

Verkündungsblatt

der Fachhochschule Erfurt

Nummer 120

Sommersemester 2026

Richtlinie Informationssicherheit

Inhaltsverzeichnis

1. Dokumenteneigenschaften.....	30
2. Dokumentenhistorie.....	30
3. Mitgeltende Dokumente.....	30
4. Allgemein	31
4.1 Einleitung.....	31
4.2 Geltungsbereich.....	31
4.3 Dokumentenlenkung	31
5. Ziele der Informationssicherheit.....	32
5.1 Stellenwert an der Fachhochschule Erfurt.....	32
5.2 Ziele der Informationssicherheit	33
6. Organisation der Informationssicherheit	35
6.1 Präsidium.....	35
6.2 Bereichsleitung	35
6.3 Informationssicherheitsmanagement-Team	36
6.4 IT-Sicherheitsbeauftragte:r.....	37
6.5 Hochschulrechenzentrum	38
6.6 IT-Administrator:innen.....	39
6.7. IT-Sicherheitskoordinator:innen	39
6.8 Mitglieder und Angehörige	39
7. Folgen von Zuwiderhandlungen	40
8. Inkrafttreten	40
Anhang 1: Schaubild Organisation der Informationssicherheit	41
Anhang 2: Weitere Verantwortlichkeiten	42
Impressum.....	43

1. Dokumenteneigenschaften

Verantwortung	Hochschulleitung
Klassifizierung	Intern
Gültigkeit	Unbegrenzt
Aktualisierungsintervall	5 Jahre
Nächste Revision	

2. Dokumentenhistorie

Status	Version	Datum	Name
Erstellt	Gliederung 0.8	12.09.2023	M. Körner
	Allg. Kapitel 0.9	19.09.2023	M. Körner
Finaler Entwurf	1.0	02.05.2024	A. Gutfreund
Ergänzung ISMan-Team	1.0.1	28.08.2024	A. Gutfreund
Ergänzung Sicherheitskoordinatoren	1.0.2	06.11.2024	A. Gutfreund
Anpassungen nach Kommentaren des Präsidiums	1.0.3	31.03.2024	T. Fröhlich
Austauschen des Schaubilds Organisation der Informationssicherheit	1.0.4	16.06.2025	U. Engelbert

3. Mitgeltende Dokumente

Name	Datei/Link	Version/Datum
Grundschutzprofil für Hochschulen		
Prozesslandkarte Hochschule		
Kompendium 2023		
BSI-Standard 200-1, 200-2, 200-3		

4. Allgemein

4.1 Einleitung

Die Fachhochschule Erfurt ist eine von mehreren Hochschulen in der Landeshauptstadt Erfurt in Thüringen. Fachlich verwandte oder kooperierende Studiengänge werden an der Fachhochschule Erfurt zu sechs Fakultäten zusammengefasst, welche sich über mehrere Standorte in Erfurt verteilen. Neben der Lehre widmet sich die Fachhochschule auch der Forschung und hat sich hierbei auf drei Schwerpunkte spezialisiert. Die Kernprozesse Lehre und Forschung werden durch Verwaltungsprozesse unterstützt, wie zum Beispiel dem Personalmanagement und der Bereitstellung zentraler IT-Dienste über das Hochschulrechenzentrum.

Neben den in Verwaltungsaufgaben üblichen Informationen werden für Hochschulen spezifische Informationen wie Bewerber:innendaten, Studierendendaten, Prüfungsdaten und Forschungsdaten verarbeitet. Die Verarbeitung erfolgt größtenteils digital und wird durch eingesetzte IT-Anwendungen sowie IT-Systeme ermöglicht.

Durch die stetig steigende Abhängigkeit der Prozesse von Informationstechnologien hat sich die Fachhochschule als Ziel gesetzt, ihre IT-Systeme so zu schützen, dass eine sichere Verarbeitung der schützenswerten Informationen gewährleistet werden kann. Dies geht einher mit wachsenden regulatorischen Anforderungen, wie zum Beispiel dem Datenschutz, Haushalts- und Steuerrecht, sowie weiteren gesetzlichen Anforderungen. Es existieren außerdem vertragliche Ansprüche zur Wahrung der Informationssicherheit aus Pflichten gegenüber Drittmittelgebern oder die Nutzung des DFN-Netzes.

