Universität Münster

AMTLICHE BEKANNTMACHUNGEN

Jahrgang 2023 | Ausgegeben zu Münster am 10. Oktober 2023 | Nr. 34

Inhalt Seite

Herausgegeben vom
Rektor der Universität Münster
Schlossplatz 2, 48149 Münster
AB Uni 2023/34
http://www.uni-muenster.de/Rektorat/abuni/index.html

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

2409

Universität Münster

Richtlinie zum Informationssicherheits-managementsystem (ISMS)

Version: 1.0.0

03.08.2023

wissen.leben

Inhalt

Zielsetzung

Die Universität Münster betreibt ein Informationssicherheitsmanagementsystem (ISMS), das auf dem IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) basiert. Das ISMS bezeichnet die Gesamtheit der Regelungen, Instrumente und Maßnahmen, die der Universität zur Erreichung der in der Informationssicherheitsleitlinie (ISL) definierten Informationssicherheitszielen und der Lenkung der auf Informationssicherheit ausgerichteten Aufgaben dienen.

Informationssicherheit wird in sämtliche Geschäftsprozesse integriert, indem das Informationssicherheitsmanagement frühzeitig bei der Neueinführung und bei wesentlichen Änderungen von Organisationsstrukturen, Geschäftsprozessen sowie IT-Projekten und IT-Systemen eingebunden wird und auch bereits bestehende Strukturen, Prozesse, Projekte und Systeme an der Universität sukzessive in den Blick nimmt und analysiert. Auf diesem Weg werden alle Geschäftsprozesse schrittweise in das ISMS aufgenommen. Als vollständig in das ISMS aufgenommen gelten solche Informationsverbünde, für die ein Sicherheitskonzept gemäß IT-Grundschutz vorliegt und im Rahmen eines PDCA-Zyklus (Plan, Do, Check, Act) kontinuierlich verbessert wird. Diese Richtlinie ergänzt und präzisiert die ISL der Universität Münster, indem sie den Aufbau des ISMS und den PDCA-Zyklus festlegt.

§ 1 Geltungsbereich

Die Richtlinie für das ISMS hat den Geltungsbereich der ISL.

§ 2 Organisationsstruktur für Informationssicherheit

Die Organisationsstruktur für das ISMS an der Universität Münster besteht aus:

- dem Rektorat (CEO),
- der*dem Chief Information Officer (CIO),
- der*dem Chief Information Security Officer (CISO),
- der*dem Datenschutzbeauftragten (DSB),
- der IT-Kommission,
- der Kommission Informationssicherheit,
- den IT-Betreibenden,
- der IV-Leitungsrunde,
- den Leitungen von Organisationseinheiten bzw. den IV-Sicherheitsbeauftragten,
- dem Computer Emergency Response Team (CERT).

Die Abbildung 1 verdeutlicht die IT-Governance-Struktur der Universität Münster, die auch für den Bereich Informationssicherheit zuständig ist.

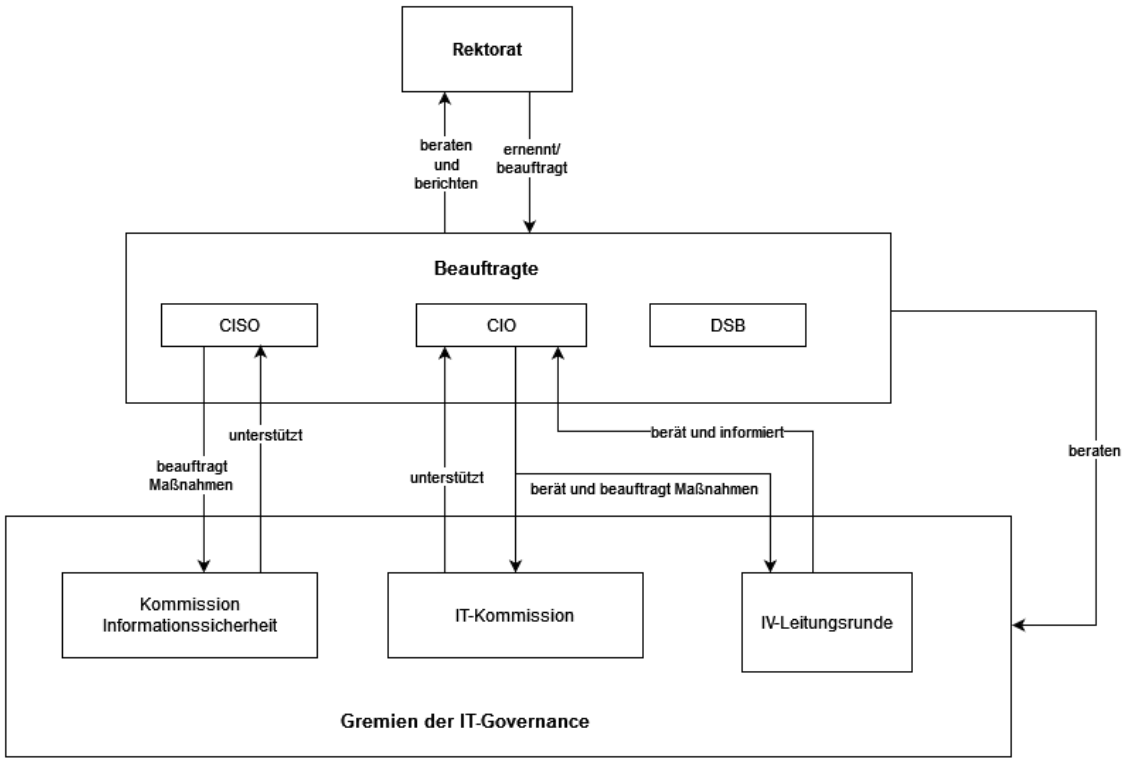

Abbildung 1: IT- Governance der Universität Münster.

Rektorat

Das Rektorat[1] leitet die Universität und ist gleichbedeutend mit dem CEO. Ihm obliegen alle Entscheidungen, für die in der Verfassung der Universität nicht ausdrücklich andere Zuständigkeiten festgelegt sind. Das Rektorat der Universität Münster trägt die Gesamtverantwortung für die Informationssicherheit und 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.

Das Rektorat beschließt die ISL sowie alle weiteren Richtlinien zur Informationssicherheit und legt an der Universität Münster dadurch die verbindlichen Rahmenbedingungen für Informationssicherheit fest.

Chief Information Officer

Die*Der Chief Information Officer (CIO)[2] ist ein*e Beauftragte*r des Rektorats und steht diesem bei IT-Angelegenheiten beratend zur Seite. Sie*Er stellt die*den Gesamtkoordinator*in der IT-Struktur der Universität Münster dar und ist daher dafür verantwortlich, die allgemeine IT-Strategie der Universität Münster, unter Beratung mit der IT-Kommission, kontinuierlich zu entwickeln. Hierfür untersucht sie*er die bisher durchgeführten Maßnahmen und existierenden IT-Strukturen und schlägt nach Beratung mit der IT-Kommission dem Rektorat angemessene Anpassungen vor.

[1] https://www.uni-muenster.de/Rektorat/
[2] https://www.uni-muenster.de/Rektorat/cio.html

Darüber hinaus berichtet sie*er dem Rektorat über ihre*seine Tätigkeit sowie über Empfehlungen und Vorlagen der IT-Kommission. Die*Der CIO informiert und beauftragt die IV-Leitungsrunde mit der Umsetzung von Maßnahmen, die sich aus den Entscheidungen der*des CIO und des Rektorats ergeben.

Chief Information Security Officer

Die*Der Chief Information Security Officer (CISO)[3] ist ein*e Beauftragte*r des Rektorats. Die CISO-Funktion ist an der Universität Münster gleichbedeutend mit der Funktion einer*eines Informationssicherheitsbeauftragten (ISB) nach BSI IT-Grundschutz. Die Hauptaufgabe der*des CISO besteht darin, die Leitung der Universität Münster bei deren Aufgabenwahrnehmung bezüglich der Informationssicherheit zu beraten und diese bei der Umsetzung zu unterstützen.

