Hochschule Niederrhein
University of Applied Sciences

Amtliche Bekanntmachungen

Herausgegeben im Auftrag des Präsidenten der Hochschule Niederrhein

49. Jahrgang Ausgegeben zu Krefeld und Mönchengladbach am 13. Mai 2025 Nr. 11

Inhalt

Hinweis zum Rügeausschluss

Gemäß § 12 Abs. 5 Hochschulgesetz kann eine Verletzung von Verfahrens- oder Formvorschriften des Hochschulgesetzes oder des Ordnungs- oder des sonstigen autonomen Rechts der Hochschule gegen diese Ordnung nach Ablauf eines Jahres seit ihrer Bekanntmachung nicht mehr geltend gemacht werden, es sei denn,

1. die Ordnung ist nicht ordnungsgemäß bekannt gemacht worden,
2. das Präsidium hat den Beschluss des die Ordnung beschließenden Gremiums vorher beanstandet,
3. der Form- oder Verfahrensmangel ist gegenüber der Hochschule vorher gerügt und dabei die verletzte Rechtsvorschrift und die Tatsache bezeichnet worden, die den Mangel ergibt, oder
4. bei der öffentlichen Bekanntmachung der Ordnung ist auf die Rechtsfolge des Rügeausschlusses nicht hingewiesen worden.

Hochschule Niederrhein
University of Applied Sciences

Das Präsidium der Hochschule Niederrhein hat gemäß § 16 Hochschulgesetz NRW i.V.m. Art. 4 Nr. 7, 24 Abs. 1 der Europäischen Datenschutzgrundverordnung (EU-DSGVO) die nachfolgende Informationssicherheits- BCM, und Datenschutz-leitlinie beschlossen.

Informationssicherheits-BCM, und Datenschutz-leitlinie

Für alle Hochschulangehörigen

Version 3.0 | Stand: April 2025

Inhaltsverzeichnis

1 Grundlagen und Anwendungsbereich

Die Wahrung von Persönlichkeitsrechten, sichere IT-Prozesse und ein im Bedarfsfall funktionierendes Notfallmanagement sind für die Hochschule Niederrhein von zentraler Bedeutung.

Zur Erfüllung ihrer Aufgaben aus dem Hochschulgesetz NRW verarbeitet die Hochschule Niederrhein eine Vielzahl von personenbezogenen Daten von ihren Mitgliedern und Angehörigen, aber auch von Bewerbern, von Forschung betroffenen Personen und externen Dienstleistern und Lieferanten. Nach Art. 8 der EU-Grundrechts-Charta hat jede Person das Recht auf Schutz der personenbezogenen Daten. Darüber hinaus wird der Schutz der informationellen Selbstbestimmung durch die EU-Datenschutzgrundverordnung, das Grundgesetz, das Landesdatenschutzgesetz und die bereichsspezifischen Regelungen zum Datenschutz an Hochschulen auch auf Länderebene weiter spezifiziert. Die Hochschule Niederrhein bekennt sich vorbehaltslos zu diesem Grundrecht und setzt sich aktiv für die Verwirklichung des Persönlichkeitsschutzes nach Maßgabe der geltenden Gesetze ein. Aus diesem Grunde verpflichtet sie sich ein Datenschutz-Management-System aufzubauen, mit dem der Schutz personenbezogener Daten an der Hochschule Niederrhein gewährleistet wird.

Besondere Bedeutung kommt auch der Informationssicherheit zu. Funktionierende und sichere Geschäftsprozesse sind eine maßgebliche Voraussetzung für die Leistungsfähigkeit einer Hochschule. Sie bilden die Grundvoraussetzung für den Daten- und Persönlichkeitsschutz. Darüber hinaus stellen sie die Arbeitsfähigkeit der Hochschule, die gute Qualität des Lehrangebots, moderne Forschungsvorhaben, aber auch die Arbeitsplätze der vielen Menschen, die an, mit oder für die Hochschule Niederrhein tätig sind, sicher. Um diese in ihrer Funktionsfähigkeit zu schützen, bedarf es einer Informationssicherheitsstrategie, dessen Kernelement ein kontinuierlicher Informationssicherheitsprozess ist. Dieser wird durch die Einführung eines Informationssicherheitsmanagementsystems initiiert, das dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) folgt. Zentrale Grundlage ist das IT-Grundschutzprofil für Hochschulen.