4.2 Geltungsbereich

Die Leitlinie zur Informationssicherheit gilt für alle Angehörigen und Mitglieder der Fachhochschule Erfurt sowie für externe Dienstleister:innen. Sie ist an allen Standorten und Einrichtungen der Hochschule verbindlich und soll sicherstellen, dass der Schutz sensibler Informationen und Daten für alle Beteiligten gewährleistet ist.

4.3 Dokumentenlenkung

Diese Leitlinie stellt die grundlegenden Regelungen zur Informationssicherheit an der Fachhochschule Erfurt dar und bildet die Basis für alle weiteren Richtlinien der Hochschule. Als übergeordnetes Dokument definiert sie die Bedeutung und die Ziele der Informationssicherheit und muss bei der Entwicklung und Umsetzung aller weiteren Richtlinien stets berücksichtigt werden.

Zudem steht sie mit den geltenden gesetzlichen Bestimmungen und anderen relevanten Vorschriften in Einklang.

5. Ziele der Informationssicherheit

5.1 Stellenwert an der Fachhochschule Erfurt

Das Präsidium übernimmt die Gesamtverantwortung für die Informationssicherheit. Informationssicherheit wird nicht als isoliertes Themengebiet betrachtet, sondern als integraler Bestandteil einer umfassenden Strategie der Fachhochschule angesehen. Die Bereitstellung der notwendigen Ressourcen sowie die Erfüllung der rechtlichen und regulatorischen Anforderungen werden vom Präsidium gewährleistet.

Für die Etablierung eines Informationssicherheitsmanagementsystems (ISMS) wurden folgende Hauptbeweggründe identifiziert:

- Schutz von organisationskritischen Informationen und Assets,
- Schutz vor Schäden,
- Erfüllung gesetzlicher und regulatorischer Anforderungen,
- Förderung des Vertrauens der Öffentlichkeit, der Nutzer:innen und weiteren Interessenträgern.

Um dies zu gewährleisten, wird sich die Informationssicherheit der Fachhochschule Erfurt an folgenden drei Schutzziele orientieren:

1. **Vertraulichkeit:** Zugriff auf Informationen wird für unautorisierte Personen unterbunden.
2. **Integrität:** Gewährleistet werden die Richtigkeit und Vollständigkeit der Informationen sowie der Verarbeitungsmethoden.
3. **Verfügbarkeit:** Bei Bedarf wird autorisierten Nutzer:innen der Zugriff auf die Informationen ermöglicht.

Bei der Erstellung von Sicherheitskonzepten orientieren wir uns am [BSI-Standard 200-2](#). Diese Methodik bietet einen strukturierten und standardisierten Rahmen für die Identifizierung und Behandlung von Informationssicherheitsrisiken und ermöglicht eine kontinuierliche Verbesserung der Informationssicherheit. Es wird ebenfalls auf das [IT-Grundschutzprofil für Hochschulen](#) zurückgegriffen, in dem bereits Systemlandschaften, Abhängigkeiten und Schutzbedarf vorgeschlagen werden.

Durch die Integration der Informationssicherheit in bestehende Prozesse unter Zuhilfenahme existierender Werkzeuge der Fachhochschule wird ein höheres Sicherheitsniveau angestrebt, ohne bestehende Abläufe und Ressourcen unnötig zu belasten.

5.2 Ziele der Informationssicherheit

Die Informationssicherheit spielt eine entscheidende Rolle bei der Erreichung der übergreifenden Ziele der Fachhochschule Erfurt. Sie ist nicht nur ein essenzielles Leistungs-, sondern auch ein Qualitätsmerkmal, das sich in allen Aspekten der IT manifestiert. Von der Entwicklung und Einführung neuer Verfahren und Produkte, über den Betrieb und die Pflege bestehender IT-Verfahren, bis hin zur Beschaffung und Beseitigung von Produkten und der Steuerung von IT-Dienstleister:innen – überall wird Informationssicherheit als integraler Bestandteil betrachtet.

Anfangs steht die Basisabsicherung nach BSI-Standard 200-2 im Vordergrund, die im Laufe der Zeit zu einer ausgereifteren Standardabsicherung weiterentwickelt wird. Dieser Ansatz ermöglicht eine kontinuierliche Verbesserung des Sicherheitsniveaus, ohne die operativen Prozesse zu stören.

