Fachhochschule
Dortmund
University of Applied Sciences and Arts

Verkündungsblatt | 45. Jahrgang | Nr. 80

# Amtliche Mitteilung

18.09.2024

## Informationssicherheitslinie (ISLL)

## der Fachhochschule Dortmund

## Dokumenteneigenschaften

| | |
|---|---|
| **Verantwortung** | Informationssicherheitsbeauftragter |
| **Klassifizierung** | intern |
| **Gültigkeitszeit** | Unbegrenzt |
| **Überarbeitungsintervall** | Jährlich |
| **Nächste Überarbeitung** | April 2026 |
| **Dateiname** | A01_ISMS_Informationssicherheitsleitlinie |

## Dokumentenhistorie

| Ver-sion | Änderung / Status | Datum | Autor |
|---|---|---|---|
| 0.1 | Erstellung | 18.09.2024 | ISB |
| 1.0 | Dokumentenlenkung | 16.04.2025 | ISB |

# Informationssicherheitsleitlinie der Fachhochschule Dortmund

## vom 18.09.2024

Das Rektorat der Fachhochschule Dortmund hat die folgende Informationssicherheitsleitlinie als interne Richtlinie mit Beschluss vom 18. September 2024 erlassen.

## § 1 Geltungsbereich und Stellenwert der Informationssicherheit

Die Nutzung von Informationstechnologie (IT) ist ein wesentlicher Bestandteil der Fachhochschule Dortmund und wird zur Unterstützung von unzähligen Arbeitsprozessen eingesetzt. Durch diese starke Abhängigkeit steigen die betrieblichen Anforderungen an die IT-Unterstützung der Arbeitsprozesse. Gleichzeitig muss IT auch vermehrt gesetzliche und andere regulatorische Vorgaben erfüllen. Diese Vorgaben stellen den Gegenstand der IT-Compliance dar.

Die Anzahl der IT-Compliance-Anforderungen, die beispielweise aus Gesetzen, Richtlinien, Verträgen oder Normen resultieren, ist in den letzten Jahren gestiegen. Dadurch erhöht sich die Gefahr einer Intransparenz bei der Erfüllung von nationalen und internationalen Compliance-Anforderungen an die IT. Die Hochschule ist somit verstärkt dem Risiko potenzieller Regelverstöße ausgesetzt und muss dadurch bei der Erfüllung von IT-Compliance-Anforderungen systematisch vorgehen, wobei diese Informationssicherheitsleitlinie einen wichtigen Baustein leistet.

Die vorliegende Informationssicherheitsleitlinie, im Folgenden auch Leitlinie genannt, bildet den Rahmen für die Gewährleistung der Informations- und IT-Sicherheit an der Fachhochschule Dortmund und die Basis für die hierfür erforderlichen Sicherheitsrichtlinien und Maßnahmen. Zum Schutz der IT sowie der Informations- und Datenverarbeitung der Fachhochschule Dortmund ist die Leitlinie und die daraus abgeleiteten Richtlinien und Maßnahmen für alle Angehörigen und Mitglieder der Fachhochschule verbindlich.

Um gerichtliche Auseinandersetzungen zu verhindern, stellt die Hochschule daher IT-Compliance Richtlinien auf, die für alle Angehörigen und Mitglieder der Fachhochschule verbindlich sind und deren Befolgung in der Hochschule überwacht und durchgesetzt werden. Nur so kann die IT erfolgreich geschützt und ein ausreichender Datenschutz gewährleistet werden.

Der Einsatz von Technologien eröffnet Chancen, birgt aber auch Risiken. Eine Hochschule ist nur arbeitsfähig, wenn ihre Mitglieder und Angehörigen einen möglichst fehlerlosen Zugang auf die IT als wesentliche Basis aller Arbeitsabläufe haben. So kann eine Beeinträchtigung der Informationssicherheit die Leistungsfähigkeit der Fachhochschule Dortmund mindern oder im Extremfall ganz zum Erliegen bringen.

Absehbare Schäden und Gefahren für die Hochschule müssen abgewehrt und ein angemessenes Schutzniveau für alle Informationen und informationsverarbeitenden Systeme und Anwendungen sichergestellt werden, um einen reibungslosen Ablauf des Hochschulbetriebes sicherzustellen.

## § 2 Regulatorische Grundlagen

Mit dem Zweck die IT- und Informationssicherheit an Hochschulen, vor allem im Rahmen der weiterhin zu nehmenden Digitalisierung von Hochschulprozessen, zu erhöhen, wurden zwischen den Universtäten und Hochschulen für angewandte Wissenschaften in Trägerschaft des Landes Nordrhein-Westfalen und dem Ministerium für Kultur und Wissenschaften des Landes Nordrhein-Westfalen folgende Vereinbarungen getroffen:

- Vereinbarung zur Cybersicherheit an den Hochschulen (VzC)
- Vereinbarung zur Informationssicherheit an den Hochschulen (VzI)

Neben der verpflichtenden Umsetzung weiterer organisatorischer und technischer Anforderungen hat sich die Fachhochschule Dortmund entschieden, ein ISMS aufzubauen, zu betreiben, zu überwachen und kontinuierlich zu verbessern (PDCA-Zyklus). Dieses Informationssicherheitsmanagementsystem (ISMS) richtet sich nach dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und nutzt relevante Vorgaben des IT-Grundschutzprofils für Hochschulen der Zentren für Kommunikation und Informationsvereinbarung e.V. (ZKI).

## § 3 ISMS der Fachhochschule Dortmund

Im Rahmen des ISMS wurden konzeptionelle Vorgaben erarbeitet und organisatorische Rahmenbedingungen geschaffen, um den ordnungsgemäßen und sicheren Umgang mit Informationen innerhalb aller relevanten hochschulinternen Prozesse und Fachaufgaben zu ermöglichen. Das oberste Ziel ist dabei die Gewährleistung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit der institutionskritischen Informationswerte (Assets).

a) Verfügbarkeit / Zugänglichkeit

Informationen und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit von jedem Arbeitsplatz bei Bedarf verfügbar sein. Voraussetzung für die Aufrechterhaltung der Informationsverfügbarkeit ist die Sicherung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle / Manipulation. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Informationen zu garantieren. Zudem müssen Informationen regelmäßig gesichert werden.

b) Integrität

Informationen und Anwendungen dürfen nicht unberechtigt manipuliert oder gelöscht werden. Um die Integrität der Informationen und Anwendungen zu gewährleisten, sind Maßnahmen, wie ein Anti-Viren- und ein Advanced-Persistent-Threats (APT)-Scanner-Programm etabliert worden, die Datenänderungen erkennen oder gänzlich verhindern.

c) Vertraulichkeit

Informationen und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt der einsetzenden Stelle. Wegen der Gestaltung und der Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist die bzw. der behördliche Datenschutzbeauftragte rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der entsprechenden Verfahren.

## § 4 Informationssicherheitspolitik

Zur Erfüllung dieses obersten Ziels gem. § 3 wurden folgende Grundsatzaussagen getroffen:

- Das Rektorat tritt als Sponsor der Informationssicherheit auf, verantwortet die Informationssicherheitsleitlinie und nimmt seine Vorbildfunktion wahr.
- Die Gesamtverantwortung verbleibt beim Rektorat. Es wurden Rollen und Verantwortlichkeiten der Informationssicherheit definiert, die mit der Umsetzung der Ziele betraut sind. Die Verantwortung und konkreten Maßnahmen in der Planung und Umsetzung der Informationssicherheit liegt neben dem Rektorat je nach Geltungsbereich auch in der Verantwortung der Fachbereiche und dem Senat, die dezentral abgestimmt werden müssen.

- Bildungs- und Awareness-Maßnahmen für Mitarbeitende werden kontinuierlich durchgeführt. Informationssicherheit ist eine Gemeinschaftsaufgabe aller Mitarbeitenden. Sie kann nur erfolgreich umgesetzt werden, wenn die Nutzerinnen bzw. Nutzer für Belange der Informationssicherheit sensibilisiert und über das Gefährdungspotential und mögliche Gegenmaßnahmen in ihrem Arbeitsumfeld informiert werden.
- Informationssicherheit ist kein Selbstzweck. Sie muss daher stets die Verhältnismäßigkeit der Maßnahmen und Mittel im Spannungsfeld zwischen Informationsoffenheit, Kosten und Nutzerakzeptanz auf der einen und dem notwendigen Grad von Informationssicherheit auf der anderen Seite berücksichtigen.
- Mögliche Risiken, potenzielle und festgestellte Schwachstellen, Abweichungen von internen / externen Regelungen, Sicherheitsvorfälle und anderweitige Nichtkonformitäten werden identifiziert, bewertet und bei Bedarf mithilfe von geeigneten (Korrektur-)Maßnahmen behandelt, sodass ein für die Fachhochschule Dortmund akzeptables Risikoniveau gewährleistet werden kann.
- Zur Kontrolle der Wirksamkeit, Aktualität und Angemessenheit des ISMS werden die Erreichung der definierten Informationssicherheitsziele sowie die Einhaltung der etablierten Vorgaben und Prozesse kontinuierlich überwacht und bewertet, die Effektivität und Angemessenheit mithilfe von internen Audits und anderen Prüfungen sichergestellt.
- Zur Sicherstellung der Informationssicherheit werden auch relevante Partner und Leistungserbringer/Dienstleister auf die Einhaltung geeigneter Maßnahmen verpflichtet.

