FH-Mitteilungen
2. Juni 2026
Nr. 72/2026

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Ordnung zur Informationssicherheit

vom 2. Juni 2026

Ordnung zur Informationssicherheit
vom 2. Juni 2026

Aufgrund der Vereinbarung zur Informationssicherheit (VzI), der Vereinbarung zur Cybersicherheit (VzC) und des § 2 Absatz 4 Satz 1 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG) vom 16. September 2014 (GV. NRW. S. 547), zuletzt geändert durch Artikel 2 des Gesetzes vom 19. Dezember 2024 (GV. NRW. S. 1222), hat die FH Aachen folgende Ordnung zur Informationssicherheit erlassen:

Inhaltsübersicht

Abkürzungsverzeichnis	2
Präambel	3
§ 1 | Gegenstand dieser Ordnung	3
§ 2 | Geltungsbereich	3
§ 3 | Sicherheitsziele und Sicherheitsstrategie	3
§ 4 | Rollen im Informationssicherheitsmanagement (ISM)	4
§ 5 | Aufgaben im Informationssicherheitsmanagement (ISM)	5
§ 6 | Gefahrenintervention	7
§ 7 | Ressourcenabsicherung	7
§ 8 | Überprüfung	7
§ 9 | Inkrafttreten und Veröffentlichung	7

Abkürzungsverzeichnis

BCMB	=	Business Continuity Management Beauftragte bzw. Beauftragter
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
DVZ	=	Datenverarbeitungszentrale
ISB	=	Informationssicherheitsbeauftragte bzw. Informationssicherheitsbeauftragter
ISM	=	Informationssicherheitsmanagement
ISMS	=	Informationssicherheitsmanagementsystem
Pro III	=	Prorektor bzw. Prorektorin Strategische Planung und IT

Präambel

Die FH Aachen hat sich mit Veröffentlichung der „Leitlinie zur Informationssicherheit“ zur Gewährleistung einer ordnungsgemäßen Verarbeitung von Informationen und mit der „Netzordnung“ – in der jeweils geltenden Fassung – zu einem sicheren Betrieb der Hochschul-IT verpflichtet und damit den hohen Stellenwert der Informationssicherheit zum Ausdruck gebracht.

Eine funktionierende und sichere Informationsverarbeitung ist eine zwingende Voraussetzung für den Erfolg einer digital agierenden Hochschule und für die Gewährleistung der nachhaltigen Erfüllung von wissenschaftlichen, administrativen und rechtlichen Anforderungen in Lehre, Forschung, Weiterbildung und in der Hochschulverwaltung essentiell notwendig.

Mit dieser Ordnung werden die wesentlichen Anforderungen der Informationssicherheit an der FH Aachen umgesetzt. Insbesondere werden die Vereinbarungen mit dem Ministerium für Kultur und Wissenschaft NRW zur Informationssicherheit und zur Cybersicherheit berücksichtigt.

Die FH Aachen orientiert sich, soweit nicht andere gesetzliche Vorgaben dadurch verletzt werden, an dem IT-Grundschutz des Bundesamt für Sicherheit in der Informationstechnik (BSI), um den Schutz ihrer digitalen und analogen Ressourcen in einem kontinuierlichen Prozess bestmöglich sicherzustellen.

§ 1 | Gegenstand dieser Ordnung

(1) Diese Ordnung legt den Aufbau der Informationssicherheitsorganisation der FH Aachen fest.

(2) Inhalte dieser Ordnung sind die Regelungen zum hochschulweiten Informationssicherheitsmanagementsystem (ISMS). Dazu gehören die erforderlichen organisatorischen Strukturen, eine Aufgabenzuordnung sowie die Zusammenarbeit der Beteiligten.

(3) Weiterhin sind in dieser Ordnung allgemeine Grundsätze der Informationssicherheit und Bedingungen definiert, unter denen die Hochschul-IT der FH Aachen betrieben und genutzt werden kann.

§ 2 | Geltungsbereich

Diese Ordnung zur Informationssicherheit gilt für alle Mitglieder und Angehörigen[1] der FH Aachen und ebenfalls für alle externen Geschäfts-, Kooperationspartner/-innen und Gäste (kurz Dritte), die Informationen der Hochschule verarbeiten, die Hochschul-IT nutzen oder diese für die FH Aachen betreiben. Sie umfasst alle Organisationseinheiten (Fachbereiche, Verwaltung, zentrale Einrichtungen) der FH Aachen und in technischer Hinsicht die gesamte Hochschul-IT.

§ 3 | Sicherheitsziele und Sicherheitsstrategie

Die anzustrebenden Sicherheitsziele sind:

- die Verfügbarkeit der Infrastruktur und der Informationen,
- die Vertraulichkeit der Informationen (Schutz vor unautorisierten Zugriffen),
- die Integrität sämtlicher IT-Systeme und Informationen und
- die Einhaltung der gesetzlichen Bestimmungen sowie sonstiger rechtsverbindlicher Regelungen.

Unsere Informationen und unsere IT-Systeme werden in allen technikabhängigen und kaufmännischen Bereichen in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandzeiten im Einzelfall toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten- und IT-Systemen sind nicht akzeptabel (Integrität), der kontinuierliche Verbesserungsprozess (Continual Service Improvement) stellt deshalb sicher, dass auftretende Vorfälle und daraus folgende Probleme ausgewertet und entsprechende Verbesserungen zur Einhaltung vereinbarter Service Level umgesetzt werden können. Die Anforderungen an die Vertraulichkeit haben ein an der Gesetzeskonformität orientiertes Niveau.

[1] Mitglieder und Angehörige einer Hochschule entsprechend § 9 HG in der jeweils geltenden Fassung.

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen.

§ 4 | Rollen im Informationssicherheitsmanagement (ISM)

(1) Rektorat, Rektorin bzw. Rektor und Prorektor bzw. Prorektorin Strategische Planung und IT (Pro III)

Die Rektorin bzw. der Rektor und Pro III der FH Aachen tragen in ihren Rollen als oberste Entscheidungsinstanz in allen Angelegenheiten der Informationsverarbeitung die Gesamtverantwortung für die Informationssicherheit und den Informationssicherheitsprozess. Die Rektorin bzw. der Rektor und Pro III sorgen für die nötige Priorität, Aufmerksamkeit und entsprechenden Ressourcen zu allen Fragen der Informationssicherheit und tragen somit primär zur nachhaltigen Gewährleistung der Informationssicherheit an der FH Aachen bei.

Die Rektorin bzw. der Rektor und Pro III delegieren die Organisation und Durchführung des Informationssicherheitsmanagementsystem (ISMS) an eine dem Rektorat zugeordneten Stabsstelle Informationssicherheit. Die Leitung der Stabstelle überträgt das Rektorat einer bzw. einem Informationssicherheitsbeauftragten. Die Delegation der entsprechenden dezentralen Aufgaben im Informationssicherheitsprozess erfolgt durch die Rektorin bzw. den Rektor und Pro III an die Leitungen der Organisationseinheiten durch entsprechende Rektoratsbeschlüsse. In ihren Rollen als oberste Entscheidungsinstanz können die Rektorin bzw. der Rektor und Pro III die Delegation aufheben und selbst entscheiden. In ihrer Rolle als Rektorin ist diese bzw. in seiner Rolle als Rektor ist dieser im Zweifel letzte Entscheidungsinstanz.

(2) Informationssicherheitsbeauftragte bzw. Informationssicherheitsbeauftragter (ISB)

Die bzw. der ISB ist für die Koordination des Aufbaus, die Entwicklung und Umsetzung sowie den Betrieb und die fortlaufende Anpassung eines effektiven ISMS nach den BSI-Standards verantwortlich. Sie bzw. er berichtet der Rektorin bzw. dem Rektor und Pro III in regelmäßigen Abständen und bei Bedarf über den Stand der Informationssicherheit. Ebenso erfolgt regelmäßig und bei Bedarf eine Berichterstattung im Rektorat.

(3) IT-Sicherheitsbeauftragte bzw. IT-Sicherheitsbeauftragter

Die bzw. der IT-Sicherheitsbeauftragte vertritt die bzw. den ISB und ist für alle Sicherheitsbelange der Geschäftsprozesse, Anwendungen und IT-Systeme im Bereich IT-Sicherheit verantwortlich.

(4) Behördliche Datenschutzbeauftragte bzw. Behördlicher Datenschutzbeauftragter

Die bzw. der Behördliche Datenschutzbeauftragte wirkt darauf hin, dass im hochkomplexen und sich schnell änderndem Umfeld der Digitalisierung die Einhaltung der Datenschutzbestimmungen gewährleistet werden. Sie bzw. er prüft den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten und stellt die Einhaltung aller relevanten Datenschutzgesetze und -richtlinien sicher und berät die verantwortlichen Gremien entsprechend.

