



Richtlinie zum Informationssicherheits- managementsystem (ISMS)

Version: 1.1.0

11.07.2025

Inhalt

Zielsetzung	1
§ 1 Geltungsbereich	1
§ 2 Organisationsstruktur für Informationssicherheit	1
Rektorat	2
Chief Information Officer	2
Chief Information Security Officer	3
Datenschutzbeauftragte*r	3
Compliance Office	4
Risikomanagement	4
IT-Kommission	5
Kommission Informationssicherheit	5
IT-Betreibende	5
IV-Leitungsrunde	6
Leitungen der Organisationseinheiten und IV-Sicherheitsbeauftragte	6
Computer Emergency Response Team	7
Alle Mitglieder und Angehörigen der Universität Münster	8
§ 3 PDCA-Zyklus für Informationssicherheit	8
§ 4 Einführungsphase	13
§ 5 Mitgeltende Dokumente	13
§ 6 Inkraftsetzung	13

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 Informationssicherheitsziele 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),
- dem Compliance Office
- dem Risikomanagement
- 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 Struktur der IT-Governance der Universität Münster, die auch für den Bereich Informationssicherheit zuständig ist.

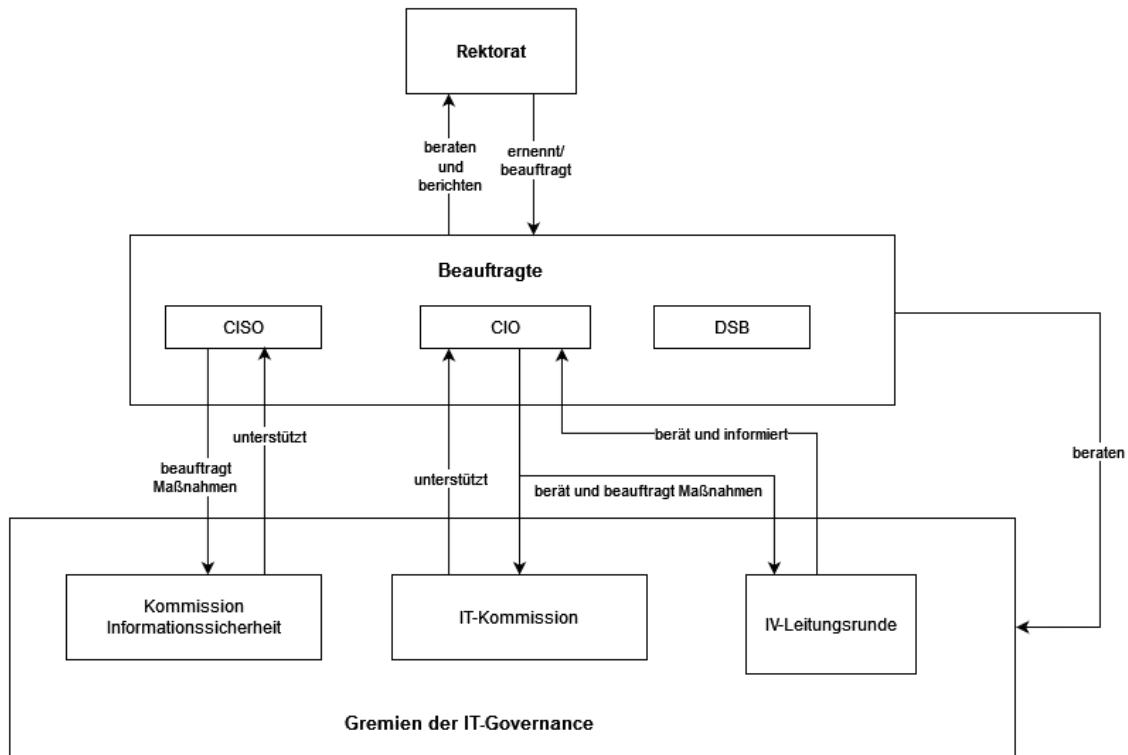


Abbildung 1: IT- Governance der Universität Münster.