Besonderer Wert wird hierbei auf die Wirtschaftlichkeit und Wirksamkeit der umgesetzten Maßnahmen gelegt. Durch sorgfältige Kosten-Nutzen-Analysen wird sichergestellt, dass jede Maßnahme nicht nur effektiv, sondern auch kosteneffizient ist. In diesem Zusammenhang wird eine Priorisierung der Sicherheitsmaßnahmen vorgenommen, wobei Risikoeinschätzungen und der potenzielle Einfluss auf die Erreichung der übergreifenden Ziele berücksichtigt werden.

Um den Erfolg der Informationssicherheitsstrategie kontinuierlich zu überprüfen, werden unabhängige, jedoch gleichartige Beurteilungen durchgeführt. Dies ermöglicht eine objektive Bewertung und sorgt für die Möglichkeit einer fortlaufenden Anpassung der Strategie.

Die Informationssicherheit trägt in vielfältiger Weise zur Erreichung zentraler Ziele bei:

a. **Bewusstsein schaffen:**

Durch gezielte Schulungen und Sensibilisierungsmaßnahmen wird ein höheres Bewusstsein für Informationssicherheit innerhalb der Fachhochschule Erfurt geschaffen, das für die Erreichung aller weiteren Ziele unerlässlich ist.

b. **Einhalten von Gesetzen und Vorschriften:**

Durch die Implementierung eines strukturierten Informationssicherheitsmanagementsystems werden Compliance-Anforderungen systematisch erfasst und erfüllt. Dies minimiert rechtliche Risiken und ermöglicht einen ordnungsgemäßen Betrieb. Die Informationssicherheit an der Fachhochschule Erfurt wird durch die nachfolgend genannten Gesetze und Verordnungen geregelt:

- [Datenschutzgrundverordnung \(DSGVO\)](#) insbesondere Artikel 24 und 32
- [Thüringer Datenschutzgesetz \(ThürDSG\)](#)
- [Gesetz zum Schutz von Geschäftsgeheimnissen \(GeschGehG\)](#)
- [Thüringer Hochschulgesetz \(ThürHG\)](#)

Die vorliegende Leitlinie zur Informationssicherheit fügt sich in ein System interner Regelungen ein, die sich die Fachhochschule Erfurt im Rahmen ihrer gesetzlichen Aufgaben selbst gegeben hat. Diese Regelungen sind bei der Anwendung dieser Leitlinie zu beachten und ergänzend heranzuziehen:

- Leitlinie Datenschutz (Entwurfsstatus)
- [HRZ-Benutzungsordnung](#)
- Rahmendienstvereinbarungen zwischen dem TMWWDG und dem HPR
- Alle [Dienstvereinbarungen der FH Erfurt](#)

Daher trägt die Informationssicherheit dazu bei, die Einhaltung von Gesetzen und Vorschriften zu gewährleisten.

c. Funktionale Aufgabenerledigung:

Die Gewährleistung der Informationssicherheit unterstützt die Fachhochschule Erfurt dabei, ihre funktionalen Aufgaben effizient und effektiv zu erfüllen, indem Datenintegrität und -verfügbarkeit sichergestellt werden.

d. Vermeidung materieller Schäden:

Durch frühzeitige Erkennung und angemessene Behandlung von Risiken lassen sich potenzielle Schäden, wie sie beispielsweise durch Cyberangriffe oder Datenverlust entstehen können, vermeiden. Besonderes Augenmerk liegt dabei auf der Verhinderung mittelbarer oder unmittelbarer finanzieller Verluste, die durch die Offenlegung sensibler Daten, ihre Manipulation oder den Ausfall einer oder mehrerer IT-Anwendungen oder -Systeme entstehen können.

e. Wahrung von Persönlichkeitsrechten und Geheimnissen:

Ein hohes Sicherheitsniveau schützt sensible Daten und wissenschaftliche Informationen, was insbesondere für die Wahrung von Persönlichkeitsrechten und die Einhaltung von Datenschutzvorgaben von Bedeutung ist. Es ist besonders wichtig, Informationen zu schützen und sicherzustellen, sodass die Vertraulichkeit und Integrität wichtiger Daten, unabhängig von ihrer Form, gewahrt bleiben.

f. Vermeidung von Ansehensverlust:

Ein angemessenes Niveau der Informationssicherheit schützt die Organisation vor dem Verlust von Ansehen und Vertrauen, der durch Sicherheitsvorfälle entstehen kann.

g. Kontinuierliche Verbesserung:

Durch ein systematisches Vorgehen, regelmäßige Überprüfungen und Anpassungen wird eine kontinuierliche Verbesserung der Informationssicherheit und damit der Hochschulprozesse erreicht.

