Universität Münster

Informations-sicherheitsleitlinie

Version: 2.0.0

02.08.2023

Inhalt

Zielsetzung

In dieser Informationssicherheitsleitlinie (ISL) werden die grundsätzlichen Aspekte der Informationssicherheit an der Universität Münster geregelt. Die ISL zeigt auf, wie Informationssicherheit verstanden wird und welche Bedeutung sie für die Universität hat. Sie beschreibt das angestrebte Sicherheitsniveau, die angestrebten Sicherheitsziele und die verfolgte Informationssicherheitsstrategie.

§ 1 Geltungsbereich

Die Informationssicherheitsleitlinie gilt für alle Organisationseinheiten, Mitglieder und Angehörige der Universität Münster.

§ 2 Stellenwert der Informationssicherheit

Informationen in analoger und digitaler Form bilden die Grundlage der Aufgabenerfüllung der Universität in Forschung und Lehre. Die Sicherheit dieser Informationen ist essentiell für den produktiven und störungsfreien Universitätsbetrieb sowie zur Vermeidung von wirtschaftlichen Schäden durch ungewollten Informationsabfluss.

Die meisten Prozesse an der Universität werden maßgeblich durch IT unterstützt. Vernetzte IT-Systeme sind angreifbar und können sowohl von innen, als auch von außen kompromittiert werden. Die **IT-Sicherheit** ist daher ein wesentlicher Teilbereich von Informationssicherheit.

Der **Datenschutz**, also der Schutz personenbezogener Daten, ist ein weiterer, wesentlicher Bereich der Informationssicherheit (siehe hierzu *Datenschutzkonzept der Universität Münster* in der jeweils aktuellen Fassung).

Die Informationssicherheit dient insbesondere der Prävention und Abmilderung von Sicherheitsvorfällen, also Ereignissen mit negativen Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Kommt es zu einem Sicherheitsvorfall:

- verursacht die Beseitigung von Schäden Kosten,
- können die Prozesse der Universität gefährdet werden,
- kann gegen geltendes Recht und gegen Verträge verstoßen werden,
- kann das Ansehen der Universität oder von Personen geschädigt werden,
- kann Leib und Leben von Personen gefährdet werden.

Die Universitätsleitung betrachtet die Informationssicherheit als einen wichtigen Faktor für die Aufrechterhaltung des Universitätsbetriebs. Sie stellt daher sicher, dass Informationssicherheit angemessen behandelt wird und bekennt sich zu ihrer Verantwortung für die kontinuierliche Überwachung und Weiterentwicklung von Informationssicherheitsstrategie, -niveau und -maßnahmen.

§ 3 Verantwortlichkeiten

Es gilt die *Ordnung für die IT-Governance an der Universität Münster*, die u. a. die Rechtsstellung und Aufgaben von CIO und CISO sowie der Gremien IT-Kommission, Kommission Informationssicherheit und IV-Leitungsrunde definiert.

1. Das **Rektorat** trägt die Gesamtverantwortung für die Informationssicherheit. Das Rektorat ist verantwortlich für die Übernahme des Gesamtrisikos, für die Bestimmung des Stellenwertes der Informationssicherheit, für ihre Integration in die Geschäftsprozesse und für die Bereitstellung angemessener Ressourcen.
2. Die*der **Chief Information Officer (CIO)** ist für die IT-strategischen Ziele und Umsetzungskonzepte verantwortlich und berät das Rektorat bezüglich Informationstechnik und Digitalisierung.
3. Die*der **Chief Information Security Officer (CISO)** entspricht der Rolle eines Informationssicherheitsbeauftragten (ISB) gemäß dem BSI IT-Grundschutz. Die*der CISO berät das Rektorat bei seiner Aufgabenwahrnehmung bezüglich der Informationssicherheit und unterstützt es bei der Umsetzung. Sie*Er ist für die Koordination übergreifender Informationssicherheitsprozesse verantwortlich.
4. Die*der **behördliche Datenschutzbeauftragte (DSB)** berät die Leitung, Mitarbeitende und Studierende der Universität im Hinblick auf ihre Pflichten bzw. Rechte nach der Datenschutz-Grundverordnung (DSGVO) sowie sonstiger datenschutzrechtlicher Vorschriften. Die*der DSB überwacht die Einhaltung datenschutzrechtlicher Vorschriften und ist Ansprechpartner*in für die Aufsichtsbehörde.
5. Die **Leitungen der WWU IT und der IV-Versorgungseinheiten (IVVen)** sind für den sicheren Betrieb der zentralen bzw. dezentralen IT und insbesondere die Umsetzung geeigneter technischer Sicherheitsmechanismen und -maßnahmen verantwortlich.
6. Die **Leitungen der einzelnen Organisationseinheiten** (Fachbereiche, zentrale Verwaltung, Betriebseinheiten und sonstige Einrichtungen) haben die Organisations-, Kontroll- und Umsetzungsverantwortung für die Informationssicherheit im jeweiligen Bereich. Dazu zählt u. a. die Umsetzung der festgelegten Informationssicherheitsprozesse und -richtlinien. Sie können dazugehörige Aufgaben an dezentrale Informationssicherheitsbeauftragte, die sogenannten **IV-Sicherheitsbeauftragten** (IV-SB) delegieren, wobei die Verantwortung weiterhin bei der Leitung liegt. Die Leitungen bzw. die IV-SB sind die Kontaktpersonen für die*den CISO und dafür verantwortlich, sie*ihn frühzeitig über die geplante Einführung sicherheitsrelevanter Projekte und Prozesse zu informieren.
7. Die **Leitung des Computer Emergency Response Teams (CERT)** ist für die universitätsweite Detektion, Koordination, Dokumentation und Auswertung sicherheitsrelevanter Informationen, Meldungen und Vorfälle verantwortlich, die in den kontinuierlichen Verbesserungsprozess des Informationssicherheitsmanagements einfließen.
8. **Alle Mitglieder und Angehörigen der Universität Münster** sind dafür verantwortlich, bestimmungsgemäß und sachgerecht mit Informationen umzugehen. Sie sind dazu verpflichtet, sich regelmäßig über die Richtlinien und die aktuellen Empfehlungen zur Informationssicherheit zu informieren und erforderliche Sicherheitsmaßnahmen zu ergreifen.
9. Jede **Führungskraft** ist verpflichtet, die ihr zugeordneten Personen sowohl bei der Einstellung als auch laufend für Informationssicherheit zu sensibilisieren und deren Teilnahme an verpflichtenden Schulungen sicherzustellen.

