UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

AMTLICHE MITTEILUNGEN

VERKÜNDUNGSBLATT DER UNIVERSITÄT PADERBORN AM.UNI.PB

AUSGABE 20.24 VOM 24. APRIL 2024

LEITLINIE ZUR INFORMATIONSSICHERHEIT DER UNIVERSITÄT PADERBORN (MIT ENGLISCHER ÜBERSETZUNG)

VOM 24. APRIL 2024

HERAUSGEBER: PRÄSIDIUM DER UNIVERSITÄT PADERBORN

Leitlinie zur Informationssicherheit der Universität Paderborn
vom 24. April 2024

Dokumenteneigenschaften

Verantwortung	CIO / Informationssicherheitsbeauftragter
Klassifizierung	S1 Öffentlich
Gültigkeitszeit	Unbegrenzt
Überarbeitungsintervall	Jährlich
Nächste Überarbeitung	März 2025
Ablageort / Dateiname	Sharepoint Informationssicherheit RL006

Dokumentenstatus und Freigabe

Status	Version	Datum	Name / Abteilung / Firma
Erstellung	0.7	2020-07-01	Oevel / CIO Brennecke / IMT Wicker / DSB Kampmeyer / IST Porombka / IST
Prüfung	0.8	2020-07-04	VP Blömer / VP Probst
Freigabe	1.0	2023-09-06	Präsidium

Dokumentenhistorie

Version	Änderung	Datum	Autor*in der Änderung
0.7	Ersterstellung	2020-07-01	Oevel / CIO Brennecke / IMT Wicker / DSB Kampmeyer / IST Porombka / IST
0.8	informationelle Selbstbestimmung als Ziel höher gesetzt	2020-07-04	Oevel / CIO
0.9	Versionsverfolgung hinzugefügt, Dokumenten-name angepasst	2022-06-21	Kampmeyer / IST
0.9a	Vorschläge der DSB angenommen	2022-06-28	Oevel / CIO
0.9b	Vorschläge von Herrn Ehrich integriert	2022-11-12	Oevel / CIO
0.9c	Überarbeitung von Verantwortung	2023-03-07	Oevel / CIO
1.1	Redaktionelle Änderungen	2024-02-20	Porombka / IST Käuper / DSM Vreyborg / IST
1.2	Dokumenten-Klassifizierung ist jetzt S1 Öffentlich	2024-04-24	Kampmeyer / IST

Präambel

Zweck und Ziel der Informationssicherheit sind die Erfüllung von gesetzlichen Verpflichtungen und Auflagen, der Schutz der an der Universität Paderborn verarbeiteten Informationen, die Aufrechterhaltung von informationstechnischen Systemen sowie die Vermeidung von materiellen und immateriellen Schäden für die Universität Paderborn sowie für die von Datenverarbeitungen betroffenen Personen und Organisationen. Es soll zusätzlich sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um das Eintreten von Informationssicherheitsvorfällen weitestgehend zu minimieren und im Bedarfsfall schnell und angemessen zu reagieren. Mit dieser Leitlinie legt das Präsidium für alle Hochschulangehörigen und im Auftrag der Universität agierenden Personen die Grundzüge der Informationssicherheit an der Universität Paderborn fest.

Zur Sicherung des Grundrechts auf informationelle Selbstbestimmung und zum Schutz personenbezogener Daten hat die Universität Paderborn zusätzlich eine Datenschutzleitlinie erlassen. Beide Leitlinien wirken auf die Umsetzung von Maßnahmen zur Sicherung der an der Universität Paderborn verarbeiteten Daten und Informationen hin, haben aber jeweils einen unterschiedlichen Fokus. Die Informationssicherheit dient der Absicherung und dem Schutz der Daten der Institution, das Datenschutzrecht schützt die Rechte und Freiheiten der von Datenverarbeitungen betroffenen Personen. Die Sicherstellung der Informationssicherheit ist damit Grundvoraussetzung für die Umsetzung des Datenschutzes. Auch wenn beide Leitlinien die Verarbeitung durch Systeme und Dienste im Bereich der Information, Kommunikation und Medien[1] besonders adressieren, gelten alle Regelungen sinngemäß auch für den Umgang mit Daten und Informationen in Wort und Schrift.

Was bedeutet Informationssicherheit für uns als Universität Paderborn?