6. Organisation der Informationssicherheit

Mit der Organisationsstruktur werden Verantwortlichkeiten und Aufgaben in der Informationssicherheit definiert. Sie stellt dar, wie die Aufgabengebiete in der Fachhochschule verteilt sind und konkretisiert das Zusammenspiel der verschiedenen Rollen in Bezug auf die Informationssicherheit. Die Zusammenhänge werden im *Anhang 1: Schaubild Organisation der Informationssicherheit* dargestellt.

6.1 Präsidium

Das Präsidium übernimmt die Gesamtverantwortung für die Informationssicherheit und stellt deren strategische Ausrichtung sicher. Es sorgt für die Bereitstellung notwendiger Ressourcen, sei es in Form von Personal, Budget oder Technologie, um eine robuste Informationssicherheitsstrategie umzusetzen. Ebenso ist es verantwortlich für die Ernennung einer:ines IT-Sicherheitsbeauftragten, die:der die Koordinierung und Überwachung der Maßnahmen übernimmt. Ein wichtiger Bestandteil der Verantwortung ist auch das Genehmigen und Überwachen eines Risikomanagementplans, der dafür sorgt, dass alle sicherheitsrelevanten Risiken identifiziert und angemessen behandelt werden.

Um die Bedeutung der Informationssicherheit in der gesamten Hochschule zu verankern, fördert das Präsidium aktiv eine Kultur der Sicherheit. Dies wird durch regelmäßige Kommunikationsmaßnahmen an alle Mitglieder und Angehörige umgesetzt. Zudem legt es großen Wert auf die Einhaltung aller gesetzlichen und regulatorischen Anforderungen, um sowohl rechtliche Risiken als auch Risiken für die Reputation der Einrichtung gering zu halten. Im Sinne einer kontinuierlichen Verbesserung werden die Maßnahmen und Prozesse in der Informationssicherheit regelmäßig überprüft und angepasst. Abschließend stellt das Präsidium sicher, dass effektive Prozesse für die schnelle Identifikation und Bearbeitung von Sicherheitsvorfällen etabliert sind.

Die Zusammensetzung des Präsidiums ergibt sich aus dem Thüringer Hochschulgesetz.

6.2 Bereichsleitung

Als Bereichsleitung wird im Kontext der Informationssicherheit die verantwortliche Führungsperson eines organisatorisch abgegrenzten Bereichs bezeichnet. Dazu zählen insbesondere Fakultäten, die jeweils durch eine:n Dekan:in geleitet werden, zentrale Einrichtungen wie beispielsweise die Hochschulbibliothek oder das Hochschulrechenzentrum (HRZ), die jeweils von einer Leitung geführt werden, Dezernate, die unter der Verantwortung der jeweiligen Dezernent:innen stehen, sowie eventuell Institute mit Institutsleitung.

Die Bereichsleitung trägt die Verantwortung für den laufenden IT-Einsatz im jeweiligen Aufgabenbereich.

Die bereichsinterne Planung von IT-Verfahren obliegt ebenfalls der Bereichsleitung. Technische und organisatorische Zuarbeiten erhält sie hierfür von den jeweils für den Bereich zuständigen IT-Administrator:innen, soweit vorhanden. Wenn nicht vorhanden, kann die:der Dekan:in eine Person benennen.

Die Bereitstellung der zentralen IT-Dienste für die zentralen Einrichtungen und Dezernate wird durch das HRZ koordiniert und umgesetzt.

Ein IT-Verfahren bezeichnet eine strukturierte Abfolge von technischen und organisatorischen Prozessen zur Verarbeitung, Speicherung und Übertragung von Informationen mit Hilfe der Informationstechnik; im Gegensatz dazu beschreibt ein IT-System die konkrete technische Infrastruktur, bestehend aus Hard- und Softwarekomponenten, die zur Durchführung eines oder mehrerer IT-Verfahren eingesetzt wird.

