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.

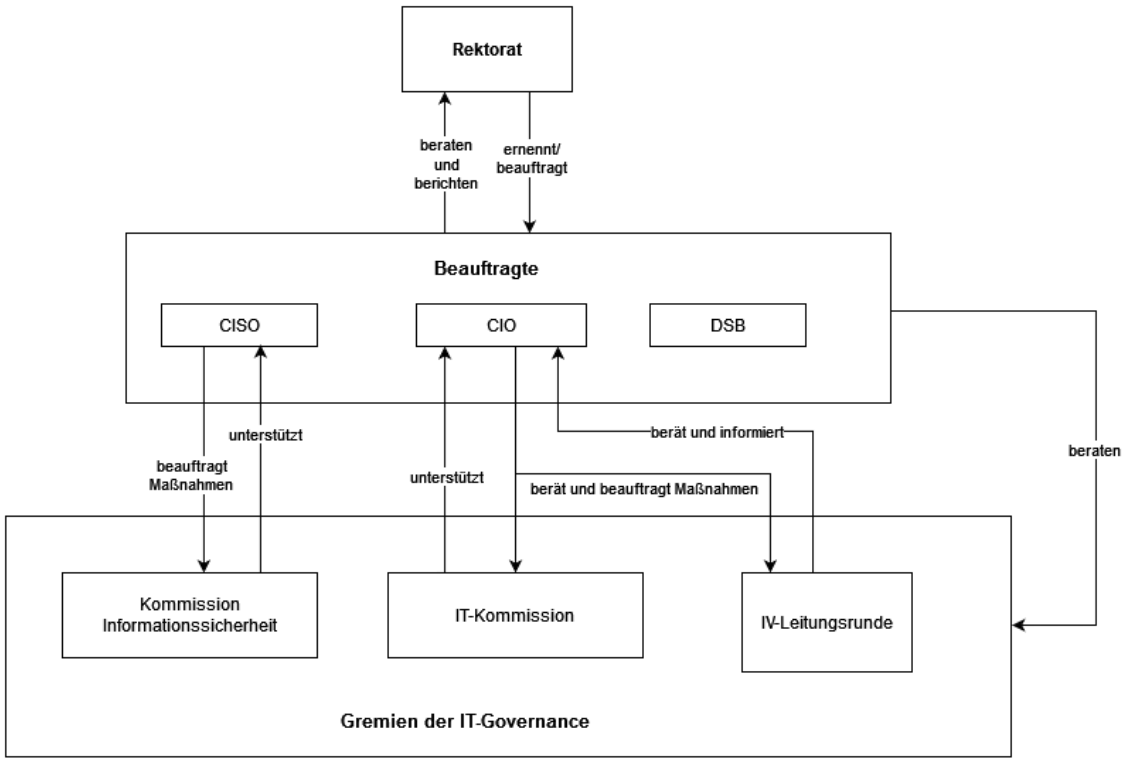

Abbildung 1: IT- Governance der Universität Münster.

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: