschen können. Insbesondere zu Themen der IT-Sicherheit sollte § 13 Abs. 7 TMG betrachtet werden. Danach ist es u. a. die Pflicht des Diensteanbieters, den Nutzer auf die Verarbeitung personenbezogener Daten hinzuweisen und Vorkehrungen zu treffen, dass kein unerlaubter Zugriff auf die genutzten technischen Einrichtungen mit Verletzung des Schutzes personenbezogener Daten möglich ist.

Die Hochschule Anhalt stellt auf verschiedenen Plattformen Online-Dienste zur Verfügung und ist in diesem Sinne ein Diensteanbieter, für den dieses Gesetz verpflichtend ist.

Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 30 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 3338)

Das Telekommunikationsgesetz regelt den Wettbewerb im Bereich der Telekommunikation. Dabei sollen die Nutzer- und Verbraucherinteressen auf dem Gebiet der Telekommunikation und das Fernmeldegeheimnis gewahrt werden.

Werden Telekommunikationsgeräte auch für private Zwecke genutzt, muss dabei zwingend auch das Fernmeldegeheimnis beachtet werden. Das bedeutet, dass weder der Inhalt des Gesprächs noch die Details der Verbindung wie Zeitpunkt, Beteiligte, Verbindungsversuche offengelegt werden dürfen.

Für die Hochschule bedeutet dies unter Umständen die Nutzer explizit darauf hinzuweisen, dass der Verstoß gegen das Fernmeldegeheimnis eine Straftat gemäß § 206 StGB ist.

IT-Strafrecht im Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 1 des Gesetzes vom 12. August 2021 (BGBl. I S. 3544)

Cybercrime ist ein Oberbegriff für Straftaten, die mittels informationstechnischer Systeme begangen werden. Das Hauptaugenmerk der Hochschule Anhalt soll auf der Vermeidung der Delikte Computersabotage, Computerbetrug und Computerspionage (also das Ausspähen und Abfangen von Daten) liegen.

Durch Schaffung von Informationssicherheit darf es unberechtigten Dritten nicht möglich sein, informationstechnische Systeme zu verändern, schützenswerte Daten zu verfälschen oder offen zu legen.

Bei Fällen der Computersabotage, Computerbetrug oder Computerspionage kommt das IT-Strafrecht zur Anwendung.

BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982)

Das Gesetz betrifft Telekommunikationsunternehmen, Anbieter von digitalen Diensten, was beispielsweise Online-Marktplätze, Suchmaschinen sowie Cloud-Computing-Dienste bereitstellt und Betreiber kritischer Infrastrukturen. Es sind Mindestanforderungen definiert, wonach die Kundendaten und die Systeme zu schützen sind.

Auch wenn die Hochschule Anhalt nicht explizit ein Adressat des IT-Sicherheitsgesetzes ist, so kann jedoch davon ausgegangen werden, dass es bei der Genehmigung von Forschungsanträgen oder bei Vertragsverhandlungen von großem Vorteil ist, wenn die Informationssicherheit entsprechend Berücksichtigung findet.

Verordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Amtsblatt L 119 vom 4.5.2016, S. 1, ber. Amtsblatt L 314 vom 22.11.2016, S. 72, Amtsblatt L 127 vom 23.5.2018, S. 2) in Geltung seit dem 25. Mai 2018

Der Artikel 32 der DSGVO bezieht sich auf die Sicherheit der Verarbeitung insbesondere von personenbezogenen Daten. Dabei geht es um den Einsatz geeigneter technischer und organisatorischer Maßnahmen unter Berücksichtigung des Stands der Technik, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Da genau das für alle Informationen (und nicht nur ausschließlich für die personenbezogenen Daten) innerhalb eines Informationssicherheitsmanagementsystem gilt, gibt es demzufolge wichtige Berührungspunkte mit dem Datenschutz.

B. Anhang – Rollenverteilung im Informationssicherheitsprozess

Bezeichnung: Präsident

Rollenbeschreibung:

Tragen der Gesamtverantwortung für die Informationssicherheit und Risikoakzeptanz, Initiierung und Unterstützung des Informationssicherheitsmanagements, Verantwortung für die organisatorische Verankerung von Aktivitäten zur Etablierung, Erhaltung und Weiterentwicklung der Informationssicherheit; oberstes beschlussfassendes Gremium und Lenkungsorgan bei übergeordneten Fragen zur Durchführung des Projekts

Bezeichnung: Vizepräsident Digitalisierung und Internationales

Rollenbeschreibung:

Integration der Informationssicherheit in die Digitalisierungsstrategie der Hochschule Anhalt, Mitarbeit bei der technischen Ausstattung und Automatisierung von Prozessen auf Basis einer Hochschuldateninfrastruktur, in der auch die Sicherheit der verarbeiteten Informationen Berücksichtigung findet