Darüber hinaus benötigt die Hochschule Niederrhein ein Business-Continuity-Management zur Steuerung sämtlicher Aktivitäten, die eine geordnete Geschäftsfortführung nach größeren Schadensereignissen zum Ziel haben. Dies umfasst die Notfallvorsorge zur Vermeidung bzw. Reduzierung von Unterbrechungen sowie die Reaktion zur Wiederherstellung von Geschäftsprozessen.

Mit dieser Leitlinie betont das Präsidium die Wichtigkeit der vorgenannten Güter und definiert gleichzeitig Schutzziele und Verantwortlichkeiten. In diesem Sinne stellt die Leitlinie ein Rahmenwerk dar, das durch konkrete Vorgaben und Prozesse auszufüllen ist. Entsprechend wird die Hochschule konkrete Richtlinien, Vorgaben und Handlungsanweisungen erlassen, um die Ziele dieser Leitlinie zu erreichen. Eine jeweils aktuelle Übersicht wird im Info-ABC bereitgestellt.

Sie gilt für die Wahrnehmung sämtlicher Aufgaben der Hochschule Niederrhein. Hinsichtlich der Informationssicherheit umfasst die Leitlinie die gesamte Informationstechnik, die zur Erfüllung der Aufgaben der Hochschule Niederrhein eingesetzt werden.

2 Ziele der Hochschule Niederrhein

Die Hochschule Niederrhein beabsichtigt sich mit wirtschaftlichem Ressourceneinsatz einem möglichst hohen Maß an Datenschutz, Informationssicherheit und Ausfallschutz zu nähern und verbleibende Restrisiken auf ein akzeptables Maß zu minimieren.

Dabei verfolgt die Hochschule einen risikobasierten Ansatz und konzentriert sich beispielsweise im Datenschutz insbesondere auf den Schutz sensibler personenbezogenen Daten und risikoreicher Verarbeitungen. Zur Umsetzung der Informationssicherheitsziele können Informationsverbünde mit unterschiedlichem Schutzniveau gebildet werden.

2.1 Datenschutz

Art. 5, Abs. 2 und Art. 24 Abs. 1 EU-DSGVO beinhalten eine Rechenschaftspflicht, nach der die datenverarbeitende Stelle nachweisen muss, dass die Verarbeitung von personenbezogenen Daten unter Einhaltung der Datenschutzbestimmungen aus Art. 5 Abs. 1 EU-DSGVO und den weiteren konkretisierenden Vorgaben aus der EU-DSGVO und dem Landesrecht erfolgt. Zu diesem Zwecke baut die Hochschule Niederrhein ein Datenschutz-Management auf, das insbesondere die folgenden materiellen Anforderungen nachweisbar sicherstellen wird:

a. Gewährleistung einer rechtmäßigen, fairen und transparenten Verarbeitung:
    a. Verarbeitungen erfolgen nur mit Rechtsgrundlage (Gesetz, Einwilligung).
    b. Vorrang der Direkterhebung bei der betroffenen Person.
    c. Transparente Informationen über Art und Umfang der Verarbeitung, Betroffenen- und Beschwerderechte.
    d. Führung eines Verzeichnisses von Verarbeitungstätigkeiten zur Ermöglichung von Kontrollen durch die Aufsichtsbehörde.
b. Einhaltung der Anforderungen zur Zweckbindung, indem Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
c. Einhaltung des Grundsatzes der Datenminimierung, indem nur die für die Aufgabenerfüllung erforderlichen Daten erhoben und verarbeitet werden.
d. Gewährleistung der sachlichen Richtigkeit der Daten, indem Maßnahmen getroffen werden, um personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich löschen oder berichtigen zu können.
e. Speicherbegrenzung, indem Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Person mit den gebotenen gesetzlichen Ausnahmen nur so lange ermöglicht, wie es für den Zweck der Verarbeitung erforderlich ist.
f. Gewährleistung von Verfügbarkeit, Integrität und Vertraulichkeit, indem die personenbezogenen Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, insbesondere den Schutz vor:
    a. Unbefugter oder unrechtmäßiger Verarbeitung,
    b. Unbeabsichtigtem Verlust,
    c. Unbeabsichtigter Zerstörung oder Schädigung.