Informationssicherheit ist eine wesentliche Voraussetzung für ein Gelingen des digitalen Wandels. Wir setzen an der Universität Paderborn dazu die gesetzlichen Regelungen und vertraglichen Auflagen im Bereich der Informationssicherheit und des Datenschutzes sowie die Grundsätze der guten wissenschaftlichen Praxis aktiv um. Wir orientieren uns an den Schutzzielen der Verfügbarkeit, Vertraulichkeit und Integrität sowie dem Recht auf informationelle Selbstbestimmung und dem Schutz personenbezogener Daten. Wir verfolgen Maßnahmen zur Informationssicherheit proaktiv.

Unter unseren Schutzzielen verstehen wir:

- **Verfügbarkeit:** Informationen und Verarbeitungsmethoden stehen in benötigten Zeiträumen abrufbar zur Verfügung.
- **Vertraulichkeit:** Informationen sind nur für einen eingeschränkten Kreis von Berechtigten zugänglich.
- **Integrität:** die Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden seit der letzten autorisierten Veränderung ist sichergestellt.
- **Recht auf informationelle Selbstbestimmung und Schutz personenbezogener Daten:** Die Universität Paderborn unterstützt aktiv das Recht auf informationelle Selbstbestimmung/den Schutz personenbezogener Daten. Ausgehend von den gesetzlich verankerten Vorgaben werden in Ergänzung zu den drei Schutzzielen der Verfügbarkeit, Vertraulichkeit und Integrität die Gewährleistungsziele
  - **Nichtverkettung:** Daten aus verschiedenen Datenverarbeitungsprozessen werden nicht zusammengeführt,

[1] Sogenannte IKM-Systeme und IKM-Dienste.

- **Datenminimierung:** die Erhebung, Speicherung und Nutzung personenbezogener Daten werden auf das notwendige Maß beschränkt,
- **Intervenierbarkeit:** Personen können jederzeit die Ihnen zustehenden Rechte in Bezug auf die sie betreffende Datenverarbeitung einfordern,
- **Transparenz:** Verarbeitungen werden durch eine allgemeinverständliche Beschreibung überprüfbar dokumentiert,

abgebildet.

Als zusätzliche Prinzipien der Informationssicherheit gelten für uns:

- **Wohlorganisiertheit:** Für alle IKM-Systeme und IKM-Dienste gibt es klare Verantwortlichkeiten und dokumentierte Konfigurationen und Prozesse.
- **Informiertheit:** Alle Nutzer*innen von IKM-Systemen und IKM-Dienste sind sich der für sie wesentlichen Sicherheitsrisiken und deren Abwehrmaßnahmen bewusst.
- **Zurechenbarkeit:** Jede an und von vernetzten Rechnern der Universität Paderborn ausgehende Aktivität kann einer Person zugeordnet werden.
- **Aktualität:** Die eingesetzten IKM-Systeme und IKM-Dienste entsprechen den jeweils aktuellen Sicherheitsempfehlungen einschlägiger Institutionen.
- **Angemessenheit:** Alle Maßnahmen werden mit Augenmaß und in Hinblick auf mögliche Gefährdungen und Risiken sowie ihr Kosten-Nutzen-Verhältnis gewählt.
- **Wahrung eines permanenten Regelkreislaufes:** Die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen werden regelmäßig überprüft. Verletzungen der Informationssicherheit werden kommuniziert und dokumentiert.

Diese Leitlinie kann Verletzungen der Informationssicherheit und des Datenschutzes nicht ausschließen. Sollte trotz aller proaktiven Maßnahmen eine solche auftreten, haben wir geregelte Prozesse für deren Feststellung und Bearbeitung, um den Schaden für die betroffenen Personen und die Universität Paderborn zu minimieren. Wir lernen aus unseren Fehlern und verbessern uns.

1) Grundlage

Der Hochschulbetrieb erfordert zunehmend die Verwendung von Verfahren und Abläufen, die sich auf Möglichkeiten der Informations-, Kommunikations- und Medientechnik (IKM) stützen. Sie sind zentrale Grundlage für die Leistungsfähigkeit der Universität Paderborn. Bei der Nutzung von IKM werden regelmäßig personenbezogene und weitere schützenswerte Daten verarbeitet.

