

Vereinbarung zur Informationssicherheit an den Hochschulen (VZI)

zwischen den

**Universitäten und Hochschulen für angewandte Wissenschaften
in Trägerschaft des Landes Nordrhein-Westfalen, den staatlichen Kunst-
und Musikhochschulen in Nordrhein-Westfalen (Hochschulen), dem Hoch-
schulbibliothekszentrum des Landes Nordrhein-Westfalen (hbz) und dem
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen
(MKW)**

im Einvernehmen mit der Digitalen Hochschule NRW (DH.NRW)

§ 1 Allgemeine Bestimmungen

Die fortschreitende Digitalisierung verändert Staat, Wirtschaft und Gesellschaft tiefgreifend. Neben vielen Chancen bringt die zunehmende Digitalisierung aller Lebensbereiche aber auch Risiken und Gefahren mit sich. So sind beispielsweise Cyberangriffe in unserer vernetzten Welt zu einer ernstesten und täglichen Bedrohung geworden. Die Landesregierung hat hierauf u.a. mit der Veröffentlichung einer „Cybersicherheitsstrategie des Landes Nordrhein-Westfalen“ reagiert.

Auch die Hochschulen werden zunehmend zu Zielen für Cyberangriffe. Daher bekommt die Informationssicherheit im Hochschulumfeld eine immer größer werdende Relevanz. Aufgrund ihrer offenen Struktur und ihrer systemisch bedingten heterogenen IT-Landschaften sehen sich Hochschulen hier einer besonderen Herausforderung gegenübergestellt, die nicht mit denen geschlossener Behörden- oder Firmennetzwerke vergleichbar ist. Diesen besonderen Bedarf haben die Hochschulen erkannt und beschlossen – begleitend zu lokalen Maßnahmen zur Informationssicherheit, wie beispielsweise dem Einsatz lokaler Informationssicherheitsbeauftragter und IT-Sicherheitskonzepte – auch weitere kooperative Maßnahmen zu ergreifen und so die lokalen Aktivitäten zu stärken.

Gemeinsam mit der Digitalen Hochschule NRW (DH.NRW) unterstützt das Land die Hochschulen bereits bei Ihren Aktivitäten zur Erhöhung der Informationssicherheit. Für die Sensibilisierung des Hochschulpersonals und der Studierenden finanziert das Land das „Fortbildungsprogramm zur Entwicklung digitaler Kompetenzen in Hochschulverwaltungen“ (DIGI-V.nrw) an der Fernuniversität in Hagen, das nach Projektende 2023 in den Regelbetrieb der Hochschul-

übergreifenden Fortbildung in Nordrhein-Westfalen (HÜF-NRW) übergeht, sowie das Projekt „Selbstlernakademie für Cyber- und Informationssicherheit“ (SecAware.nrw), dessen Ergebnis im Landesportal ORCA.nrw und in den landesweiten digitalen Selbstlernkurs für Studierenden zum Thema „Digitale Kompetenzen“ (DIGI-KOMP.nrw) eingebunden wird. Aktuell unterstützt das Land die Hochschulen in 2023 auch bei der Verbesserung der Krisenresilienz im Bereich der Cybersicherheit durch Mittel in Höhe von 41,15 Mio. EUR aus dem Sondervermögen des Landes zur Krisenbewältigung.

Diese Unterstützung will das Land sowohl auf der lokalen Ebene der Hochschulen als auch bei hochschulübergreifenden Unterstützungsangeboten durch die DH.NRW für die Hochschulen ausbauen. Hierzu wird die vorliegende Vereinbarung abgeschlossen. Sie stellt eine qualitative Fortschreibung der bisherigen Ziele und Maßnahmen dar, die in § 8 und § 10 der „Vereinbarung zur Digitalisierung“ (VzD 2025) festgehalten sind und ersetzt diese beiden Bestimmungen.

§ 2 Maßnahmen

- (1) Die Hochschulen und das hbz verpflichten sich, ab spätestens 2023 zu beginnen, die Basis-Absicherung nach IT-Grundschutz-Methodik des BSI oder das „IT-Grundschutz-Profil für Hochschulen“ des Vereins „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V.“ (ZKI e.V.) einzuführen. Die Umsetzung erfolgt stufenweise.

Im Rahmen des Netzwerkes Informationssicherheit.nrw berichten die Hochschulen und das hbz ab 2023 jährlich zur Gefährdungslage und zum Umsetzungsstand der Informationssicherheit an ihren Hochschulen und am hbz in einem vom Netzwerk festzulegendem einheitlichen Format. Der Bericht wird dem MKW zur Kenntnis gegeben.

- (2) Für die Verwaltungs-IT gilt über Absatz 1 hinaus die Einführung der Standard-Absicherung nach IT-Grundschutz-Methodik des BSI. Zusätzlich wird in den Bereichen der Hochschulen und des hbz mit Daten oder IT-Services mit hohem Schutzbedarf ebenfalls die Standard-Absicherung implementiert. In anderen Bereichen wird gemäß Absatz 1 schrittweise mindestens ein Basisschutz eingeführt.

- (3) Die Universitäten, Hochschulen für angewandte Wissenschaften sowie die Folkwang Universität der Künste für die Kunst- und Musikhochschulen und das hbz verpflichten sich jeweils eine Vollzeitstelle (100%) einer Informationssicherheitsbeauftragten/eines Informationssicherheitsbeauftragten gemäß BSI-Standard 200-2 einzurichten. Diese Stelle ist außerhalb der IT oder der Rechenzentren einzurichten und muss direkt der Leitungsebene zugeordnet sein. Details sind dem Punkt „8 Handlungsempfehlung“ des als Anlage beigefügten Konzept „Netzwerk Informationssicherheit.nrw“ zu entnehmen.

- (4) Für den Fall, dass die jeweilige Hochschule oder das hbz bereits eine Informationssicherheitsbeauftragte/einen Informationssicherheitsbeauftragten gemäß BSI-Standard 200-2 eingerichtet hat, müssen die unter § 3 Absatz 1 aufgeführten Personalmittel zweckgebunden im Bereich der Informationssicherheit außerhalb der IT oder Rechenzentren eingesetzt werden (z.B. zur Einrichtung einer Stellvertretung zu Absatz 3).
- (5) Die Informationssicherheitsbeauftragten im Sinne des Absatz 3 oder ihre Vertretung nehmen regelmäßig an den Treffen der Landesarbeitsgruppe der Informationssicherheitsbeauftragten NRW teil.
- (6) Die Hochschulen und das hbz verpflichten sich zur aktiven Teilnahme und Umsetzung des hochschulübergreifenden Konzepts „Netzwerk Informationssicherheit.nrw“ der DH.NRW, das als Anlage beigefügt ist. Das Konzept wird von der DH.NRW und dem MKW unter den Hochschulen ausgeschrieben und startet am 1.7.2023. Die dort in Kapitel 4 aufgeführten Phasen verschieben sich um ein halbes Jahr.
- (7) Die Hochschulen und das hbz benennen bis zum 1. Juli 2023 feste Ansprechpartnerinnen/Ansprechpartner für das hochschulübergreifend einzusetzende NRW-Team gemäß dem als Anlage beigefügten Konzept „Netzwerk Informationssicherheit.nrw“ (InfoSicHochschulen.nrw).
- (8) Die Hochschulen und das hbz unterstützen die themenbezogenen flexiblen Arbeitsgruppen im Rahmen des „Netzwerk Informationssicherheit.nrw“ durch aktive Mitarbeit.
- (9) Der Informationsfluss zu Sicherheitsmeldungen (u.a. Sicherheitslücken, Cyberangriffe etc.) erfolgt zwischen den Hochschulen und dem hbz dem NRW Team und CERT NRW.
- (10) Die Hochschulen und das hbz verpflichten sich, Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit für das Hochschulpersonal und die Studierenden zu initiieren und koordinieren. Hierzu greifen die Hochschulen und das hbz auch auf das Angebot von SecAware.nrw und DIGI-KOMP.nrw im Landesportal ORCA.nrw zurück.
- (11) Die Hochschulen, das hbz und das „Netzwerk Informationssicherheit.nrw“ kooperieren auf geeignete Weise mit der „Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen“.
- (12) Die DH.NRW und das MKW erhalten jährlich einen gemeinsamen Bericht des „Netzwerk Informationssicherheit.nrw“ und der Informationssicherheitsbeauftragten an den Hochschulen und des hbz mit einer Management Summary von max. anderthalb Seiten. Der erste Bericht erfolgt im ersten Quartal 2024.