    Hier soll die Verzahnung mit dem bestehenden Informationssicherheits-Management an der Hochschule Niederrhein zu größtmöglichen Synergien führen, soweit kein Konflikt zwischen Sicherheitsmaßnahmen und Datenschutz besteht.

g. Verwirklichung der Betroffenenrechte durch Strukturen und Meldewege, die Auskünfte und daran anknüpfende weitere Betroffenenrechte ermöglichen.
h. Einhaltung der gesetzlichen Anforderungen bei der Einbindung von Dritten in die eigene oder gemeinsame Datenverarbeitung.
i. Prüfung der Rechtmäßigkeit von Datentransfers an Stellen außerhalb der EU.
j. Strukturelle und organisatorische Sicherstellung der Meldepflichten aus Art. 33 und 34 EU-DSGVO bei Datenschutzverstößen gegenüber Aufsichtsbehörde und betroffenen Personen. Hierzu gehört insbesondere die Sensibilisierung und Schulung der Mitarbeitenden, damit Vorfälle vermieden, richtig erkannt, richtig eingeordnet und richtig gemeldet werden.
k. Durchführung von Datenschutz-Folgeabschätzungen bei Vorliegen der Voraussetzungen aus Art. 35 EU-DSGVO.

2.2 Informationssicherheit

Bezogen auf die Bewahrung der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität verfolgt die Hochschule die folgenden allgemeingültigen Informationssicherheitsziele:

- Einführung und kontinuierliche Weiterentwicklung eines Informationsmanagementsystems nach BSI IT-Grundschutz,
- Zuverlässige Unterstützung des Hochschulbetriebs und der Geschäftsprozesse durch die IT,
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Organisation,
- Schutz von Daten und Informationen unter Berücksichtigung ihrer spezifischen Anforderungen (personenbezogene Daten, Verwaltungs- oder Forschungsdaten usw.),
- Schutz der Infrastruktur gegen Missbrauch von innen und außen,
- Minimierung von Schäden basierend auf Sicherheitsvorfällen,
- Einhaltung gesetzlicher Vorgaben zum Umgang mit Informationen und Systemen,
- Gewährleistung des informationellen Selbstbestimmungsrechts des Betroffenen bei der IT-gestützten Verarbeitung personenbezogener Daten,
- Aufrechterhaltung der positiven Außendarstellung,
- Fachbereiche und Organisationseinheiten können für ihren Bereich weitere, individuelle Informationssicherheitsziele formulieren.

2.3 Business-Continuity-Management

Für den Bereich des Business-Continuity-Management, mit dem Schwerpunkt der Vefügbarkeit, verfolgt die Hochschule die folgenden Ziele:

- Einführung und kontinuierliche Weiterentwicklung eines Business-Continuity-Management nach BSI 200-4,
- Erstellung eines Notfallhandbuch, dass die notwendigen Maßnahmen nach BCM-Standard BSI 200-4 enthält, die bei Eintritt eines Notfalls getroffen werden müssen,
- Bekanntgabe des Notfallhandbuch an alle Beteiligten und Ergänzung um zielgruppenspezifische Notfallchecklisten und –leitfäden.

Die Hochschulleitung verflichtet sich zur kontinuierlichen Aktualität des Handbuches. Einschränkungen im Betrieb und Nutzung von IT-Anwendungen, IT-Systemen und Dienstleistungen erfolgen nur soweit, wie es zur Erreichung der Schutzziele – abgeleitet aus der Hochschulstrategie - notwendig ist.

3 Organisation und Verantwortlichkeiten

Um die Ziele des Datenschutzes und der Informationssicherheit zu erreichen, hat die Hochschule Niederrhein Verantwortlichkeiten definiert und geschaffen, die sich aus dem Gesetz und unserer Organisationsstruktur ergeben.

