Hochschule Merseburg
University of Applied Sciences

Amtliche Bekanntmachungen
Nr. 01/2021

Herausgeber: Rektor

Redaktion: Dezernat Akademische Angelegenheiten

Merseburg,
07. Januar 2021

Inhaltsverzeichnis

Professor Dr.-Ing. Jörg Kirbs
Rektor

Leitlinie für Informationssicherheit der Hochschule Merseburg

Inhalt

Präambel

Die Verarbeitung von teilweise sensiblen Informationen, wie Prüfungsdaten oder Forschungsergebnissen, gehört zu den Kernaufgaben der Hochschule Merseburg. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert, dass Hochschulen für die Sicherheit dieser Informationen Sorge tragen. Hierzu müssen die Schutzziele der Informationssicherheit, Vertraulichkeit, Verfügbarkeit und Integrität sowie die Zurechenbarkeit von Informationen, eingehalten sein.

Konkret bedeutet dies: Vertrauliche Informationen müssen nicht nur im Sinne des Datenschutzes vor unberechtigten Zugriffen Dritter geschützt werden. Die IT-Infrastruktur der Hochschule muss derart verfügbar sein, dass der Ablauf kritischer Geschäftsprozesse, wie der Prüfungsprozess, sicher durchgeführt werden kann. Personenbezogene Daten und Informationen von Mitarbeitenden und Studierenden, z. B. in Personal- und Studierendenakten, müssen korrekt, lückenlos und zurechenbar (revisionssicher) verarbeitet und gespeichert werden.

Die Leitlinie dient als Grundlage für das Informationssicherheitskonzept der Hochschule Merseburg. Neben den Zielen werden der Geltungsbereich und eine klare Verantwortungsstruktur durch die Rektorin oder den Rektor benannt. Die Leitlinie trägt damit zur sicheren Nutzung und dem Betrieb der IT-Infrastruktur an der Hochschule Merseburg bei. Dabei gilt es, die gesetzlichen Vorgaben und die Freiheit von Forschung und Lehre zu beachten.

1 Geltungsbereich

Diese Leitlinie findet Anwendung für alle Mitglieder und Angehörige der Hochschule Merseburg gem. § 58 Abs. 1 - 3 HSG LSA sowie auf alle sonstigen Nutzerinnen und Nutzer der IT-Dienste.

2 Ziele der Informationssicherheit

Für die Stellen der unmittelbaren Landesverwaltung Sachsen-Anhalt, und damit ebenfalls für die Hochschule Merseburg, wurden die nachstehenden Sicherheitsziele festgelegt:

a) **Vertraulichkeit**
   Informationen dürfen ausschließlich einem berechtigten Personenkreis zur Verfügung stehen.
b) **Integrität**
   Die physische und logische Unversehrtheit von Systemen, Anwendungen und Daten muss jederzeit gewahrt sein. Dies umfasst den Schutz vor unberechtigter Erstellung oder Änderung von Informationen.
c) **Verfügbarkeit**
   Systeme, Anwendungen und Daten müssen den Berechtigten stets wie vorgesehen zur Verfügung stehen.
d) **Zurechenbarkeit (Revisionssicherheit)**
   Es muss rechtssicher erkennbar sein, wer welche Informationen in Verwaltungsprozessen oder im Bereich der Forschung und Lehre wann wie erstellt und verändert hat.

Um diese Ziele zu erreichen ist, die Verhältnismäßigkeit der eingesetzten Mittel zum Wert der schützenswerten Güter zu beachten. Standardisierung und ein einheitliches und gemeinsames Vorgehen mit anderen Hochschulen und Stellen der unmittelbaren Landesverwaltung Sachsen-Anhalt sollen dabei helfen.

Die Informationstechnik stellt an der Hochschule Merseburg die führende und teilweise sogar die ausschließlich genutzte Kommunikations- und Arbeitsinfrastruktur in den jeweiligen Bereichen dar. Diese ist damit zur Erfüllung der Geschäfts- und Verwaltungsaufgaben ein unverzichtbarer Grundwert, der zu schützen ist.

Als Stelle der unmittelbaren Landesverwaltung Sachsen-Anhalts müssen die gesetzlichen Vorschriften, u.a. zum Datenschutz ((Datenschutzgesetze des Landes Sachsen-Anhalt, Bundesdatenschutzgesetz, Datenschutzgrundverordnung (sog. DSGV)) eingehalten werden sowie Dienst- und Geschäftsgeheimnisse gewahrt bleiben. Dienstleistungen für Studium, Lehre und Forschung sowie Wirtschaft müssen sicher, zuverlässig und vertrauenswürdig erbracht werden.

Die Auswirkungen eines eventuellen Schadensfalls sind durch angemessene Vorsorgemaßnahmen auf ein vertretbares Maß zu reduzieren. Bereits investierte Werte in Technik, Informationen, Arbeitsprozesse und Wissen müssen geschützt bleiben. Darüber hinaus sind Ansehens- und Vertrauensverluste durch die Verletzung der Sicherheitsziele zu vermeiden.

3 Informationssicherheitsstrategie

Um ein angemessenes Maß an Sicherheit zu erreichen, wird ein Informationssicherheitsmanagementsystem (ISMS) eingerichtet. Kontinuierliche Verbesserungsprozesse erhöhen in angemessener Weise die Sicherheit und ermöglichen die Adaptierung der Sicherheitsprozesse an den Stand der Technik.

Ziel des ISMS der Hochschule Merseburg ist es:

a) organisatorische Rahmenbedingungen zur Gewährleistung der Informationssicherheit aufrechtzuerhalten und weiterzuentwickeln,

b) die Informationssicherheit kontinuierlich zu verbessern,

c) abgestimmte Sicherheitsstandards einschließlich der Definition von Verantwortlichkeiten, Befugnissen, Richtlinien und Bestimmungen fortzuschreiben und

d) Komponenten zur Steigerung der Informationssicherheit zu zentralisieren und standardisieren und alle Sicherheitsvorkehrungen und -maßnahmen hinreichend zu dokumentieren.

Zur Umsetzung dieser Leitlinie für Informationssicherheit sollen zukünftig von einem oder einer Informationssicherheitsbeauftragen (ISB) und dem Arbeitskreis Datenschutz und Informationssicherheit (ISM-Team) detaillierte Richtlinien, Vorschriften und Anweisungen erarbeitet und in geeigneter Form durch die Kanzlerin oder den Kanzler veröffentlicht werden.

Diese Richtlinien, Vorschriften und Anweisungen sollen sich sowohl am IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI), als auch an den Empfehlungen der DIN ISO/IEC 27001 und den Vorgaben der DSGVO orientieren. Das BSI stellt für typische Gefährdungen spezielle Gegenmaßnahmen bereit, mit denen ein angemessenes Schutzniveau erreicht wird. Mit dem IT-Grundschutzprofil für Hochschulen wird eine spezielle Vorgehensweise für Hochschulen bereitgestellt. Ausgehend von der Basisabsicherung der kritischen Standardprozesse einer Hochschule, soll das Sicherheitsniveau kontinuierlich gesteigert werden. Für Bereiche, in denen ein höherer Schutzbedarf angestrebt wird, sind ergänzende Sicherheitsmaßnahmen durchzuführen und zu dokumentieren.

Der kontinuierliche Verbesserungsprozess orientiert sich an dem bekannten PDCA-Zyklus (plan-do-check-act) und umfasst folgende Schritte:

a) **Planung**
   Festlegung der Vorgaben für den Sicherheitsprozess und des ISMS nach den Vorgaben des Landes Sachsen-Anhalt und Abstimmung im ISM-Team der Hochschule Merseburg.
b) **Umsetzung**
   Aufbau eines ISMS, Erstellung und Umsetzung eines Sicherheitskonzepts sowie Etablierung des Sicherheitsprozesses.
c) **Überprüfung**
   Erfolgskontrolle der Erreichung der Ziele der Informationssicherheit.
d) **Aufrechterhaltung**
   Durchführung von Korrekturen zur Optimierung des Sicherheitsprozesses und der Organisationsstruktur der ISMS. Das ISMS soll dem jeweiligen Schutzzweck entsprechend angemessene Sicherheitsmaßnahmen definieren und für deren wirtschaftliche Umsetzung sorgen. Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen ist darauf zu achten, dass das erforderliche Sicherheitsniveau erreicht wird, ohne den Ablauf von Verwaltungs- und Geschäftsprozessen unnötig zu beeinträchtigen.

Um die Bedeutung hervorzuheben, wird die Sicherheitsstrategie von den folgenden Grundsätzen der Informationssicherheit geprägt:

a) **Sicherstellung der Verfügbarkeit**
   Um eine langfristige Verfügbarkeit zu erreichen, kann eine kurzfristige Einschränkung bei Funktionalität und Komfort vertretbar sein.
b) **Prinzip des Schutzbedarfs**
   Der Schutzbedarf von IT-Systemen wird vom Schutzbedarf der darauf verarbeiteten, gespeicherten oder übertragenen Daten bestimmt.
c) **Minimalprinzip des Zugriffs**
   Der Zugriff auf IT-Systeme und Daten wird auf die notwendigen Personen und Systeme beschränkt.
d) **Restriktives Nutzungsprinzip**
   Jeder Nutzer oder jede Nutzerin erhält nur die Zugriffsrechte, die er oder sie zur Erfüllung seiner oder ihrer Aufgaben benötigt.
e) **Einbindung aller Nutzerinnen und Nutzer**
   Alle Nutzerinnen und Nutzer werden in den Sicherheitsmanagementprozess zur Unterstützung der Sicherheitsstrategie eingebunden und hinsichtlich der Informationssicherheit sensibilisiert.
f) **Zentrale Rolle der Informationssicherheit**
   Die Informationssicherheit wird bei Änderungen und Neuerungen von Beginn an berücksichtigt.
g) **Verhältnismäßigkeit der Sicherheitsmaßnahmen**
   Aufwand und Ergebnis der eingesetzten Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinanderstehen.
h) **Bereitstellung von Ressourcen**
   Die Hochschulleitung und der Senat unterstützen die Informationssicherheit durch geeignete und verhältnismäßige Maßnahmen und Ressourcen.

4 Verantwortlichkeiten und Organisationsstruktur

Die Rektorin oder der Rektor trägt die Gesamtverantwortung für die Informationssicherheit an der Hochschule Merseburg. Die Verantwortung für die Informationssicherheit in der

Verwaltung trägt der Kanzler oder die Kanzlerin. Näheres regelt die Geschäftsordnung des Rektorates.

Der oder die Informationssicherheitsbeauftragte unterstützt hierbei beratend. Er oder sie ist bei allen Fragen zur Informationssicherheit heranzuziehen.

Folgende Personen oder Organisationseinheiten sind an der Hochschule Merseburg mit dem Thema Informationssicherheit beauftragt:

a) Leitungsebene
Das Rektorat trägt die Verantwortung für die Umsetzung der Informationssicherheit. Näheres regelt die Geschäftsordnung des Rektorates.

b) Informationssicherheitsbeauftragte (ISB)
Der oder die Informationssicherheitsbeauftragte wird durch die Kanzlerin oder den Kanzler benannt. Er oder sie fördert die Informationssicherheit in der Hochschule Merseburg und steuert und koordiniert den Sicherheitsprozess. Der oder die Informationssicherheitsbeauftragte ist Mitglied der Rektoratskommission für Digitalisierung und IT (ReDIT) an der Hochschule Merseburg. Er oder Sie muss neue IT gestützte Fachverfahren freigeben. Der oder die Informationssicherheitsbeauftragte hat die Möglichkeit, dem Rektorat bei Bedarf direkt zu berichten und jederzeit Vor-Ort-Kontrollen durchzuführen. In Abstimmung mit dem oder der Datenschutzbeauftragten, prüft er oder sie ob die Maßnahmen zur Sicherstellung der Informationssicherheit im Einklang mit den datenschutzrechtlichen Bestimmungen stehen.

c) Datenschutzbeauftragte (DSB)
Der oder die Datenschutzbeauftragte wird durch die Kanzlerin oder den Kanzler benannt. Die Aufgaben ergeben sich aus § 20 DSAG LSA. Er oder sie führt das Verzeichnis der Verarbeitungstätigkeiten, nimmt Vorabkontrollen vor und wirkt auf die Einhaltung des Datenschutzes hin. Der oder die Datenschutzbeauftragte wirkt bei der Einhaltung der Meldepflicht von sicherheitsrelevanten Vorfällen bei der Verarbeitung von personenbezogenen Daten mit und ist in dem Prozess zu beteiligen. Der oder die Datenschutzbeauftragte agiert weisungsfrei und hat die Möglichkeit, der Kanzlerin oder den Kanzler bei Bedarf direkt zu berichten und jederzeit Vor-Ort-Kontrollen durchzuführen.

d) Leiter oder Leiterin IT-Servicezentrum
Der Leiter oder die Leiterin des IT-Servicezentrums (ITZ) der Hochschule Merseburg koordiniert und stellt die Umsetzung der technischen Maßnahmen sicher, welche sich aus dem Informationssicherheitsprozess ergeben.

e) Informationssicherheitsmanagement-Team (ISM-Team, AK Datenschutz und Informationssicherheit)
Das ISM-Team berät und unterstützt den oder die Informationssicherheitsbeauftragte bei der Umsetzung und Steuerung des Informationssicherheitsprozesses. Außerdem wird der oder die Datenschutzbeauftragte bei der Einschätzung schwerwiegender Datenschutzverletzungen unterstützt. Das ISM-Team besteht aus den oben genannten Personen und oder Ihren Vertretern und Vertreterinnen, sowie im Bedarfsfall aus Vertretern und Vertreterinnen der Anwender, Mitgliedern der Personalvertretung und dem oder der Digitalisierungsbeauftragen.

Alle Nutzerinnen und Nutzer sind dafür verantwortlich, dass die Sicherheitsmaßnahmen in dem von ihnen beeinflussbaren Bereich umgesetzt werden. Hierbei werden sie durch wiederholte sensibilisierende Schulung und Benutzerbetreuung am Arbeitsplatz durch den Informationssicherheitsbeauftragten oder die Informationssicherheitsbeauftragte unter

stützt. Im Rahmen der jeweiligen Möglichkeiten sollen die Nutzerinnen und Nutzer Sicherheitsvorfälle von innen und außen vermeiden sowie sicherheitsrelevante Ereignisse den Zuständigen umgehend melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können, mit dem Ziel, Gefahren abzuwenden und zu vermeiden. Hierzu werden nutzerfreundliche Handlungsanweisungen zur Verfügung gestellt.

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme werden in den Bereichen verantwortliche Personen benannt, die den jeweiligen Schutzbedarf und die Zugriffsberechtigungen bestimmen. Dabei sind unter Berücksichtigung von Finanzierbarkeit und Wirtschaftlichkeit die jeweils angemessenen Sicherheitsmaßnahmen zu ergreifen.

5 Fortschreibung

Im Rahmen des Informationssicherheitsprozesses wird diese Leitlinie anlassbezogen durch den Informationssicherheitsbeauftragten oder die Informationssicherheitsbeauftragte, spätestens aber nach 24 Monaten, auf ihre Aktualität hin überprüft und gegebenenfalls aktualisiert.

6 Inkrafttreten

Die Leitlinie tritt am Tag nach der Veröffentlichung in Kraft.

Merseburg, 07. Januar 2021

Prof. Dr. Jörg Kirbs
Rektor

Dr. Karen Ranft
Kanzlerin