Unter diesen Bedingungen kommt der Informationssicherheit eine grundsätzliche und strategische Bedeutung zu. Auf Grund der sich schnell weiter entwickelnden technischen Möglichkeiten, der Heterogenität der IKM-Landschaft und der verteilten Aufgaben muss ein kontinuierlicher Informationssicherheitsprozess realisiert werden, der den besonderen Bedingungen der Universität Paderborn gerecht wird. Die Entwicklung und Fortschreibung des Informationssicherheitsprozesses sollen sich zum einen an den gesetzlich festgelegten Aufgaben der Universität Paderborn sowie an ihrem Mandat zur Wahrung der akademischen Freiheit orientieren, zum anderen aber auch einem verlässlichen Prozess mit geregelten Verantwortlichkeiten entsprechen.

2) Zielsetzung

Die Informationssicherheit wird im Sinne des Informationssicherheitsprozesses durch organisatorische, prozessuale und technische Maßnahmen realisiert und umfasst folgende Aufgaben:

a) Verantwortlichkeiten definieren und festlegen,

b) Schutzbedarfe von Informationen und zugehörigen IKM-Systemen feststellen, mögliche Risiken erfassen und bewerten,

c) technische und organisatorische Maßnahmen für den Zugang zu und den Zugriff auf Informationen sowie Art und Umfang der Autorisierung im Sinne eines Benutzerberechtigungskonzepts definieren und festlegen,

d) Sicherheits- und Kontrollmaßnahmen inkl. Schulungsmaßnahmen festlegen, umsetzen, regelmäßig überprüfen und aktualisieren,

e) auf Informationssicherheitsvorfälle schnell und angemessen reagieren,

f) den Stand der Informationssicherheit an der Universität Paderborn regelmäßig dokumentieren.

Für die Umsetzung muss allen Informationen und zugehörigen Informationssystemen ein Schutzbedarf der folgenden Kategorien zugeordnet werden:

a) normaler Schutzbedarf: die Auswirkungen eines Schadens sind begrenzt und überschaubar,

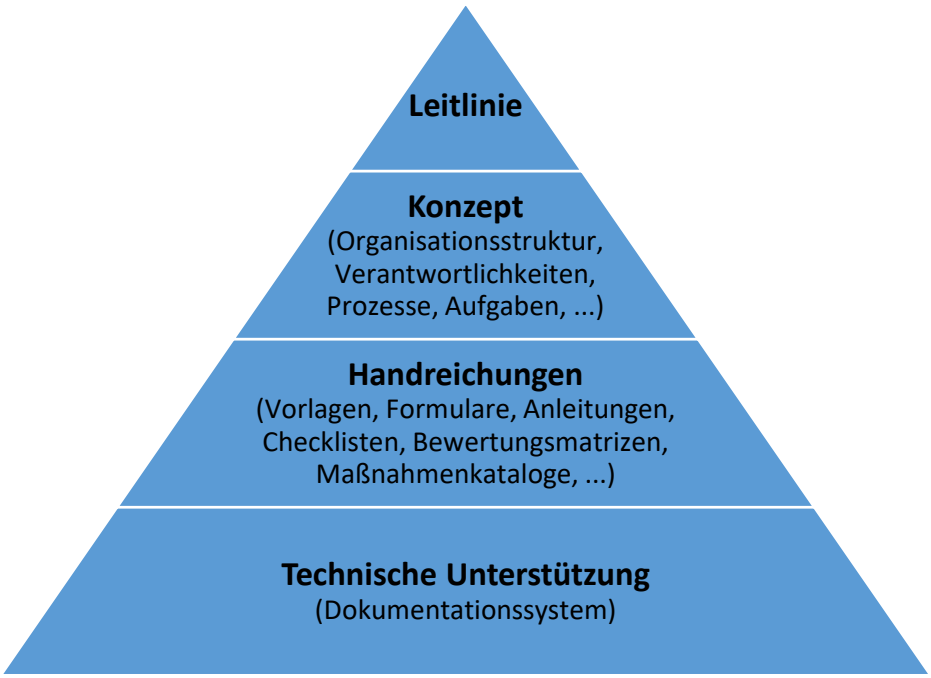
b) hoher Schutzbedarf: die Auswirkungen eines Schadens sind erheblich,

c) sehr hoher Schutzbedarf: die Auswirkungen eines Schadens können einen gesellschaftlichen und/oder wirtschaftlichen Ruin oder eine Gefahr für Leib und Leben bedeuten.