Bestimmung des Organisationsleiters, Übertragung der Realisierung der Aufgabe auf den Organisationsleiter; klare Auftragserteilung, Festlegung von Zielen und Strategien sowie Übernahme der Verantwortung für das Projekt-Budget; Interessenvertretung nach außen

Bezeichnung: Leiterin der Verwaltung

Rollenbeschreibung:

Hoheit über die Finanzierung der Institution mit Auswirkungen auf die finanziell zur Verfügung stehenden Mittel für IT-Beschaffungen, welche sich aus einer begründeten Notwendigkeit der festgelegten Sicherungsmaßnahmen ergeben müssen

Bezeichnung: IT-Beauftragter der Hochschule Anhalt

Rollenbeschreibung:

Unterstützung durch technische Beratung des Vizepräsidenten Digitalisierung und Internationales und der IT-Kommission

Bezeichnung: Informationssicherheitsbeauftragter

Rollenbeschreibung:

Ermittlung und Überwachung bestehender Schwachstellen, Reaktion auf Bedrohungslagen zusammen mit den Mitgliedern des CERT-Teams der Hochschule, Schulung der Mitarbeiter, Ansprechpartner bei Fragen zum Thema Informationssicherheit, Definition und Kommunikation von Dokumenten der Informationssicherheit

Bezeichnung: Datenschutzbeauftragter

Rollenbeschreibung:

Einhaltung der Datenschutzvorschriften im Rahmen der Datenerfassung, -verarbeitung und -weitergabe

Bezeichnung: IT Security Manager

Rollenbeschreibung:

Identifikation von technischen Sicherheitslücken in der IT-Infrastruktur, Entwicklung von Präventivmaßnahmen zum Schutz der IT-Systeme und Vorstellung dieser Maßnahmen in der IT-Kommission im Rahmen einer beratenden Funktion

Bezeichnung: Leiter IT-Service Center

Rollenbeschreibung:

Leitung des IT-Service Centers, Planung und Koordination der Prozesse innerhalb des IT-Service Centers, Repräsentation des IT-Service Centers nach außen

Bezeichnung: CERT-Team

Rollenbeschreibung:

Team von Sicherheitsexperten und IT-Fachleuten; Mitwirkung an der Lösung von konkreten Sicherheitsvorfällen; Lieferung von Lösungsansätzen oder Warnung vor Sicherheitslücken; Unterstützung bei der Aufdeckung und Analyse von Sicherheitsvorfällen, Koordination der Aktivitäten der Teilnehmer innerhalb des Informationssicherheitsvorfall-Prozesses; Bewältigung von präventiven Aufgaben neben reaktiven Aufgaben bei Vorfällen und qualitätssichernden Aufgaben im gesamten Informationssicherheitsprozess

Bezeichnung: Senatskommission für Informationstechnologien

Rollenbeschreibung:

Vorbereitungen für Beschlussfassungen übergeordneter strategischer Entscheidungen im Bereich der Informationstechnologien für die gesamte Hochschule und deren Umsetzung in den technischen und organisatorischen Maßnahmen.

Bezeichnung: IT-Verantwortlicher / IT-Administrator für den Fachbereich / die zentrale Betriebseinheit / Labor- und Projektmitarbeiter mit administrativer Verantwortung

Rollenbeschreibung:

Umsetzung der von der IT-Kommission zusammen mit dem IT-Beauftragten und der Arbeitsgruppe „Informationssicherheit" festgelegten technischen und organisatorischen Maßnahmen zur Absicherung einer aktuellen IT-Infrastruktur in ihrem jeweiligen Fach- bzw. Verantwortungsbereich mit entsprechenden weitreichenden Berechtigungen innerhalb der IT-Infrastruktur (auch auf nur lokalen Geräten); Beratung zur Beschaffung von informationssichernder Hard- und Software; Sicherstellung des Betriebs aller Komponenten der Datensicherung durch Updates, Sicherungskopien oder andere geeignete Maßnahmen; Reaktion auf Anomalien beim Betrieb des IT-Systems im Sinne einer Schadensverhinderung bzw. Schadensbegrenzung; Beratung der IT-Nutzer in Fragen der Informationssicherheit

Bezeichnung: IT-Beauftragter für den Fachbereich

Rollenbeschreibung:

Kommunikation der in der Kommission getroffenen Entscheidungen sowie Festlegung und Durchsetzung von Maßnahmen zur Verbesserung und Kontrolle zur Erhaltung der Informationssicherheit in ihrem jeweiligen Fachbereich bzw. ihrer jeweiligen Struktureinheit

Bezeichnung: Technischer Standortleiter

Rollenbeschreibung:

Ressourceneinsatzplanung zur Sicherstellung reibungsloser technischer und informationssicherer Prozesse am jeweiligen Standort, Überwachung von Fremdpersonal bei notwendigen Reparaturen, Erteilung von Zutrittsberechtigungen

Bezeichnung: Personaldezernent

Rollenbeschreibung:

Personalbedarfsplanung und Personaleinstellung unter Beachtung entsprechender Sicherheitsaspekte

Bezeichnung: Nutzer der Hochschulinfrastruktur

Rollenbeschreibung:

Anwendung und Einhaltung der Sicherheitsmaßnahmen und -mechanismen, die für die sichere Nutzung der ihnen überlassenen IT-Infrastruktur notwendig sind; Benutzer sind neben Studierenden, auch Lehrende und weitere Hochschulangehörige und Mitarbeiter sowie externe Nutzer; Information des IT-Verantwortlichen bei Feststellung von Abnormalitäten im Betrieb des IT-Systems; sichere Passwortwahl und sicherer Passwortumgang;

Bezeichnung: IT-Werte Manager (Asset Manager)

Rollenbeschreibung:

Planung und Umsetzung des optimalen Einsatzes der Hard- und Softwarewerte (Daten, Systeme, Netze, Anwendungen) der Organisation

Bezeichnung: Prozess-Eigner

Rollenbeschreibung:

Verantwortlich für die Prozesse und deren Gestaltung, die innerhalb des Projekts bezüglich ihrer Informationssicherheit von der Arbeitsgruppe bewertet und zusammen mit dem Prozess-Eigner ggf. angepasst werden

C. Anhang – Rollenmatrix

Bezeichnung	Beschreibung	Inhaber	Mitglied in der AG Informations-sicherheit ja/nein	Vertretung
Präsident	Gesamtverantwortung	Hr. Prof. Bagdahn	Nein	Hr. Prof. Kaftan
Leiter der Verwaltung	Finanzierung der Informationssicherheit	Fr. Thalmann	Nein	Hr. Severin
Vizepräsident Digitalisierung/ Internationales	Arbeitsgruppenverantwortung	Hr. Prof. Koppers	Ja	Hr. Prof. Strauß
IT-Beauftragter	Technische Beratung	Hr. Prof. Strauß	Ja	Keine
Informationssicherheitsbe-auftragter	Organisatorische Überwachung	Fr. Nitschke	Ja	Keine
Datenschutzbeauftragter	Datenschutz	Hr. Prof. Volkmann	Ja	Nachbesetzung Hr. Knopf
IT Security Manager	Technische Überwachung	Hr. Zinner	Ja	Hr. Pätzold
Leiter IT-Service-Center (ISC)	Koordination des ISC	Hr. Gast	Ja	Hr. Lingner
CERT-Team	Informationssicherheitsvor-fallbearbeitung	gem. VA_U03_00_R01	Teilweise	Gegenseitig
IT-Kommission	Vorbereitung von Beschlüssen	Hr. Prof. Koppers, Hr. Gast, Hr. Prof. Pietsch, Hr. Prof. Strauß, Hr. Prof. Lange, Hr. Prof. Baumann, Hr. Prof. Neubert, Hr. Prof. Schlechtweg, Hr. Prof. Chmielewski, Fr. Prof. Lang, Hr. Zinner, Hr. Sadina, Fr. Heckemüller, Fr. Wilhelm, Fr. Hennicke, Hr. Severin, Fr. Lewandrowski, Hr. Prof. Siemens, Hr. Giesa	Teilweise	Gegenseitig
IT-Verantwortlicher/ Administrator im Fachbereich/ in der Betriebseinheit	Technische Umsetzung	Hr. Krehan, Hr. Werner, Hr. Klein, Hr. Hummel, Hr. Königsberg, Hr. Bieniek, Hr. Engelmann, Fr. Hennicke, Hr. Winkelmann	Teilweise	Gegenseitig
IT-Beauftragter Fachbereich	Maßnahmenfestlegung Fachbereich	Hr. Prof. Knauer, Fr. Prof. Lang, Hr. Prof. Baumann, Hr. Prof. Lange, Hr. Prof. Chmielewski, Hr. Prof. Schlechtweg, Hr. Prof. Neubert	Nein	Keine
Prozess-Eigner	Prozessverantwortung	Diverse	Nein	-
Technischer Standortleiter	Standortressourcenverwaltung	Fr. Börner, Fr. Ceglarek, Fr. Scholz	Nein	Keine
Personaldezernent	Personalauswahlverfahren für IT-Bereich	Hr. Severin	Nein	Fr. Lorenz
Nutzer	Nutzung der Hochschulinfrastruktur	Diverse	Nein	-
IT-Werte-Manager	Inventarisierung sicherheitsrelevanter Assets	Hr. Hampe	Nein	keine

Stand: 22.06.2022