§ 4 Sicherheitsziele

Das Rektorat der Universität Münster legt die folgenden Ziele für die Informationssicherheit fest:

1. Die **Vertraulichkeit** von Informationen ist stets sichergestellt. Sie stehen ausschließlich dem berechtigten Personenkreis im Rahmen der vorgesehenen Nutzung zur Verfügung und werden vor unberechtigtem Zugriff geschützt.
2. Die **Integrität**, also die physische und logische Unversehrtheit von Systemen, Anwendungen und Informationen, ist stets sichergestellt.
3. Die **Verfügbarkeit** ist stets sichergestellt. Das heißt Dienstleistungen, Netze, Systeme, Anwendungen und Informationen stehen dem berechtigten Personenkreis in den definierten Zeiträumen zur Nutzung bereit.
4. Gesetzliche Vorschriften, sonstige rechtliche Bestimmungen und Verträge werden eingehalten, insbesondere diejenigen zur Wahrung von Dienst- und Amtsgeheimnissen sowie von Persönlichkeitsrechten.
5. Die Mitglieder und Angehörigen der Universität Münster sind für den sicheren und verantwortungsvollen Umgang mit Informationen und IT sensibilisiert. Regelmäßige, zielgruppenorientierte Schulungs- und Sensibilisierungsmaßnahmen sind Bestandteil des Informationssicherheitsprozesses.
6. Die Sicherheitsmaßnahmen werden im Rahmen eines kontinuierlichen Verbesserungsprozesses regelmäßig überprüft und entsprechend aktualisiert, um ein angemessenes Sicherheitsniveau aufrecht zu erhalten. Die Informationssicherheitsmaßnahmen werden in Form von Sicherheitskonzepten nach der IT-Grundschutz Methodik dokumentiert.
7. Das Management von Risiken in Bezug auf die Informationssicherheit ist in das zentrale Risikomanagement der Universität Münster eingebettet. Sicherheitsmaßnahmen werden daher in Hinblick auf ihre Wirksamkeit und das zu tragende Restrisiko sowie die wirtschaftliche Angemessenheit bewertet. Informationssicherheitsrisiken werden analysiert und gesteuert.
8. IT-Verfahren werden einer geordneten Vorgehensweise entsprechend in Betrieb genommen und geändert, wobei die Informationssicherheit angemessen berücksichtigt wird.
9. Verträge mit Externen, z. B. Dienstleistern oder angegliederten Einrichtungen, werden so gestaltet, dass die Einhaltung der Informationssicherheit sowie der datenschutzrechtlichen Vorschriften gewährleistet ist.
10. Ein Notfallmanagement ist etabliert und ermöglicht es der Universität, die negativen Auswirkungen von Notfällen anhand von Plänen zur Behandlung von Notfallszenarien zu minimieren und den Betrieb betroffener Bereiche schnell wieder aufzunehmen. Geplante Notfallmaßnahmen werden in regelmäßigen Notfallübungen überprüft.