§ 3 Finanzierung

- (1) Jede Universität und Hochschule für angewandte Wissenschaften sowie das hbz erhält ab dem 1. Juli 2023 Personalmittel in Höhe von 80.100

EUR pro Jahr (gemäß Personalmittelsatz der DFG für das Jahr 2023 für eine Stelle nach TV-L E 13 Stufe 3 bis E 14 Stufe 2). Für die Kunst- und Musikhochschulen erhält die Folkwang Universität der Künste in Essen diese Mittel für eine gemeinsame Stelle. Vorbehaltlich der Zustimmung des Haushaltsgesetzgebers ist eine dauerhafte Übertragung dieser Mittel in die jeweiligen Hochschulkapitel ab dem Haushaltsjahr 2024 vorgesehen.

- (2) Die Trägerhochschule der Aufgaben des Verbundrechenzentrums der Kunst- und Musikhochschulen erhält zusätzlich Personalmittel gemäß Absatz 1 für eine Stelle der IT-Sicherheit.
- (3) Zur Unterstützung der IT an den Kunst- und Musikhochschulen werden die Personalmittel für das Projekt „IT-Sourcing der Kunst- und Musikhochschulen“ gemäß § 8 VzD 2025 an die Personalmittelsätze der DFG für das Jahr 2022 angepasst und ab dem Haushaltsjahr 2023 in den jeweiligen Hochschulkapiteln verstetigt. Die Personalmittel für die Einrichtung und den Betrieb eines Identitäts-Management-Systems (IDM) an den Kunst- und Musikhochschulen im Verbundrechenzentrum an der Hochschule für Musik in Detmold werden auf 77.400 EUR erhöht.
- (4) Das MKW finanziert das als Anlage beigefügte Konzept „Netzwerk Informationssicherheit.nrw“ aus Mitteln der Digitalisierungsoffensive gemäß Förderempfehlung der DH.NRW in Höhe von zunächst bis zu insgesamt zwei Millionen EUR. Für die Leitung und deren Stellvertretung des im Konzept genannten „NRW Teams“ werden jeweils Personalmittel im Hochschulkapitel derjenigen Hochschule, die das Konzept umsetzen wird, verstetigt. Für die Leitung Personalmittel in Höhe von 94.500 EUR (gemäß Personalmittelsatz der DFG für das Jahr 2023 für eine Stelle nach TV-L E 14 Stufe 5 bis E 15 Stufe 4) und die Stellvertretung gemäß Absatz 1.

§ 4 Monitoring

Die Überwachung der Umsetzung dieser Vereinbarung wird in das regelmäßige Monitoring der DH.NRW gemäß § 12 Vereinbarung zur Digitalisierung (VzD 2025) integriert.

Diese Vereinbarung tritt zum 01.07.2023 in Kraft.

Düsseldorf, den 07. Februar 2023

Ministerium für Kultur und Wissenschaft
des Landes Nordrhein-Westfalen
- Die Staatssekretärin -


Gonca Türkeli-Dehnert

Digitale Hochschule NRW - Die Vorsitzende des Vorstands -	 (Prof. Dr. Ada Pellert)
Technische Hochschule Aachen - Der Kanzler -	 (Manfred Nettekoven)
Universität Bielefeld - Der Kanzler -	 (Dr. Stephan Becker)
Universität Bochum - Die Kanzlerin -	 (Dr. Christina Reinhardt)
Universität Bonn - Der Kanzler -	 (Holger Gottschalk)
Technische Universität Dortmund - Der Kanzler -	 (Albrecht Ehlers)
Universität Düsseldorf - Der Kanzler -	 (Dr. Martin Goch)
Universität Duisburg-Essen - Der Kanzler -	 (Jens Andreas Meinen)
Fernuniversität in Hagen - Die Kanzlerin -	 (Birgit Rimpo-Repp)
Universität Köln - Der Kanzler -	 (Karsten Gerlof)
Deutsche Sporthochschule Köln - Die Kanzlerin -	 (Marion Steffen)
Universität Münster - Der Kanzler -	 (Matthias Schwarte)

Universität Paderborn - Die Vizepräsidentin für Wirtschafts- und Personalverwaltung -	(Simone Probst)
Universität Siegen - Der Kanzler -	(Ulf Richter)
Universität Wuppertal - Der Kanzler -	(Dr. Roland Kischkel)
Fachhochschule Aachen - Der Kanzler -	(Volker Stempel)
Fachhochschule Bielefeld - Die Vizepräsidentin für Wirtschafts- und Personalverwaltung -	(Gehsa Schnier)
Hochschule Bochum - Der Kanzler -	(Markus Hinsenkamp)
Hochschule Bonn-Rhein-Sieg - Die Kanzlerin -	(Angela Fischer)
Fachhochschule Dortmund - Der Kanzler -	(Jochen Drescher)
Hochschule Düsseldorf - Der Vizepräsident für Organisation, Qualitäts- und Digitalisierungsmanagement -	(Jan Eden)
Westfälische Hochschule - Der Kanzler -	(Dr. Heiko Geruschkat)
Hochschule für Gesundheit in Bochum - Der Kanzler -	(Werner Brüning)

Hochschule Hamm-Lippstadt - Die Kanzlerin -	(Sandra Schlösser)
Fachhochschule Südwestfalen - Der Kanzler -	(Heinz-Joachim Henkemeier)
Hochschule Rhein-Waal - Der Kanzler -	(Michael Strotkemper)
Technische Hochschule Köln - Die Vizepräsidentin für Wirtschafts- und Personalverwaltung -	(Dr. Ursula Löffler)
Hochschule Ostwestfalen-Lippe - Die Kanzlerin -	(Nicole Soltwedel)
Hochschule Ruhr-West - Der Kanzler -	(Dr. Jörn Hohenhaus)
Fachhochschule Münster - Der Kanzler -	(Guido Brebaum)
Hochschule Niederrhein - Die Kanzlerin -	(Dr. Köller-Marek)

Hochschule für Musik Detmold - Der Kanzler -	 (Hans Bertels)
Kunstakademie Düsseldorf - Die Kanzlerin -	 (Johanna Boeck-Heuwinkel)
Robert-Schumann-Hochschule Düsseldorf - Die Kanzlerin -	 (Dr. Cathrin Müller-Brosch)
Folkwang Universität der Künste - Der Kanzler -	 (Christian Renno)
Hochschule für Musik und Tanz Köln - Der Kanzler -	 (Dr. Gunther Zander)
Kunsthochschule für Medien Köln - Die Kanzlerin -	 (Dr. Sabine Schulz)
Kunstakademie Münster - Der Kanzler -	 (Frank Bartsch)
Hochschulbibliothekszenrum des Landes NRW - Die Dienststellenleiterin -	 (Dr. Silke Schomburg)

Konzept „Netzwerk Informationssicherheit.nrw“

zur Stärkung der Informationssicherheit an den NRW-Hochschulen und zum Aufbau einer Informationssicherheitskultur

Autor*innen:

- Programmausschuss der DH.NRW
- Geschäftsstelle der DH.NRW
- Redaktionsteam Informationssicherheit (Irmgard Blumenkemper, Julia Dauwe, Birgit Feldmann, Robert Hellwig, Sandra Mahr, Dr. Marius Mertens, André Nording, Malte Stock)

1 Zusammenfassung

Im Rahmen der *Vereinbarung zur Digitalisierung* wurde zwischen den Universitäten und Hochschulen für angewandte Wissenschaften in Trägerschaft des Landes Nordrhein-Westfalen sowie den staatlichen Kunst- und Musikhochschulen in Nordrhein-Westfalen und dem Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen (MKW) im Einvernehmen mit der Digitalen Hochschule NRW (DH.NRW) u. a. vereinbart, dass eine Struktur geschaffen werden soll, „die die Hochschulen bei der Umsetzung der Absicherung nach BSI-Methodik, im Havariefall und in der Zusammenarbeit mit dem CERT NRW fachlich unterstützt.“¹

Die Zielsetzung des vorliegenden Konzepts ist der Aufbau eines Netzwerks zur kooperativen Stärkung der Informationssicherheit und des Datenschutzes an den NRW-Hochschulen. Wesentlicher Teil dieses Netzwerks sind die vorhandenen und durch die Vereinbarung zur Informationssicherheit (VzI) geförderten zusätzlichen Stellen an den lokalen Hochschulen. Unterstützend dazu wird die Einrichtung eines koordinierenden zentralen NRW-Teams, mit der Funktion vergleichbar zu einer Beratungs- und Koordinierungsstelle mit entsprechenden Lenkungsstrukturen für das Team sowie flexibler Arbeitsgruppen vorgeschlagen. Bereits etablierte Strukturen, Werkzeuge, Publikationen, Handreichungen, Schnittstellen und bestehende Dienstleistungen sollen im Rahmen des Aufbaus des NRW-Teams berücksichtigt sowie nachgenutzt werden, um Doppelungen und Eigenentwicklungen zu vermeiden. **Das vorliegende Konzept beschreibt die initiale Phase, die bei positiver Evaluation zum 01.01.2026 in einen Regelbetrieb übergehen soll.**

¹ S. §10, VzD 2025: [Link zur VzD 2025](#)

Die Basis des Netzwerks Informationssicherheit bilden die lokalen Strukturen zu Informationssicherheit und Datenschutz an den Hochschulen, die mit der „Vereinbarung zur Informationssicherheit“ (VZI) an den öffentlich-rechtlichen Universitäten und Hochschulen für Angewandte Wissenschaften sowie den staatlichen Kunsthochschulen in Nordrhein-Westfalen aufgebaut bzw. unterstützt werden. Denn die zentralen Elemente des Netzwerks Informationssicherheit.nrw können in den meisten Bereichen nur eine unterstützende Rolle übernehmen.

Der Tätigkeitsschwerpunkt der zentralen Struktur liegt auf der Bereitstellung von fachlichen Einschätzungen und lösungsorientierten Handlungsempfehlungen, Hilfestellungen, Sammlungen zu Best Practice Beispielen etc. z. B. zum Umgang mit Warnmeldungen zu Schwachstellen, Risikomanagement im Kontext Informationssicherheit oder ähnlichem. Die finale Entscheidung bzgl. der Umsetzung von Sicherheitsmaßnahmen muss immer lokal durch die jeweilige Hochschulleitung getroffen werden.

Inhaltsverzeichnis

1	Zusammenfassung	1
2	Begriffsdefinitionen	3
3	Einleitung	3
3.1	Zusammenspiel der zentralen Struktur und der lokalen Hochschulakteur*innen	4
3.2	Priorisierung der Tätigkeiten und Themen des NRW-Teams	5
4	Begründung und Erfolgsfaktoren Netzwerk Informationssicherheit.nrw	5
4	Vorgehensweise	7
4.1	Zielstruktur Netzwerk Informationssicherheit.nrw.....	8
4.2	Lokale Strukturen in den Bereichen Informationssicherheit und Datenschutz an den NRW-Hochschulen.....	8
4.3	NRW-Team.....	9
4.4	Flexible Arbeitsgruppen.....	10
4.5	Lenkungsstrukturen	10
5	Tätigkeiten und Themenfelder des NRW-Teams	10
5.1	IST-Stand-Erhebung und Bedarfsermittlung	10
5.2	Aufbau der zentralen NRW-Strukturen / Kommunikation.....	11
5.3	Unterstützung operative Informationssicherheit.....	12
5.4	Informationssicherheitsmanagement.....	13
5.5	Datenschutz & IT-Recht	15
5.6	Unterstützung der Landesarbeitsgruppe Informationssicherheit der DH.NRW	15
5.7	Evaluation	16
5.8	Umsetzungsreihenfolge der Leistungsschwerpunkte.....	16
6	Kostenschätzung	17
7	Abkürzungsverzeichnis.....	19

8	Handlungsempfehlungen.....	20
---	----------------------------	----

2 Begriffsdefinitionen

Informationssicherheit i. S. d. Konzepts sind alle Maßnahmen zum Schutz von Informationen. *„Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit.“²*

Der/die Informationssicherheitsbeauftragte (kurz IS-Beauftragter oder ISB) i. S. d. Konzepts ist für die strategische Erfüllung der Aufgabe "Informationssicherheit" zuständig. Andere Bezeichnungen sind CISO (Chief Information Security Officer) oder Informationssicherheitsmanager (ISM).

„Die Rolle des ISB sollte von einer Person mit eigener Fachkompetenz zur Informationssicherheit in einer Stabsstelle [...] wahrgenommen werden“³, (s. auch Abschnitt 8 Handlungsempfehlungen). Die Bezeichnung „IT-Sicherheitsbeauftragte/r“ wird nicht verwendet, da die Bezeichnung auf eine begrenzte Zuständigkeit für den Teilbereich der IT-Security hindeutet.

3 Einleitung

Die Bedeutung und Notwendigkeit der Informationssicherheit und die einer gelebten Informationssicherheitskultur wird nicht zuletzt durch die Cyberangriffe auf die deutsche Hochschullandschaft deutlich. Auch die NRW-Hochschulen wurden bereits Opfer größerer Angriffe mit teilweise massiven Auswirkungen. Das Ziel muss es sein, erfolgreiche Angriffe, soweit möglich, komplett zu verhindern oder deren Auswirkungen zu minimieren und in allen Geschäftsprozessen eine sichere Informationsverarbeitung zu gewährleisten.

Die Informationssicherheit an den NRW-Hochschulen muss daher grundlegend gestärkt werden, weshalb die Hochschulen sich mit der Unterzeichnung der *Vereinbarung zur Informationssicherheit*, VzI⁴, dazu verpflichten, *„ab 2023 die Basis-Absicherung nach IT-Grundschutz-Methodik des BSI oder das IT-Grundschutz-Profil für Hochschulen des ZKI e. V. anzuwenden“* sowie für die Services des Rechenzentrums sowie die Verwaltungs-IT *„die Anwendung der Standard-Absicherung nach IT-Grundschutz-Methodik des BSI“*.

² S. Internetauftritt BSI (Stand 23.02.22): <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html>

³ S. Internetauftritt BSI (Stand 23.02.22): <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html>

⁴ LINK VzI wenn veröffentlicht

Des Weiteren wurde im Rahmen der VzD vereinbart: „Die Hochschulen verpflichten sich, bis zum 31. März 2022 ein in der DH.NRW abgestimmtes Konzept für eine Struktur vorzulegen, die die Hochschulen bei der Umsetzung der Absicherung nach BSI-Methodik, im Havariefall und in der Zusammenarbeit mit dem CERT NRW sowie der Koordinierungsstelle Cybersicherheit NRW fachlich unterstützt. Die Ressourcenausstattung wird über ein Förderverfahren der DH.NRW sichergestellt. Der Testbetrieb der Struktur wird am 01.07.2023 aufgenommen. Zudem bauen die Hochschulen innerhalb der DH.NRW hochschulübergreifende Strukturen für den Austausch unter den Informationssicherheitsbeauftragten und der Zusammenarbeit mit dem CERT NRW und der Koordinierungsstelle Cybersicherheit NRW auf.“ (VzD 2025, § 10)

Dieses Konzept ist das Ergebnis von zwei DH.NRW-öffentlichen Bar Camps, intensiven Beratungen im Rahmen eines für diesen Anlass gegründeten Redaktionsteams, des Programmausschusses sowie des Vorstands der DH.NRW.

3.1 Zusammenspiel der zentralen Struktur und der lokalen Hochschulakteur*innen

Auch wenn eine zentrale Unterstützungsstruktur Themen und Dienste gebündelt erarbeiten und die Netzwerkarbeit unter den Hochschulen und mit externen Beteiligten **stark** vorantreiben kann, **liegen viele essentielle Aufgaben zwangsläufig weiterhin bei den jeweiligen Hochschulen, ebenso sind die Hochschulen die Basis der Kooperationen.**

Zudem liegt die Verantwortung für die Informationssicherheit bei der jeweiligen Hochschulleitung.

Beispiele lokaler Aufgaben sind:

- Strategieentwicklung in den Bereichen Informationssicherheit und Datenschutz für die lokale Hochschule
- Planung, Umsetzung & Dokumentation lokaler Maßnahmen
- Anpassungen von Richtlinien an lokale Gegebenheiten
- Erarbeitung von Sicherheitskonzepten
- Etablierung des Notfallmanagements
- Etablierung des Risikomanagements
- Aufbau von Schnittstellen/Kontakten zum NRW-Team, um (interne) Prozesse anzustoßen, bspw. bei Bekanntwerden von Sicherheitsvorfällen mit Relevanz für die Hochschulen oder in der Zusammenarbeit bei der Bearbeitung von Sicherheitsvorfällen
- Unterstützung und aktive Mitarbeit der bzw. in den Arbeitsgruppen und Erfahrungsaustauschen
- Beförderung einer lokalen Informationssicherheitskultur

3.2 Priorisierung der Tätigkeiten und Themen des NRW-Teams

Die Priorisierung der Tätigkeiten und Themen des NRW-Teams (s. 5.8) stellt die geplante zeitliche Reihenfolge im Rahmen des Aufbaus des Netzwerks Informationssicherheit.nrw dar und keine allgemeine Gewichtung oder Bewertung der Schwerpunkte. Dabei liegt der fachliche Schwerpunkt zunächst stärker auf der operativen Informationssicherheit, da im Rahmen der Beratungen des Vorgehens aktuell der größte Handlungsbedarf gesehen wird.

Der Themenschwerpunkt Information Security Management System (ISMS) wird ein zentrales Thema sein.

4 Begründung und Erfolgsfaktoren Netzwerk Informationssicherheit.nrw

Im Folgenden werden nach der Methodik einer SWOT-Analyse die Stärken, Schwächen, Chancen und Risiken für das Netzwerk Informationssicherheit.nrw aufgezeigt:

Stärken

- Erhöhte Wahrnehmung der Informationssicherheit an den öffentlich-rechtlichen DH.NRW-Mitgliedshochschulen
- Synergieeffekte durch Austausch und Kooperation bei speziellen fachlichen Themen, zentrale Beratungs- und Schulungsangebote oder Stellungnahmen, bspw. bei hochschulübergreifend eingesetzten IT-Verfahren
- Initiierung weiterer kooperativer Maßnahmen, unter anderem in Bereichen, in denen aufwendige Maßnahmen (bspw. im Bereich der operativen Informationssicherheit) nur bedingt durch einzelne Hochschulen umgesetzt werden können
- Stärkung des Informationsaustausches, der Netzwerkbildung sowie Etablierung bzw. Ausbau einer Informationssicherheitskultur
- Unterstützung der Hochschulen im Havarie-Fall, bspw. durch Rahmenverträge mit spezialisierten Unternehmen
- Zusammenarbeit und Vernetzung über die Bundesländer hinaus – unter Hochschulen, Forschungseinrichtungen, Landesbehörden sowie damit verbundenen Instituten und Einrichtungen
- Stärkung der Landesarbeitsgruppe Informationssicherheit DH.NRW hinsichtlich Organisation, Sichtbarkeit und Öffentlichkeitsarbeit
- Erarbeitung von Einheitliche Konzepten und Mustern bzw. Vorlagen und Beispielen, Erarbeitung eines Datenschutzmanagement-Programms, landesweite Vorgaben Empfehlungen bzgl. der Freigabe von internen Informationen, Unterstützung des Datenschutzes bei der Umsetzung eines Datenschutzmanagementsystems gemäß des Standard-Datenschutzmodells

Schwächen

- Erschwerte Fachkräftegewinnung über alle Themenfelder des NRW-Teams (Informationssicherheit, IT-Sicherheit, Datenschutz und IT-Recht), unter anderem durch die Aufstockung der lokalen Teams an den Hochschulen, die ein vergleichbares Fachkräfte- bzw. Bewerbendenfeld ansprechen und so zwangsweise in Konkurrenz zueinander treten
- Overhead durch zentrale Strukturen und ggf. „Trägheit“ innerhalb des Netzwerks durch breite Beteiligung(-sformate)
- Bidirektionale Abhängigkeiten bei der Konzeptumsetzung

Risiken

- Verzögerungen durch Abhängigkeiten zwischen der Aufbauphase des NRW-Teams sowie dem Auf-/Ausbau der lokalen Hochschulteams
- Zusatzbelastung der lokalen Ansprechpersonen während des Aufbaus des NRW-Teams, bis eine Entlastung eintreten kann. Auch die Mitarbeit in den flexiblen Arbeitsgruppen bindet lokale Ressourcen. Hier könnte ein Engpass entstehen, wenn die lokalen Teams personell nicht ausreichend aufgestellt sind. Zur Stärkung der Informationssicherheit und Minimierung der Zusatzbelastung durch das Netzwerk erfolgt eine lokale Förderung der Hochschulen durch die VzL.
- Aufbau der Leistungsschwerpunkte am tatsächlichen Bedarf der Hochschulen vorbei – bspw. auf Grund zu geringer Sensibilisierung der Beteiligten bezüglich der Teilnahme an den Abfrageformaten oder durch die Einbeziehung ungeeigneter Zielgruppen bei den Erhebungen
- Unsicherheiten bei den Zuständigkeiten durch ungenau kommunizierte Aufgabenteilung zwischen NRW-Team und lokalen Ansprechpersonen können zu unerwünschtem lokalen Ressourcenabbau und Unklarheiten über Verantwortungsbereiche führen
- Aufwändige Auswahl bzw. Etablierung einer Organisations-/Rechtsform zur rechtlichen Absicherung der Tätigkeitsfelder (abhängig von den konkreten Aufgaben, die sich über die Phasen hinweg ändern können)
- Gefahr der Beschränkung des thematischen Geltungsbereichs auf reine IT-Sicherheit bzw. reine IT-Infrastruktur
- Risiko durch Einschränkung auf technische Umsetzungen und Maßnahmen wie bspw. die Beschaffung von neuer IT-Infrastruktur

Chancen

- Förderung der Strategie- und Konzeptentwicklung an den Hochschulen im Handlungsfeld Informationssicherheit
- Bedarfsorientierte Unterstützung der Hochschulen bei der Umsetzung der Initialisierungsphasen als auch im Kontext eines kontinuierlichen PDCA-Zyklus zum Informationssicherheitsprozess

- Stärkung der Fachexpertise der lokalen Einheiten (bspw. durch ein zentrales Wissensmanagementsystem, gezielte Fortbildungsangebote, Beratungshotline)
- Beschleunigung der Umsetzung präventiver Maßnahmen
- Etablierung eines vergleichbaren lokalen Mindeststandards bei der gemeinschaftlichen Erbringung von IT-Diensten: In diesem Kontext ist es wichtig, dass alle beteiligten Hochschulen ein vorher definiertes Mindestmaß an Informationssicherheit umsetzen, da ein Verbund nur so sicher sein kann, wie „sein schwächstes Glied“. Dies gilt ebenso im Bereich des Datenschutzes. Das bedeutet, wenn eine weniger stark abgesicherte Hochschule durch Cyberkriminelle bedroht wird, könnten auch kooperierende Hochschulen durch den Angriff in Mitleidenschaft gezogen werden. Unabhängig von einem potentiellen Angriff ist ein vergleichbares oder ein einheitliches Sicherheitsniveau eine gute Basis für die Kooperation unter den Hochschulen, jedoch könnte sich die Schaffung einer gemeinsamen Basis sowie die Bewertung dieser als komplex herausstellen.
- Klärung der Zuständigkeiten zwischen den beteiligten Stakeholdern
- Schaffung von Transparenz durch die Vereinheitlichung von Prozessen etc.

Die oben genannten Faktoren sollen unter anderem im Kontext der Evaluation des Netzwerks Informationssicherheit.nrw Berücksichtigung finden.

4 Vorgehensweise

Im Rahmen der Antragsstellung müssen die antragstellenden Hochschulen ihre geplante Vorgehensweise zur Umsetzung des Konzepts Netzwerk Informationssicherheit.nrw beschreiben. Die Planung soll so erfolgen, dass mit Start des Testbetriebs (s. §10 1. Fortschreibung VzD, 01.07.2023) die Ist-Standerhebung/Bedarfsermittlung abgeschlossen ist, siehe Abbildung 1. Die Evaluation zur Überführung des Vorhabens in den Regelbetrieb sollte so durchgeführt werden, dass dieser bei positivem Ausgang zum 01.01.2026 beginnen kann.



Abb. 1: Dreistufiges Vorgehen Netzwerk Informationssicherheit.nrw

4.1 Zielstruktur Netzwerk Informationssicherheit.nrw

Das Netzwerk Informationssicherheit.nrw soll aus zwei Ebenen bestehen: einer kooperativen Ebene und einer NRW-Hochschulebene.

Die **kooperative Ebene** beinhaltet das NRW-Team sowie die landesweiten Arbeitsgruppen und Erfahrungsaustausche, mit denen es kooperieren soll. Die **NRW-Hochschulebene** beinhaltet die NRW-Hochschulen mit ihren lokalen Sicherheits- und Datenschutzteams bzw. -organisationen sowie flexible, themenspezifische Arbeitsgruppen und verwandte (zukünftige) DH.NRW-Vorhaben.

Die Arbeitsgruppen und DH.NRW-Vorhaben stellen ein Bindeglied zur kooperativen Ebene dar. Des Weiteren werden Schnittstellen zu Arbeitskreisen und externen Partner*innen mitgedacht.

Die eben genannten Strukturen und Akteur*innen werden in den nächsten Abschnitten näher beschrieben.