Die*Der CISO leitet die Stabsstelle des Rektorats für Informationssicherheit und wird von dieser in der Aufgabenerfüllung unterstützt. Die Stabsstelle Informationssicherheit ist eine Säule der Compliance-Organisation der Universität Münster. Die*Der CISO nimmt ihre*seine Aufgaben selbstständig wahr und ist von anderen Stellen der IT-Governance unabhängig. Sie*Er ist ausschließlich dem Rektorat gegenüber auskunftspflichtig. Zu den Aufgaben der*des CISO gehören u.a.:

- Unterstützung des Rektorats bei der Erstellung der ISL
- Weiterentwicklung des ISMS, d.h. Aufstellung von Verfahren und Regeln innerhalb der Universität Münster, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.
- Erarbeitung und Definition der sicherheitsrelevanten Objekte, der Bedrohungen und Risiken und der daraus abgeleiteten Sicherheitsziele
- Ausarbeitung und laufende Anpassung von Sicherheitsrichtlinien
- Initiierung von Sicherheitsmaßnahmen
- Überwachung der Umsetzung der Sicherheitsstandards, u.a. durch Auditierung der Einrichtungen und IT-Systeme der Universität Münster
- Überwachung der Informationssicherheit und Entwicklung von Verbesserungsstrategien
- Mitwirkung an Projekten mit Auswirkungen auf die Informationssicherheit
- Schaffung eines Bewusstseins für Informationssicherheit an der Universität Münster durch die Initiierung und Durchführung von Sensibilisierungs- und Schulungsangeboten sowie Kampagnen
- Vorsitz in der Kommission Informationssicherheit

Datenschutzbeauftragte*r

Die*Der behördliche Datenschutzbeauftragte (DSB) hat an der Universität Münster die Leitung der Stabsstelle Datenschutz[4] inne. Die*der behördliche DSB ist ein*e Beauftragt*e des Rektorats, unterliegt aber gem. Art. 38 Abs. 3 DSGVO bei der Wahrnehmung ihrer*seiner Aufgaben keinen Weisungen der Hochschulleitung.

Die*Der behördliche DSB hat u.a. folgende Aufgaben:

[3] https://www.uni-muenster.de/Rektorat/ciso.html
[4] https://www.uni-muenster.de/Verwaltung/orga/stabsstelle_datenschutz.html

- Beratung der Hochschulleitung, der Leiter*innen von Organisationseinheiten sowie von Mitarbeiter*innen und Studierenden im Hinblick auf ihre Pflichten bzw. Rechte nach der Datenschutz-Grundverordnung (DSGVO) sowie sonstiger datenschutzrechtlicher Vorschriften
- Überwachung der Einhaltung der DSGVO und sonstiger datenschutzrechtlicher Vorschriften an der Universität Münster
- Ansprechpartner*in für die Aufsichtsbehörde, d.h. für die*den Landesbeauftragte*n für Datenschutz und Informationssicherheit Nordrhein-Westfalen (LDI), in datenschutzrechtlichen Fragen

CIO, CISO und DSB arbeiten eng zusammen und stimmen sich regelmäßig ab.

IT-Kommission

Die IT-Kommission ist dem Senat und dem Rektorat als gemeinsame Kommission zugeordnet und berät die*den CIO. Sie ist für Empfehlungen zur Digitalisierung und IT-Strategie an der Universität Münster zuständig. Sie unterstützt daher die*den CIO in diesem Themenbereich und bringt dabei unterschiedliche Perspektiven zusammen. Die IT-Kommission wird ihrerseits durch drei Arbeitsgruppen zu Forschung und IT, Lehre und IT sowie Verwaltung und IT unterstützt.

Kommission Informationssicherheit

Die Kommission Informationssicherheit entspricht dem IS-Management-Team nach BSI IT-Grundschutz. Sie unterstützt die*den CISO bei der Koordination übergreifender Maßnahmen, der Bündelung von Informationen und der Durchführung von Kontrollaufgaben. Die Kommission Informationssicherheit besteht aus Expert*innen der WWU IT und der IVVen. Die Vertreter*innen der IVVen werden durch die IV-Leitungsrunde gewählt. Zu den Aufgaben der Kommission Informationssicherheit gehören u.a.:

- Bearbeitung von Aufträgen der*des CISO
- Entwicklung der Informationssicherheitsziele und -strategien
- Erarbeitung und universitätsweite Abstimmung wirksamer Sicherheitsstandards und Betriebsregelungen
- Überwachung der Umsetzung und Einhaltung der Sicherheitsstandards
- Austausch bezgl. aktueller sicherheitsrelevanter Entwicklungen und Vorfälle
- Aufstellung und Fortschreibung eines Ausbildungs- und Schulungskonzepts zur Informationssicherheit für Benutzende und Administrierende, das für Informationssicherheit und die Einhaltung der Sicherheitsstandards sensibilisieren soll
- Ansprechpartner für die Leitungen der Organisationseinheiten und IV-Sicherheitsbeauftragten

IT-Betreibende

Die Universität Münster hat ein zweistufiges Modell für die Versorgung mit IT-Dienstleistungen etabliert.