3.1 Präsidium

Das Präsidium leitet gem. § 16 Abs. 1 S. 1 HG NRW die Hochschule Niederrhein. Es trägt die Gesamtverantwortung für den Datenschutz, die Informationssicherheit und das Business-Continuity-Management. Es erlässt verbindliche Regeln für die genannten Bereiche und gibt sie den Hochschulangehörigen bekannt. Ihm obliegt wegen des Fehlens einer anderweitigen Zuständigkeitsregelung die Verantwortung und Rechenschaftspflicht nach Art. 5 Abs. 2 und Art. 24 Abs. 1 EU-DSGVO. Das heißt, dass das Präsidium sicherstellt und nachweist, dass die Verarbeitung von personenbezogenen Daten in der Hochschule unter Einhaltung der Datenschutzbestimmungen der EU-Datenschutzgrundverordnung und den weiteren konkretisierenden Vorgaben des Bundes- und Landesrechts, insbesondere des DSG NRW, erfolgt. Das Präsidium trägt dieser Anforderung dadurch Rechnung, dass es die erforderlichen finanziellen, personellen und zeitlichen Ressourcen für die Umsetzung des Datenschutzes zur Verfügung stellt. Es trägt weiterhin dafür Sorge, dass Mitglieder und Angehörige der Hochschule durch Informationsangebote oder Schulungen für den Datenschutz und die Sicherheit personenbezogener Daten sensibilisiert werden.

3.2 DSB: Datenschutzbeauftragter

Die Hochschule Niederrhein hat einen behördlichen Datenschutzbeauftragten und einen Stellvertreter bestellt. Diese nehmen die Pflichten nach Art. 39 EU-DSGVO wahr und sind insbesondere Ansprechpartner für betroffene Personen und für die zuständige Datenschutzaufsichtsbehörde.

3.3 Governance, Compliance und Datenschutz Lab

Das Governance, Compliance und Datenschutz Lab unterstützt insbesondere das Präsidium und die Führungskräfte bei der Wahrnehmung der vorgenannten Pflichten. Dabei wirkt es auf die Entwicklung, Implementierung und Optimierung von datenschutzrechtlichen Regelungen und Prozessen hin und unterstützt als zentrale Koordinations- und Anlaufstelle für den operativen Datenschutz und die Informationssicherheit bei der Einhaltung der gesetzlichen Bestimmungen. Darüber hinaus bietet es Beratung, Unterstützung und Schulungen für die Datenschutzkoordinator:innen und andere Angehörigen der Hochschule Niederrhein.

3.4 Datenschutzkoordinator :innen

Alle Fachbereiche, Organisationseinheiten und Einrichtungen sollen Datenschutzschutzkoordinator:innen benennen, um die jeweilige Leitung in Angelegenheiten des Datenschutzes zu beraten und als Multiplikator vor Ort (bereichsinterne) Prozesskenntnisse und Datenschutzkenntnisse zu verbinden. So können Verarbeitungsvorgänge personenbezogener Daten vor Ort aufgeklärt, dargestellt, datenschutzfreundlich gestaltet und dokumentiert werden. Die Nähe zur praktischen Umsetzung ermöglicht eine kontinuierliche Aktualisierung der Dokumentationen, auch wenn sich die Abläufe in der Praxis ändern. Die Datenschutzkoordinator:innen sind Teil der

hochschulweiten Datenschutzkultur und Ihre ersten Ansprechpersonen in allen Belangen rund um den Datenschutz.

3.5 ISB: Informationssicherheitsbeauftragter

Der Informationssicherheitsbeauftragte wird von der Hochschulleitung bestellt und übernimmt innerhalb der Stabsstelle Informationssicherheit eine steuernde Funktion und koordiniert den hochschulweiten Informationssicherheitsprozess. Dies umfasst präventive, dedektive sowie reaktiven Maßnahmen im Rahmen deines Informationssicherheitsmanagementsystems (ISMS). Der Informationssicherheitsbeauftragte ist in allen für die Informationssicherheit relevanten Themen zu informieren bzw. bei grundlegenden Entscheidungen, Vorhaben und Änderungen, die die Informationssicherheit berühren können frühzeitig einzubeziehen und anzuhören.