§ 5 Sicherheitsstrategie

Die Sicherheitsstrategie der Universität Münster hat zum Ziel, mit verhältnismäßigem Ressourceneinsatz im Hinblick auf den Wert der zu schützenden Informationen ein möglichst hohes Maß an Sicherheit zu erreichen und verbleibende Restrisiken sowie deren Auswirkungen im Schadensfall zu minimieren.

Die Universität Münster orientiert sich bei der Gestaltung der Informationssicherheit an der **IT-Grundschutz-Methodik** des Bundesamts für Sicherheit in der Informationstechnik (BSI). Basierend auf dem IT-Grundschutz wird ein **Informationssicherheitsmanagementsystem (ISMS)** implementiert. Das ISMS steht für die Gesamtheit der Regelungen, Instrumente und Maßnahmen, die der Universität Münster zur Erreichung der Informationssicherheitsziele und der Lenkung der auf Informationssicherheit ausgerichteten Aufgaben dienen. Es stellt die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen sicher, die im Rahmen der universitären Geschäftsprozesse verarbeitet werden und dient insbesondere dem Schutz vor Sicherheitsvorfällen.

Entsprechend der *Vereinbarung zur Informationssicherheit an den Hochschulen* mit dem Ministerium für Kultur und Wissenschaft des Landes verpflichtet sich die Universität Münster, das *IT-Grundschutz-Profil für Hochschulen* des Vereins "Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V." (ZKI e.V.) stufenweise umzusetzen. Die Universität strebt dabei das Schutzniveau der **Basisabsicherung** nach der IT-Grundschutz Methodik an. Für die Verwaltungs-IT sowie für bestimmte Informationen, Prozesse und IT-Systeme mit hohem Schutzbedarf wird mindestens das Schutzniveau der **Standardabsicherung** angestrebt.

Die Geschäftsprozesse werden schrittweise in das ISMS aufgenommen. Als vollständig in das ISMS aufgenommen gelten solche Informationsverbünde, für die ein Sicherheitskonzept gemäß IT-Grundschutz vorliegt. Zukünftig wird Informationssicherheit in alle Geschäftsprozesse integriert.

Um das definierte Sicherheitsniveau aufrecht zu erhalten, müssen implementierte Sicherheitsmaßnahmen, Dokumente zur Informationssicherheit und Informationssicherheitsprozesse fortlaufend kontrolliert und verbessert werden. Die*der CISO überwacht die Informationssicherheit und berichtet dem Rektorat mindestens zweimal im Jahr über den Umsetzungsstand und Erfolg des Informationssicherheitsmanagementsystems sowie die Gefährdungslage und legt ggfs. Verbesserungsstrategien zur Beschlussfassung vor. Das Rektorat nutzt die Berichte, um einen kontinuierlichen Verbesserungsprozess (KVP) für das ISMS und die Informationssicherheit zu gewährleisten. Die *Richtlinie zum ISMS* beschreibt, wie die Universität diesen KVP sicherstellt.

§ 6 Sicherheitsmaßnahmen

Das Informationssicherheitsmanagement umfasst Regelungen und Maßnahmen technischer, organisatorischer, personeller sowie infrastruktureller Art. Sicherheitsmaßnahmen dienen der Umsetzung sicherheitsrelevanter Richtlinien sowie der Etablierung von Normen, Standards und dem aktuellen Stand der Technik. Sicherheitsmaßnahmen müssen angemessen sein und die Aufgaben der Universität berücksichtigen. Der (finanzielle) Aufwand muss in einem angemessenen Verhältnis zu dem Wert der zu schützenden Informationen, IT-Systeme und Prozesse stehen.

Im Einzelfall können Sicherheitsmaßnahmen eine Einschränkung von Funktionalität und Bedienbarkeit bedeuten, wodurch zwischen verschiedenen Interessen abgewogen werden muss. Alle Personen, die die Infrastruktur der Universität betreiben oder nutzen, müssen daher Kompromisse akzeptieren, eingehen und mittragen.

Ausnahmen von verbindlichen Richtlinien bedürfen der Genehmigung der*des CISO. Die Genehmigung erfolgt auf Basis einer Risikobetrachtung, die durch beantragende Personen mit dem Antrag und einer Beschreibung des Sachverhalts vorgelegt werden muss. Der*Die CISO stimmt sich

vor der Genehmigung von Ausnahmen, die ein Risiko der Klassen A und B gemäß Risikohandbuch der Universität verursachen würden, mit dem Risikomanagement der Universität ab. Ausnahmen, die ein Risiko der Klasse C verursachen, werden jährlich ans Risikomanagement berichtet. Ausnahmen müssen durch die beantragende Person einer jährlichen Überprüfung unterzogen werden. Das Ergebnis ist dem*der CISO zur Genehmigung einer Verlängerung der Ausnahme vorzulegen.