Die Bereichsleitung benennt Verfahrensverantwortliche für die eingesetzten IT-Verfahren. Die Verfahrensverantwortlichen sind bereits in der Einführungsphase eines IT-Verfahrens zu benennen. Sie sind in Zusammenarbeit mit der:dem IT-Sicherheitsbeauftragten für die Erstellung des Sicherheitskonzeptes für das jeweilige IT-Verfahren verantwortlich. Sowohl bei der Einführung als auch während des Betriebs eines IT-Verfahrens überwacht die:der Verfahrensverantwortliche die Einhaltung der Sicherheitsanforderungen hinsichtlich der Informationssicherheit und des Datenschutzes. Gemeinsam mit den zuständigen Verfahrensverantwortlichen gibt die Bereichsleitung auf Grundlage der Ergebnisse der Risikoanalysen den Einsatz eines IT-Verfahrens frei.

Die Bereichsleitung ist verpflichtet, Vorgaben des Präsidiums bezüglich IT-Sicherheit und Informationssicherheit unverzüglich zu befolgen und es gilt die HZR-Benutzungsordnung.

6.3 Informationssicherheitsmanagement-Team

Um den Aufbau einer einheitlichen Informationssicherheitsorganisation zu gewährleisten, wird ein Informationssicherheitsmanagement-Team (ISM-Team) eingerichtet. Dieses Team stellt sicher, dass alle zu ergreifenden Maßnahmen im Vorfeld abgestimmt und regulatorische Vorgaben eingehalten werden. Zur Sicherstellung der Informationssicherheitsprozesse an der Fachhochschule Erfurt setzt sich das ISM-Team aus ständigen, nicht ständigen und beratenden Mitgliedern zusammen.

Ständige Mitglieder sind:

- die:der IT-Sicherheitsbeauftragte (ISB FH-Erfurt)
- die:der Datenschutzbeauftragte
- die:der Leiter:in der Hochschulrechenzentrens (Leitung HRZ)

Nichtständige Mitglieder können bei Bedarf vom ISB FH-Erfurt zu den Sitzungen eingeladen werden. Darüber hinaus können weitere Stellen oder Mitglieder der Fakultäten bei spezifischen Anlässen als Berater:innen hinzugezogen werden. Insbesondere könnten dies:

- der Personalrat oder
- Vertretungen aus den Fakultäten sein.

6.4 IT-Sicherheitsbeauftragte:r

Die:Der IT-Sicherheitsbeauftragte unterstützt das Präsidium bei der Wahrnehmung aller Aufgaben rund um das Thema Informationssicherheit. Sie:Er ist innerhalb der Stabsstelle IT-Sicherheit direkt der:dem Kanzler:in unterstellt. Zur Priorisierung steht die:der IT-Sicherheitsbeauftragte in engem Austausch mit der:dem Leiter:in des Hochschulrechenzentrums.

Die:Der IT-Sicherheitsbeauftragte ist für die Koordination, Steuerung und Überwachung des Informationssicherheitsprozesses an der Hochschule verantwortlich. Dazu gehören insbesondere folgende Aufgaben:

- Unterstützung des Präsidiums bei der Erstellung der Leitlinie Informationssicherheit
- Erstellung des Sicherheitskonzeptes, zugehöriger Teilkonzepte und Richtlinien
- Erstellung von Realisierungsplänen für Sicherheitsmaßnahmen und Initiieren der Überprüfung von deren Umsetzung
- Bericht gegenüber der Hochschulleitung und Sicherheitsverantwortlichen über den Status der Informationssicherheit
- Koordinierung sicherheitsrelevanter Projekte
- Untersuchung sicherheitsrelevanter Vorfälle
- Initiierung und Koordinierung von Sensibilisierungen und Schulungen zur IT-Sicherheit

Um dieser Aufgabe wirksam nachkommen zu können, soll die:der IT-Sicherheitsbeauftragte Maßnahmen initiieren, insbesondere in folgenden Situationen und Bereichen:

- Behandlung von Sicherheitsvorfällen und IT-Störungen: Die:Der IT-Sicherheitsbeauftragte ist befugt, im Falle eines sicherheitsrelevanten Vorfalls oder einer Störung verbindliche Maßnahmen zur Eindämmung, Analyse und Behebung zu initiieren.
- Durchsetzung technischer und organisatorischer Sicherheitsmaßnahmen: Die:Der IT-Sicherheitsbeauftragte kann gegenüber Fachabteilungen und IT-Dienstleistern sicherheitsrelevante Anforderungen verbindlich kommunizieren, sofern diese zur Einhaltung der Sicherheitsstandards notwendig sind.