(5) Business Continuity Management Beauftragte bzw. Beauftragter (BCMB)

Die bzw. der BCMB ist zuständig für den Aufbau, den Betrieb und die kontinuierliche Verbesserung des Business Continuity Management Systems. Sie bzw. er ist zuständig für die Absicherung der (zeit-)kritischen Geschäftsprozesse in Notfall- und Krisenzeiten durch die Erstellung von Notfallplänen und Vorsorgemaßnahmen und berät und unterstützt die Hochschulleitung bei sämtlichen Aspekten, die für das Business Continuity Management relevant sind.

(6) Leitung der Datenverarbeitungszentrale (DVZ-Leitung)

Die DVZ-Leitung ist im Auftrag des Rektorats für alle Aufgaben der taktisch/operativen Führung des IT-Betriebes der Hochschule und der bereichsübergreifenden operativen Vorgaben verantwortlich. Die DVZ-Leitung nimmt damit auch für die Informationssicherheit der FH Aachen wichtige zentrale Aufgaben wahr und trägt durch ihr Handeln entscheidend zur nachhaltigen Gewährleistung der Informationssicherheit der FH Aachen – insbesondere im Bereich der IT-Sicherheit – bei.

(7) Informationssicherheitsmanagement-Team (ISM-Team)

Die FH Aachen setzt zur Unterstützung der bzw. des ISB ein ISM-Team ein. Das ISM-Team ist für die zentralen Steuerungsaufgaben des Informationsmanagements und damit auch für die Informationssicherheit verantwortlich. Es bindet alle Organisationseinheiten, insbesondere die DVZ, in den Informationssicherheitsprozess ein.

Mitglieder des ISM-Teams sind:

- die bzw. der ISB und ihre bzw. seine Vertretung,
- die DVZ-Leitung,
- das taktisch/operative Sicherheitsteam der DVZ,
- die bzw. der BCMB
- eine Vertretung aus Forschung und Lehre (FB05 Lehrgebiet IT-Sicherheit) als Kooperationspartnerin bzw. Kooperationspartner

Weiterführende Informationen finden sich im Rollenkonzept.

Die Mitglieder des ISM-Teams werden von Pro III in Absprache mit dem Rektorat der FH Aachen benannt.

(8) Leitungen einer Organisationseinheit sowie Ansprechpersonen der Informationssicherheit

Informationssicherheit ist integraler Bestandteil aller Arbeitsabläufe der FH Aachen. Daraus folgt, dass die Leitungen der Organisationseinheiten der FH Aachen (Fachbereiche und zentralen Einrichtungen sowie Dezernate und Stabsstellen) grundsätzlich zuständig für die Informationssicherheit in ihren Bereichen sind. Das heißt, sie nehmen die Rolle der bzw. des Prozessverantwortlichen für die in ihrem Bereich verorteten Prozesse (inklusive IT-Verfahren) ein. Dies trifft auch auf übergreifende Prozessabläufe zu, wenn der Organisationseinheit die Gesamtverantwortung für den Geschäftsprozess zugeordnet wurde.

Es sind zudem je eine Ansprechperson Informationssicherheit für Organisatorisches und eine für fachlich/technische Angelegenheiten zu benennen. Die Leitung einer Organisationseinheit übernimmt diese Rollen und ihre Aufgaben standardmäßig. Ihr ist es auch überlassen, die Aufgaben der Rollen an ein geeignetes Mitglied der Organisationseinheit zu delegieren. Für die Übertragung der Rolle der Ansprechperson für fachlich/technische Angelegenheiten empfiehlt sich in der Regel ein Mitglied aus der Fach- oder Systemadministration.

Die Delegation von Aufgaben entlässt die Leitung der Organisationseinheit der FH Aachen nicht aus ihrer Zuständigkeit für die Informationssicherheit in ihrem Bereich.

(9) Übergreifende Organisationsstruktur

Grundsätzlich ist jedes Mitglied der FH Aachen für die in seinem Verantwortungs- und Aufgabenbereich liegenden Daten und Informationen und damit für die Gewährleistung der Schutzziele sowie die Umsetzung von Sicherheitsmaßnahmen zuständig.

(10) Rollenkonzept

Detaillierte Beschreibungen der oben genannten Rollen und weitere Rollen werden in einem separaten Rollenkonzept beschrieben. Das Rollenkonzept ist Teil eines Organisationsplans, der eine geeignete übergreifende Organisationsstruktur für die Informationssicherheit (ISM-Organisation) festlegt. Organisationsplan und Rollenkonzept (Zugriff nur für berechtigte Personen) werden vom Rektorat auf Vorschlag des ISB/ISM-Teams beschlossen und den berechtigten Personen an geeigneter Stelle zugänglich gemacht.