4.2 Lokale Strukturen in den Bereichen Informationssicherheit und Datenschutz an den NRW-Hochschulen

Wie bereits in Abschnitt 3 beschrieben, setzt dieses Konzept darauf auf, dass die NRW-Hochschulen weiterhin die Gesamtverantwortung für die Informationssicherheit an ihrer Hochschule haben und eigene Strukturen im Kontext Informationssicherheit und Datenschutz etabliert wurden. Dies entspricht auch dem in §10 VzD vereinbarten Vorgehen zur Umsetzung von Informationssicherheit nach BSI IT-Grundschutz (z. B. Baustein ISMS.1 Sicherheitsmanagement⁵, Basisanforderungen).

Zur Stärkung der lokalen Stellen werden über die Vereinbarung zur Informationssicherheit zusätzliche dauerhafte Stellen an den Hochschulen gefördert.

Den lokalen Stellen kommt eine zentrale Rolle zu:

⁵ Siehe BSI IT-Grundschutz, ISMS.1: Sicherheitsmanagement (Edition 2021, zuletzt abgerufen 18.10.2021): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/01_ISMS_Sicherheitsmanagement/ISMS_1_Sicherheitsmanagement_Edition_2021.html

Das NRW-Team unterstützt die lokalen Sicherheits- und Datenschutzteams – unter anderem mit Blick auf die Netzwerkarbeit, Unterstützung bei Vorfällen und der Entwicklung präventiver Maßnahmen (s. Abschnitt 5 *Leistungsverzeichnis*). Dazu ist es nötig, einerseits feste Ansprechpersonen für das Team an den Hochschulen sowie im gemeinsamen IT-Dezernat der Kunst- und Musikhochschulen zu haben und andererseits die internen Prozesse zu definieren, wie bspw. mit Warnmeldungen und dem Kommunikationsfluss zwischen den lokalen Teams und dem NRW-Team umgegangen werden soll. Außerdem haben die lokalen Mitarbeitenden neben der Expertise im Bereich Informationssicherheit und Datenschutz in der Regel sehr gute Kenntnisse über die Bedürfnisse der Hochschule und Erfahrungswerte zu bestimmten Themenbereichen, die das NRW-Team nicht mitbringen kann.

Für den Erfolg des Netzwerks Informationssicherheit.nrw ist es wichtig, sowohl lokale Ansprechpersonen festzulegen, als auch den Austausch zwischen allen Hochschulen in diesem Bereich sicherzustellen, bspw. durch die Teilnahme der Hochschulen an Netzwerktreffen, Treffen der Landesarbeitsgruppe der Informationssicherheitsbeauftragten sowie an themenbezogenen Arbeitsgruppen. Die lokalen Ansprechpersonen an den Hochschulen sind unterstützend bei der Umsetzung der Informationssicherheit in Geschäftsprozessen und im operativen Umfeld tätig. Das Konzept für das Netzwerk Informationssicherheit.nrw setzt auf die aktive Beteiligung der Hochschulen.

4.3 NRW-Team

Der personelle Aufbau des Teams soll zunächst wie folgt aussehen, um die Schwerpunktthemen (s. Abschnitt 5) entsprechend umzusetzen. Die Wertigkeit der Stellen wird wie folgt vorgeschlagen und im Rahmen der Kostenschätzung wie angegeben berücksichtigt:

- 1.0 VZÄ Teamleitung mit fachl. Schwerpunkt Informationssicherheit (TV-L E15)
- 1.0 VZÄ Expert*in Informationssicherheit und stellv. Leitung (TV-L E14)
- 1.0 VZÄ Expert*in IT-Sicherheit (TV-L E13)
- 1.0 VZÄ Leitungsassistentin und Sachbearbeitung (TV-L E9)

Gesamtbedarf: 4,0 VZÄ zzgl. externer Expertise für den Bereich Datenschutz und IT-Recht

Die zu Grunde liegenden Zahlen und Werte sind erste Schätzungen und Vorschläge. Ein weiterer Ausbau des NRW-Teams nach Abschluss des Testbetriebs ist bedarfsabhängig möglich, ein entsprechender Änderungsantrag muss zeitnah vor Beendigung des Testbetriebs gestellt werden.

Es wird davon ausgegangen, dass die Projektpauschale von den antragsstellenden Hochschulen u. a. für die Bereitstellung angemessener Räumlichkeiten und Arbeitsmittel für das NRW-Team eingesetzt wird.

4.4 Flexible Arbeitsgruppen

Die bereits in 4.2 genannten flexiblen Arbeitsgruppen sollen dazu dienen, den Austausch anzuregen, komplexere Themen gemeinschaftlich zu erarbeiten sowie Wissen unter allen Hochschulen zu teilen. Die aktive Mitarbeit der Hochschulen an den Arbeitsgruppen ist essentiell für den Erfolg dieser.

Dem NRW-Team kommt hier eine eher koordinierende Rolle zu, ggf. leistet es aber auch eine fachliche Unterstützung (wenn thematisch passend und gewünscht). Außerdem stellt es die Arbeitsergebnisse an zentraler Stelle für alle Hochschulen bereit.

Die Arbeitsgruppen sollen bedarfsabhängig eingerichtet werden. Der Bedarf soll im Laufe des Vorhabens initial ermittelt und regelmäßig angepasst werden.

4.5 Lenkungsstrukturen

Die Identifikation von Schwerpunktthemen im Rahmen der Tätigkeiten des NRW-Teams sowie insbesondere deren Priorisierung erfolgt in Absprache mit dem Vorstand der DH.NRW. Dazu berichtet die Leitung des NRW-Teams regelmäßig, mind. zu den quartalsweise stattfindenden Sitzungen, schriftlich über die Geschäftsstelle der DH.NRW sowie ggf. nach Einladung zur Sitzung an den Vorstand. Dieser übernimmt, ggf. nach Beratung durch den Programmausschuss sowie mit Unterstützung der Geschäftsstelle der DH.NRW, Steuerungsfunktionen u. a. bzgl. der Überprüfung der Zielerreichung gemäß der festgelegten Kriterien und ggf. Nachsteuerung der beeinflussenden Parameter (Stakeholder).

5 Tätigkeiten und Themenfelder des NRW-Teams

Im Folgenden werden die geplanten Aufgaben für das NRW-Team erläutert. Die Umsetzung sowie der Aufbau des NRW-Teams entsprechend Abschnitt 4.3 sind durch die Antragssteller*innen in Form einer Meilenstein- und Ressourcenplanung (s. Leitfaden zur Antragsstellung der DH.NRW) darzulegen. Die eigenen Dienstleistungen des NRW-Teams können während der üblichen Geschäftszeiten abgerufen werden, darüberhinausgehende Anforderungen sollen bedarfsabhängig über Rahmenverträge abgedeckt werden.

5.1 IST-Stand-Erhebung und Bedarfsermittlung

Im Rahmen des Arbeitspaktes „IST-Stand-Erhebung und Bedarfsermittlung“ sollen die folgenden Aufgaben umgesetzt werden:

- Durchführung von Sachstanderhebungen / Bedarfsermittlungen in Form von strukturierten Interviews (z. B. auf Basis von BSI-Bausteinen) sowie offenen Formaten wie World-Cafés, Bar Camps etc., insbesondere mit Blick auf potentielle Schulungs- und Zertifizierungsbedarfe
- Schaffung von Transparenz im Sinne der nachhaltigen Nutzbarkeit bereits vorhandener Konzepte, Ansätze, Schnittstellen und Plattformen

- Erstellung von Übersichten über die an den NRW-Hochschulen vorhandenen lokalen Strukturen zu Informationssicherheit
- Identifikation der Bedarfe bzgl. operativer Informationssicherheit und stetiger Abgleich mit den aktuellen BSI-Anforderungen
- NRW-Team intern: Ermittlung von internen Bedarfen des NRW-Teams
 - Identifikation von Weiterbildungs- und Zertifizierungsbedarfen wie z. B. zu informationssicherheitsrelevanten Standards
 - Teilnahme an notwendigen Schulungen zur Gewährleistung eines hochwertigen Dienstangebots des NRW-Teams und regelmäßige Auffrischung des Kenntnisstands entsprechend des Stands der Technik

5.2 Aufbau der zentralen NRW-Strukturen / Kommunikation

Im Rahmen dieses Aufgabenpakets sollen die zentralen Strukturen für das Netzwerk Informationssicherheit.nrw aufgebaut werden:

- Schaffung von Kommunikationskanälen sowie ggf. Initiierung der Zusammenarbeit bzw. des Austauschformats mit
 - den lokalen Informationssicherheitsbeauftragten und Datenschutzbeauftragten der Hochschulen bzw. deren Stellvertretungen und Teams
 - weiteren Ansprechpersonen in den Hochschulen zusammen mit den lokalen Teams (bedarfsabhängig, bspw. zur Ermittlung von speziellen Schulungsbedarfen in Rechenzentren etc.)
 - den Gremien Programmausschuss und Vorstand sowie Zusammenarbeit mit der KDU.NRW und der Geschäftsstelle der DH.NRW
 - der Landesarbeitsgruppe Informationssicherheit NRW (inkl. organisatorische Unterstützung) sowie dem ERFA der Datenschutzbeauftragten
 - dem ARNW, den ITMZ-Leiter*innen sowie dem Verbundrechenzentrum der Kunst- und Musikhochschulen
 - laufenden (und ggf. geplanten) DH.NRW-Projekten zur Informationssicherheit in Absprache und mit Unterstützung durch die Geschäftsstelle der DH.NRW
 - externen Partner*innen wie bspw. DFN-CERT, CERT NRW, Koordinierungsstelle Cybersicherheit NRW und weiteren Informationsquellen
- Identifikation von weiteren Akteur*innen im Kontext Informationssicherheit (z. B. über vergleichbare Gruppen wie Netzexperten NRW) und Durchführung von Netzwerkveranstaltungen

- Die bundeslandübergreifende Zusammenarbeit (bspw. mit dem Kernteam und weiteren Akteur*innen aus Baden-Württemberg) soll durch das Team vorangetrieben werden. Dabei soll der Fokus unter anderem auf dem Austausch zu Fachthemen und dem Informationsfluss zu Schwachstellen/Sicherheitslücken liegen. Entwicklungen, bspw. bei der Erarbeitung nationaler Schnittstellen oder Standards soll ebenso durch das Kernteam beobachtet und ggf. umgesetzt werden.
- Die Umsetzung sowie der Aufbau und Unterbringung des NRW-Teams entsprechend Abschnitt 4.3 sind durch das antragsstellende Konsortium in Form einer Meilenstein- und Ressourcenplanung (gemäß Leitfaden zur Antragstellung für Vorhaben der DH.NRW) darzulegen.

5.3 Unterstützung operative Informationssicherheit

Der Bereich operative Security⁶ soll mit einer hohen Priorität aufgebaut und durch Kooperationen unter den Hochschulen sowie mit externen Partner*innen sollen Synergien geschaffen werden. Die Bereiche Incident-Response-Management⁷, in Form von Unterstützung der lokalen Mitarbeitenden an den Hochschulen bei der Vorfallsbearbeitung bzw. in Havariefällen durch Rahmenverträge mit entsprechenden Dienstleistenden, sowie die kooperative Umsetzung präventiver Maßnahmen durch Security-as-a-Service-Dienste, die ggf. über Förderverfahren im Rahmen der DH.NRW umgesetzt werden sollen, ~~sollen~~ bilden hierbei die Schwerpunkte.

Im Rahmen einer landesweiten Security-as-a-Service-Struktur **sollen entsprechend der Ergebnisse der durchgeführten Bedarfsanalysen**

- die existierenden oder geplanten DH.NRW-Vorhaben zur operativen Informationssicherheit zusammengefasst (Netzwerkbildung) und
- der Abruf von Leistungen aus Rahmenverträgen mit Dritten und ggf. eigene zentrale Dienstleistungen angeboten werden.
Beispiele für die anzubietenden Dienstleistungen und Maßnahmen sind:
 - Durchführung von Schwachstellenscans, Pen-Testing sowie IT-Forensik
 - Security-Systeme für alle HS (ggf. durch Externe), zentrales Scrubbing Center, SIEM-Tool (Security Information and Event Management) etc. und Austausch von sicherheitsrelevanten Informationen zu in der Hochschullandschaft weit verbreiteten Diensten, Produkten und Systemen (z. B. WLAN, HISinOne etc.) unter den Hochschulen und mit externen Partner*innen
 - Aufbau und Pflege eines Dienstleistungsnetzwerks

⁶ Unter der Bezeichnung „operative Security“ werden hier hauptsächlich die technischen Maßnahmen zur Informationssicherheit zusammengefasst.

⁷ Störungs-/Vorfalls-Bearbeitung

- Bereitstellung von speziellen Lizenzen wie etwa für Forensik-Tools, Entwicklungsumgebungen, Logging-Software etc. nach Bedarf (ggf. abhängig von der gewählten Rechtsform der zentralen Struktur⁸),
- Aufbau organisatorische Unterstützung bei Sicherheitsvorfällen, z. B. durch ext. Expert*innen-Netzwerk
- Organisatorische Unterstützung bei der Nachbereitung von Vorfällen / Erstellung von Lessons Learned

Bestehende Dienste, die die Hochschulen bereits nutzen, sollten ergänzend mit in die Konzeption einfließen. Bestehende Kooperationen unter den Hochschulen oder mit anderen Partnereinrichtungen sollten ebenso weiterhin bestehen bleiben und ggf. für alle DH.NRW-Mitgliedshochschulen nutzbar gemacht sowie deren Expertise eingeholt werden (z. B. DFN-CERT, EDUCV, GWDG SEC, ZKI AK Informationssicherheit etc.). Das CERT NRW sollte bei der Etablierung der landesweiten Security-as-a-Service-Struktur hinzugezogen werden.

Die Struktur bzw. die enthaltenen Dienste sollen auch selbst entsprechend des Schutzbedarfes die BSI-Vorgaben erfüllen, damit die Hochschulen mit der Nutzung der Dienste auch diesen Vorgaben entsprechen und die Attraktivität der Dienste auch dahingehend sichergestellt wird.

5.4 Informationssicherheitsmanagement

Das NRW-Team berät die Hochschulen bei der Konzeption, Einführung und Weiterentwicklung des ISMS sowie bei der Auswahl / Einführung von ausgewählten ISMS-Tools, insbesondere mit Blick auf gemeinsame Schnittstellen unter Berücksichtigung der notwendigen Prozesse. Betrachtet werden sollten sowohl die Initialisierungsphase als auch ein kontinuierlicher PDCA-Zyklus zum Informationssicherheitsprozess und ganz wesentlich der Aufbau einer Informationssicherheitskultur in den Hochschulen. Dabei sollen die folgenden Leistungen angeboten werden:

- Etablierung eines bedarfsgerechten Beratungsangebotes für die lokalen Ansprechpartner*innen/Teams & ggf. Hochschulleitungen zum Themenfeld ISMS, insbesondere in den Themenbereichen des BSI und ggf. ergänzend zu anderen Standards
- Bereitstellung von Mustern/Vorlagen zum Informationssicherheitsmanagement, zu Sicherheitsmaßnahmen und von Mustergeschäftsprozessen

⁸ Im Rahmen des Konzepts wurde bisher die Frage nach einer Rechtsform nicht betrachtet, sollte aber nachgelagert mitgedacht werden. Der Schwerpunkt liegt auf der Konzeption des Netzwerks.

- Konzeption und Durchführung von Schulungs- und Sensibilisierungsprogrammen für die verschiedenen Zielgruppen (inkl. der Informationssicherheitsbeauftragten sowie IT-Personal) - nach Sichtung bereits vorhandener oder sich im Aufbau befindlicher Programme wie SecAware.NRW (Zielgruppe: Studierende und Wissenschaftler*innen), um Dopplungen zu vermeiden; Bereitstellung von Fortbildungsempfehlungen für lokale CISOs und DSBs
- kontinuierliche Pflege der durch das NRW-Team erarbeiteten Materialien sowie regelmäßige Überprüfung der im Rahmen von DH.NRW-Vorhaben erarbeiteten Lehr-Lern-Materialien zur Informationssicherheit und Datenschutz, die auf ORCA.NRW zum Austausch und als Selbstlerneinheiten zur Verfügung gestellt werden, auf Aktualität
- Koordination
 - Informationsaustausch unter den HS, CERT NRW und externen Partner*innen (u. a. zu sicherheitsrelevanten Meldungen)
 - Vernetzung der Akteur*innen zu flexiblen Arbeitsgruppen, ggf. Beratung und Moderation
- Beratung der Hochschulen bei der Evaluation von Sicherheitsmaßnahmen
- ggf. Audit-Angebote im Rahmen der Anwendung des BSI-IT-Grundschutzes bzw. zur Vorbereitung auf den Erwerb eines BSI Testats nach der Basis-Absicherung
- Beratung zur lokalen Dokumentation, Auswahl und ggf. Bereitstellung eines nutzer*innenfreundlichen Dokumentationswerkzeuges (mit Schnittstellen zu gängigen anderen Systemen)
- Gewährleistung eines toolbasierten, nachhaltigen Wissensmanagements
- Auf Anforderung des Vorstands oder des Programmausschusses der DH.NRW Einschätzungen/Stellungnahmen bzgl. Sicherheit bei hochschulübergreifend eingesetzten IT-Produkten im Rahmen der DH.NRW
- Netzworkebildung mit Expert*innen, Austausch mit anderen Partnerinstitutionen, interne Weiterbildung
- Beratung der DH.NRW-Projekte bei Fragen zur Informationssicherheit

Da die Anwendung der BSI-Vorgaben ein zentrales Thema für die Hochschulen sein wird, kann die Erarbeitung von Muster-Umsetzungskonzepten für die Hochschulen sehr hilfreich sein. Diese könnten Ressourcenschätzungen beinhalten und modular aufgebaut werden, damit auch Hochschulen profitieren können, die bzgl. der Umsetzung der BSI-Vorgaben bereits weiter sind.