- Sicherheitsüberprüfungen und Audits: Die:Der IT-Sicherheitsbeauftragte ist berechtigt, Prüfungen durchzuführen und bei festgestellten Mängeln entsprechende Maßnahmen zu initiieren.

Mit der Freigabe dieser Leitlinie verpflichtet sich das Präsidium, die formale Bestellung der:des IT-Sicherheitsbeauftragten durch Ausstellung einer Bestellurkunde zu vollziehen.

6.5 Hochschulrechenzentrum

Als zentraler IT-Dienstleister plant, realisiert, betreibt und gestaltet das Hochschulrechenzentrum (HRZ) die IT-Infrastrukturen und -Services für die Einrichtungen der Fachhochschule Erfurt. Das HRZ bezieht dabei unter anderem Leistungen aus dem Hochschul-IT-Zentrum (HS-ITZ) der Thüringer Hochschulen.

Das Hochschulrechenzentrum hat eine entscheidende Rolle bei der Sicherstellung der Informationssicherheit. In enger Abstimmung mit der:dem IT-Sicherheitsbeauftragten ist das Hochschulrechenzentrum für die Implementierung und Wartung von technischen Sicherheitsmaßnahmen verantwortlich. Dazu gehören etwa die Einrichtung von Firewalls, die Aktualisierung von Software und die Überwachung des Netzwerkverkehrs auf potenzielle Sicherheitsvorfälle.

Darüber hinaus sorgt das Rechenzentrum für die Datensicherheit durch Verschlüsselung und regelmäßige Backups. Es stellt sicher, dass alle gesetzlichen und regulatorischen Anforderungen, insbesondere im Datenschutz, erfüllt sind.

Ein besonderer Fokus liegt auf der Reaktion auf IT-Sicherheitsvorfälle. Das Rechenzentrum hat Prozesse etabliert, um Sicherheitsvorfälle effektiv zu identifizieren, zu analysieren und zu bewältigen. Diese reaktive Rolle wird durch proaktive Maßnahmen ergänzt, die das Bewusstsein für Informationssicherheit bei den Hochschulangehörigen fördern. Dazu gehören regelmäßige Schulungen und die Bereitstellung von Informationsmaterialien, die auch Hinweise zur Erkennung und Meldung von Sicherheitsvorfällen beinhalten.

Durch diese integrierte Herangehensweise an Reaktion und Prävention leistet das Hochschulrechenzentrum einen wesentlichen Beitrag zur Umsetzung der strategischen Ziele der Hochschule in der Informationssicherheit und trägt zur kontinuierlichen Verbesserung der Sicherheitslage bei.

6.6 IT-Administrator:innen

Mit IT-Administrator:innen sind die IT-Administrator:innen der Fakultäten und des HRZ gemeint. Die IT-Administrator:innen sind maßgeblich für die Sicherheit der Informationssysteme und Daten innerhalb ihres Verantwortungsbereichs verantwortlich. Dies umfasst die Einhaltung der festgelegten Sicherheitsrichtlinien sowie die Implementierung und Aufrechterhaltung angemessener Sicherheitsmaßnahmen. Es ist ihre Aufgabe, Mitarbeitende und Studierende für Sicherheitsrisiken zu sensibilisieren und Schulungen zur Informationssicherheit anzubieten. Darüber hinaus müssen sie sicherstellen, dass sensible Daten entsprechend klassifiziert sowie geschützt werden und nur autorisierten Personen zugänglich sind.

Die enge Zusammenarbeit mit dem Hochschulrechenzentrum ist von entscheidender Bedeutung, um sicherzustellen, dass technische Sicherheitsmaßnahmen wirksam implementiert und gewartet werden. Im Falle von Sicherheitsvorfällen oder Verdachtsfällen sind die Fakultäten verpflichtet, diese unverzüglich an den HRZ-Servicedesk zu melden und bei der Untersuchung und Behebung mitzuwirken. Durch die Förderung eines Sicherheitsbewusstseins und die Benennung von IT-Sicherheitskoordinator:innen innerhalb jeder Fakultät tragen diese dazu bei, die Informationssicherheit an der Hochschule zu gewährleisten.