3.6 BC-Manager

Der BC-Manager übernimmt innerhalb der Stabsstelle Informationssicherheit eine steuernde Funktion und koordiniert das Business-Continuity-Management nach BSI Standard 200-4. Er ist dafür zuständig, das BCMS sowie die zugehörigen Prozesse, Methoden, Verfahren und Rollen in Abstimmung mit der Institutionsleitung zu definieren, zu implementieren und weiterzuentwickeln. Dazu erfolgt eine enge Zusammenarbeit mit dem Notfall- und Krisenmanagement der Hochschule. Ferner kann der BC-Manager weitere erforderliche Rollen der BCM-Organisation und deren Zuständigkeiten, z.B. der besonderen Aufbauorganisation (BAO) für den Notfall, gemeinsam mit der Institutionsleitung definieren.

3.7 CIO: Chief Information Officer

Die zentrale interne Instanz für die operative Informationssicherheit der zentral betriebenen IT-Systeme ist die IT-Leitung (CIO). Sie verantwortet den sicheren Betrieb und die Umsetzung geeigneter Sicherheitsmechanismen. In Zusammenarbeit mit dem Informationssicherheitsbeauftragten, BC-Manager und dem Datenschutzbeauftragten bringt sie bei allen IT-Projekten frühzeitig die für die spezifischen Aspekte und Anliegen ein und ist für die Umsetzung geeigneter Sicherheitsmaßnahmen zuständig.

3.8 Vorgesetzte

Ungeachtet der Verantwortlichkeit der Hochschulleitung und der IT-Leitung sind Datenschutz und Informationssicherheit ein integraler Bestandteil der jeweiligen Fachaufgabe. Somit übernehmen Vorgesetzte an der Hochschule Niederrhein die Zuständigkeit für den Datenschutz in ihrem Geschäftsbereich. Die Vorgesetzten haben eine Vorbildfunktion. Es obliegt ihnen, den Datenschutz und die Informationssicherheit in ihrem Bereich umzusetzen, aufrecht zu erhalten und bei Bedarf an neue rechtliche, technische und organisatorische Gegebenheiten anzupassen. In Bereichen, in denen IT-Infrastruktur eigenverantwortlich betrieben wird, verantworten die Vorgesetzten den technisch sicheren und rechtssicheren Betrieb der IT und überwachen die Umsetzung geeigneter Sicherheitsmaßnahmen. Eine Definition der verschiedenen Vorgesetzten ist der Dienstanweisung zur Bestimmung der Vorgesetzten an der Hochschule Niederrhein (Amtliche Bekanntmachung Nr. 21/2024) zu entnehmen.

3.9 Mitarbeitende

Jede/r Beschäftigte der Hochschule Niederrhein, d.h. jede Professorin und jeder Professor, wissenschaftliche Mitarbeiter/in sowie Mitarbeiter/in aus Technik und Verwaltung, studentische Aushilfe sowie studentische (SHK) und wissenschaftliche Hilfskraft (WHK), übernimmt persönlich die Verantwortung dafür, dass bei Erledigung der ihnen übertragenen Aufgaben des eigenen Verantwortungsbereichs die einschlägigen Bestimmungen des Datenschutzes und der Informationssicherheit beachtet werden. Sie nehmen die angebotenen Informations- und Schulungsangebote wahr und nutzen die ihnen zugänglichen personenbezogenen Daten nur im Rahmen der ihnen übertragenen Aufgaben. Bei studentischen Beschäftigten haben die direkten Vorgesetzen eine angemessene Sensibilisierung sicherzustellen, die dem Aufgabengebiet entspricht.

Die Mitarbeitenden sollen sich stets der Bedeutung der Informationssicherheit bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken. Sie müssen verantwortungsbewusst mit den Informationssystemen und den darauf gespeicherten und dort verarbeiteten Daten umgehen und auf die Wahrung von Betriebs- und Geschäftsgeheimnissen achten. Bei Unregelmäßigkeiten müssen die Mitarbeitenden unverzüglich den Informationssicherheitsbeauftragten bzw. Datenschutzbeauftragen und ihre Vorgesetzten informieren, ggf. unter Zuhilfenahme von Möglichkeiten des Hinweisgeberschutzes. Es wird erwartet, dass alle Nutzenden von IT-Systemen die vorliegende Leitlinie kennen und beachten. Im Rahmen der BCM-Organisation stellen alle Hochschulangehörige einen wichtigen Bestandteil des BCM dar, um die Institution gegenüber Schadensereignissen und deren Auswirkungen resilienter zu machen. Daher sind alle Hochschulangehörige aufgefordert, in ihren jeweiligen Aufgabenbereichen die BCM-Organisation dabei zu unterstützen, das BCMS zu etablieren, aufzubauen und kontinuierlich weiterzuentwickeln.