Die WWU IT[5] ist das zentrale Dienstleistungs- und Kompetenzzentrum der Universität Münster für alle Belange der IT-Infrastruktur sowie der Kommunikations- und Medientechnik und der Vermittlung von Medienkompetenz. Es sorgt für eine optimale Unterstützung der verschiedenen Nutzergruppen bei ihren Aufgaben und Zielen, insbesondere in Forschung, Lehre und Studium.

Auf der dezentralen Ebene existieren durch die Fachbereiche und Einrichtungen der Universität eingerichtete IV-Versorgungseinheiten (IVVen)[6]. Die an den IVVen beteiligten Fachbereiche und Einrichtungen bestimmen deren interne Organisationsform und stellen die Finanzierung sicher. Weiterhin betreiben auch Einrichtungen außerhalb der WWU IT und der IVVen IT-Systeme in eigener Verantwortung.

Die Leitungen der Einrichtungen, die IT-Systeme betreiben, sind in Ihrem Bereich im Rahmen ihrer Verantwortung für die Informationssicherheit auch für den ordnungsgemäßen Betrieb der IT-Infrastruktur und die Einhaltung zugehöriger Richtlinien zuständig. Die Leitungen können für einzelne Aufgabenbereiche Verantwortlichkeiten delegieren. Es ist zu regeln, wer für die einzelnen Geschäftsprozesse, Anwendungen, IT-Systeme und Räumlichkeiten in den Organisationseinheiten zuständig ist und die Vorgaben der Richtlinien umsetzt. Bei der Strukturierung der Aufgaben muss sichergestellt werden, dass unvereinbare Aufgaben, wie operative und kontrollierende Funktionen, von unterschiedlichen Personen wahrgenommen werden. Dies ist auch bei den Stellvertreterregelungen entsprechend zu berücksichtigen.

IV-Leitungsrunde

Die IT-Betreibenden insbesondere der Fachbereiche und Einrichtungen der Universität werden über die IV-Leitungsrunde in die IT-Governance integriert. Die IV-Leitungsrunde berät und informiert die*den CIO und die*der CIO kann die IV-Leitungsrunde mit der Umsetzung von Maßnahmen beauftragen.

Leitungen der Organisationseinheiten und IV-Sicherheitsbeauftragte

Die Leitungen der einzelnen Organisationseinheiten innerhalb der Universität Münster nehmen die Organisations-, Kontroll- und Umsetzungsverantwortung für die Informationssicherheit des jeweiligen Bereiches wahr. Leitungspersonen können dazugehörige Aufgaben an dezentrale Informationssicherheitsbeauftragte, die IV-Sicherheitsbeauftragten delegieren, wobei die Verantwortung weiterhin bei der Leitung liegt. Die Organisationseinheiten melden den Namen und die Kontaktdaten von aktuellen IV-Sicherheitsbeauftragten an die*den CISO und informieren sie*ihn entsprechend über Änderungen.

Die Festlegung von Verantwortlichkeiten und die Zuweisung von Zuständigkeiten in der jeweiligen Organisationseinheit muss transparent erfolgen, alle Mitarbeitenden sind geeignet darüber zu informieren.

[5] https://www.uni-muenster.de/IT/
[6] https://www.uni-muenster.de/IVV/

Die Leitungen bzw. die IV-Sicherheitsbeauftragten sind die Kontaktpersonen für die*den CISO und dafür verantwortlich, sie*ihn frühzeitig über die geplante Einführung sicherheitsrelevanter Projekte und Prozesse zu informieren.

Zu der Verantwortung der Leitungspersonen gehört u. a.:

- einen angemessenen Schutz von Informationen sicherzustellen, abhängig von ihrem jeweiligen Schutzbedarf
- die Einhaltung geltender Regelungen zur Informationssicherheit sowie zum Notfall- und Risikomanagement sicherzustellen
- bei der Einführung neuer Prozesse und IT-Systeme die Informationssicherheit und den Datenschutz zu berücksichtigen; vor der Einführung neuer Prozesse sind die*der CISO und die*der DSB unter Verwendung des Formulars zur Einführung neuer Prozesse zu informieren
- als Ansprechpersonen für die*den CISO zu fungieren und bei Bedarf notwendige Informationen zur Informationssicherheit weiterzuleiten
- Informationssicherheit vorzuleben und das Sicherheitsbewusstsein im Bereich zu fördern
- Informationen über Schulungs- und/oder Sensibilisierungsbedarf von Angehörigen des Bereichs zu ermitteln und an die*den CISO weiterzuleiten