6.7. IT-Sicherheitskoordinator:innen

Die Rolle einer:eines IT-Sicherheitskoordinatorin:IT-Sicherheitskoordinators (ITSK) wird von der Bereichsleitung benannt, um die Fachadministrator:innen in ihrer Tätigkeit zu unterstützen. Die:Der ITSK koordiniert die Erstellung von Sicherheitskonzepten im Rahmen von Projekten und arbeitet eng mit Fachkolleg:innen zusammen.

6.8 Mitglieder und Angehörige

Die Mitglieder und Angehörigen der Fachhochschule (definiert nach [§ 21 ThürHG](#)) werden dazu angehalten, stets die Bedeutung der Informationssicherheit zu erkennen und aktiv zur Abwehr und Bekämpfung von materiellen und ideellen Schäden beizutragen. Ein verantwortungsbewusster Umgang mit Informationssystemen sowie den darauf gespeicherten und verarbeiteten Daten ist erforderlich, wobei die Wahrung von Betriebs- und Geschäftsgeheimnissen von besonderer Bedeutung ist. Die Sicherung der Integrität, Verfügbarkeit und Vertraulichkeit von Werten liegt in der Verantwortung der jeweiligen Eigentümer:innen. Bei jeglichen Unregelmäßigkeiten sind die Mitglieder und Angehörigen dazu angehalten, den:der IT-Sicherheitsbeauftragten und ihre Vorgesetzten unverzüglich zu informieren.

Es wird erwartet, dass jedes Mitglied und jeder Angehörige der Fachhochschule die vorliegende Informationssicherheitsleitlinie kennt und befolgt.

Weiter gilt, dass das erforderliche Niveau der Informationssicherheit an der Hochschule nur dann erreicht werden kann, wenn alle Mitglieder und Angehörigen der Fachhochschule ihre Kompetenzen und Pflichten kennen und verantwortungsbewusst handeln. Um die notwendigen Fähigkeiten im Bereich der Informationssicherheit zu entwickeln und zu vertiefen, werden alle Mitglieder und Angehörige angemessen sensibilisiert und qualifiziert. Zudem werden sie über relevante Themen und Regelungen zur Informationssicherheit durch geeignete Kommunikationskanäle informiert.

Weitere Verantwortliche werden in *Anhang 2: Weitere Verantwortliche* erklärt.

7. Folgen von Zuwiderhandlungen

Beabsichtigte oder fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitglieder und Angehörigen schaden oder den Ruf der Fachhochschule Erfurt gefährden. Vorsätzliche oder grob fahrlässige Verstöße gegen die Sicherheitsregelungen können neben Regressforderungen auch arbeits- oder dienstrechtliche Folgen nach sich ziehen.

8. Inkrafttreten

Die Richtlinie tritt mit Veröffentlichung im Verkündungsblatt zum 04.05.2026 in Kraft. Ausgefertigt durch Beschluss des Präsidiums vom 29.04.2026.

Erfurt, 29.04.2026

Prof. Dr. Frank Setzer
Präsident der Fachhochschule Erfurt

Anhang 2: Weitere Verantwortlichkeiten

Systemverantwortliche

Die:Der Systemverantwortliche ist für die Konfiguration und den Betrieb von IT-Systemen verantwortlich. Sie:Er stellt sicher, dass die Systeme ordnungsgemäß betrieben werden und die Informationssicherheit gewährleistet ist. Dazu plant, implementiert und wartet sie:er IT-Systeme, überwacht den Betrieb, behebt Störungen, erstellt und pflegt Dokumentationen und arbeitet mit anderen Bereichen der Hochschule zusammen. Für die Erfüllung dieser Aufgaben sind IT-spezifische Fachkenntnisse, Kenntnisse der Informationssicherheit und Erfahrung in der Konfiguration und dem Betrieb von IT-Systemen erforderlich. Für jedes von der Fachhochschule Erfurt betriebene System existiert ein:e entsprechende:r Systemverantwortliche:r oder/und ein Dienstleistungsvertrag, um dazu beizutragen, dass die Informationssicherheitsziele der Fachhochschule Erfurt erreicht werden.