Sicherheitsmaßnahmen müssen im Rahmen eines kontinuierlichen Prozesses formuliert, kommuniziert, realisiert, überwacht und fortentwickelt werden.

§ 7 Verstöße und Gefahrenintervention

Verstöße gegen die Informationssicherheit können erhebliche Schäden zur Folge haben. Darunter werden u. a. folgende Handlungen durch interne oder externe Personen verstanden:

- Verstöße gegen verpflichtende Sicherheitsrichtlinien,
- die Planung, Beauftragung oder Durchführung von Aktivitäten, die erwartbar zu einer Kompromittierung von Informationen, Daten, IT-Systemen oder Anwendungen führen oder führen können,
- der unberechtigte Zugriff auf oder die nicht bestimmungsgemäße Verwendung von Informationen und IT-Systeme,
- sowie die unberechtigte Änderung, Nutzung oder Weitergabe von schutzbedürftigen Informationen.

Akute Sicherheitsvorfälle müssen an das CERT gemeldet werden, um eine zügige Behandlung zu gewährleisten. Generelle Hinweise auf Verstöße gegen die Informationssicherheit können über die zuständige Führungskraft oder direkt an den*die CISO gemeldet werden. Bei wesentlichen Verstößen oder Sorge vor persönlichen Nachteilen können Meldende sich alternativ, wahlweise vollständig anonym, an das Compliance Office als zentrale interne Meldestelle wenden. Entsprechend Ihrer Zuständigkeiten informieren sich CISO und Compliance Office über Hinweise und festgestelltes Fehlverhalten.

Vorsätzliche und grob fahrlässige Verstöße können arbeitsrechtliche, zivilrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben. Weiterhin können Einschränkungen (z. B. von Zugriffs-, Zugangs- oder Nutzungsrechten) bei schwerwiegenden Verstößen oder Gefahr im Verzug durch die Leitungen der betroffenen Organisationseinheiten oder das CERT veranlasst werden.[1] Die Entscheidung über dauerhafte Einschränkungen trifft die Kanzlerin bzw. der Kanzler auf Antrag der*des CISO. Einschränkungen sind ausschließlich in Absprache mit der*dem CISO aufzuheben.

Nutzer*innen können zudem gemäß der *IT-Benutzungsordnung*[2] vorübergehend oder dauerhaft in der Benutzung der zentralen IT-Infrastrukturen und Dienste beschränkt oder hiervon ausgeschlossen werden.

[1] Für die IT-Infrastruktur und Dienste sind die Details in der *IT-Benutzungsordnung*[3] geregelt
[2] https://www.uni-muenster.de/IT/wwu-it/ordnungen/benutzungsordnung.html

§ 8 Inkraftsetzung

Die Richtlinie tritt am Tage nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Universität Münster in Kraft.

Änderungshistorie

Version	Datum	Änderungen gegenüber der vorherigen Version	Ersteller/in
2.0.0	02.08.2023	Anpassung an die „Ordnung für die IT-Governance an der Universität Münster“, Vollständige Überarbeitung und Kürzung, Anpassung an das neue Design	Ludger Becker (CISO)
1.4.2	03.02.2021	Anpassung an Feedback aus IV-K-Sitzung	Thorsten Küfer
1.4.1	01.02.2021	Anpassung an Feedback aus IV-L und IVV-Leiter-Sitzung, Schaffung von Bereichs-Sicherheitsbeauftragten	Thorsten Küfer
1.4	16.11.2020	Anpassungen an IT-Grundschutz, neues CISO-Statut	Thorsten Küfer
1.3	10.03.2020	Fusion WWU IT (ZIV und Stabsstelle IT) (unveröffentlicht)	Thorsten Küfer
1.2	01.06.2019	Ergänzung Datenschutz (unveröffentlicht)	Thorsten Küfer
1.1	30.10.2017	Überarbeitung für neue CIO-Ordnung und UKM-Trennung (unveröffentlicht)	Thorsten Küfer
1.0	28.04.2016	Erste Version v1.0 (Beschluss des Rektorats vom 07.07.2016, veröffentlicht am 18.10.2016)	Thorsten Küfer

---

Ausgefertigt aufgrund des Beschlusses des Rektorats der Universität Münster vom 21.09.2023. Die vorstehende Ordnung wird hiermit verkündet.

Es wird darauf hingewiesen, dass gemäß § 12 Abs. 5 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG NRW) eine Verletzung von Verfahrens- oder Formvorschriften des Ordnungs- oder des sonstigen autonomen Rechts der Hochschule nach Ablauf eines Jahres seit dieser Bekanntmachung nicht mehr geltend gemacht werden kann, es sei denn

1. die Ordnung ist nicht ordnungsgemäß bekannt gemacht worden,
2. das Rektorat 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.

Münster, den 06.10.2023

Der Rektor

Prof. Dr. Johannes W e s s e l s