Computer Emergency Response Team

Das Computer Emergency Response Team (CERT)[7] der Universität Münster ist die zentrale Koordinationsstelle für IT-Sicherheitsinformationen, -probleme und -vorfälle. Das Ziel des CERT ist der Schutz der Universität, ihrer Angehörigen und ihrer Infrastruktur vor fahrlässiger oder illegaler Nutzung ihrer IP-Adressen und Ressourcen. Das CERT unterstützt die Universitätsangehörigen bei proaktiven Maßnahmen, die das Risiko von IT-Sicherheitsvorfällen reduzieren, sowie bei der Reaktion auf Sicherheitsvorfälle.

Zu den Aufgaben des CERT gehören u. a.:

- Analyse der aktuellen Bedrohungs- und Sicherheitslage
- Aufbereitung von sicherheitsrelevanten Informationen (z. B. in Form von Lageberichten und Handlungsempfehlungen)
- Überprüfung von Hinweisen auf Sicherheitsprobleme und sicherheitsrelevante Ereignisse
- Betrieb und Auswertung von IT-Sicherheitssystemen
- Überprüfung des IT-Sicherheitsniveaus und der Umsetzung von Sicherheitsmaßnahmen (z. B. durch Schwachstellenscans, Sicherheitstests, interne Audits)
- Annahme, Koordination und Dokumentation von sicherheitsrelevanten Meldungen und Vorfällen
- Koordination und Unterstützung bei
    - der Reaktion auf Vorfälle (z. B. bei Cyber-Angriffen, Sicherheitslücken, Schadsoftware, Spam-Versand, Urheberrechtsverletzungen)
    - der Untersuchung von Vorfällen (z. B. IT-Forensik)

[7] https://www.uni-muenster.de/CERT/

    - der Durchführung von Eindämmungsmaßnahmen (z. B. Sperrung von Kennungen oder Systemen)
- Austausch und Kooperation mit nationalen und internationalen Sicherheitsorganisationen (z. B. DFN-CERT)
- Weiterentwicklung des Dokumentationswerkzeugs SecDoc der Universität Münster
- Zusammenarbeit u.a. mit der*dem CISO, der*dem DSB und der Kommission Informationssicherheit

Das CERT der Universität Münster ist in der WWU IT eingerichtet.

Alle Mitglieder und Angehörigen der Universität Münster

Die Mitglieder und Angehörigen müssen sich über die relevanten geltenden Regelungen zur Informationssicherheit informieren und die Umsetzung der zugehörigen Vorgaben sicherstellen. Insbesondere sind die Mitglieder und Angehörigen der Universität Münster dafür verantwortlich, bestimmungsgemäß und sachgerecht mit Informationen umzugehen. Näheres regelt die *Richtlinie zur Klassifizierung von Informationen*.

Bei sicherheitsrelevanten Vorfällen ist stets das CERT der Universität Münster zu informieren. Weitere Informationen dazu finden sich in der *Richtline zur Detektion und Behandlung von Sicherheitsvorfällen*.

§ 3 PDCA-Zyklus für Informationssicherheit

Informationssicherheitsmanagement ist ein kontinuierlicher Prozess, in dem regelmäßig alle Elemente des ISMS und die zu Prozessen sowie zugehörigen Anwendungen und IT-Systemen korrespondierenden Sicherheitskonzepte auf Angemessenheit sowie Wirksamkeit überprüft und aktualisiert werden müssen. Die zugehörigen Teil-Prozesse folgen dem PDCA-Zyklus aus den Phasen ***Plan, Do, Check*** und ***Act***.

Der Umgang mit den verschiedenen Dokumenten des ISMS wie Richtlinien, Konzepten und Betriebsdokumentationen wird in einer gesonderten *Richtlinie zur Lenkung von Dokumenten* beschrieben. Im Rahmen ihrer Berichtspflicht erstellt die Stabsstelle Informationssicherheit einen Jahresbericht, in dem unter anderem die umgesetzten, geplanten und notwendigen Maßnahmen sowie die Zielerreichung thematisiert wird.