Applikationsverantwortliche

Die:Der Applikationsverantwortliche ist für den Applikationsbetrieb verantwortlich. Sie:Er stellt sicher, dass die Software den Anforderungen der Organisation entspricht und ordnungsgemäß betrieben wird. Dazu gehört beispielsweise die Anpassung der Benutzeroberfläche, die Definition von Workflows und die Integration der Software in bestehende Systeme. Ebenso gehören die Definition von Rollen und Berechtigungen zu den Aufgaben der:des Applikationsverantwortlichen. Sie:Er unterstützt die Benutzer:innen bei der Nutzung der Software, überwacht die Softwarenutzung und führt Anwender:innenschulungen zur Software durch. Für die Erfüllung dieser Aufgaben sind Fachkenntnisse über die Anwendung, Kenntnisse der Informationssicherheit und Erfahrung in der Administration von Software erforderlich.

Verfahrensverantwortliche

Die:Der Verfahrensverantwortliche organisiert die Einführung und den laufenden Betrieb eines IT-Verfahrens einschließlich aller Komponenten und Schnittstellen. Sie:Er ist für die Durchführung einer Fachaufgabe bzw. eines Dienstes verantwortlich und in der Regel Dateneigner:in im Verfahren verarbeiteter Daten. Somit tragen Verfahrensverantwortliche die Verantwortung für die Einhaltung der Sicherheitsanforderungen, insbesondere bei der Einführung und dem Betrieb der IT-Verfahren. Ihnen fällt die Aufgabe zu, die technische Umsetzung der Datenschutz-Informationssicherheitsvorgaben zu koordinieren.

Dienstleister:innen

Die Einbindung von Dienstleister:innen in die Sicherheitsleitlinie ist von entscheidender Bedeutung, um die Integrität, Vertraulichkeit und Verfügbarkeit von Daten zu gewährleisten. Dienstleister:innen müssen die Sicherheitsstandards und -richtlinien der Hochschule strikt einhalten und sicherstellen, dass angemessene Sicherheitsmaßnahmen implementiert sind.

Bereits bei der Beschaffung neuer Software und Systeme werden die Sicherheitsanforderungen der Fachhochschule Erfurt als Teil der Leistungsanforderungen festgelegt.

Vor der Zusammenarbeit erfolgt eine Überprüfung, um sicherzustellen, dass Dienstleister:innen den vereinbarten Standards entsprechen. In den Verträgen werden klare Sicherheitsanforderungen festgelegt, einschließlich Maßnahmen zur Datensicherheit und Zugangskontrolle. Die Hochschule überwacht regelmäßig die Sicherheitspraktiken der Dienstleister:innen und erwartet eine unverzügliche Meldung von Sicherheitsvorfällen. Über den Beschaffungsprozess hinweg überwacht die:der für diesen Verantwortliche gemeinsam mit der Hochschule die Einhaltung dieser Sicherheitsstandards. Dienstleister:innen sind außerdem verpflichtet, ihre Mitarbeitenden für Sicherheitsrisiken zu sensibilisieren und Schulungen zur Informationssicherheit anzubieten. Durch diese Maßnahmen wird sichergestellt, dass Dienstleister:innen aktiv zur Sicherheit der Hochschulressourcen beitragen und potenzielle Sicherheitsrisiken minimieren.

IMPRESSUM

IMPRESSUM

Herausgeber:

Fachhochschule Erfurt,
Präsident der FH Erfurt, Postfach 45 01 55, 99051 Erfurt

Redaktion:

Victoria Völker, Altonaer Straße 25, 99085 Erfurt
Tel. (0361) 6700-7567, E-Mail: victoria.voelker@fh-erfurt.de

Gestaltung:

Zentrum für studentische und akademische Angelegenheiten
Lisa Schaffrik, Altonaer Straße 25, 99085 Erfurt

Das „Verkündungsblatt der FH Erfurt“ ist das in § 3 Absatz 2 des Thüringer Hochschulgesetzes (ThürHG) vom 10. Mai 2018 (GVBl. S. 149 ff), zuletzt geändert durch Artikel 31 des Gesetzes vom 2. Juli 2024 (GVBl. S. 277), vorgesehene amtliche Verkündungsblatt der Hochschule. Einzelheiten zu Erscheinungsweise, Verbreitung, Bezugsmöglichkeiten und Bezugsbedingungen sind in der „Richtlinie für das Verkündungsblatt der FH Erfurt“ geregelt, auf die hiermit ausdrücklich verwiesen wird.