§ 5 | Aufgaben im Informationssicherheitsmanagement (ISM)

(1) Informationssicherheitsmanagement-Team (ISM-Team)

Das ISM-Team ist die zentrale Organisation der FH Aachen für die Informationssicherheit. Es wird von der bzw. dem ISB geleitet und ist für die Entwicklung, Fortschreibung, Umsetzung und Überwachung des Informationssicherheitsmanagementsystems (ISMS) verantwortlich. Zu den Aufgaben des ISM-Teams gehören außerdem die Erstellung bzw. Überarbeitung von Regelungen zur Informationssicherheit und die Erstellung regelmäßiger Berichte zur Informationssicherheit für das Rektorat. Die verbindliche Beschlussfassung der Regelungen obliegt dem Rektorat nach Zustimmung des Pro III. Das ISM-Team soll regelmäßig (mindestens alle 2 Monate) zur kontinuierlichen Weiterentwicklung des ISMS und der Regelungen zur Informationssicherheit beraten.

Das ISM-Team kann anlassbezogene Arbeitsgruppen einrichten, beispielsweise zur Unterstützung von operativen Aufgaben. Die Auswahl der Mitglieder einer Arbeitsgruppe obliegt der bzw. dem ISB.

(2) Informationssicherheitsbeauftragte bzw. Informationssicherheitsbeauftragter (ISB)

Die bzw. der ISB berät als verantwortliche Ansprechperson für Informationssicherheit die Hochschulleitung in Fragen der Informationssicherheit und berichtet zur aktuellen Sicherheitslage. Sie bzw. er hat unmittelbares Vortragsrecht beim Rektorat und ist bei der Ausübung ihrer bzw. seiner Aufgaben

weisungsfrei. Ihr bzw. ihm dürfen durch die Wahrnehmung ihrer bzw. seiner Aufgaben keine Nachteile entstehen.

Ferner obliegen folgende Aufgaben der bzw. dem ISB:

- Dokumentation sicherheitsrelevanter Vorfälle und Koordination der Meldepflichten gemäß § 2 Absatz 10 VzC NRW,
- Entwicklung eines Schulungskonzeptes zur Informationssicherheit für die Sensibilisierung aller Mitglieder und Angehörigen der FH Aachen,
- Koordination und Steuerung der Umsetzung des Informationssicherheitsprozesses mit Unterstützung des ISM-Teams und den Ansprechpersonen Informationssicherheit sowie
- Ansprechperson in allen Belangen zur Informationssicherheit.

Sie bzw. er ist berechtigt, die Umsetzung des Informationssicherheitsprozesses und die Einhaltung der Richtlinien zu prüfen und Audits in den einzelnen Organisationseinheiten durchzuführen. Sie bzw. er ist weiterhin beauftragt, Erkenntnisse oder Abweichungen zu dokumentieren und die Umsetzung zu überwachen. Die Ansprechpersonen Informationssicherheit für fachlich/technische Angelegenheiten unterstützen die bzw. den ISB bei ihren bzw. seinen Aufgaben und gewähren ihr bzw. ihm Zugang zu allen erforderlichen Informationen zu den von ihnen zu verantwortenden Prozessen.

Vor wesentlichen Änderungen an Informationssystemen muss die Abstimmung mit der bzw. dem ISB erfolgen. Sie bzw. er ist rechtzeitig an IT-Vorhaben zu beteiligen.

(3) Ansprechpersonen Informationssicherheit

Die Ansprechpersonen Informationssicherheit für Organisatorisches koordinieren und begleiten die Umsetzung des Informationssicherheitsprozesses in ihrer Organisationseinheit. In ihrer potenziellen Rolle als Prozessverantwortliche sind sie zuständig für die Erstellung von Sicherheitskonzepten. In den Sicherheitskonzepten sind alle Sicherheitsmaßnahmen und deren Umsetzung dokumentiert. Sie werden regelmäßig aktualisiert. Für den Fall, dass sie nicht selbst die Leitungsrolle wahrnehmen, informieren die Ansprechpersonen Informationssicherheit für Organisatorisches die Leitung ihrer Organisationseinheit und die bzw. den ISB regelmäßig über den Stand der Umsetzung und über aktuelle Problemfälle.

Die Ansprechpersonen für Informationssicherheit für Organisatorisches und für fachlich/technische Angelegenheiten unterstützen das ISM-Team bei der Erarbeitung von Richtlinien und übergreifenden, hochschulweit relevanten Konzepten.