5.5 Datenschutz & IT-Recht

Für den Bereich Datenschutz und IT-Recht soll zunächst nur in einem kleineren Umfang ein unterstützendes Beratungsangebot (explizit ausgenommen ist der Tätigkeitsbereich Rechtsinformationsstelle eLearning der DH.NRW⁹) aufgebaut werden, welches u.a. durch Einholung von externer Expertise durch das NRW-Team umgesetzt werden soll:

- Beratung bei der Auswahl von Awareness-Kampagnen, Schulungsangeboten und -konzepten
- Für DH.NRW-Vorhaben: Unterstützung bei Vorbereitung sowie Beratung zu:
 - Datenschutzrechtlichen Einschätzungen/Stellungnahmen zu hochschulübergreifend eingesetzten IT-Produkten und Sicherheitsmaßnahmen
 - Auftragsdatenverarbeitungsverträgen, Verträgen zur gemeinsamen Verantwortlichkeit, Datenschutzfolgenabschätzungen
 - Fragen zu internationalem Datentransfer
- Bereitstellung von Musterrichtlinien, Vorlagen etc.
- Unterstützung bei der Optimierung der lokalen Dokumentation (Toolauswahl etc.)
- Interner Datenschutz/IT-Recht:
 - Erstellung von Einschätzungen bzw. Stellungnahmen zum eigenen Angebot des NRW-Teams (Dienste, Sicherheitsmaßnahmen etc.) zum Thema Datenschutzrecht und IT-Recht
 - Übernahme von Team-internen Aufgaben zum Datenschutz (Dokumentation, Erstellung von ADV etc.)
- enger Austausch mit dem ERFA der bDSB der Hochschulen in NRW sowie weiteren bundeslandübergreifenden Arbeitsgruppen

5.6 Unterstützung der Landesarbeitsgruppe Informationssicherheit der DH.NRW

Das NRW-Team soll eine bedarfsabhängige Unterstützung der Landesarbeitsgruppe Informationssicherheit der DH.NRW (Arbeitsgruppe der Informationssicherheitsbeauftragten der DH.NRW-Mitgliedshochschulen), in Absprache mit der HÜF-NRW, bei den folgenden Punkten leisten:

- Themenfindung
- Kontaktherstellung zu und Finanzierung von Referent*innen für die Arbeitsgruppentreffen
- organisatorische Aspekte der Durchführung von Veranstaltungen (z. B. Moderation, Protokollführung)

⁹ <https://www.dh.nrw/kooperationen/Rechtsinformation%20zum%20E-Learning-61>

- Konzeption von weiteren Veranstaltungsformaten sowie Organisation von themenbezogenen Arbeitsgruppen
- Mitgliederverwaltung
- Mitwirkung bei der Außendarstellung der Landesarbeitsgruppe (z. B. Öffentlichkeitsarbeit, Internetauftritt, Erarbeitung von Pressemitteilungen)

5.7 Evaluation

Zum Abschluss des Projektes ist eine Evaluationsphase vorgesehen. Dazu wird vorgeschlagen, eine externe Evaluation über den Rahmenvertrag der DH.NRW zu beauftragen.

Die unter Abschnitt 3 aufgeführten Faktoren sind bei einer Evaluation zu berücksichtigen und nicht als verbindliche Wertungskriterien bei der geplanten Förderausschreibung zur Umsetzung des vorliegenden Konzeptes zu verstehen.

5.8 Umsetzungsreihenfolge der Leistungsschwerpunkte

Die zeitliche Reihenfolge bei der Umsetzung der Leistungsschwerpunkte soll wie in Tabelle 1 dargestellt eingehalten werden:

Tabelle 1 Zeitliche Priorisierung der Leistungsschwerpunkte

Schwerpunkt	Zeitl. Priorisierung
5.1 IST-Stand-Erhebung und Bedarfsermittlung	1
5.2 Aufbau der zentralen NRW-Strukturen / Kommunikation	2
5.3 Operative Informationssicherheit	2
5.4 Informationssicherheitsmanagement	3
5.5 Datenschutz & IT-Recht	4
5.6 Unterstützung der Landesarbeitsgruppe Informationssicherheit NRW	3
5.7 Evaluation	

6 Kostenschätzung

Die Kostenschätzung beläuft sich aktuell auf ca. 2,04 Mio. Euro. Diese verteilen sich wie in Tabelle 2 dargestellt und im Folgenden erläutert:

		2023	2024	2025
gesamt :	2.038.890,00	731.630,00	653.630,00	653.630,00
davon Personalausgaben	901.800,00	300.600,00	300.600,00	300.600,00
Leitung (E 15)	275.400,00	91.800,00	91.800,00	91.800,00
Assistenz/Sachbearbeitung (E9)	179.100,00	59.700,00	59.700,00	59.700,00
Inf. Sicherheit & Stellv. (E14)	232.200,00	77.400,00	77.400,00	77.400,00
IT-Sicherheit (E 13/14)	215.100,00	71.700,00	71.700,00	71.700,00
davon Sachausgaben	1.092.000,00	416.000,00	338.000,00	338.000,00
Schulungs- /Zertifizierungs-kosten Personal intern	30.000,00	20.000,00	5.000,00	5.000,00
Dienstreisen	12.000,00	4.000,00	4.000,00	4.000,00
Spezielle Hardware / Lizenzen	9.000,00	3.000,00	3.000,00	3.000,00
Externe Dienst-/Beratungs-leistungen a 1.500 Euro / Tag (Verteilung auf die Jahre: 126, 84, 84) im Bereich Informationssicherheit	441.000,00	189.000,00	126.000,00	126.000,00
Externe Dienst-/Beratungs-leistungen im Bereich Datenschutz	600.000,00	200.000,00	200.000,00	200.000,00
davon Investitionen	0,00	0,00	0,00	0,00
Projektpauschale	45.090,00	15.030,00	15.030,00	15.030,00
nachrichtlich Eigenanteil (soweit vorgesehen)	0,00			
Kostenschätzung				
gesamt :	2.038.890,00	731.630,00	653.630,00	653.630,00
davon Personalausgaben	901.800,00	300.600,00	300.600,00	300.600,00
davon Sachausgaben	1.092.000,00	416.000,00	338.000,00	338.000,00
davon Investitionen	0,00	0,00	0,00	0,00
Projektpauschale	45.090,00	15.030,00	15.030,00	15.030,00
nachrichtlich Eigenanteil (soweit vorgesehen)	0			

Tabelle 2: Kostenschätzung

Die zu Grunde liegenden Zahlen und Werte sind erste Schätzungen und Vorschläge, die sich wie folgt zusammensetzen:

Sachmittel

Die geschätzte Summe der Sachmittel setzt sich sowohl aus Kosten für externe Dienst- und Beratungsleistungen (s.u.), als auch aus weiteren Kosten für Dienstreisen, spezielle Hardware und/oder Lizenzen sowie Schulungs- und Zertifizierungskosten zusammen. Die Kosten für Dienstreisen werden auf ca. 4.000 Euro jährlich geschätzt, da davon ausgegangen wird, dass der größte Teil der Termine in virtueller Form stattfinden wird. Für spezielle Hardware oder Lizenzen, u.a. zu Testzwecken, werden ca. 3.000 Euro jährlich geschätzt.

Meist handelt es sich bei Schulungen/Zertifizierungen im Kontext der Handlungsfelder des Kernteams um höherpreisige Angebote, weshalb dieser Kostenpunkt auf insgesamt ca. 30.000 Euro geschätzt wird. Es wird davon ausgegangen, dass die Team-Mitglieder insbesondere im ersten Jahr verstärkt Schulungen besuchen werden (abhängig von der Qualifikation der Teammitglieder) und in den Folgejahren „Auffrischungen“ erfolgen werden.