Auf der Basis möglicher Schadensereignisse und ihrer Ursachen und Auswirkungen sind unter Berücksichtigung des finanziellen und organisatorischen Aufwands mögliche Risiken zu bewerten und in einem Risikobehandlungsplan durch Maßnahmen der Risikominderung, Risikovermeidung, Risikoübertragung oder Risikoakzeptanz zu behandeln.

3) Umsetzung

Zur Einhaltung der Informationssicherheit baut die Universität Paderborn auf Grundlage dieser Leitlinie ein Informationssicherheitsmanagementsystem (ISMS) auf. Dieses beinhaltet Regelungen wie beispielsweise ein Informationssicherheitskonzept, in dem eine Organisationsstruktur mit Verantwortlichkeiten, Prozessen und Aufgaben festgelegt sind. Ergänzt wird die Leitlinie und das Konzept durch Handreichungen (Vorlagen, Formulare, Anleitungen, Checklisten, Bewertungsmatrizen, Maßnahmenkataloge, Schulungsunterlagen etc.). Weitere Bestandteile sind die technische Unterstützung der Prozesse und der Dokumentation (Dokumentationssystem) sowie Anleitungen zur Umsetzung der Risikobewertung und -behandlung.



4) Verantwortlichkeiten

- **Präsidium:** Das Präsidium trägt die Gesamtverantwortung für die Einhaltung der Informationssicherheit. Es ist verantwortlich für die Einführung und Weiterentwicklung eines Informationssicherheitsmanagementsystems. Es trägt durch seine Entscheidungen dem Organisationsziel Rechnung und stellt die erforderlichen finanziellen, personellen und zeitlichen Ressourcen für die Umsetzung der Informationssicherheit zur Verfügung. Das Präsidium trägt dafür Sorge, dass Mitglieder und Angehörige der Universität Paderborn durch Informationsangebote oder Schulungen für die Informationssicherheit sensibilisiert und zu deren Umsetzung befähigt werden.

- **Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter (ISB) und Informationssicherheitsteam (IST):** Die oder der Informationssicherheitsbeauftragte wird vom Präsidium benannt, berät das Präsidium bei allen Fragen zur Informationssicherheit und verantwortet den Aufbau des Informationssicherheitsmanagementsystems. Sie oder er wird durch ein Informationssicherheitsteam unterstützt, das Nutzer*innen der IKM-Systeme, Gremien und Bereiche zu Themen der Informationssicherheit berät und Empfehlungen zu technischen und organisatorischen sowie Awareness-Maßnahmen gibt. Es ist zudem die technische Kontaktstelle bei Informationssicherheitsvorfällen und unterstützt die verantwortlichen IKM-Betreiber, um Schäden für die Universität Paderborn zu begrenzen. Das Informationssicherheitsteam nimmt damit auch die Aufgaben eines hochschulweiten Computer Notfallteams (Computer Emergency Response Team (CERT) wahr. ISB und IST tauschen sich regelmäßig und darüber hinaus anlassbezogen mit der oder dem behördlichen Datenschutzbeauftragten zur Ordnungsmäßigkeit der Verarbeitungstätigkeiten, Maßnahmen der Informationssicherheit und zu datenschutzrelevanten Sicherheitsvorfällen aus. Im Falle eines Konflikts einer Sicherheitsmaßnahme mit dem Datenschutz verpflichten sich ISB und IST, an einer Lösung mitzuwirken, die beiden Aspekten angemessen Rechnung trägt.

- **Behördliche Datenschutzbeauftragte oder Datenschutzbeauftragter (DSB):** Die oder der bestellte Datenschutzbeauftragte überwacht die Einhaltung der gesetzlichen Vorgaben zum Datenschutz und nimmt die Aufgaben gemäß Datenschutz-Grundverordnung (DS-GVO) wahr. Sie oder er ist Ansprechpartnerin oder Ansprechpartner für betroffene Personen und für die zuständige Datenschutzaufsichtsbehörde.

- **Chief Information Officer (CIO):** Das Präsidium bestellt zur Koordination aller Aktivitäten im Bereich der digitalen Infrastruktur der Universität Paderborn eine Generalverantwortliche oder einen Generalverantwortlichen, den oder die Chief Information Officer (CIO). Diese Person berät das Präsidium in allen einschlägigen Fragestellungen, entwickelt die strategischen Ziele und deren Abbildung in der Universität Paderborn weiter und übernimmt zusätzlich Koordinations- und Steuerungsaufgaben. Der oder die CIO hat Richtlinienkompetenz für den ordnungsgemäßen Betrieb von Informationssystemen. Sie oder er arbeitet in allen Aspekten der Informationssicherheit in enger Abstimmung mit der oder dem ISB sowie dem oder der behördlichen DSB.

- **Führungskräfte (Leiter*innen der Fakultäten, Zentralen Einrichtungen und Dezernate sowie Professor*innen):** Ungeachtet der Gesamtverantwortung des Präsidiums ist die Unterstützung der Umsetzung von Regelungen der Universität Paderborn im Bereich Informationssicherheit ein integraler Bestandteil der jeweiligen Fachaufgabe. Dabei ist dafür Sorge zu tragen, dass konkrete Vorgaben aus den verbindlichen Handreichungen gemäß ISMS bei Mitarbeiter*innen Beachtung finden und umgesetzt werden können. Notwendig kann es sein, technische, organisatorische oder personelle Voraussetzungen zu realisieren, und die Möglichkeit zur Teilnahme an Schulungsangeboten zu eröffnen. Hervorzuheben ist hierbei die Sensibilisierung der Mitarbeiter*innen durch Informationen und Schulungen, die vom Informationssicherheitsteam in Abstimmung mit der Personalentwicklung angeboten werden.

  Falls Regelungen nicht umgesetzt werden können, ist dies der Hochschulleitung über die Leitungen der Fakultäten, Zentralen Einrichtungen bzw. Dezernate mitzuteilen.

- **IKM-Betreiber:** IKM-Betreiber sind alle Organisationseinheiten und die zugehörigen Personen, die für den technischen Betrieb von IKM-Systemen zuständig sind. Sie achten darauf, dass nur Berechtigte auf die von ihnen verwalteten Informationen und Systeme Zugriff haben, dokumentieren die getroffenen technischen Maßnahmen, setzen die Maßnahmen des Informationssicherheitskonzeptes um, unterstützen proaktiv dessen Weiterentwicklung, berichten an ihre Führungskräfte zum Stand der Informationssicherheit und melden Informationssicherheitsvorfälle.

- **Nutzer*innen:** Alle Nutzer*innen von IKM-Systemen, insbesondere diejenigen, die ständig oder regelmäßig Umgang mit digitalen Informationen haben, nehmen angebotene Schulungs- und Informationsmöglichkeiten wahr und achten darauf, dass nur Berechtigte auf die von ihnen verwalteten Informationen, Dokumente und Systeme Zugriff haben. Sie haben Regelverletzungen oder Sicherheitslücken unverzüglich der Führungskraft und/oder dem Vorfallteam und/oder dem oder der behördlichen Datenschutzbeauftragten und/oder der oder dem IT-/Informationssicherheitsbeauftragten mitzuteilen.

- **Vorfallteam**: Das Vorfallteam beurteilt Informationssicherheitsvorfälle in Hinblick auf Verdachtsfälle zur Offenlegung von und den unerlaubten Umgang mit sensiblen und/oder personenbezo-

genen Daten. Das Vorfallteam besteht aus der*dem Datenschutzbeauftragten, der*dem Informationssicherheitsbeauftragte*n und der*dem CIO. Weitere Personen können bedarfsorientiert oder dauerhaft zugezogen werden. Im Vorfallteam wird jeder datenschutzrelevante Vorfall – auch bzgl. einer möglichen Meldepflicht an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes NRW – geprüft und bewertet. Dem Präsidium werden daraus abgeleitete Empfehlungen gegeben.

5) Inkrafttreten

Diese Leitlinie tritt am Tag nach ihrer Veröffentlichung in den Amtlichen Mitteilungen der Universität Paderborn in Kraft.

Ausgefertigt aufgrund der Einführung eines Informationssicherheitsmanagementsystems an der Universität Paderborn sowie nach Genehmigung durch das Präsidium der Universität Paderborn vom 6. September 2023.