Rektorat

Das Rektorat¹ 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. Darüber hinaus berichtet sie*er dem Rektorat über ihre*seine Tätigkeit sowie über

¹ <https://www.uni-muenster.de/Rektorat/>

² <https://www.uni-muenster.de/Rektorat/cio.html>

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*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, Bedrohungen und Risiken und der daraus abgeleiteten Sicherheitsziele
- Ausarbeitung und laufende Anpassung von Sicherheitsrichtlinien
- Überwachung der Umsetzung der Sicherheitsstandards, u.a. durch Auditierung der Einrichtungen und IT-Systeme der Universität Münster
- Überwachung der Informationssicherheit und Entwicklung von Verbesserungsstrategien, Initiierung von Sicherheitsmaßnahmen und regelmäßige Überprüfung auf der Wirksamkeit sowie Angemessenheit dieser Maßnahmen
- 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 Schulungsmaßnahmen und Kampagnen sowie der Bereitstellung von Schulungsangeboten
- Vorsitz in der Kommission Informationssicherheit

Datenschutzbeauftragte*r

Die*Der behördliche Datenschutzbeauftragte (DSB) hat an der Universität Münster die Leitung der Stabsstelle Datenschutz⁴ inne. Die*der behördliche DSB ist ein*e Beauftragte*r 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:

- Beratung der Hochschulleitung, der Leiter*innen von Organisationseinheiten sowie von Mitarbeiter*innen und Studierenden im Hinblick auf ihre Pflichten bzw. Rechte nach der

³ <https://www.uni-muenster.de/Rektorat/ciso.html>

⁴ https://www.uni-muenster.de/Verwaltung/orga/stabsstelle_datenschutz.html

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.

Compliance Office

Das Compliance Office⁵ ist als Stabsstelle des Rektorats die zentrale Koordinationsstelle für das Compliance Management, also die organisatorische und prozessuale Unterstützung zur Einhaltung und Kommunikation der verschiedenen an der Universität Münster zu beachtenden Regeln und Normen. Im Compliance Office werden Orientierungshilfen, Kommunikations- und Schulungsangebote entwickelt, die präventiv zu mehr Compliance und der Stärkung der Compliance Kultur der Universität beitragen. Damit sollen auch Interessenkonflikte und Informationsdefizite abgebaut und die Eigenverantwortung der Mitglieder und Angehörigen gestärkt, deren Handlungssicherheit erhöht und ungewollte Fehler vermieden werden.

Das Compliance Office bildet das Dach zur Vernetzung zahlreicher Compliance-Aktivitäten an der Universität Münster, Die Stabsstelle Informationssicherheit ist eine Säule dieser Compliance-Organisation. Die regelmäßige Abstimmung im Rahmen dieser Organisation wird fallweise u.a. durch die folgenden Maßnahmen ergänzt:

- Richtlinien und begleitende Handreichungen zur Informationssicherheit werden entsprechend vor der Freigabe mit dem Compliance Office abgestimmt.
- Die Kommunikation zu Richtlinien zur Informationssicherheit erfolgt zielgruppenabhängig über die Compliance-Organisation.
- Entsprechend Ihrer Zuständigkeiten informieren sich CISO und Compliance Office über Hinweise auf und festgestelltes Fehlverhalten.
- Die Dokumentation über gesetzliche, vertragliche und sonstige Vorgaben mit Auswirkungen auf die Informationssicherheit wird in der Stabsstelle Informationssicherheit geführt und regelmäßig aktualisiert.

Risikomanagement

Ziel des Risikomanagements der Universität Münster ist primär die Sicherstellung von Funktionsfähigkeit und Ordnungsmäßigkeit. Es ist auf operative, betriebliche Prozesse und Ziele ausgerichtet. In diesem Sinne ist das betriebliche Risikomanagementsystem ein Instrument der verschiedenen Bereiche und der Hochschulleitung, um

- in Entscheidungsprozessen adressatengerechte Informationen kurzfristig und transparent bereitzustellen,
- Gefährdungen frühzeitig zu erkennen,
- eine präventive und aktive Risikosteuerung zu ermöglichen,
- die Erfüllung universitärer Aufgaben unter Beachtung externer Vorgaben sicherzustellen.

⁵ <https://www.uni-muenster.de/Verwaltung/orga/compliance-office.html>

Die Stabsstelle Informationssicherheit und Risikomanagement stimmen sich regelmäßig ab. Die *Richtlinie zur ISMS-Risikoanalyse* beschreibt die Integration der Risikoanalyse nach BSI 200-3 in das Risikomanagement der Universität und regelt die zugehörigen Meldewege.

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 des CIT, der IVVen und des ULB IT-Service. 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.