Die nachfolgende Tabelle erläutert den PDCA-Zyklus für das ISMS, Prozesse und Sicherheitskonzepte:

Plan			
	ISMS	**Prozesse**	**Sicherheitskonzepte nach IT-Grundschutz**
Definition von Zielen (Soll-Zustand)	• Festlegung von Informationssicherheitszielen der Universität durch das Rektorat in der Informationssicherheitsleitlinie	• Feststellung des Bedarfs für neuen IT-Prozess • Definition des Ziels/Zwecks des Prozesses	• Bestimmung und Abgrenzung eines Informationsverbundes
Analyse von Rahmenbedingungen • Ist-Zustände • Stakeholder • Schutzbedarf von Informationen	• Beschreibung des Ist-Zustands der Informationssicherheit im Jahresbericht • Zielgruppenanalyse für Schulungs- und Awarenessmaßnahmen gemäß *Awareness Konzept*	• Prozessbeschreibung • Identifikation benötigter Anwendungen und IT-Systeme • Feststellung der Arten von verarbeiteten Informationen • Festlegung von Zuständigkeiten	• Strukturanalyse • Ermittlung des Schutzbedarfs gemäß *Richtlinie zur Schutzbedarfsfeststellung* • Dokumentation des Ist-Zustands in SecDoc
Risikomanagement	• Identifizierung von Risiken im Risikobericht der Universität sowie im Jahresbericht • Planung der Risikobehandlung im Jahresbericht	• Identifizieren von Risiken mittels des Formulars zur Etablierung neuer IT-Prozesse • Planung der Risikobehandlung mittels des Formulars	• Identifizieren von Risiken und Risikoanalyse gemäß der *Richtlinie zur Risikoanalyse* • Planung der Risikobehandlung im Realisierungsplan
Anforderungsmanagement	• Betrachtung der Rahmenbedingungen (Gesetze, Standards) der Informationssicherheit im Jahresbericht	• Identifizieren von Anforderungen (Gesetze, Richtlinien, Standards, vertragliche Bestimmungen) • Beteiligung von DSB und CISO mittels des Formulars zur Etablierung neuer IT-Prozesse	• Identifizieren von für den Geltungsbereich relevanten IT-Grundschutz Bausteinen
Umsetzungsplanung	• Planung der Umsetzung im Rahmen des Jahresberichts • Ggf. Überarbeitung von Richtlinien planen	• Planung der Umsetzung der festgelegten Maßnahmen über das Formular zur Etablierung neuer IT-Prozesse	• Planung der Umsetzung im Realisierungsplan

Plan			
	ISMS	**Prozesse**	**Sicherheitskonzepte nach IT-Grundschutz**
	• Ressourcenplanung • Zeitplanung	• Ggf. Überarbeitung des geplanten Prozesses und erneute Einreichung des Formulars	• Festlegung umzusetzender Maßnahmen zur Erreichung des Ziel-/Soll-Zustands • Festlegen von Verantwortlichkeiten • Ressourcenplanung • Zeitplanung
Definition von Leistungsindikatoren	• Festlegung von Messwerten zur Erfolgskontrolle der Zielerreichung im Jahresbericht		• Festlegung von Messwerten zur Erfolgskontrolle der Zielerreichung im Realisierungsplan

Do			
	ISMS	**Prozesse**	**Sicherheitskonzepte nach IT-Grundschutz**
Umsetzung geplanter Maßnahmen durch die Verantwortlichen	• Maßnahmen zur Risikobehandlung • Erhebung von Leistungsindikatoren	• Maßnahmen zur Risikobehandlung • Verträge mit Externen, z. B. Dienstleistern oder angegliederten Einrichtungen	• Maßnahmen zur Risikobehandlung • Erhebung von Leistungsindikatoren
Dokumentation der Umsetzung	• SecDoc und Jahresbericht	• SecDoc und ergänzende Betriebsdokumentation	• SecDoc und ergänzende Betriebsdokumentation
Dokumentation von Erkenntnissen über Verbesserungspotential aus dem laufenden Betrieb („Lessons Learned“)			

Kommunikation und Öffentlichkeitsarbeit	• Durchführung von zentralen Schulungs- und Awarnessmaßnahmen • Stakeholderkommunikation • Gremienarbeit	• Stakeholderkommunikation • Durchführung von für den Prozess nötigen Schulungen	• Stakeholderkommunikation • Durchführung von Projekt-spezifischen Schulungen