Paderborn, den 24. April 2024

Die Präsidentin
der Universität Paderborn

Professorin Dr. Birgitt Riegraf

Guideline on information security at Paderborn University
24 April 2024

Document properties

Responsibility	CIO / Information Security Officer
Classification	S2 Internal
Validity period	Unlimited
Revision interval	Annual
Next revision	March 2025
Storage location / file name	Sharepoint Informationssicherheit RL006

Document status and release

Status	Version	Date	Name / Department / Company
Creation	0.7	2020-07-01	Oevel / CIO Brennecke / IMT Wicker / DSB Kampmeyer / IST Porombka / IST
Review	0.8	2020-07-04	VP Blömer / VP Probst
Clearance	1.0	2023-09-06	Presidium

Document history

Version	Amendment	Date	Author of the change
0.7	Initial creation	2020-07-01	Oevel / CIO Brennecke / IMT Wicker / DSB Kampmeyer / IST Porombka / IST
0.8	Informational self-determination set as a higher goal	2020-07-04	Oevel / CIO
0.9	Version tracking added, document name adjusted	2022-06-21	Kampmeyer / IST
0.9a	DPO proposals adopted	2022-06-28	Oevel / CIO
0.9b	Proposals from Mr. Ehrich integrated	2022-11-12	Oevel / CIO
0.9c	Revision of responsibility	2023-03-07	Oevel / CIO
1.1	Editorial changes	2024-02-20	Porombka / IST Käuper / DSM Vreyborg / IST
1.2	Document classification is now S1 Public Added Effective Date section	2024-04-24	Kampmeyer / IST

Preamble

The purpose and aim of information security is to fulfil legal obligations and requirements, to protect the information processed at Paderborn University, to maintain information technology systems and to avoid material and immaterial damage to the university and to the persons and organizations affected by data processing. It should also be ensured that appropriate and state-of-the-art security measures are taken to minimize the occurrence of information security incidents as far as possible and to react quickly and appropriately if necessary. With this guideline, the Executive Board sets out the basic principles of information security at Paderborn University for all university members and persons acting on behalf of the university.

To safeguard the fundamental right to informational self-determination and to protect personal data, the university has also issued a data protection guideline. Both guidelines work towards the implementation of measures to secure the data and information processed at the university, but each has a different focus. Information security serves to safeguard and protect the institution's data, while data protection law protects the rights and freedoms of persons affected by data processing. Ensuring information security is therefore a basic prerequisite for the implementation of data protection. Even though both guidelines specifically address processing by systems and services in the area of information, communication and media[2] (Abbreviated here by translation from German as IKM), all regulations also apply mutatis mutandis to the handling of data and information in written and spoken form.

What does information security mean for us as a university?

Information security is an essential prerequisite for the success of the digital transformation. At the university, we actively implement the legal regulations and contractual requirements in the area of information security and data protection as well as the principles of good scientific practice. We are guided by the protection goals of availability, confidentiality and integrity as well as the right to informational self-determination and the protection of personal data. We proactively pursue information security measures.

We understand our protection goals to mean:

- **Availability:** Information and processing methods are available at the required times.
- **Confidentiality:** Information is only accessible to a limited group of authorized persons.
- **Integrity:** The accuracy and completeness of information and processing methods since the last authorized alteration is ensured.
- **Right to informational self-determination and protection of personal data:** The University actively supports the right to informational self-determination/the protection of personal data. In addition to the three protection goals of availability, confidentiality and integrity, the following guarantee goals are defined on the basis of the statutory requirements:
  - **Non-linking:** Data from different data processing operations are not merged.
  - **Data minimization:** The collection, storage and use of personal data is limited to what is necessary.
  - **Intervenability:** Individuals may at any time claim the rights to which they are entitled in relation to the data processing concerning them.

[2] so-called IKM systems and IKM services

- **Transparency:** Processing operations are documented in a verifiable manner by means of a generally understandable description.

The following additional principles of information security apply to us:

- **Well-organizedness:** There are clear responsibilities and documented configurations and processes for all IKM systems and IKM services.
- **Informedness:** All users of IKM systems and IKM services are aware of the main security risks for them and their defensive measures.
- **Attributability:** Every activity on and from networked computers at Paderborn University can be attributed to a person.
- **Up-to-dateness:** The IKM systems and IKM services used comply with the latest security recommendations of the relevant institutions.
- **Appropriateness:** All measures are selected with a sense of proportion and regard to possible hazards and risks as well as their cost-benefit ratio.
- **Maintaining a permanent control loop:** The effectiveness and appropriateness of the security measures are regularly reviewed. Information security breaches are communicated and documented.