## § 5 Informationssicherheitsziele

(1) Funktionale Aufgabenerledigung: Die IT-Komponenten müssen so betrieben werden, dass Informationen hinreichend schnell verfügbar sind. Ausfälle, die zu Unterbrechungen von kritischen Hochschulprozessen von mehr als 48 Stunden (Servicetage / Arbeitstage der Hochschule / Werktage) führen, sind nicht tolerierbar.

(2) Vermeidung materieller Schäden: Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Informationen, die Veränderung dieser oder den Ausfall einer IT-Anwendung oder eines IT-Systems entstehen.

(3) Wahrung von Persönlichkeitsrechten und Hochschulgeheimnissen: Vertraulichkeit und Integrität der für die Hochschule wichtigen Informationen sind zu schützen, unabhängig davon, in welcher Form sie vorliegen. Auch im Umgang mit

elektronischen und nicht-elektronischen Dokumenten und Informationen ist daher den Anweisungen zur Vertraulichkeit strikt Folge zu leisten.

(4) Vermeidung von Ansehensverlust bzw. Imageschaden: ein negatives Image für die Hochschule muss verhindert werden, da auch hier finanzielle Schäden drohen können.

(5) Kontinuierliche Verbesserung: Das ISMS der Fachhochschule Dortmund mit seinen Richtlinien, Maßnahmen, Prozessen, Verfahren und Anwenderregelungen zur Informationssicherheit werden kontinuierlich aufgestellt bzw. weiterentwickelt und den betreffenden Mitarbeitenden zur Verfügung gestellt, um Risiken zu vermeiden bzw. diese adäquat zu behandeln.

## § 6 Rollen und Verantwortlichkeiten

Das Rektorat ist sich seiner Verantwortung in Bezug auf die Informationssicherheit und die Informationssicherheitsziele bewusst. Aus diesem Grund steht es in vollem Umfang hinter der vorliegenden Leitlinie. Es wird des Weiteren die Maßnahmen, die zum Erreichen der Informationssicherheitsziele notwendig sind, aktiv und dauerhaft unterstützen. Dazu gehört insbesondere auch das Bereitstellen der notwendigen personellen und finanziellen Ressourcen sowie die Aufrechterhaltung und kontinuierliche Verbesserung des ISMS.

Die Hochschul-IT ist verantwortlich für die Weiterentwicklung und Umsetzung der zentralen Informationssicherheitsbelange gemäß den Vereinbarungen zur Informationssicherheit und Cybersicherheit sowie den Betrieb des ISMS und wirkt somit in die gesamte Hochschule hinein (inkl. Umsetzung der Leitlinie, Erstellung der Informationssicherheitskonzepte sowie allgemeiner und zielgruppengerechter Sicherheitsrichtlinien). Dezentral besteht darüber hinaus die Verantwortung, Informationssicherheit im Sinne dieser Leitlinie mitzudenken und den Informationssicherheitsbeauftragten sowie das Team IT-Sicherheit der Hochschul-IT (Dez. VI Abt. 1 SG2) proaktiv einzubinden. So wird sichergestellt, dass die Informationssicherheit in allen Organisationseinheiten und Prozessen integriert wird und bei allen größeren Projekten sowie bei der Einführung neuer Anwendungen und IT-Systeme frühzeitig beteiligt wird.

Alle Mitarbeitenden der Fachhochschule Dortmund sind verpflichtet, die allgemeinen sowie die für seinen Wirkbereich spezifischen Informationssicherheitsvorgaben zu beachten und einzuhalten sowie Informationssicherheitsvorfälle unverzüglich zu melden. Dafür werden die Mitarbeitenden in den Sicherheitsprozess integriert, indem sie kontinuierliche zu den relevanten Gefährdungen, die ihren Arbeitsplatz betreffen, sensibilisiert werden, bzw. in die Lage versetzt werden, Sicherheitsmaßnahmen und organisatorische

Regelungen aktiv mitzugestalten und zu relevanten Sicherheitsrichtlinien und -werkzeugen informiert werden. Dies findet im Einklang mit der gültigen IT-Benutzungsordnung der Fachhochschule Dortmund statt.

## § 7 Folgen bei Nichteinhaltung

Werden Vorgaben nicht umgesetzt, kann dies an die/ den direkten Vorgesetzten und ggf. an Rektor/-in und/ oder Kanzler/-in mitgeteilt werden. Diese können Weisungen erteilen.

Ausgefertigt aufgrund des Beschlusses des Rektorats der Fachhochschule Dortmund vom 18.09.2024.

Dortmund, den 18.09.2024
Die Rektorin

Prof. Dr. Tamara Appel