Externe Dienst-/Beratungsleistungen

Die **294 Tagessätze** (2023: 126, 2024: 84, 2025: 84) zu 1.500€ sind wie untenstehend eingeplant. Die Tagessätze und die benötigte Anzahl stellen eine unverbindliche Schätzung dar; die tatsächlichen Werte können entsprechend abweichen:

- **42 Tagessätze** entfallen auf Beratungs- und Dienstleistungen im Rahmen der Bedarfserhebungen. Diese sollen mit externer Unterstützung erfolgen, da diese zeitnah nach dem Projektstart vorgesehen sind, eine hohe Relevanz für den weiteren Verlauf haben und gleichzeitig noch Stellen besetzt werden müssen.
 - Ein Tag pro Hochschule zur Durchführung der Befragungen etc. (Ermittlung „Mindestbedarf“, IST-Stand-Erhebungen, fachl. Bedarfe etc.), insgesamt **37 Tage**
 - **5 Tage** für Vorbesprechung und Auswertung
- **252 Tagessätze** entfallen auf operative Informationssicherheit, davon: ca. 222 Tage über 3 Jahre (3 Jahre * 2 Tage * 37 HSen) zzgl. 30 Tage (3 Jahre * 10 Tage) für Auswertung / Puffer für technische Probleme

Abhängig vom ermittelten Bedarf an den HSen sollen verschiedene Angebote im Bereich operative Informationssicherheit gemacht werden können (bspw. Schwachstellenscans, Pen-Tests) mit einem Kontingent von ca. 2 Tagen pro Jahr pro Hochschule.

Für den Bereich Datenschutz werden ca. 200.000 Euro jährlich als Sachkosten für die Einholung externer Expertise geschätzt und eingeplant.

Personalmittel

Die folgenden Personalbedarfe werden zur Umsetzung des kooperativen Teils des Konzepts geschätzt (die Werte in der obigen Tabelle entsprechen den Personalmittelsätzen der DFG für das Jahr 2022):

- Stelle 1: Leitung 1 VZÄ E15
- Stelle 2: Assistenz/Sachbearbeitung 1 VZÄ E9
- Stelle 3: Informationssicherheit & Stellvertretung 1 VZÄ E14
- Stelle 4: IT-Sicherheit 1 VZÄ E13/14

Sofern Dienstleistungen außerhalb der üblichen Dienstzeiten zu erbringen sind – wie z. B. im Havariefall – können diese z. B. über externe Dienstleister geleistet werden. Die Organisation und Koordination muss aber zwingend über eine Hochschule erfolgen.

7 Abkürzungsverzeichnis

ARNW	Arbeitskreis der Leiter*innen wissenschaftlicher Rechenzentren in NRW
AV-Gateway	Antivirus Gateway
bDSB	Behördliche Datenschutzbeauftragte/r
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CIO	Chief Information Officer
DFN	Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DH.NRW	Digitale Hochschule NRW
DSB	Datenschutzbeauftragte/r
ERFA	Erfahrungsaustausch
HS	Hochschule
IKM	Information, Kommunikation und Medien
ISB	Informationssicherheitsbeauftragte/r
ISM	Informationssicherheitsmanager
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik
ITMZ-Leiter	Arbeitskreis der Leiter*innen der IT- und Medienzentren an den Fachhochschulen in NRW
KPI	Key Performance Indicators / Schlüsselkennzahlen
MKW	Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen
MWIDE	Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen
PDCA	Plan – Do – Check – Act
Pen-Test	Penetrations-Test
VZÄ	Vollzeitäquivalent
ZKI	Verein der „Zentren für Kommunikationsverarbeitung in Forschung und Lehre“ e. V.

8 Handlungsempfehlungen

Zur besseren Abgrenzung der Aufgabenfelder zu existierenden Stellen und Positionen werden im Folgenden Empfehlungen bzgl. der Modellierung der Rolle der/des Informationssicherheitsbeauftragten (gemäß BSI-Standard 200-2) mit ihren benötigten Qualifikationen gegeben sowie zum besseren Verständnis abgrenzende Begriffsdefinitionen getroffen:

Definitionen:

- Informationssicherheit ≠ IT-Sicherheit
- ISB = Informationssicherheitsbeauftragte/r = CISO
- ISB ≠ IT-Sicherheitsbeauftragte/r
- ISB ≠ Notfallbeauftragte/r gem. BSI 200-4
- ISB ≠ Datenschutzbeauftragte/r
- ISB ≠ IT-Administrator*in, IT-Leitung
- ISB ≠ Vorfallsbearbeitung, operative Informationssicherheit

Anforderungen an die Stelle der/des Informationssicherheitsbeauftragten und deren/dessen Vertretung:

- Gem. BSI 200-2
- Weisungsfrei (gegenüber der IT-Leitung oder weiteren Beteiligten wie der/dem DSB)
- Ansiedlung der Funktion als Stabsstelle des Rektorates / der Hochschulleitung
- nicht in der IT-Abteilung oder unter dem CIO verortet
- Direkter Berichtsweg an Hochschulleitung
- beratende, unterstützende Funktion bei der Umsetzung von Maßnahmen zur Verbesserung der Informationssicherheit, z. B. Richtung Rektorat, Hochschulleitung, DSB, CIO, ...
- kein Interessenskonflikt durch weitere Tätigkeitsfelder und Aufgaben

Qualifikationsprofil der Stelle

M = Muss, S = Soll, K = Kann ("empfehlenswert")

fachliche Qualifikationen

- **M** Idealerweise qualifizierter wissenschaftlicher Hochschulabschluss, z. B. Master/Diplom (natur-, geistes-, wirtschaftswissenschaftliche oder vergleichbare Fachrichtung) *oder* vergleichbare Qualifikation
- **M** nachweislich Kenntnisse ISMS
- **M** nachweislich Kenntnisse IT-Grundschutz (z. B. Grundschutz Praktiker, CISO/ISB Zertifikat)
- **M** sehr gute Kenntnisse der deutschen Sprache in Wort und Schrift
- **S** sehr gutes Verständnis für IT (ohne Vorgabe eines festen Niveaus oder Abfrage bestimmter Zertifikate; übergreifende Kenntnisse sind fachspezifischem "Inselwissen" vorzuziehen)
- **S** nachweislich Kenntnisse Projektmanagement (optional Zertifikate wie ISO 69901, Prince 2, ...)
- **K** Kenntnisse Prozessmanagement und Geschäftsprozessmodellierung
- **K** Kenntnisse IT-Servicemanagement (wie z. B. ITIL-Zertifizierung, fitSM etc.)
- **K** Kenntnisse Recht, Compliance

übergreifende Qualifikationen ("Soft Skills")

- **M** Strategisches, analytisches, konzeptionelles und fachübergreifendes Denkvermögen
- **M** hohes Maß an Kommunikationsfähigkeit, Verhandlungsgeschick
- **M** Fähigkeit zur zielgruppengerechten Präsentation
- **M** selbstständige Arbeitsweise, Eigeninitiative, Organisationsgeschick
- **K** Kenntnisse der Hochschullandschaft/-verwaltung

Auf Grund der sich aus den o. g. Tätigkeitsmerkmalen ergebenden Anforderungen wird empfohlen, die Stellen mit Aufgaben entsprechend der Eingruppierungsstufe 14 zu planen. Andernfalls ist davon auszugehen, dass auf Grund der Marktlage und der Konkurrenzsituation zur freien Wirtschaft eine Stellenbesetzung erheblich erschwert wird.

Die formulierten Anforderungen bezüglich der fachlichen und persönlichen Fähigkeiten sind angelehnt an den BSI Standard 200-4.

Digitale Hochschule NRW

Vorstand

Vorsitzende	Prof. Dr. A. Pellert
Stellvertreter	Dr. T. Grünewald
Mitglieder	Dr. S. Becker, Prof. Dr. T. Grosse, Dr. U. Löffler, T. Menne, Dr. C. Reinhardt, Prof. Dr. B. Riegraf, B. Rimpo-Repp, R. Thönnissen, Dr. H.-P. Zils

Programmausschuss

Sprecher*innen	F. Klapper Prof. Dr. S. Heuchemer, Dr. K. Ilg, Prof. Dr. A. Kienle
Mitglieder	Th. Bieker, Dr. R. Bockholt, Dr. S. Drees, Prof. Dr. A. Frommer, Prof. Dr. A. Hadjakos, Prof. Dr. A. Klawonn

Geschäftsstelle

Leitung	B. Feldmann
Stellv. Leitung und Referentin für digitale Infrastruktur	J. Dauwe
Referent für Forschungsunterstützung	Dr. K. Fritsch
Referent für Administration	Dr. T. Schöttler
Referent für Studium & Lehre	M. Kroll
Sachbearbeitung und Leitungsassistentz	A. Cramer
Anschrift	DH.NRW c/o FernUniversität in Hagen Feithstr. 129 58097 Hagen
Homepage	www.dh.nrw