This guideline cannot rule out breaches of information security and data protection. Should such a breach occur despite all proactive measures, we have regulated processes for identifying and dealing with it in order to minimize the damage to the persons affected and the university. We learn from our mistakes and improve.

1) Basis

University operations increasingly require the use of procedures and processes that are based on information, communication and media technology (IKM). They are the central basis for the efficiency of Paderborn University. When using IKM, personal and other sensitive data is regularly processed.

Under these conditions, information security is of fundamental and strategic importance. Due to the rapidly evolving technical possibilities, the heterogeneity of the IKM landscape and the distributed tasks, a continuous information security process must be implemented that does justice to the special conditions of the university. The development and updating of the information security process should, on the one hand, be based on the legally defined tasks of the university and its mandate to safeguard academic freedom, but on the other hand also correspond to a reliable process with regulated responsibilities.

2) Objective

Information security is implemented as part of the information security process through organizational, procedural and technical measures and includes the following tasks:

a) Define and specify responsibilities,

b) Determine protection requirements for information and associated IKM systems, identify and evaluate possible risks,

c) Define and specify technical and organizational measures for admission and access to information as well as the type and scope of authorization in terms of a user authorization concept,

d) Define, implement, regularly review and update safety and control measures, including training measures,

e) Respond quickly and appropriately to information security incidents,

f) Regularly document the status of information security at the university.

For implementation, all information and associated information systems must be assigned a protection requirement in the following categories:

a) normal protection requirement: the effects of damage are limited and manageable,

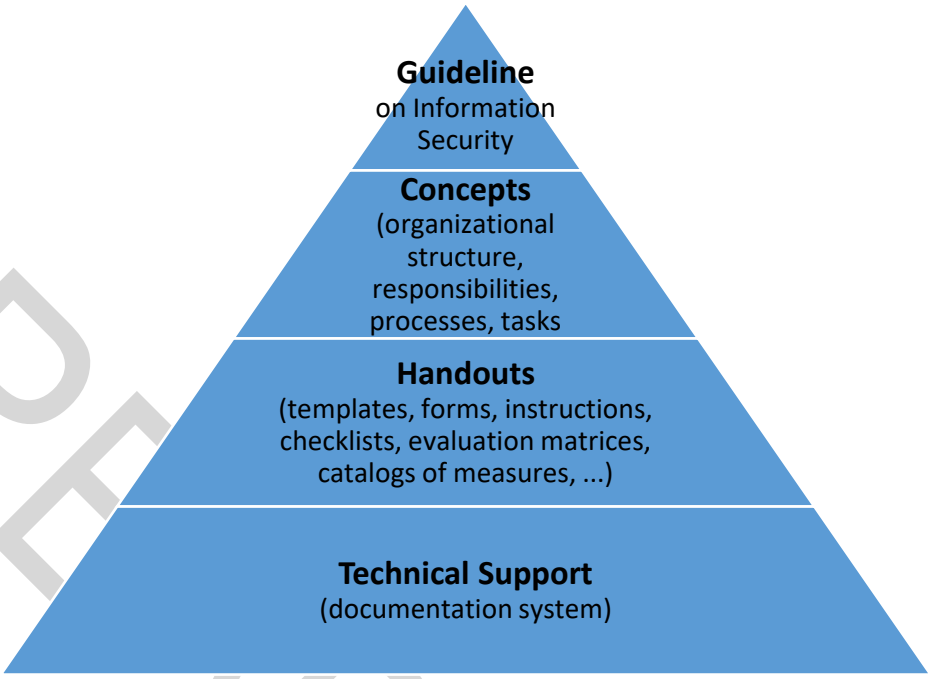
b) high protection requirement: the effects of damage are considerable,

c) very high protection requirement: the effects of damage can mean social and/or economic ruin or a danger to life and limb.

Based on potential damage events and their causes and effects, possible risks must be assessed considering the financial and organizational effort. These risks should then be addressed in a risk treatment plan through measures of risk reduction, risk avoidance, risk transfer, or risk acceptance.

3) Implementation

Paderborn University is establishing an information security management system (ISMS) on the basis of this guideline to ensure compliance with information security. This includes regulations such as an information security concept in which an organizational structure with responsibilities, processes and tasks are defined. The guideline and the concept are supplemented by handouts (templates, forms, instructions, checklists, evaluation matrices, catalogs of measures, training documents, etc.). A further component is the technical support of the processes and documentation (documentation system) as well as instructions for implementing the risk assessment and treatment.