Check			
	ISMS	**Prozesse**	**Sicherheitskonzepte nach IT-Grundschutz**

Erfolgskontrolle
• Entsprechend der *Richtlinie zur Überprüfung und Verbesserung der Informationssicherheit*
• Durchführung von:
  ○ Internen und externen Audits
  ○ Technischen Sicherheitstests
  ○ Analysen und Bewertungen detektierter Sicherheitsvorfälle
  ○ Prüfungen von Dokumentationen
  ○ Befragungen
  ○ Analysen und Bewertungen der Hinweise aus dem Hinweisgebersystem
• Soll-Ist-Vergleich anhand von Leistungsindikatoren			

Identifikation von Verbesserungspotential	• Durch den zentralen IT-Grundschutz-Check • Durch regelmäßige Auswertung der Dokumentationen sowie der Leistungsindikatoren	• Durch regelmäßige Auswertung der Dokumentationen	• Durch den dezentralen IT-Grundschutz-Check • Durch regelmäßige Auswertung der Dokumentationen sowie der Leistungsindikatoren

Act			
	ISMS	**Prozesse**	**Sicherheitskonzepte nach IT-Grundschutz**
Analyse von Verbesserungspotential	• Identifizierung von Ursachen für Abweichung vom Soll-Zustand im Jahresbericht • Identifizierung von Handlungsfeldern für die nächste Plan-Phase im Realisierungsplan	• Identifizierung von Prozessänderungen	• Identifizierung von Anpassungen • Anpassung der Anforderungen für den nächsten Durchlauf
Sicherung der Erfahrungen und Erkenntnisse	• Ableitung von Standards für zukünftiges Vorgehen	• Anpassung der Betriebsdokumentation • Ggf. erneute Einreichung des Prozessformulars	• Anpassung des Realisierungsplans und der Betriebsdokumentation
Initiieren von Verbesserungen (Aktualisierung der Umsetzungsplanung durch Neubeginn in der Plan-Phase)			

§ 4 Einführungsphase

Der in § 3 beschriebene PDCA-Zyklus wird für das ISMS, neue Prozesse und Sicherheitskonzepte nach IT-Grundschutz mit Inkraftsetzung dieser Richtlinie etabliert.

Bestehende Prozesse, zugehörige Anwendungen und IT-Systeme werden schrittweise und risikoorientiert in das ISMS überführt. Die IT-Betreibenden bestimmen zu diesem Zweck den Schutzbedarf aller IT-Systeme, über die Services erbracht werden. Die Systeme werden anschließend risikoorientiert betrachtet, beginnend mit den Systemen mit sehr hohem Schutzbedarf. Für diese IT-Systeme werden im Rahmen einer Strukturanalyse u. a. die zugehörigen Prozesse und Anwendungen ermittelt. Anschließend wird für sie ein Sicherheitskonzept erstellt oder sie werden in bestehende Sicherheitskonzepte intergiert, sodass eine Überführung in das ISMS erfolgen kann.

Neue Prozesse werden in das ISMS aufgenommen, indem sie zunächst den PDCA-Zyklus gemäß § 3 durchlaufen. Anschließend wird für sie ein Sicherheitskonzepte erstellt, oder sie werden in bestehende Sicherheitskonzepte intergiert.

Die Infrastruktur wird unter Koordination der Stabsstelle Informationssicherheit durch die zuständigen Stellen der Verwaltung der Universität in das ISMS aufgenommen.

§ 5 Mitgeltende Dokumente

Die vorliegende Richtlinie zum ISMS referenziert andere, ggf. noch nicht verabschiedete bzw. veröffentlichte Richtlinien und Konzepte, die bestimmte Aspekte der Informationssicherheit im Detail regeln und weiter erläutern. Dabei handelt es sich um die folgenden Dokumente:

- Richtlinie zur Klassifizierung von Informationen
- Richtlinie zur Lenkung von Dokumenten
- Richtlinie zur Schutzbedarfsfeststellung
- Richtlinie zur Risikoanalyse
- Richtlinie zur Überprüfung und Verbesserung der Informationssicherheit
- Richtlinie zur Detektion und Behandlung von Sicherheitsvorfällen
- Konzept zur Informationssicherheits-Awareness

§ 6 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
1.0.0	02.06.2023	Erste Version aufgrund der Überarbeitung der ISL	Ludger Becker (CISO)

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