(4) Datenverarbeitungszentrale (DVZ)

Die DVZ ist für den Betrieb der grundlegenden IT-Infrastruktur und zentraler IT-Basisdienste verantwortlich und damit von entscheidender Bedeutung für die Informationssicherheit. Sie unterstützt durch das „Taktisch Operative Sicherheitsteam“ (TOS-Team) die bzw. den ISB, die Ansprechpersonen Informationssicherheit und das ISM-Team in technischen Fragen.

(5) Informations- und Kommunikationssystem

Die bzw. der ISB konzipiert in Zusammenarbeit mit der DVZ ein hochschulweites Informations- und Kommunikationssystem, über das alle Beteiligten am Informationssicherheitsprozess in Kontakt stehen und Informationen austauschen können.

(6) Personelle Kontinuität

Bei der Benennung der im Informationssicherheitsprozess aktiven Personen ist die erforderliche personelle Kontinuität zu berücksichtigen. Deshalb sollen die Personen möglichst zum hauptamtlichen Personal der Hochschule gehören oder über langfristige Verträge verfügen.

(7) Meldepflicht

Alle Mitglieder und Angehörigen der FH Aachen sowie Nutzende der Hochschul-IT sind verantwortlich für den ordnungsgemäßen und sorgsamen Umgang mit verarbeiteten Informationen und verwendeten IT-Systemen. Sie sind zur Meldung sicherheitsrelevanter Ereignisse an die Ansprechpersonen Informationssicherheit ihrer Einrichtung und die bzw. den ISB verpflichtet.

(8) Rollenkonzept

Detaillierte Beschreibungen der Aufgaben und Zuständigkeiten im Informationssicherheits-management werden in einem separaten Rollenkonzept (siehe § 4 Absatz 10) beschrieben.

§ 6 | Gefahrenintervention

Maßnahmen zur Gefahrenintervention werden nach einem in das Notfall- und Krisenmanagement integrierten und vom Rektorat auf Vorschlag des ISB/ISM-Teams beschlossenen Incident Response Plan (Zugriff nur für berechtigte Personen) abgearbeitet.

§ 7 | Ressourcenabsicherung

(1) Informationssicherheit ist integraler und untrennbarer Bestandteil jeder Ablauforganisation, jedes Prozesses, jedes IT-Verfahrens und jedes Projektes. Die personellen und finanziellen Ressourcen für angemessene Maßnahmen zur Gewährleistung der Informationssicherheit sind durch die Verantwortlichen nach § 4 Absatz 8 mit zu planen.

(2) Die bzw. der ISB ordnet in Abstimmung mit dem ISM-Team die geplanten Maßnahmen nach Dringlichkeit in einer Liste. Mit einer Begründung der Prioritäten schlägt sie bzw. er dem Rektorat über Pro III die Finanzierung vor.

(3) Die Planung der Gesamtressourcen aller hochschulweiten, zentralen Maßnahmen zur Informationssicherheit erfolgt durch das Rektorat. Die Finanzierung erfolgt aus zentralen Mitteln.

§ 8 | Überprüfung

Die Ordnung zur Informationssicherheit soll alle vier Jahre überprüft und gegebenenfalls angepasst werden.

§ 9 | Inkrafttreten und Veröffentlichung

(1) Diese Ordnung tritt mit ihrer Veröffentlichung im Verkündungsblatt der FH Aachen (FH-Mitteilungen) in Kraft.

Sie soll alle vier Jahre überprüft und gegebenenfalls angepasst werden.

(2) Ausgefertigt aufgrund des Beschlusses des Senats der FH Aachen vom 28. Mai 2026.

Hinweis nach § 12 Absatz 5 HG:
Die Verletzung von Verfahrens- oder Formvorschriften des Hochschulgesetzes oder des Ordnungs- oder sonstigen autonomen Rechts der FH Aachen kann gegen diese Ordnung nach Ablauf eines Jahres seit ihrer Bekanntmachung nicht mehr geltend gemacht werden, es sei denn,

a) die Ordnung ist nicht ordnungsgemäß bekanntgemacht worden,
b) das Rektorat hat den Beschluss des zuständigen Gremiums vorher beanstandet oder
c) der Form- oder Verfahrensmangel ist gegenüber der Hochschule vorher gerügt und dabei die verletzte Rechtsvorschrift und die Tatsache bezeichnet worden, die den Mangel ergibt.

Aachen, den 2. Juni 2026

Der Rektor
der FH Aachen

gez. Ritz

Prof. Dr.-Ing. Thomas Ritz