Das CIT⁶ 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)⁷ und der ULB IT-Service. Die an diesen IT-

⁶ <https://www.uni-muenster.de/IT/>

⁷ <https://www.uni-muenster.de/IVV/>

Betreibenden beteiligten Fachbereiche und Einrichtungen bestimmen auf Basis der Vorgaben des Rektorats deren interne Organisationsform und stellen die Finanzierung sicher. Weiterhin betreiben auch Einrichtungen außerhalb des CIT, der IVVen und des ULB IT-Service IT-Systeme in eigener Verantwortung. Jede Organisationseinheit der Universität Münster wird durch das CIT, eine IVV oder den ULB IT-Service in das ISMS eingebunden.

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.

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)⁸ 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)
 - der Durchführung von Eindämmungsmaßnahmen (z. B. Sperrung von Kennungen oder Systemen)
- Austausch und Kooperation mit nationalen und internationalen Sicherheitsorganisationen (z. B. DFN-CERT)
- Zusammenarbeit u.a. mit der*dem CISO, der*dem DSB und der Kommission Informationssicherheit

Das CERT der Universität Münster ist im CIT eingerichtet.

⁸ <https://www.uni-muenster.de/CERT/>

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 *Richtlinie 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 <i>Awareness Konzept</i>	• Prozessbeschreibung • Identifikation benötigter Anwendungen und IT-Systeme • Feststellung der Arten von verarbeiteten Informationen • Festlegung von Zuständigkeiten	• Strukturanalyse • Ermittlung des Schutzbedarfs gemäß <i>Richtlinie zur Schutzbedarfsfeststellung</i> • Dokumentation des Ist-Zustands im GRC⁹-Tool der Universität Münster
Risikomanagement	• Identifizierung von Risiken im Risikobericht der Universität sowie im Jahresbericht • Planung der Risikosteuerung im Jahresbericht	• Identifizieren von Risiken mittels des Formulars zur Etablierung neuer IT-Prozesse • Planung der Risikosteuerung mittels des Formulars	• Identifizieren von Risiken und Risikobehandlung gemäß der <i>Richtlinie zur ISMS-Risikoanalyse</i> • Planung der Risikosteuerung 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	• Planung der Umsetzung der festgelegten Maßnahmen über das	• Planung der Umsetzung im Realisierungsplan

⁹ Governance Risk Compliance (GRC)

Plan			
	ISMS	Prozesse	Sicherheitskonzepte nach IT-Grundschutz
	- Ggf. Überarbeitung von Richtlinien planen - Ressourcenplanung - Zeitplanung	Formular zur Etablierung neuer IT-Prozesse 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. Dienstleistungen oder angegliederten Einrichtungen	- Maßnahmen zur Risikobehandlung - Erhebung von Leistungsindikatoren
Dokumentation der Umsetzung	GRC-Tool und Jahresbericht	GRC-Tool und ergänzende Betriebsdokumentation	GRC-Tool und ergänzende Betriebsdokumentation
Dokumentation von Erkenntnissen über Verbesserungspotential aus dem laufenden Betrieb („Lessons Learned“)			

Kommunikation und Öffentlichkeitsarbeit	• Durchführung von zentralen Schulungs- und Awarenessmaßnahmen • 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 <i>Richtlinie zur Überprüfung und Verbesserung der Informationssicherheit</i> • Durchführung von: ○ Internen und externen Audits ○ Sicherheitsbegehungen ○ 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 Prozesseigentümer:innen bestimmen zu diesem Zweck den Schutzbedarf ihrer Geschäftsprozesse und benennen die Anwendungen, auf denen diese basieren. Im Rahmen der Strukturanalyse ermitteln die IT-Betreibenden zugehörige IT-Systeme und weitere Anwendungen, zu denen Abhängigkeiten bestehen. Anschließend wird für diese Zielobjekte ein Sicherheitskonzept erstellt oder sie werden in bestehende Sicherheitskonzepte integriert, sodass eine Überführung in das ISMS erfolgen kann. Die Priorisierung dieser Schritte erfolgt unter Berücksichtigung des festgelegten Schutzbedarfs.

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

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 ISMS-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
1.1.0	11.07.2025	Ersatz von SecDoc durch ein GRC-Tool, Umbenennung WWU IT in CIT, Anpassung von §4 an geändertes Vorgehen, Berücksichtigung von Compliance Office und Risikomanagement in §3, Umbenennungen	Ludger Becker (CISO)
1.0.0	03.08.2023	Erste Version aufgrund der Überarbeitung der ISL	Ludger Becker (CISO)

Ausgefertigt aufgrund des Beschlusses des Rektorats der Universität Münster vom 24.07.2025. 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 Richtlinie 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 28.07.2025

Der Rektor

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