4 Monitoring und kontinuierliche Verbesserung

Zu Sicherhstellung der Qualität des ISMS, BCMS und DSMS kommt das PDCA-Modell mit den Phasen Planen, Durchführen, Überwachen und Optimieren zur Anwendung. Es wird in regelmäßigen Abständen geprüft, ob das gewählte Vorgehen mit den Rahmenbedinungen übereinstimmt, die Sicherheitsziele noch angemessen sind und die Aktualität der Leitlinien gegeben ist. Im Rahmen von interen und externen Audits wird die Wirksamkeit der Managementsysteme sichergestellt.

5 Folgen von Zuwiderhandlungen

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten sowie Mitarbeitende, Geschäftspartner und Kunden schädigen oder den Ruf der Hochschule Niederrhein gefährden. Allen, die an der Hochschule Niederrhein personenbezogene Daten verarbeiten oder IT-Systeme nutzen, muss ihre Verantwortung beim Umgang mit diesen bekannt sein. Es ist darauf hinzuweisen, dass sämtliche Nichteinhaltungen oder bewusste Verletzung dieser Leitlinie oder der daraus abgeleiteten ausdrücklichen Regelungen eine Verletzung der Dienstpflicht ist, die dienst-, arbeits-, straf- und zivilrechtliche Folgen nach sich ziehen kann.

Diese Richtlinie tritt zum 06.05.2025 in Kraft. Gleichzeitig treten die Datenschutz-Leitlinie der Hochschule Niederrhein vom 3. Januar 2019 und die Leitlinie zur Informationssicherheit an der Hochschule Niederrhein vom 14.02.2019 außer Kraft.

Ausgefertigt aufgrund des Beschlusses des Präsidiums der Hochschule Niederrhein vom 06.05.2025

Krefeld, 06.05.2025

Dr. Thomas Grünewald

Präsident

der Hochschule Niederrhein

6 Dokumenteneigenschaften

6.1 Allgemeine Eigenschaften

Klassifizierung	**TLP:CLEAR** - **Unbegrenzte Weitergabe**: Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
Berechtigte Rollen (Verteilerkreis)	Alle Angehörige der Hochschule Niederrhein und Externe
Freigegeben am / durch	Die Personalräte: PR-Wiss 30.04.2025, PR-TuV 25.04.2025 Präsidiumsbeschluss: 06.05.2025
Gültigkeitszeit	Unbegrenzt
Überprüfungsintervall	Jährlich
IT-Grundschutz-Baustein	ISMS.1
Ablageort	Intranet
Übergeordnete Dokumente	Hochschulentwicklungsplan

6.2 Änderungshistorie

Die Hauptversionsnummer bezeichnet signifikanten inhaltliche Änderungen. Die Nebenversionsnummer wird bei redaktionellen bzw nicht signifikaten Änderungen erhöht.

Version	Datum	Name	Beschreibung
1.0	05.06.2012	M. Grofe-Juhlk (ISB)	Erstellung der Informationssicherheitsleitlinie
2.0	19.12.2018	Patrick Feldmann (ISB)	Aktualisierung der Leitlinie Informationssicherheit
	03.01.2019		Verabschiedung Datenschutz-Leitlinie
2.1	14.02.2019	Malte Stock (ISB)	Aktualisierung der Leitlinie Informationssicherheit, Organigramm der Hochschule Niederrhein entfernt und durch Link zur Webseite ersetzt
3.0	22.04.2025	Christian ter Stein (ISB), Prof. Dr. Timo Schwarzwälder (DSB) David Peters (stv. DSB) Salah Hajou (BCMB)	Konsekutive Neufassung der Leitlinie auf Basis IT- Grundschutz-Kompendium Edition 2023 des BSI. Zusammenführung mit der Datenschutz-Leitlinie und Ergänzung um BCM