4) Responsibilities

- **Executive Committee:** The Executive Committee bears overall responsibility for compliance with information security. It is responsible for the introduction and further development of an information security management system. Through its decisions, it takes account of the organizational goal and provides the necessary financial, personnel and time resources for the implementation of information security. The Executive Board ensures that members and affiliates of the university are made aware of information security through information services or training courses and are enabled to implement them.

- **Information Security Officer (ISO) and Information Security Team (IST):** The Information Security Officer is appointed by the Executive Board, advises the Executive Board on all matters relating to information security and is responsible for setting up the information security management system. He or she is supported by an information security team that advises users of the IKM systems, committees and departments on information security issues and makes recommendations on technical, organizational and awareness measures. It is also the technical point of contact in the event of information security incidents and supports the responsible IKM operators in order to limit damage to the university. The information security team thus also performs the tasks of a university-wide Computer Emergency Response Team (CERT). The ISB and IST exchange information with the data protection officer on a regular and ad hoc basis regarding the correctness of processing activities, information security measures and data protection-related security incidents. In the event of a conflict between a security measure and data protection, ISB and IST undertake to cooperate in finding a solution that takes appropriate account of both aspects.

- **Data Protection Officer (DPO):** The appointed data protection officer monitors compliance with the legal requirements on data protection and performs the tasks in accordance with the General Data Protection Regulation (GDPR). He or she is the contact person for data subjects and for the competent data protection supervisory authority.
- **Chief Information Officer (CIO):** The Executive Board appoints a general manager, the Chief Information Officer (CIO), to coordinate all activities relating to the university's digital infrastructure. This person advises the Executive Board on all relevant issues, further develops the strategic goals and their mapping in the university and also takes on coordination and management tasks. The CIO has the authority to issue guidelines for the proper operation of information systems. He or she works closely with the ISB and the official DPO on all aspects of information security.
- **Managers (heads of faculties, central institutions and departments as well as professors):** Irrespective of the overall responsibility of the Executive Board, supporting the implementation of Paderborn University regulations in the area of information security is an integral part of the respective specialist task. It must be ensured that specific requirements from the binding guidelines in accordance with the ISMS are observed and can be implemented by employees. It may be necessary to implement technical, organizational or personnel requirements and to provide the opportunity to participate in training courses. The sensitization of employees through information and training offered by the information security team in coordination with personnel development should be emphasized here.

  If regulations cannot be implemented, this must be communicated to the university management via the heads of the faculties, central institutions or departments.
- **IKM operators:** IKM operators are all organizational units and the associated persons who are responsible for the technical operation of IKM systems. They ensure that only authorized persons have access to the information and systems they manage, document the technical measures taken, implement the measures of the information security concept, proactively support its further development, report to their managers on the status of information security and report information security incidents.
- **Users:** All users of IKM systems, especially those who constantly or regularly handle digital information, take advantage of the training and information opportunities offered and ensure that only authorized persons have access to the information, documents and systems they manage. They must immediately notify the manager and/or the incident team and/or the data protection officer and/or the IT/information security officer of any breaches of rules or security gaps.
- **Incident team**: The incident team assesses information security incidents with regard to suspected disclosure and unauthorized handling of sensitive and/or personal data. The incident team consists of the Data Protection Officer, the Information Security Officer and the CIO. Other persons can be called in as required or on a permanent basis. The incident team examines and evaluates every incident relevant to data protection - also with regard to a possible reporting

obligation to the State Commissioner or the State Commissioner for Data Protection and Freedom of Information of the State of North Rhine-Westphalia. Recommendations are then made to the Executive Board.

5) Coming into force

This guideline comes into force on the day after its publication in the Official Notices of Paderborn University.

Issued due to the introduction of an information security management system at Paderborn University and after approval by the Presidential Board of Paderborn University on September 6, 2023

Paderborn, on April 24, 2024

The President
of the Paderborn University

Professor Dr. Birgitt Riegraf

HERAUSGEBER
PRÄSIDIUM DER UNIVERSITÄT PADERBORN
WARBURGER STR. 100
33098 PADERBORN

HTTP://WWW.UNI-PADERBORN.DE

ISSN 2199-2819