  

  

  DFN-CERT Services GmbH Logo

Informationssicherheit und Datenschutz

Technische und organisatorische Maßnahmen entsprechend der Vorgaben der EU-DSGVO und dem DSG NRW n. F.

Änderungshistorie

|  |  |  |
| --- | --- | --- |
| Was | Wer | Wann |
| Initiale Version V1 | Projektteams | 31.12.2018 |
|  |  |  |

Die Nutzung dieses Dokuments ist zulässig unter der Lizenz **CC BY-SA 3.0**    
<https://creativecommons.org/licenses/by-sa/3.0/de/legalcode>  
Autor: Projektgruppen zur Umsetzung der EU-DSGVO an den Hochschulen in NRW, „Datenschutzmanagementsysteme“ und „Sensibilisierung“ 2018

Inhaltsverzeichnis

[Einleitung 5](#_Toc1727292)

[Technische und organisatorische Maßnahmen 6](#_Toc1727293)

[1.1 Vorgehensweise 6](#_Toc1727294)

[1.2 Informationssicherheitsmanagement 7](#_Toc1727295)

[1.2.1 Gesamtverantwortung für Informationssicherheit und Festlegung der Sicherheitsziele und -strategie 7](#_Toc1727296)

[1.2.2 Organisation der Informationssicherheit / Verantwortlichkeiten 7](#_Toc1727297)

[1.2.3 Grundsätze für den Einsatz von Informationstechnik 8](#_Toc1727298)

[1.2.4 Umgang mit Sicherheitsvorfällen / Abwehr von Gefahren 8](#_Toc1727299)

[1.2.5 Aufrechterhaltung der Informationssicherheit 9](#_Toc1727300)

[1.2.6 Integration der Mitarbeiter in den Sicherheitsprozess 9](#_Toc1727301)

[1.2.7 Regelmäßige Berichte zur Informationssicherheit 10](#_Toc1727302)

[1.2.8 Anforderungsmanagement / Compliance 10](#_Toc1727303)

[1.2.9 Zusätzliche Maßnahmen 11](#_Toc1727304)

[1.3 Organisation und Personal 12](#_Toc1727305)

[1.3.1 Festlegung von Verantwortlichkeiten 12](#_Toc1727306)

[1.3.2 Aufgabenverteilung und Funktionstrennung 12](#_Toc1727307)

[1.3.3 Berechtigungsmanagement (Zutritt, Zugang, Zugriff) 13](#_Toc1727308)

[1.3.4 Arbeitsplätze / Regelungen für Mitarbeiter 13](#_Toc1727309)

[1.3.5 Einweisung und Beaufsichtigung von Fremdpersonen 14](#_Toc1727310)

[1.3.6 Kryptographie 14](#_Toc1727311)

[1.3.7 Umgang mit mobilen Endgeräten und Datenträgern 15](#_Toc1727312)

[1.3.8 Entsorgung von schützenswerten Betriebsmitteln und Daten 16](#_Toc1727313)

[1.3.9 Angemessene Personalausstattung 16](#_Toc1727314)

[1.3.10 Sorgfältige Personalauswahl 17](#_Toc1727315)

[1.3.11 Verfahren bei Einstellung und Ausscheiden von Mitarbeitern 17](#_Toc1727316)

[1.3.12 Qualifizierung und Schulung 18](#_Toc1727317)

[1.3.13 Zusätzliche Maßnahmen 18](#_Toc1727318)

[1.4 Hard- und Softwareeinsatz 20](#_Toc1727319)

[1.4.1 Standardisierung und Beschaffung 20](#_Toc1727320)

[1.4.2 Kontrollierter Hard- und Softwareeinsatz 20](#_Toc1727321)

[1.4.3 Softwareentwicklung 21](#_Toc1727322)

[1.4.4 Test- und Freigabeverfahren 21](#_Toc1727323)

[1.4.5 Planung, Dokumentation und Umsetzung von Fach- und IT-Verfahren 22](#_Toc1727324)

[1.4.6 Zentralisierung wichtiger Dienste und IT-Verfahren 22](#_Toc1727325)

[1.4.7 Zusätzliche Maßnahmen 24](#_Toc1727326)

[1.5 Infrastruktur 25](#_Toc1727327)

[1.5.1 Sicherheitsbereiche / Serverräume 25](#_Toc1727328)

[1.5.2 Sicherung der Netzknoten und deren Verkabelung 25](#_Toc1727329)

[1.5.3 Elektrotechnik 26](#_Toc1727330)

[1.5.4 Klimatisierung 26](#_Toc1727331)

[1.5.5 Brandschutz 27](#_Toc1727332)

[1.5.6 Schutz vor Wasserschäden 27](#_Toc1727333)

[1.5.7 Regelmäßige Wartung der technischen Infrastruktur 28](#_Toc1727334)

[1.5.8 Überwachung der technischen Infrastruktur 28](#_Toc1727335)

[1.5.9 Zusätzliche Maßnahmen 29](#_Toc1727336)

[1.6 Betrieb der Informationstechnik 31](#_Toc1727337)

[1.6.1 Ordnungsgemäße IT-Administration 31](#_Toc1727338)

[1.6.2 Sichere Installation und Konfiguration von IT-Systemen 32](#_Toc1727339)

[1.6.3 Management von IT-Arbeitsplätzen 33](#_Toc1727340)

[1.6.4 Virtualisierung 34](#_Toc1727341)

[1.6.5 Speichersysteme 34](#_Toc1727342)

[1.6.6 Drucker, Kopierer und sonstige Multifunktionsgeräte 35](#_Toc1727343)

[1.6.7 Patch- und Änderungsmanagement 35](#_Toc1727344)

[1.6.8 Schutz vor Schadsoftware 36](#_Toc1727345)

[1.6.9 Protokollierung und Monitoring 36](#_Toc1727346)

[1.6.10 Regelmäßige technische Sicherheitsprüfungen 37](#_Toc1727347)

[1.6.11 Datensicherung 37](#_Toc1727348)

[1.6.12 Entsorgung von IT-Systemen u. Datenträgern / Reparatur 38](#_Toc1727349)

[1.6.13 Zusätzliche Maßnahmen 39](#_Toc1727350)

[1.7 Netze und Kommunikation 41](#_Toc1727351)

[1.7.1 Netzwerkzugänge 41](#_Toc1727352)

[1.7.2 Geeignete Segmentierung des Netzwerks 41](#_Toc1727353)

[1.7.3 Kommunikation zwischen unterschiedlichen Sicherheitsniveaus 42](#_Toc1727354)

[1.7.4 Sichere Installation und Konfiguration von aktiven Netzkomponenten 43](#_Toc1727355)

[1.7.5 Netzwerkmanagement- und Monitoring 43](#_Toc1727356)

[1.7.6 Zusätzliche Maßnahmen 44](#_Toc1727357)

[1.8 Datenschutz 47](#_Toc1727358)

[1.9 Datenminimierung 48](#_Toc1727359)

[1.10 Vertraulichkeit 48](#_Toc1727360)

[1.11 Integrität 49](#_Toc1727361)

[1.12 Verfügbarkeit 50](#_Toc1727362)

[1.13 Transparenz 50](#_Toc1727363)

[1.14 Intervenierbarkeit 51](#_Toc1727364)

[1.15 Nichtverkettung 52](#_Toc1727365)

[1.16 Weitere Maßnahmen 53](#_Toc1727366)

[1.16.1 Pseudonymisierung und Anonymisierung 53](#_Toc1727367)

[1.16.2 Auftragsverarbeitung 53](#_Toc1727368)

[1.16.3 Durchführung von Datenschutzaudits 54](#_Toc1727369)

# Einleitung

Die Hochschulen in Nordrhein-Westfalen (NRW) setzen in hohem Maße IT-Infrastruktur in ihren Geschäftsprozessen ein. Dies gilt sowohl für die Kernprozesse in Forschung und Lehre als auch in der Verwaltung. Im Rahmen der Digitalisierung ist zukünftig mit einem steigenden Einsatz von Informationstechnik zu rechnen.

Auf Grund von gesetzlichen Anforderungen (z.B. Datenschutz), vertraglichen Anforderungen (z.B. Revisionspflicht gegenüber Drittmittelgebern) und der Selbstverpflichtung ist ein zuverlässiger und sicherer Einsatz der Informationstechnologie zu gewährleisten.

Mit dieser Handreichung sollen die Hochschulen unterstützt werden, ein angemessenes Sicherheitsniveau mit einem vertretbaren Aufwand zu erreichen. Um dieses Ziel zu erreichen, enthält dieses Dokument eine Zusammenstellung wesentlicher Sicherheitsmaßnahmen aus dem IT-Grundschutz und der internationalen Normung, üblich als Best Practices bezeichnet.

Bei der Einführung von neuen IT-Verfahren muss mittels einer Schutzbedarfsfeststellung und ggf. einer Schwellwertanalyse geprüft werden, ob die getroffenen Maßnahmen ausreichend sind oder die Umsetzung zusätzlicher Maßnahmen erforderlich ist.

*Anmerkung:*

*Diese Handreichung ersetzt nicht die Etablierung eines Managementsystems und die Erstellung einer Sicherheitskonzeption, sondern ist lediglich als Hilfestellung für die agierenden Personen gedacht. Die Revisionsfähigkeit erfordert eine kontinuierliche Dokumentation in den Bereichen Informationssicherheit und Datenschutz, damit Entwicklungen und Entscheidungen nachvollziehbar zurückverfolgt werden können. In Sicherheitskonzepten müssen die konkreten Sicherheitsmaßnahmen beschrieben und deren Umsetzung dokumentiert werden.*

*Es muss bei Störungen oder Sicherheitsvorfällen möglich sein, den gewünschten Soll-Zustand der Geschäftsprozesse und der Informationstechnik wiederherzustellen. Technische Einzelheiten und Arbeitsabläufe sind daher so zu dokumentieren, dass dies in angemessener Zeit möglich ist.*

# Technische und organisatorische Maßnahmen

## Vorgehensweise

Die Zusammenstellung der wesentlichen Sicherheitsmaßnahmen (Best Practices), die sich für eine Standard- bzw. Grundabsicherung etabliert haben, gliedert sich in folgende Themenbereiche:

* Informationssicherheitsmanagement
* Organisation und Personal
* Hard- und Softwareeinsatz
* Infrastruktur
* Betrieb der Informationstechnik
* Netze und Kommunikation
* Datenschutz

Die Beschreibung jeder Maßnahme ist wie folgt gegliedert:

* Verantwortlichkeiten

Zu jeder Sicherheitsmaßname werden Rollen genannt, die üblicherweise für die Initiierung und für die Umsetzung verantwortlich sind. Es werden überwiegend die in den Anhängen zum Sensibilisierungskonzept eingeführten Rollenbezeichnungen verwendet.

* Beschreibung

Jede Sicherheitsmaßnahme wird kurz erläutert, so dass deutlich wird, was die Zielsetzung der konkreten Ausprägung einer Maßnahme sein soll, bzw. welche Gefährdungen damit adressiert werden.

* Umsetzungshinweise/Dokumentation

Dieses Feld enthält Hinweise, in welcher Form eine Umsetzung erfolgen kann und welche Hilfsmittel zielführend sein können.

Am Ende jedes Abschnitts sind Hinweise aufgeführt, welche Maßnahmen bei einem erhöhten Schutzbedarf in Betracht gezogen werden können, um das in der Risikoanalyse bestimmte Schutzniveau erreichen zu können.

## Informationssicherheitsmanagement

### Gesamtverantwortung für Informationssicherheit und Festlegung der Sicherheitsziele und -strategie

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung |
| Verantwortlich für die Umsetzung |  | Organisationsleitung, CIO |
| Die Gesamtverantwortung für Informationssicherheit trägt die Hochschulleitung. Der Sicherheitsprozess muss durch die Leitung der Hochschule initiiert, gesteuert und kontrolliert werden. Ebenso muss sich die Hochschulleitung sich über mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen informieren lassen. Dafür müssen Sicherheitsziele sowie eine Strategie für Informationssicherheit festgelegt und dokumentiert werden. | | |
| Umsetzung / Dokumentation |  | Leitlinie zur Informationssicherheit[[1]](#footnote-1) |

### Organisation der Informationssicherheit / Verantwortlichkeiten

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung |
| Verantwortlich für die Umsetzung |  | CIO, CISO |
| Die Hochschulleitung muss festlegen, wie die Organisation der Informationssicherheit erfolgen und der Sicherheitsprozess umgesetzt werden soll. Üblicherweise benennt die Hochschulleitung einen Informationssicherheits-beauftragten (CISO) und stattet diesem mit angemessenen Ressourcen und Befugnissen aus, so dass ein Informationssicherheitsmanagementsystem (ISMS) implementiert und betrieben werden kann.  Der CISO muss bei allen größeren Projekten sowie bei der Einführung neuer Anwendungen, Fachverfahren bzw. IT-Verfahren frühzeitig beteiligt werden. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung (Verankerung), ggf. Richtlinie zum ISMS |

### Grundsätze für den Einsatz von Informationstechnik

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung |
| Verantwortlich für die Umsetzung |  | CIO |
| Die Grundvoraussetzungen für den Einsatz von Informationstechnik müssen kommuniziert und dokumentiert werden. Insbesondere muss sichergestellt werden, dass   * keine Gefährdungen für die IuK-Infrastruktur der Hochschule ausgehen und * das Ansehen der Hochschule keinen Schaden nehmen darf.   Ebenso müssen Beschaffung, Entwicklung und der Einsatz von IT-Verfahren nach den Vorgaben der Hochschule erfolgen. Ebenso sind die Rechte und Pflichten der Nutzer und Betreiber festzulegen. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung, ggf. Nutzungsordnung |

### Umgang mit Sicherheitsvorfällen / Abwehr von Gefahren

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | CISO, zentraler IT-Betreiber |
| Die Behandlung von Sicherheitsvorfällen ist eine wichtige Aufgabe des Informationssicherheitsmanagements. Primäre Zielsetzung ist die Schadens-minimierung und die Verhinderung von Sicherheitsvorfällen. Dazu ist eine geeignete Vorgehensweise zur Behandlung von Sicherheitsvorfällen zu etablieren, um die Reaktionsfähigkeit und Handlungsfähigkeit sicherzustellen. Durch Dokumentation und Aufarbeitung der Sicherheitsvorfälle soll der Sicherheitsprozess kontinuierlich verbessert werden (‚Lessons Learned‘). Diese Aufgaben werden üblicherweise durch ein Computer Emergency Response Team (CERT)[[2]](#footnote-2) wahrgenommen.  Bei Gefahr im Verzuge kann der CISO eine vorübergehende Stilllegung betroffener IT-Systeme bzw. eine Sperrung von Netzanschlüssen (ggf. auch ohne vorherige Benachrichtigung der Betroffenen) anordnen, wenn zu befürchten ist, dass ein gravierender Schaden nicht anders abzuwenden ist. Die Wiederinbetriebnahme nach Stilllegung bzw. Sperrung erfolgt erst nach der Durchführung hinreichender Sicherheitsmaßnahmen in Abstimmung mit dem CISO. Bei Vorfällen, die möglicherweise Straftatbestände berühren, ist eine Abstimmung mit dem Justiziariat (/Rechtsabteilung) der Hochschule erforderlich. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung |

### Aufrechterhaltung der Informationssicherheit

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | CISO, Revision |
| Die Prozesse und Dokumente des ISMS (u.a. Leitlinie, Ordnungen, Richtlinien und Sicherheitskonzepte) müssen regelmäßig auf Wirksamkeit und Angemessenheit überprüft und aktualisiert werden. Ebenso müssen technische und organisatorische Maßnahmen regelmäßig auf ihre Umsetzung, Einhaltung und Eignung überprüft werden, um das angestrebte Sicherheitsniveau aufrechtzuerhalten und fortlaufend zu verbessern.  Diese Prüfungen/Audits sollten regelmäßig (jährlich) sowie anlassbezogen durchgeführt werden. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung, ggf. Richtlinie zum ISMS |

### Integration der Mitarbeiter in den Sicherheitsprozess

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Bereichsleitung (Vorgesetzte) |
| Verantwortlich für die Umsetzung |  | Prozessverantwortliche, CISO, IT-Beauftragte |
| Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter, Angehörige und Gäste einer Hochschule, daher muss jeder Einzelne, entsprechend seiner Aufgabenstellung, durch geeignete Maßnahmen (z.B. Schulung und Sensibilisierung) in die Lage versetzt werden, Schäden durch verantwortungsbewusstes Handeln zu vermeiden. Dies wird nur gelingen, wenn aktuelle Gefährdungen kommuniziert werden und alle Mitarbeiter die Sicherheitsmaßnahmen kennen und umsetzen, die ihr Arbeitsumfeld betreffen. | | |
| Umsetzung / Dokumentation |  | Schulungs- u. Sensibilisierungskonzept |

### Regelmäßige Berichte zur Informationssicherheit

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | CISO |
| Die Hochschulleitung (CIO, entsprechende Gremien) sollte regelmäßig über den Stand der Informationssicherheit informiert werden. Diese Berichte sollen Informationen über die aktuelle Gefährdungslage, identifizierte Risiken sowie über Wirksamkeit und Effizienz des Sicherheitsprozesses enthalten. Sofern erforderlich sind klar priorisierte und mit realistischen Abschätzungen des zu erwartenden Umsetzungsaufwands versehene Maßnahmenvorschläge beizufügen.  Die Management-Entscheidungen über erforderliche Aktionen, Umgang mit Restrisiken und mit Veränderungen von sicherheitsrelevanten Prozessen müssen dokumentiert werden. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung, ggf. Richtlinie zum ISMS |

### Anforderungsmanagement / Compliance

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung |
| Verantwortlich für die Umsetzung |  | CIO, Prozessverantwortliche |
| Wie in jeder Institution gibt es auch für Hochschulen gesetzliche, vertragliche, strukturelle und interne Richtlinien/Vorgaben, die beachtet werden müssen. Diese Rahmenbedingungen und Anforderungen müssen identifiziert und dokumentiert werden, wenn diese Auswirkungen auf die Informationssicherheit und Datenschutz haben. Die Organisationsleitung muss die Einhaltung der Anforderungen durch die Etablierung von angemessenen Prozessen und Überwachungsmaßnahmen sicherstellen.  Ebenso muss der Umgang mit Ausnahmen geregelt und dokumentiert werden. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung, ggf. Richtlinie Compliance-Management |

### Zusätzliche Maßnahmen

#### Zielgruppenspezifische Richtlinien / Arbeitsanweisungen

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | CISO, Datenschutzbeauftragte |
| In Abhängigkeit vom Schutzbedarf der Fach- bzw. IT-Verfahrens der Hochschule kann es zielführend sein, für einzelne Mitarbeiter oder Organisationseinheiten zielgruppenspezifische Regelungen zu erstellen, beispielsweise bei der Verarbeitung von personenbezogen, finanzrelevanten oder sonstigen vertraulichen Daten. | | |
| Umsetzung / Dokumentation |  | Spezifische Richtlinie oder Arbeitsanweisung |

#### Aufrechterhaltung der Informationssicherheit II

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | CISO, Datenschutzbeauftragte, Revision |
| Bei Fach- bzw. IT-Verfahren mit einem höheren Schutzbedarf sollten die regelmäßigen Prüfungen/Audits in kürzeren Zeitabständen durchgeführt werden, um entsprechend auf Bedrohungen und Risiken reagieren zu können. | | |
| Umsetzung / Dokumentation |  | Spezifische Regelung |

## Organisation und Personal

### Festlegung von Verantwortlichkeiten

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung, CIO |
| Verantwortlich für die Umsetzung |  | Prozessverantwortliche, IT-Verfahrensverantwortliche, CISO |
| Für alle Informationen, Geschäftsprozesse, Anwendungen und IT-Systeme der Hochschule muss festgelegt werden, wer für diese und deren Sicherheit verantwortlich ist. Die Verantwortungsbereiche sind so zu gestalten, dass es keine Zuständigkeitslücken oder Überschneidungen gibt. Für alle wesentlichen Geschäftsprozesse und Aufgaben müssen auch praktikable Vertretungsregelungen etabliert werden. Voraussetzung dafür ist, dass die entsprechende Dokumentation vollständig und aktuell ist und die Vertreter über die erforderlichen Kenntnisse verfügen. Das Prinzip der Funktionstrennung darf nicht verletzt werden.  Darüber hinaus muss geregelt sein, welche Informationen mit wem ausgetauscht werden dürfen und wie diese dabei zu schützen sind. Alle betroffenen Angehörigen der Hochschule müssen Kenntnis von diesen Regelungen haben. | | |
| Umsetzung / Dokumentation |  | Richtlinie, Verfahrensdokumentation, Betriebshandbücher, Intranet |

### Aufgabenverteilung und Funktionstrennung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche |
| In der Hochschule sollen alle relevanten Aufgaben und Funktionen in Bezug auf die Informationstechnik und IT-Verfahren definiert und voneinander abgegrenzt werden. Neben der Aufgabenverteilung muss festgelegt und dokumentiert werden, welche Funktionen (Rollen) nicht miteinander vereinbar sind und nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Eine Trennung ist grundsätzlich zwischen operativen und kontrollierenden Rollen (z.B. Systemadministration und Revision) vorzunehmen. Weitere Vorgaben können sich auch aus rechtlichen Bestimmungen ergeben (u. a. Datenschutz). Abschließend erfolgt eine Zuordnung von Rollen zu Mitarbeiterinnen und Mitarbeitern. | | |
| Umsetzung / Dokumentation |  | Rollen- u. Berechtigungskonzepte (u.a. Betriebshandbücher, Verfahrensdokumentation) |

### Berechtigungsmanagement (Zutritt, Zugang, Zugriff)

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Prozessverantwortliche (, IT-Betreiber) |
| Verantwortlich für die Umsetzung |  | IT-Betreiber, Haustechnik, IT-Verfahrensverantwortliche |
| Jede Person benötigt zur Wahrnehmung ihrer Aufgabe entsprechende Zutritts-, Zugangs- und Zugriffsrechte. Für die Vergabe und den Entzug dieser Berechtigungen (u.a. Schlüssel, Chipkarten, Transponder, Benutzeraccounts) müssen geregelte Verfahren etabliert sein. Die Dokumentation der Berechtigungen muss aktuell und vollständig sein, so dass jederzeit nachvollziehbar ist, wer über welche Berechtigungen verfügt. Grundsätzlich sind Berechtigungen möglichst restriktiv zu vergeben, d.h. nur wie es für die Aufgabenwahrnehmung notwendig ist ("Need-to-Know-Prinzip"). Grundlage hierfür ist die Aufgabenverteilung und Funktionstrennung. | | |
| Umsetzung / Dokumentation |  | Rollen- u. Berechtigungskonzepte, Schlüsselbuch |

### Arbeitsplätze / Regelungen für Mitarbeiter

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | Mitarbeiterinnen, Mitarbeiter, IT-Personal, Haustechnik |
| Alle IT-Arbeitsplätze in der Hochschulverwaltung verfügen über angemessene Schutzmaßnahmen (u.a. AV-Scanner, lokale Firewall, Bildschirmsperre) und verfügen über aktuelle und lizensierte Software- und Betriebssystemversionen. Den Mitarbeitern ist nicht gestattet, diese Schutzmaßnahmen zu deaktivieren, auch ist die Installation von Software untersagt (dazu auch die Abschnitte 2.4.2 u. 2.6.3). Jeder Mitarbeiter ist verpflichtet, bei Abwesenheit vom Arbeitsplatz sicherzustellen, dass keine sensiblen Informationen / Unterlagen oder mobilen Datenträgern frei zugänglich sind. Dazu müssen die Büroräume mit verschließbaren Behältnissen ausgestattet werden. Sind Büroräume oder sonstige Arbeitsbereiche öffentlich zugänglich, dann sind diese zu verschließen, wenn sie nicht besetzt sind. | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie für Mitarbeiter[[3]](#footnote-3) |

### Einweisung und Beaufsichtigung von Fremdpersonen

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, CISO |
| Verantwortlich für die Umsetzung |  | Mitarbeiterinnen, Mitarbeiter |
| Fremdpersonen, wie beispielsweise Gäste, Dienstleister, Handwerker, Wartungs- und Reinigungspersonal dürfen sich nicht unbeaufsichtigt in Sicherheitsbereichen der Hochschule aufhalten.  Der Aufenthalt von Fremdpersonen in Arbeitsbereichen (Büroräume) ist nur statthaft, wenn keine Datenträger, Dokumente oder IT-Systeme zugänglich sind.  Bei Arbeiten an IT-Systemen mit erhöhtem Schutzbedarf, muss die Beaufsichtigung durch fachkundiges IT-Personal erfolgen, so dass nicht autorisierte Handlungen erkannt werden können. Diese Arbeiten sind zu dokumentieren. | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie für Mitarbeiter |

### Kryptographie

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, CISO |
| Verantwortlich für die Umsetzung |  | IT-Betreiber |
| In der Hochschule sollte übergreifend festgelegt sein, welche kryptographische Verfahren und ggf. Produkte eingesetzt werden dürfen, um bei gespeicherten oder übertragenden Daten die Vertraulichkeit, Integrität und Authentizität zu gewährleisten.  Damit rechtliche Anforderungen erfüllt werden, sollten die technischen Richtlinien des BSI[[4]](#footnote-4) berücksichtigt werden. Diese enthalten Empfehlungen zu kryptographischen Mechanismen, Schlüssellängen und Protokollen. | | |
| Umsetzung / Dokumentation |  | Richtlinie |

### Umgang mit mobilen Endgeräten und Datenträgern

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, CISO |
| Verantwortlich für die Umsetzung |  | Mitarbeiterinnen, Mitarbeiter |
| Die Nutzung mobiler Endgeräte (u.a. Notebooks und Tablets) stellt ein erhöhtes Risiko für Informationen (Verlust oder Kompromittierung) und die IT-Infrastruktur der Hochschule dar. Daher müssen bei mobilen Endgeräten zusätzliche Sicherheitsmaßnahmen umgesetzt werden, um diesen Gefährdungen angemessen begegnen zu können. Dazu zählen u.a.: die Sensibilisierung der über die Risiken, Authentifizierung des Benutzers und Sperrung des Geräts bei Inaktivität und Deaktivierung nicht benutzter Kommunikationsschnittstellen.  Für die Nutzung von mobilen Datenträgern sollten folgende grundlegende Aspekte geregelt sein:   * Festlegung, welche Informationen auf Datenträgern gespeichert werden dürfen und wie diese vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden müssen (Verschlüsselung). * Weitergabe von Datenträgern an Dritte oder Dienstleister. * Vorgaben zur Löschung von Datenträgern. * Maßnahmen zum Schutz vor Schadsoftware. * Nutzung privater Datenträger   Für die Verschlüsselung der Datenträger und ggf. für die Nutzung eines VPN-Zugangs zum Netzwerk der Hochschule, werden durch den zentralen IT-Betreiber geeignete Sicherheitsdienste zur Verfügung gestellt (dazu auch die Abschnitte 2.4.7.2 u. 2.7.6.4). | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie für Mitarbeiter |

### Entsorgung von schützenswerten Betriebsmitteln und Daten

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CISO, Datenschutzbeauftragte |
| Verantwortlich für die Umsetzung |  | Mitarbeiterinnen, Mitarbeiter |
| Es sind Regelungen zu treffen, die das Löschen und die Entsorgung schützenswerter Betriebsmittel und Informationen betreffen. Alle Mitarbeiter müssen Kenntnis haben, unter welchen Voraussetzungen die Löschung und Entsorgung zu erfolgen hat, bzw. wo entsprechende Entsorgungs- und Vernichtungseinrichtungen zur Verfügung stehen.  Erfolgt die Entsorgung durch Outsourcing-Dienstleister, dann sollte die ordnungsgemäße Durchführung regelmäßige überprüft werden.  Darüber hinaus sollte festgelegt sein, mit welchen technischen Methoden und Verfahrensweisen IT-Systeme, Datenträger und sonstige Betriebsmittel behandelt werden. | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie für Mitarbeiter |

### Angemessene Personalausstattung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche |
| Ein zuverlässiger und sicherer Betrieb der IT-Infrastruktur und der IT-Verfahren erfordert eine angemessene Personalausstattung. Die Personalausstattung muss so bemessen sein, dass für die IT-Infrastruktur und IT-Verfahren mit zentraler Bedeutung für die Hochschule, die Dienstqualität sowie Anforderungen hinsichtlich Informationssicherheit und Datenschutz jederzeit ausreichend gewährleistet werden können. | | |
| Umsetzung / Dokumentation |  | Stellenplan |

### 

### Sorgfältige Personalauswahl

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung (Vorgesetzte) |
| Verantwortlich für die Umsetzung |  | Beteiligte bei der Personalauswahl |
| Für sensible Aufgabenbereiche, beispielsweise die Administration auf Netzwerk- und Systemebene, sollten nur ausgewählte, ausreichend qualifizierte und vertrauenswürdige Mitarbeiter betraut werden. Daher sollte bei der Personalauswahl mit der gebotenen Sorgfalt vorgegangen und die vorgelegten Unterlagen auf ihre Glaubhaftigkeit hin überprüft werden.  Befristet beschäftigte Mitarbeiter sollten nach Möglichkeit keine sensiblen Aufgaben übernehmen, die nur mit Administratorrechten ausgeführt werden können. | | |
| Umsetzung / Dokumentation |  | Bewerbungsgespräch, Prüfung von Unterlagen. |

### Verfahren bei Einstellung und Ausscheiden von Mitarbeitern

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung (Vorgesetzte) |
| Verantwortlich für die Umsetzung |  | Vorgesetzte, Personalabteilung, IT-Personal |
| Alle Mitarbeiter müssen in ihre neuen Aufgaben eingearbeitet und in die Benutzung der IT-Systeme eingewiesen bzw. geschult werden, die sie für ihre Aufgabenerfüllung benötigen. Ebenso müssen sie darauf verpflichtet werden, einschlägige Gesetze, Vorschriften und interne Regelungen (u.a. Umgang mit sensiblen Informationen und personenbezogenen Daten) einzuhalten.  Durch die Personalabteilung sollten die erforderlichen Prozesse angestoßen werden, um den Mitarbeiter mit den erforderlichen Betriebsmitteln und Berechtigungen auszustatten. Verlässt ein Mitarbeiter die Hochschule, müssen alle im Rahmen ihrer Tätigkeit erhaltenen Unterlagen, Betriebsmittel und Berechtigungen eingezogen, bzw. gelöscht werden. Auch sollte noch einmal auf Verschwiegenheits-verpflichtungen hingewiesen werden. | | |
| Umsetzung / Dokumentation |  | Dienstanweisung |

### Qualifizierung und Schulung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche |
| Das IT-Personal soll entsprechend ihrer Tätigkeiten regelmäßig geschult werden, damit sie auf dem aktuellen Stand der Technik sind. Ebenso sollte die Möglichkeit gegeben werden, dass sich die Mitarbeiter im Rahmen ihres Tätigkeitsfeldes weiterqualifizieren können.  Darüber hinaus sollten alle Mitarbeiter regelmäßig in den Bereichen Informationssicherheit und Datenschutz geschult werden, um aktuelle Regelungen, Bedrohungen und mögliche Gegenmaßnahmen zu vermitteln und um einen ausreichenden Grad der Sensibilisierung sicherzustellen. Die erfolgreiche Teilnahme an einer Schulungsmaßnahme sollte geeignet dokumentiert werden. | | |
| Umsetzung / Dokumentation |  | Interne Regelungen |

### Zusätzliche Maßnahmen

#### Klassifizierung von Informationen

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | CISO, Datenschutzbeauftragte, Revision |
| An Hochschulen gibt es in vielen Bereichen Informationen, die einen höheren Schutzbedarf haben oder besonderen Restriktionen unterliegen, z. B. personenbezogene, finanzrelevante, vertrauliche oder sonstige geschützte Daten. Je nach Art unterliegen diese Informationen unterschiedlichen Beschränkungen im Umgang mit ihnen. Daher sollten alle Informationen entsprechend ihrem Schutzbedarf klassifiziert und, soweit möglich, gekennzeichnet werden (z.B. öffentlich, intern, vertraulich und ggf. geheim). Mitarbeiter, die regelmäßig mit klassifizierten Informationen arbeiten, müssen auf den sorgfältigen Umgang hingewiesen und über Restriktionen informiert werden. | | |
| Umsetzung / Dokumentation |  | Spezifische Regelung, ggf. IT-Ordnung |

#### Vertiefende Schulungen für Mitarbeiter in besonderen Funktionen

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CISO |
| Verantwortlich für die Umsetzung |  | Prozessverantwortliche, IT-Betreiber |
| Mitarbeiter, die in der Wahrnehmung ihrer Funktion Zugang zu Informationen mit einem hohen oder sehr hohen Schutzbedarf haben oder IT-Systeme administrieren, mit denen diese Informationen verarbeitet werden, sollten entsprechend ihrer Tätigkeiten vertiefende Schulungen in Hinblick auf die spezifischen Gefährdungen erhalten. | | |
| Umsetzung / Dokumentation |  | Interne Regelungen |

#### Notfallvorsorge

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche, IT-Betreiber |
| Unter Notfall ist eine Situation zu verstehen, in der durch eine Betriebsstörung, einen Sicherheitsvorfall oder höhere Gewalt die Sicherheit der Informationstechnik und der Schutz der Daten nicht mehr gegeben ist. Üblicherweise ist ein Notfall mit einer verhältnismäßig hoher Schadenswirkung verbunden.  In Notfallplänen sollen u.a. Regelungen zu Verantwortlichkeiten, zum Wiederanlauf von IT-Systemen, zur Wiederherstellung von Daten und zum Einsatz von Ausweichmöglichkeiten enthalten sein. Mindestens sollte ein Alarmierungsplan erstellt werden, in dem die Meldewege und die Kontaktdaten der beteiligten Stellen und Personen im Notfall beschrieben sind. | | |
| Umsetzung / Dokumentation |  | Notfallhandbücher, Alarmierungspläne |

## Hard- und Softwareeinsatz

### Standardisierung und Beschaffung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung, CIO |
| Verantwortlich für die Umsetzung |  | Zentraler IT-Betreiber, IT-Beauftragte, Einkauf |
| Durch eine Standardisierung der IT-Landschaft soll eine optimale Verwendung der zur Verfügung stehenden Ressourcen erreicht, die Qualität des Betriebs gesteigert und ein angemessenes und ausreichendes Sicherheitsniveau erreicht werden. Die Standards werden auf Grundlage der vom CIO formulierten Strategie durch den zentralen IT-Betreiber, unter Berücksichtigung der Bedürfnisse der Bereiche und zentralen Einrichtungen, entwickelt und regelmäßig an die Anforderungen angepasst. Die Beschaffung von Soft- und Hardware erfolgt grundsätzlich über Rahmenverträge durch den zentralen Einkauf der Hochschule. Die eingesetzten IT-Systeme (Hard- und Software) müssen dokumentarisch erfasst werden (Asset Management). | | |
| Umsetzung / Dokumentation |  | IT-Ordnung (Verankerung), Liste der Standard IT-Systeme, Asset-Management |

### Kontrollierter Hard- und Softwareeinsatz

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung, CIO |
| Verantwortlich für die Umsetzung |  | Zentraler IT-Betreiber, IT-Beauftragte, Mitarbeiter |
| Um die Sicherheit von zentralen IT-Verfahren gewährleisten zu können, dürfen mit den Netzen der Hochschulverwaltung nur IT-Systeme verbunden werden, die durch den zentralen IT-Betreiber freigegeben wurden. Die Installation von nicht freigegebener, privater oder aus dem Internet heruntergeladener Software ist auf diesen IT-Systemen grundsätzlich verboten. Nur so kann sichergestellt werden, dass die Software aus einer zuverlässigen Quelle stammt, die Lizenzierung gegeben ist und Sicherheitsvorgaben eingehalten werden.  Für alle anderen an der Hochschule betriebenen IT-Systeme ist kein oder nur ein eingeschränkter Zugriff auf zentrale Dienste möglich. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung (Verankerung) bzw. Richtlinie |

### Softwareentwicklung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Verfahrensverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Die Entwicklung von Software für IT-Verfahren oder das Customizing von Standardsoftware muss nach standardisierten Verfahren durchgeführt werden. Dazu gehören u.a. eine Spezifikation der fachlichen und technischen Anforderungen, ein Projektmanagement und Vorgaben zur Qualitätssicherung und Freigabeverfahren.  Die Entwicklung oder Anpassung von IT-Verfahren darf nicht in der Produktionsumgebung erfolgen, sondern muss in einer separaten Entwicklungsumgebung durchgeführt werden. Die Überführung der Software von der Entwicklung in den Produktivbetrieb bedarf einer Freigabe. In der Entwicklungsumgebung dürfen keine personenbezogenen Daten verwendet werden.  Für kleinere Vorhaben im Rahmen des IT-Betriebs können vereinfachte Verfahren zur Anwendung kommen, jedoch sind die grundlegenden Anforderungen an Dokumentation, Entwicklungsumgebung und Freigabeverfahren zu berücksichtigen. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung o. Richtlinie, Verfahrensdokumentation |

### Test- und Freigabeverfahren

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Verfahrensverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Vor dem Einsatz neuer Software oder neuer Versionen muss auf Testsystemen überprüft werden, ob die technischen und fachlichen Anforderungen eingehalten werden. Es sind grundsätzlich Testsysteme zu verwenden, die von produktiven IT-Systemen getrennt betrieben werden. Das Testergebnis ist zu dokumentieren. Erst nach einem positiven Votum durch den IT-Verfahrensverantwortlichen, dem CISO und ggf. dem Datenschutzbeauftragten darf neue Software/IT-Verfahren in den produktiven Betrieb überführt werden. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung o. Richtlinie, Verfahrensdokumentation |

### Planung, Dokumentation und Umsetzung von Fach- und IT-Verfahren

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | Prozessverantwortliche (fachlich), IT-Verfahrensverantwortliche (operativ) |
| Für jedes Fach- bzw. IT-Verfahren ist eine entsprechende Verfahrensdokumentation zu erstellen. Zu den unverzichtbaren Bestandteilen eines Fach- und Umsetzungskonzepts gehören:   * Zweck des IT-Verfahrens, Verantwortlichkeiten, Nutzungsberechtigte * Systemarchitektur, Komponenten, Datenmodel, Schnittstellen (vollständige Spezifikation in einem Detaillierungsgrad, so dass die anwendungsspezifische Konfiguration daraus abzuleiten ist.) * Schutzbedarfsfeststellung, ggf. Risikoanalyse und DSFA * Rollen und Berechtigungskonzept * Betriebs- und Sicherheitskonzept   Ein Fach- bzw. IT-Verfahren darf erst in die Produktionsphase überführt werden, wenn die Verfahrensdokumentation vollständig vorliegt und freigegeben wurde. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung (Verankerung), Verfahrensdokumentation |

### Zentralisierung wichtiger Dienste und IT-Verfahren

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Organisationsleitung, CIO |
| Verantwortlich für die Umsetzung |  | Zentraler IT-Betreiber, IT-Verfahrens-verantwortliche |
| Um einen sicheren und effizienten Betrieb der Informationstechnik gewährleisten zu können, sind hochschulweit genutzte Dienste und IT-Verfahren grundsätzlich zentral zu betreiben. Dazu zählen insbesondere alle Dienste, die für den Betrieb des Intranets der Hochschule erforderlich sind (u.a. DHCP, DNS, IP-Adressmanagement), sowie Verzeichnisdienste / IDM, E-Mail und Kollaborationsanwendungen. Durch die Zentralisierung von wesentlichen Teilen der Informationstechnik können Ressourcen (z.B. Infrastruktur, IT-Personal) bestmöglich eingesetzt und die Reaktionsfähigkeit bei Sicherheitsvorfällen gesteigert werden.  Dienste und IT-Verfahren, die an den spezifischen Bedürfnissen eines Fachbereichs oder Einrichtung ausgerichtet sind, müssen nicht zwingend zentral betrieben werden, sofern der erforderliche Schutz der verarbeiteten Informationen gewährleistet ist. Voraussetzung dafür ist die Durchführung einer Schutzbedarfsfeststellung und ggf. einer Risikoanalyse. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung (Verankerung), Verfahrensdokumentation, Betriebshandbücher |

### Zusätzliche Maßnahmen

#### Mehr-Faktor-Verfahren für die Authentisierung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CISO |
| Verantwortlich für die Umsetzung |  | Zentraler IT-Betreiber |
| Bei einem erhöhtem Schutzbedarf sollten übliche Methoden der Benutzerauthentisierung, wie beispielsweise Benutzername und Passwort, durch stärkere Verfahren ersetzt werden.  Dazu zählen so genannte Mehr-Faktor-Methoden, bei denen der Benutzer weitere Merkmale besitzen und nachweisen muss. Dies kann der Besitz eines physischen Gegenstands wie eine Smartcard oder Security-Tokens sein oder ein körperliches Merkmal wie der Fingerabdruck oder die Iris.  Mehr-Faktor-Verfahren werden üblicherweise in Verbindung mit VPNs (dazu auch Abschnitt 2.7.6.4 ) eingesetzt. | | |
| Umsetzung / Dokumentation |  | Richtlinie |

#### Bereitstellung von Verschlüsselungsverfahren

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CISO |
| Verantwortlich für die Umsetzung |  | Zentraler IT-Betreiber |
| Sollen sensible Daten auf Datenträgern gespeichert oder übermittelt werden, dann ist Verschlüsselung ein adäquates Mittel (z.B. §34 EU-DSGVO[[5]](#footnote-5)).  Auf Grundlage der Kryptographie-Richtlinie sollten entsprechende Lösungen für Datei- bzw. Festplattenverschlüsselung und für die Absicherung von E-Mails bereitgestellt werden. | | |
| Umsetzung / Dokumentation |  | Richtline |

## Infrastruktur

### Sicherheitsbereiche / Serverräume

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | IT-Betreiber, Gebäudemanagement |
| Alle IT-Systeme, die für die Erbringung zentraler Dienste und IT-Verfahren erforderlich sind (u.a. Server, Speichersysteme, aktive Netzkomponenten) müssen in separaten, besonders gesicherten Räumen aufgestellt werden. Je nach Schutzbedarf und in Abhängigkeit der Lage der Sicherheitsbereiche (z.B. öffentlich zugängliche Bereiche) sind entsprechende bauliche und technische Sicherheitsmaßnahmen zu treffen, beispielsweise durch den Verbau von Wänden, Türen u. Fenstern mit hohen Widerstandsklassen oder einer Gefahrenmeldeanlage, um ein gewaltsames Eindringen zu verhindern. Alle IT-Komponenten sind in verschließbaren Schutzschränken unterzubringen  Für den Schutz gegen unbefugten Zutritt zu einem Sicherheitsbereich muss ein Zutrittskontrollsystem vorhanden sein (dazu auch die Abschnitte 2.3.3, 2.3.5 und 2.5.9.2). | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation |

### Sicherung der Netzknoten und deren Verkabelung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | IT-Betreiber, Gebäudemanagement |
| Aktive Netzkomponenten (u.a. Switches, Router) und Verteiler/Patchfelder sind grundsätzlich in verschlossenen Räumen oder in verschlossenen Schränken einzurichten, die gegen unbefugten Zutritt und Zerstörung ausreichend gesichert sind. Die Zugangskontrolle zu allen Räumen, in denen Komponenten für die Kommunikationsinfrastruktur der Hochschule untergebracht sind, liegt beim zentralen IT-Betreiber.  Kabeltrassen für die Kommunikationsinfrastruktur Hochschule sind so zu führen, dass mögliche Gefährdungen (z.B.: Beschädigungen, Umwelteinflüssen und Zugriffs durch nicht autorisierte Personen) minimiert werden. | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, Schlüsselbuch |

### Elektrotechnik

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement, IT-Personal |
| Bei allen elektrotechnischen Installationen sind die entsprechenden Normen (u.a. DIN, ISO, VDE) und Vorschriften einzuhalten und fachgerecht durchzuführen, so dass der aktuelle Stand der Technik umgesetzt wird.  Alle wichtigen IT-Systeme (z.B. Server, Speichersysteme und Netzwerkkomponenten) müssen an eine ausreichend dimensionierte, redundante und gegen Überspannungen abgesicherte Stromversorgung anzuschließen. Dies wird üblicherweise durch eine unterbrechungsfreie Stromversorgung (USV) realisiert. Durch den Einsatz einer USV werden Spannungsschwankungen überbrückt und ein rechtzeitiges und kontrolliertes Herunterfahren der Systeme gewährleistet.  Die elektrischen und die IT-Verkabelungen sind angemessen zu dokumentieren, d.h. eine kontinuierliche Fortschreibung und die Kennzeichnung der Kabel.  Für den Notfall sollte es geeignete Möglichkeiten geben, die Sicherheitsbereiche spannungsfrei zu schalten (z.B. Not-Aus-Schalter). | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation |

### Klimatisierung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement |
| Der normale Luft- und Wärmeaustausch eines Serverraums reicht zumeist nicht aus, um den zulässigen Temperaturbereich für den Betrieb von IT-Systemen zu gewährleisten, so dass der Einbau einer Klimatisierung erforderlich ist. Die Dimensionierung der Klimatisierungsanlage sollte auf Grundlage einer Wärmelastberechnungen) ermittelt werden. Die Klimatechnik ist in separaten Räumen unterzubringen. | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation |

### Brandschutz

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber, Brandschutzbeauftragte |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement, IT-Personal |
| Serverräume sollten in einem Brandabschnitt angelegt sein, der getrennt von den Räumen der technischen Infrastruktur (u.a. USV, Klimatechnik, NEA) ist. Ebenso muss das Datenträgerarchiv in einem anderen Brandabschnitt platziert werden. Grundsätzlich müssen die Regeln des vorbeugenden Brandschutzes beachtet und eingehalten werden. Papier, leere Verpackungen und andere leicht entflammbare Materialien dürfen in Serverräumen und Räumen für technische Infrastruktur nicht gelagert werden.  Grundsätzlich sind Brandmeldeeinrichtungen und Feuerlöscher in ausreichender Anzahl vorzusehen, die so angebracht werden, dass sie im Brandfall gut erreichbar sind. Darüber hinaus sind regelmäßig Brandschutzbegehungen und Übungen zum Brandschutz durchzuführen. Weitere Maßnahmen (u.a. Brandschutztüren) sind mit den Brandschutzbeauftragten abzustimmen. | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation |

### Schutz vor Wasserschäden

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement |
| Räume für technische Infrastruktur sind grundsätzlich so zu gestalten, dass eine Gefährdung durch einen Wasserschaden nicht gegeben ist. Sind Versorgungsleitungen nicht zu vermeiden, dann sind entsprechende Maßnahmen (u.a. Wassermeldeanlage, ausreichend dimensionierte Abflüsse, Rückschlagventilen und Pumpen) umzusetzen, um eintretendes Wasser von den IT-Systemen fernzuhalten. | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation |

### Regelmäßige Wartung der technischen Infrastruktur

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement |
| Um einen kontinuierlichen Betrieb der IT-Infrastruktur gewährleisten zu können, müssen alle Komponenten der technischen Infrastruktur (u.a. USV, Klimatechnik, NEA, Sensorik, Brandschutz) regelmäßig inspiziert und gewartet werden. Dabei müssen die vom Hersteller empfohlenen oder durch Normen festgelegten Intervalle und Vorschriften eingehalten werden. Diese Tätigkeiten müssen protokolliert werden. | | |
| Umsetzung / Dokumentation |  | Wartungsprotokolle |

### Überwachung der technischen Infrastruktur

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement |
| Alle von den Sensoren erfassen Störungsmeldungen der technischen Infrastruktur (u.a. USV, Klimatechnik, NEA, Leckageüberwachung) sollten überwacht und möglichst mit einer Fernanzeige ausgestattet werden, so dass im Störungsfall eine zeitnahe Reaktion erfolgen kann. | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation |

### Zusätzliche Maßnahmen

#### Redundanz der technischen Infrastruktur

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement, IT-Betreiber |
| Um eine hohe Verfügbarkeit der IT-Infrastruktur gewährleisten zu können, ist der Aufbau von Redundanzen ein bewährtes Mittel. Je nach Anforderungen kann dies zu einem Betrieb von zwei identischen Rechenzentren an unterschiedlichen Standorten führen. Solche hohen Anforderungen haben Hochschulen üblicherweise nicht, jedoch kann es erforderlich sein, für einzelne IT-Verfahren und die Vernetzung Redundanzen durch funktional gleiche technische Systeme oder vergleichbarer Ressourcen vorzuhalten. Auch sollten die technischen Komponenten zur Datensicherung in separaten Brandabschnitten bzw. Gebäuden untergebracht sein. | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation |

#### Gefahrenmeldeanlage

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement |
| Um eine schnelle Reaktion im Fall von Gefährdungen sicherzustellen, sollten die verschiedenen Sensoren (Einbruch, Feuer, Wasser, Gas, …) in den Kernbereichen der Informationstechnik (Sicherheitsbereiche/Serverräume) an eine Gefahrenmeldeanlage angebunden werden, die Alarme an eine ständig besetzte Stelle weiterleitet. | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation, Alarmierungspläne |

#### Netzersatzanlage

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement |
| Bei hohen Anforderungen an die Verfügbarkeit ist die Absicherung der Energieversorgung durch eine USV für die Kernbereiche der Informationstechnik zumeist nicht ausreichend, da die sekundäre Energie nur für einen begrenzten Zeitraum geliefert wird.  In diesen Fällen sollte eine Netzersatzanlage (NEA). üblicherweise ein Dieselgenerator vorgehalten werden. Alternativ kann auch eine zusätzliche Stromeinspeisung durch einen zweiten Energieversorgers in Betracht gezogen werden. | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation |

#### Löschtechnik

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, Brandschutzbeauftragte |
| Verantwortlich für die Umsetzung |  | Gebäudemanagement |
| Sind Rauch- bzw. Brandmeldetechniken und Handfeuerlöscher nicht ausreichend, dann muss in den Kernbereichen der Informationstechnik Löschtechnik installiert werden. Für den Brandschutz in eignen sich Löschsysteme, die elektrisch nichtleitend sind und im Brandfall keine Löschmittelrückstände hinterlassen, wie beispielsweise Stickstoff oder Argon. | | |
| Umsetzung / Dokumentation |  | Gebäudepläne, technische Dokumentation |

## Betrieb der Informationstechnik

### Ordnungsgemäße IT-Administration

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Eine ordnungsgemäße IT-Administration ist eine Voraussetzung für die Gewährleistung eines sicheren Betriebs der Informationstechnik. Eine Vielzahl der Tätigkeiten muss systematisch durchgeführt werden, andererseits muss auf Ereignisse reagiert werden, um die Betriebsbereitschaft aufrechtzuerhalten. Bedingt durch die Administrationsprivilegien ergeben sich zusätzliche Gefährdungen für die Informationssicherheit. Folgende Anforderungen müssen umgesetzt werden:   * Zugangskontrolle   Der Zugang zu allen IT-Systemen ist reglementiert und wird geeignet kontrolliert.   * Zugriffskontrolle   Nur berechtigte Nutzer haben einen Zugriff (dazu Abschnitt 2.3.3 Berechtigungsmanagement).   * Personenbezogene Nutzerkennungen   Die Vergabe von Nutzerkennungen erfolgt grundsätzlich personenbezogen. Das IT-Personal arbeitet wie ein normaler Nutzer mit eingeschränkten Rechten.   * Administrative Kennungen / Protokollierung   Müssen administrative Tätigkeiten ausgeführt werden, erfolgt ein Wechsel in eine administrative Rolle. Es muss protokolliert werden, so dass nachvollziehbar ist, wann, auf welchem Weg und unter welcher Nutzerkennung Aktionen durchgeführt wurden.   * Sichere Passwörter   Es muss die Verwendung sicherer Passwörter durchgesetzt werden (technische Maßnahmen, Richtlinie). Automatische Sperrung von Nutzerkennungen bei mehrfach fehlerhafter Passworteingabe.   * Fernzugriff   Erfolgt die Administration nicht an der Konsole, dann dürfen die Tätigkeiten ausschließlich über verschlüsselte Verbindungen erfolgen.   * Änderungen   Alle Änderungen an IT-System sollten in geeigneter Form dokumentiert werden (beispielsweise in der CMDB). | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinien, Betriebshandbücher, CMDB |

### Sichere Installation und Konfiguration von IT-Systemen

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Es ist zu empfehlen, dass allgemeine Sicherheitsrichtlinien für Server und den darauf betrieben Anwendungen erstellt werden (beispielsweise für Windows und Linux). Wesentliche Punkte sind u.a.: Partitionslayout, Verschlüsselung der Dateisysteme, administrative Zugänge, Systemaktualisierungen, serverseitige Verwendung von SSL/TLS, Dienste, Protokollierung, Datensicherung, Außerbetriebnahme und letztendlich die Einbindung in die Systemumgebung beim IT-Betreiber.  Die Vorgaben zur Installation und Konfiguration eines IT-Systems ist abhängig vom Einsatzzweck. Grundsätzlich sollte die Einrichtung eines IT-Systems in einer sicheren Umgebung vorgenommen und nur Datenträger aus einer verlässlichen Quelle verwendet werden. Wichtige Maßnahmen zur Grundhärtung sind u.a.:   * Lokale Paketfilter * Deinstallation oder Deaktivierung nicht benötigter Dienste * Integritätsprüfung * Kritische Prüfung der Standardeinstellungen (u.a. Accounts, Rechte, Passwörter) * Protokollierung * Zugangsbeschränkungen / restriktive Rechtevergabe * Nur ein Dienst pro Server (/Application Whitelisting)   Wichtige Information zur so genannten Systemhärtung sind Best Practices verschiedener Organisationen und den Empfehlungen der Hersteller zu entnehmen. Die Administration der IT-Systeme sollte über ein gesondertes Managementnetz erfolgen.  In einem zweiten Schritt müssen die spezifischen Dienste und Anwendungen (u.a. Verzeichnisdienste, DNS, Groupware/E-Mail, Webanwendungen, Datenbanken) auf den Serversystemen konfiguriert werden, auch dazu sollten Best Practices verschiedener Organisationen und Empfehlungen der Hersteller/Distributoren verwendet werden.  Wenn bei IT-Verfahren speziell entwickelte Software, Standardsoftware oder Softwaresysteme mit einem hohen Aufwand für das Customizing (z.B.: Campusmanagementsysteme) zum Einsatz kommen, dann müssen entsprechende Fach- und Umsetzungskonzepte vorliegen, in denen Aspekte der Informationssicherheit und Datenschutz behandelt werden, so dass eine entsprechende Konfiguration vorgenommen werden kann. In diesen Fällen sollten vor der Inbetriebnahme technische Sicherheitsprüfungen (z.B. Penetrationstests, Code-Review) durchgeführt werden. Dies gilt insbesondere für webbasierte Anwendungen (dazu auch die Abschnitte 2.4.4 u. 2.4.5).  Die Installation und Konfiguration der IT-Systeme und Anwendungen ist geeignet zu dokumentieren (z.B.: CMDB), so dass Änderungen nachvollziehbar sind und eine sichere und konsistente Systemverwaltung ermöglicht wird. Ein sicherer Betrieb von IT-Systemen erfordert eine regelmäßige Aktualisierung der eingesetzten Software (dazu auch Abschnitt 0). | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinien, Betriebshandbücher, CMDB, Fach- und Umsetzungskonzepte |

### Management von IT-Arbeitsplätzen

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Alle IT-Arbeitsplätze in der Hochschulverwaltung müssen fachkundig verwaltet und administriert werden. Die IT-Arbeitsplätze müssen so konfiguriert werden, dass die Anwender die Aufgaben in ihrem Verantwortungsbereich wahrnehmen können. Dabei gelten folgende Rahmenbedingungen, die in einer Richtlinie dokumentiert werden sollten:   * Protokollierung sicherheitsrelevanter Ereignisse * Installation einer Anwendung zur Erkennung von Schadsoftware * Regelmäßige und zeitnahe Aktualisierung des Betriebssystems und der Anwendungen durch Patches oder Updates * Regelmäßige Datensicherung von ausgezeichneten Bereichen der lokalen Datenträger * Lizenzverwaltung * (Fernwartung/Support)   Zur Verwaltung und Administration dieser IT-Arbeitsplätze werden üblicherweise vom IT-Betreiber Managementsysteme (z.B.: System Center Configuration Manager) oder entsprechende Werkzeuge und Dienste eingesetzt. Wenn IT-Arbeitsplätze nicht unter diesen Rahmenbedingungen betrieben werden, dann müssen diese als unsichere IT-Systeme betrachtet werden (dazu Abschnitt 2.4.2).  Von IT-Arbeitsplätzen dürfen grundsätzlich keine Dienste über das Netzwerk bereitgestellt werden. | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie, Betriebshandbücher, CMDB |

### Virtualisierung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Bei der Planung, Umsetzung und Betrieb einer virtuellen IT-Infrastruktur müssen zusätzliche Anforderungen berücksichtigt werden, da ein neues Infrastruktur-Element eingeführt wird. Die Vorteile der Virtualisierung fordern einen Tribut, welcher sich in der Komplexität des Betriebs- und Sicherheitsmanagements niederschlägt. Dazu muss u.a. eine neue administrative Rolle mit entsprechenden Berechtigungen eingeführt und die strikte Trennung des Managementnetzes der Virtualisierungsinfrastruktur von produktiven Netzen sichergestellt werden. Bei der Virtualisierung sind darüber hinaus folgende Grundsätze zu beachten:   * keine Virtualisierung von IT-Systemen mit einem sehr hohen Schutzbedarf * nur IT-Systeme / Netze mit gleichem Schutzbedarf auf einem Virtualisierungsserver * kein Mischbetrieb von DMZ und anderen internen Netzsegmenten   Soll von diesen Grundsätzen abgewichen werden, dann müssen im Rahmen einer Risikoanalyse geeignete Sicherheitsmaßnahmen bestimmt werden. | | |
| Umsetzung / Dokumentation |  | Fachkonzept |

### Speichersysteme

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Speicherlösungen werden in der Regel durch ein dediziertes Speichernetz zwischen Speichersystemen und angeschlossenen Servern (Storage Area Networks - SAN) oder Endgeräten (Network Attached Storage - NAS) realisiert. Gegenüber traditionellen Direct-Attached-Storage Systemen werden in zentralen Speicherlösungen Daten von verschiedenen IT-Verfahren gespeichert. Daher muss wie bei der Virtualisierung ein besonderes Augenmerk auf die Isolation und Trennung der Daten der unterschiedlichen IT-Verfahren gelegt werden. Aktuelle Speicherlösungen stellen dazu eine Reihe von Sicherheitsfunktionen (u.a. Port-Zoning, LUN Binding u. Masking, VSANs und sichere Übertragungsprotokolle) zur Verfügung, diese sind entsprechend des Schutzbedarfs der Daten anzuwenden. Grundsätzlich sind Speichersysteme und Speichernetze als eigenständige Sicherheitszonen auszulegen und abzusichern. | | |
| Umsetzung / Dokumentation |  | Fachkonzept |

### Drucker, Kopierer und sonstige Multifunktionsgeräte

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Grundsätzlich sind auch für diese Kategorie von IT-Systemen die Hinweise zur sicheren Installation, Konfiguration und Aktualisierung sinngemäß nach den Abschnitten 2.6.2 u. 0 anzuwenden.  Werden durch diese IT-Geräte Daten mit einem erhöhten Schutzbedarf gedruckt oder gescannt, müssen diese so aufgestellt werden, dass nur befugte Benutzer zu ihnen Zutritt haben (z.B. ein verschließbarer Druckerraum). Alternativ müssen zusätzliche Sicherheitsmaßnahmen in Betracht gezogen werden (u.a. gesicherte Netzanbindung, Benutzerauthentifizierung und -sensibilisierung). | | |
| Umsetzung / Dokumentation |  |  |

### Patch- und Änderungsmanagement

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Schwachstellen in Betriebssystemen und Anwendungen öffnen Angreifern ein Tor zur Kompromittierung eines IT-Systems. Daher ist es unabdingbar, dass Patches und Updates der Hersteller zeitnah eingespielt werden. Das IT-Personal muss sich daher regelmäßig über bekannt gewordene Schwachstellen und neue Bedrohungen informieren (u.a. Warn- und Informationsdienst des DFN-CERT).  Um diese Aufgabe bewältigen zu können, müssen Prozesse definiert werden, die zum Ziel haben, dass alle Anpassungen an der IT-Infrastruktur kontrolliert, effizient und unter Minimierung von Risiken für den Betrieb betriebener IT-Verfahren durchgeführt werden.  Wichtige Werkzeuge in diesem Kontext sind Trouble-Ticket-Systeme (TTS) und Configuration-Management-Databases (CMDB). | | |
| Umsetzung / Dokumentation |  | TTS, CMDB |

### Schutz vor Schadsoftware

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Das Eindringen und die Verbreitung von Schadprogrammen in der Informationsinfrastruktur einer Hochschule muss durch geeignete Sicherheitsmaßnahmen erschwert bzw. unterbunden werden. Neben der Minimierung der Angriffsfläche, u.a. durch den Einsatz von aktueller Software und Sicherheitsgateways, sind Schutzprogramme zur Erkennung von Schadsoftware auf zentralen IT-Systemen (z.B. Mailserver) und IT-Arbeitsplätzen (dazu Abschnitt 2.6.3) einzusetzen. | | |
| Umsetzung / Dokumentation |  | Auswertung der Ergebnisse der eingesetzten Werkzeuge |

### Protokollierung und Monitoring

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Je nach den Möglichkeiten des Betriebssystems, der Dienste und Anwendungen sind alle sicherheitsrelevanten Ereignisse (u.a. abgewiesene Verbindungen, Konfigurationsänderungen, fehlerhafte Prüfsummen, Systemstart, erfolgreiche u. erfolglose Anmeldungen) automatisch zu protokollieren. Die Protokolle müssen zeitnah und regelmäßig ausgewertet werden. Es muss dabei sichergestellt sein, dass nur IT-Personal mit einer kontrollierenden Rolle die Auswertung vornimmt (dazu auch Abschnitt 2.3.2). Welche Ereignisse insgesamt protokolliert werden, hängt primär vom Schutzbedarf der IT-Systeme und deren potentiellen Angriffsfläche ab und ist in einem Protokollierungskonzept festzuhalten.  Da Protokolldateien personenbezogene Daten beinhalten können, sind die Vorgaben der EU-DSGVO und dem DSG NRW unbedingt einzuhalten. Auch müssen ggf. gesetzliche Aufbewahrungsfristen und Löschpflichten beachtet werden. Daher ist eine Freigabe durch den CISO, dem Datenschutzbeauftragten und der Personalvertretung erforderlich. | | |
| Umsetzung / Dokumentation |  | Protokollierungskonzept und Freigabe |

### Regelmäßige technische Sicherheitsprüfungen

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Neben der Überprüfung der Protokolldateien, sollten auch regelmäßige technische Sicherheitsprüfungen durchgeführt werden, um Schwachstellen oder Verletzungen der Sicherheitsvorgaben zu erkennen. Der Umfang und die Häufigkeit von technischen Sicherheitsprüfungen sind abhängig vom Schutzbedarf. Übliche Maßnahmen sind: Integritätsprüfung der System- und Konfigurationsdateien, Penetrationstests und Schwachstellenscans[[6]](#footnote-6). | | |
| Umsetzung / Dokumentation |  | Auswertung der Ergebnisse der eingesetzten Werkzeuge |

### Datensicherung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Für die Datensicherung ist grundsätzlich ein Datensicherungskonzept zu erstellen, welches sich an dem Schutzbedarf der zu sichernden Daten der IT-Systeme und der IT-Verfahren orientiert (System-, Konfigurations- und Programmdateien / Anwendungsdaten). Nach Möglichkeit sollten die Konfigurationen der aktiven Netzkomponenten in eine regelmäßige Datensicherung einbezogen werden. Ein Datensicherungskonzept sollte mindestens folgende Regelungen beinhalten:   * Umfang der zu sichernden Daten * Zeitpunkte u. Zeitintervalle * Anzahl der aufzubewahrenden Generationen / Speichermedien * Dokumentation der Sicherungen / Bestandsverzeichnis der Speichermedien * Verschlüsselung der Datensicherung * Aufbewahrung der Datensicherungsmedien (Datenträgerarchiv)   Die Konsistenz der Datensicherungsläufe ist sicherzustellen, dazu sollte die Wiederherstellbarkeit der Datensicherung regelmäßig geprüft und geübt werden. Im Falle personenbezogener Daten sind die geforderten Mindest- bzw. Höchstspeicherzeiträume zu beachten. Daher ist eine Freigabe durch den CISO und durch den Datenschutzbeauftragten erforderlich. | | |
| Umsetzung / Dokumentation |  | Datensicherungskonzept u. Freigabe |

### Entsorgung von IT-Systemen u. Datenträgern / Reparatur

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Vor der Entsorgung von IT-Systemen und Datenträgern, muss festgelegt sein, wie mit den Geräten weiter verfahren werden soll (Vernichtung, Weitergabe innerhalb der Hochschule oder Verkauf.)  Es muss vor allem sichergestellt werden, dass keine Daten verloren gehen, die auf IT-Systemen u. Datenträgern gespeichert sind oder vertrauliche bzw. personenbezogene Daten zurückbleiben. Je nach Art der Speicherung und des Schutzbedarfs ist festzulegen, mit welchen Methoden diese Daten gelöscht werden müssen (physikalische Zerstörung, mehrfaches Überschreiben mit Zufallszahlen, Einsatz von Löschgeräten und Aktenvernichtern). Ebenso ist darauf zu achten, dass keine Geräte vergessen werden, wie beispielsweise Drucker, Kopierer, Tablets, Smartphones oder sonstige IoT-Geräte.  Im Falle einer Reparatur von IT-Geräten muss darauf geachtet werden, dass vertrauliche bzw. personenbezogene Daten vorher zuverlässig gelöscht bzw. die Datenträger ersetzt werden. Ansonsten muss das mit der Reparatur beauftragte Unternehmen auf entsprechende Vertraulichkeitsvereinbarungen verpflichtet werden. | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie, Betriebshandbücher, Protokoll |

### Zusätzliche Maßnahmen

#### SIEM

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | IT-Betreiber |
| Die Auswertung der erhobenen Logdaten ist arbeitsintensiv und ohne den Einsatz geeigneter Werkzeuge ineffizient. Um sicherheitsrelevante Ereignisse oder Angriffe zeitnah identifizieren zu können, sollte ein Security Information and Event Management System (SIEM) eingesetzt werden. Ein SIEM sammelt und analysiert Ereignisdaten von Netzwerk-, Server-, Client- und Sicherheitskomponenten (z.B. Firewall, Schwachstellenscanner) an zentraler Stelle. Dabei werden die Ereignisdaten Normalisiert, Aggregiert mit Informationen aus anderen Quellen wie z.B. Asset-, User- oder Konfigurationsdatenbanken korreliert, so dass sicherheitsrelevante Ereignisse effizient erkannt und nachverfolgt werden können. | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie, Betriebshandbücher |

#### Verschlüsselung von Datenbanken

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche |
| Bei einem erhöhtem Schutzbedarf hinsichtlich der Vertraulichkeit, ist die Sicherheit der Verarbeitung ggf. durch Einsatz von Verschlüsselung (u.a. §32 EU-DSGVO) zu gewährleisten. Werden beispielsweise personenbezogene Daten in Datenbanken verarbeitet, muss eine Verschlüsselung in Betracht gezogen werden. Ob die Verschlüsselung einzelner Datenbanktabellen ausreicht oder die komplette Datenbank verschlüsselt werden sollte, ist Gegenstand der entsprechenden Fach- und Umsetzungskonzepte. | | |
| Umsetzung / Dokumentation |  | Fach- u. Umsetzungskonzepte, Betriebshandbücher |

#### Schutz privilegierte Zugänge / Vier-Augen-Prinzip

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche, IT-Personal |
| Bei einem erhöhtem Schutzbedarf oder aus Gründen des Datenschutzes (u.a. Nichtverkettbarkeit) kann es erforderlich sein, dass die Separation von Rollen (dazu Abschnitt 2.3.2) nicht ausreichend ist. Benötigt ein Administrator beispielsweise zur Aufgabenerfüllung Zugang zu vertraulichen Daten, sollte dies nur nach dem Vier-Augen-Prinzip möglich sein, d.h. nur unter Mitwirkung eines anderen Administrators oder des Datenschutzbeauftragten. | | |
| Umsetzung / Dokumentation |  | Betriebshandbuch, Arbeitsanweisung |

#### Public Key Infrastruktur

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO |
| Verantwortlich für die Umsetzung |  | Zentraler IT-Betreiber |
| Für die abgesicherte Kommunikation, die Authentisierung von Personen oder zum Erzeugen von elektronischen Signaturen kommen üblicherweise kryptographische Verfahren zum Einsatz, die Zertifikaten auf Basis des X.509 Standards verwenden. Die Ausstellung, die Verteilung und die Prüfung von Zertifikaten erfolgt durch Zertifizierungsstellen, allgemein auch als Public Key Infrastruktur (PKI) bezeichnet.  Für die Absicherung der internen Kommunikation kann eine eigne Zertifizierungsstelle etabliert werden, soll auch eine geschützte Kommunikation mit externen Parteien möglich sein, dann können die Zertifikate von kommerziellen Anbieter bezogen werden, deren Root-Zertifikat in den üblichen Browsern verankert sind. Die wirtschaftlichste Alternative dürfte jedoch die Teilnahme an der DFN-PKI sein.  Zur Anwendung zertifikatsbasierter Kryptographie auch die Abschnitte (2.3.6, 2.4.7.2 u. 2.7.6.2). | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie |

## Netze und Kommunikation

### Netzwerkzugänge

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, zentraler IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Der Anschluss von IT-Systemen erfolgt ausschließlich über die vorgesehen Netzzugänge bzw. Übergabepunkte im Intranet der Hochschule, die vom zentralen IT-Betreiber bereitgestellt und administriert werden. Jedem IT-System der Hochschule ist dabei ein DNS-Eintrag (Domain Name System) im zentralen DNS-System der Hochschule zugeordnet.  Die Einrichtung und der Betrieb von Netzwerkkomponenten (z.B. WLAN Access Points), sowie die Schaffung von Netzverbindungen (z.B. DSL-Anschlüsse) zum Intranet der Hochschule ist strengstens untersagt.  Sind spezifische Netzwerkzugänge oder Kommunikationsverbindungen gewünscht (z.B. dezentrale WLANs, Fernwartung), erfolgt eine Prüfung und ggf. eine Genehmigung durch den CISO und den zentralen IT-Betreiber.  Nicht benötigte Netzwerkzugänge sind deaktiviert, um einen unbefugten Zugang zum Netz der Hochschule zu erschweren. | | |
| Umsetzung / Dokumentation |  | IT-Ordnung, Netzwerkdokumentation, Genehmigungsverfahren |

### Geeignete Segmentierung des Netzwerks

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Zentraler IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| In Abhängigkeit vom Schutzbedarf der IT-Verfahren ist das Netzwerk der Hochschule (Intranet) physisch oder logisch in Subnetze zu unterteilen, die geeignet gegeneinander abgeschottet werden. Bei der Segmentierung (Bildung von Sicherheitszonen) sollten folgende Grundsätze beachtet werden:   * Trennung von Arbeitsplätzen und Servern * Trennung von intern und extern angebotenen Diensten (DMZ) * Subnetze für die Administration * Subnetze für Protokollierung, Überwachung und Angriffserkennung * Subnetze für die Hochschulverwaltung * Subnetze für Gäste und öffentlich zugängliche Netzzugänge (z.B. WLAN)   In Netzsegmenten mit erhöhten Sicherheitsanforderungen ist darüber hinaus durch geeignete Maßnahmen sicherzustellen, dass nur zugelassene und registrierte IT-Systeme einen Zugang zum Netzwerk erhalten (beispielsweise nach IEEE 802.1x). Öffentlich zugängliche Netzzugänge (z.B. WLAN) sind mit einem angemessenen Authentifizierungsverfahren abzusichern. | | |
| Umsetzung / Dokumentation |  | Netzkonzept u. -dokumentation |

### Kommunikation zwischen unterschiedlichen Sicherheitsniveaus

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Zentraler IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Die gesamte Kommunikation zwischen Netzen mit unterschiedlichem Sicherheitsniveaus und insbesondere dem Internet darf ausschließlich über kontrollierte Kanäle erfolgen, die durch geeignete Sicherheitsdienste (z.B. Sicherheitsgateway/Firewall) abgesichert werden. Eine Umgehung dieser Sicherheitsdienste muss wirkungsvoll unterbunden werden.  Die Konfiguration bzw. die Einrichtung geeigneter Filterregeln erfolgt für jeden Netzübergang auf Grundlage einer Sicherheitsrichtlinie. Grundsätzlich werden dabei alle Verbindungen blockiert, die nicht explizit erlaubt sind. Die Änderungen einer Sicherheitsrichtlinie kann ausschließlich nach Prüfung und Genehmigung durch den CISO / zentralen Dienstleister erfolgen.  Der Aufbau eines Sicherheitsgateways, zumindest bei Übergängen mit erhöhtem Schutzbedarf, sollte sich an der Architektur "Paketfilter – Application-Level-Gateway – Paketfilter (P-A-P)“ orientieren und aus mehreren Komponenten bestehen.  Kommunikationsverbindungen, die über unsichere Netze (u.a. Internet) verlaufen, sollten grundsätzlich verschlüsselt werden (dazu auch Abschnitt 2.7.6.4).. | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie, Netzwerkdokumentation |

### Sichere Installation und Konfiguration von aktiven Netzkomponenten

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Zentraler IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Für aktive Netzkomponenten (u.a. Router, Switches, Sicherheitsgateways) gelten sinngemäß die Ausführungen aus Abschnitt 2.6.2. Jedoch müssen bei diesen Komponenten die Installation und jede Änderung der Konfiguration ausreichend getestet werden, da bei einer Fehlkonfiguration einzelne Netzsegmente oder das gesamte Netzwerk der Hochschule ausfallen kann oder Sicherheitsfunktionen außer Kraft gesetzt werden können.  Der Zugang zu den aktiven Netzkomponenten muss durch geeignete organisatorische, infrastrukturelle und technische Maßnahmen (z.B. durch separate Netzsegmente für die Administration) abgesichert und darf nur durch autorisierte Personen administriert werden. | | |
| Umsetzung / Dokumentation |  | Netzkonzept, Betriebshandbücher, CMDB |

### Netzwerkmanagement- und Monitoring

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Um Störungen im Netzwerk erkennen, lokalisieren und zeitnah beheben zu können, muss ein angemessenes Netzwerkmanagement etabliert werden. Neben der Statusüberwachung und Konfigurationsverwaltung der aktiven Komponenten kann eine Netzwerkmanagementlösung zur frühzeitigen Erkennung und zur Abwehr von Angriffen weitere sicherheitsrelevante Ereignisse (u.a. unautorisierte Zugriffe bzw. Zugriffsversuche) erfassen. Ebenso ist grundsätzlich auch die Auswertung von Verkehrsdaten möglich.  Das Netzwerkmanagement sollte daher in das Protokollierungskonzept (dazu Abschnitt 2.6.9) eingebunden werden, für das entsprechende Freigaberegelungen gelten.  Die für diesen Zweck genutzten Werkzeuge sind entsprecht abzusichern und dürfen nur von autorisierten Personen bedient werden. Darüber hinaus muss ein separates Netzsegment für das Netzwerkmanagement verwendet werden. | | |
| Umsetzung / Dokumentation |  |  |

### Zusätzliche Maßnahmen

#### Erkennung und Abwehr von Angriffen

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Zentraler IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Zur Erkennung und Abwehr sollten zusätzliche Sicherheitsdienste implementiert werden, beispielsweise Intrusion Detection oder Prevention Systeme (IDS/IPS), Analyse von Netflows und Honeypods. Ebenso sollten aktuelle Informationen zur Bedrohungslage der IT-Sicherheit durch Cyberangriffe und andere Gefahren („Threat Intelligence“) bezogen werden. Hierfür werden Daten aus unterschiedlichen Quellen erfasst, analysiert und in aufbereiteter Form (u.a. IDS-Signaturen, Listen von bekannten Command-and-Control-Servern, Hashsummen von Schadprogrammen, …) zur Verfügung gestellt. Neben kommerziellen Anbietern, liefern u.a. das BSI und das DFN-CERT entsprechende Informationen und Dienstleistungen.[[7]](#footnote-7)  Die Kombination mit einem SIEM (Abschnitt 2.6.13.1) ermöglicht eine ganzheitliche Sicht auf die Sicherheit der Informationstechnologie der Hochschule. | | |
| Umsetzung / Dokumentation |  |  |

#### Verschlüsselung von Kommunikationsverbindungen

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Prozessverantwortliche, IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche |
| Bei einem erhöhtem Schutzbedarf oder bei regulatorischen Anforderungen kann es erforderlich sein, dass auch Kommunikationsverbindungen innerhalb des Netzwerks der Hochschule verschlüsselt werden müssen. Beispielsweise die Verbindungen zwischen Web-, Anwendungs- und Datenbankservern, administrative Zugänge aber auch Client-Server Verbindungen. Sofern die Anwendungen nicht direkt entsprechende Verfahren anbieten, kommen zur Verschlüsselung von Daten im Netzwerk das Internet Protocol Security (IPSec) und Secure Sockets Layer (SSL) häufig zum Einsatz. | | |
| Umsetzung / Dokumentation |  | Fach- und Umsetzungskonzepte, Betriebshandbücher |

#### Web-Application Firewall

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Prozessverantwortliche, IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche |
| Werden sensible Informationen oder personenbezogene Daten durch webbasierte Anwendungen verarbeitet, die auch aus dem Internet erreichbar sind, sollten die Daten auf der Anwendungsebene gefiltert werden. Durch den Einsatz einer Web Application Firewall (WAF) wird das HTTP-Protokoll und die darüber übertragenen Daten analysiert. Somit werden Angriffsmuster bzw. -versuche frühzeitig erkannt und nicht mehr an die Webanwendung weitergeleitet. | | |
| Umsetzung / Dokumentation |  | Fach- und Umsetzungskonzepte, Betriebshandbücher |

#### VPN

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Zentraler IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Müssen Standorte untereinander vernetzt oder sollen Mitarbeiter über mobile Endgeräte auf IT-Verfahren (auch Telearbeit und Fernadministration) aus dem Internet zugreifen, dann müssen virtuelle private Netzwerke (VPN) eingerichtet werden. Voraussetzung für die Einrichtung ist die Verwendung starker Verschlüsselungs- und Authentifizierungsverfahren (dazu auch die Abschnitte 2.3.6, 2.4.7.1 und 0). | | |
| Umsetzung / Dokumentation |  | Sicherheitsrichtlinie |

#### Einsatz zertifizierter Produkte

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche |
| Bei sehr hohen Sicherheitsanforderungen kann der Einsatz zertifizierte Produkte nach den "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik", kurz Common Criteria (CC), zur Steigerung der Qualität technischer Sicherheitsmaßnahmen zielführend sein. Primäre Anwendungsfelder sind u.a. Virtualisierung, Sicherheitsgateways oder allgemein kryptographische Verfahren. Es gibt darüber hinaus auch Anwendungsfelder, bei den der Einsatz zertifizierter Produkte gefordert wird, beispielsweise bei den Anschlussbedingungen für das NdB-Verbindungsnetz. | | |
| Umsetzung / Dokumentation |  |  |

#### Hochverfügbarkeit

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CIO, zentraler IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Die zentralen Komponenten des internen Netzwerks der Hochschule (Backbone - Verkabelung, Router/Switches) sowie die Sicherheitskomponenten (Sicherheitsgateways) sollten redundant ausgelegt werden und die Fähigkeit besitzen, bei Ausfall einer Komponente einen uneingeschränkten Betrieb zu gewährleisten (Hochverfügbarkeit). | | |
| Umsetzung / Dokumentation |  | Netzkonzept u. -dokumentation |

#### Physische Trennung von Sicherheitssegmenten

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | CISO, IT-Betreiber |
| Verantwortlich für die Umsetzung |  | IT-Personal |
| Bei sehr hohen Sicherheitsanforderungen sollte die Segmentierung des Netzwerks nicht ausschließlich auf Basis von „Virtual Local Area Networks (VLAN)“ erfolgen. Ausgezeichnete Sicherheitssegmente (u.a. Administrations- oder Managementnetze, DMZ) sollten physisch durch separate Switches getrennt werden. | | |
| Umsetzung / Dokumentation |  | Netzkonzept u. -dokumentation |

## Datenschutz

Die primäre Zielsetzung dieser Handreichung ist die Etablierung eines angemessenen Sicherheitsniveaus an einer Hochschule. Darüber hinaus soll auch ein praktikabler Weg aufgezeigt werden, wie die rechtlichen Vorgaben der EU-DSGVO umgesetzt werden können.

Eine Orientierung bietet das "Standard-Datenschutzmodell" (SDM[[8]](#footnote-8)) der deutschen Datenschutzaufsichtsbehörden. Bei der SDM Methode werden zunächst die datenschutzrechtlichen Anforderungen in einen einheitlichen Katalog elementarer Schutzziele – Gewährleistungsziele – überführt. Dies sind:

* Datenminimierung
* Vertraulichkeit
* Integrität
* Verfügbarkeit
* Transparenz
* Intervenierbarkeit
* Nichtverkettung

Die Gewährleistungsziele beinhalten die klassischen Schutzziele der Informationssicherheit und sind somit grundsätzlich durch diese Handreichung adressiert. In den folgenden Abschnitten werden - aus Sicht des Datenschutzes – für alle Gewährleistungsziele die wesentlichen technischen und organisatorischen Maßnahmen aufgeführt, durch die die Anforderungen der EU-DSVGO erfüllt werden können.

*Anmerkung:*

*Die als erforderlich erkannten technischen und organisatorischen Sicherungsmaßnahmen sollen in einem standardisierten Maßnahmenkatalog aufgeführt werden, der als Anhang zum SDM konzipiert ist. Dieser Anhang ist jedoch noch nicht veröffentlicht worden.*

## Datenminimierung

Das SDM betrachtet die Datenminimierung als grundlegendes Gewährleistungsziel:

„*Datenminimierung konkretisiert und operationalisiert im Verarbeitungsprozess den Grund-satz der Notwendigkeit, der von diesem Prozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Verarbeitungszwecks benötigt werden.*

*…*

*Die Verfolgung dieses Gewährleistungsziels setzt voraus, dass zunächst die Legitimität der Zwecksetzung sowie die Angemessenheit, Erheblich- und Notwendigkeit der zu erhebenden Daten für die vorgesehenen Zwecke datenschutzrechtlich beurteilt worden sind, auf einer abstrakten Ebene, noch ohne Berücksichtigung prozeduraler und technischer Zwänge.[[9]](#footnote-9)“*

Die Begrenzung der Datenverarbeitung auf das erforderliche Maß kann nicht Gegenstand des operativen Verarbeitungsprozess sein, sondern muss im Vorfeld der Datenverarbeitung beurteilt werden.

Maßnahmen:

Ausgehend von der als zulässig bewerteten Zwecksetzung und Datengrundlage, müssen die einzelnen Verarbeitungsschritte in den entsprechenden Fachkonzepten definiert und beschrieben werden.

* Planung, Dokumentation und Umsetzung von IT- und Fachverfahren (2.4.5)
* Pseudonymisierungs- und Anonymisierungsverfahren (2.16.1)

## Vertraulichkeit

„Das Gewährleistungsziel Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen kann. Unbefugte sind nicht nur Dritte außerhalb der verantwortlichen Stelle, mögen sie mit oder ohne kriminelle Absicht handeln, sondern auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einer Verarbeitungstätigkeit oder zu der oder dem jeweiligen Betroffenen haben.“[[10]](#footnote-10)

Maßnahmen:

* Festlegung von Verantwortlichkeiten, Rollen und Berechtigungskonzepte (2.3.1, 2.3.2, 2.3.3)
* Benutzerauthentifizierung (2.4.6, 2.4.7.1, 2.6.1)
* Qualifiziertes Personal (2.3.2, 0, 2.3.12)
* Festgelegte Kommunikationskanäle (2.7.1, 2.7.3)
* Geeignete Serverräume und Büroräume (2.3.4, 2.5.1)
* Organisatorische Abläufe und interne Regelungen (2.2.6, 2.3.11, 2.3.13.2, 2.4.5)
* Verschlüsselung von gespeicherten oder transferierten Daten (2.3.6, 2.6.13.2, 2.7.6.2)
* Vermeidung, Erkennung und Abwehr von Angriffen (2.2.4, 2.4.2, 0, 0, 2.6.9, 2.7.5, 2.7.6.1)

## Integrität

*„Das Gewährleistungsziel Integrität bezeichnet einerseits die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden. Integrität bezeichnet andererseits die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen wer-den oder zumindest feststellbar sein, damit sie berücksichtigt bzw. korrigiert werden können.“[[11]](#footnote-11)*

Maßnahmen:

* Berechtigungskonzepte und dokumentierte Zuweisung (2.3.3, 2.4.5)
* Einsatz von Prüfsummen und Signaturen (2.3.6, 2.6.2, 0, **Fehler! Verweisquelle konnte nicht gefunden werden.**, 2.7.6.2, 2.7.6.4)
* Aufrechterhaltung der Aktualität von Daten (2.2.5, 2.6.2, 2.6.9)
* Sollverhalten von Prozessen, Durchführung von Tests und Bewertung von Risiken von Sicherheitslücken (2.4.2, 2.4.4, 2.4.5, 0)
* Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen.

## Verfügbarkeit

„Das Gewährleistungsziel Verfügbarkeit bezeichnet die Anforderung, dass personenbezogene Daten zur Verfügung stehen müssen und ordnungsgemäß im vorgesehenen Prozess verwendet werden können. Dazu müssen sie im Zugriff von Berechtigten liegen und die vorgesehenen Methoden zu deren Verarbeitung müssen auf sie angewendet werden können.“[[12]](#footnote-12)

Maßnahmen:

* Anfertigung von Sicherheitskopien (2.4.4, 2.4.5, 2.6.9, 2.6.11)
* Vermeidung, Erkennung und Abwehr von Angriffen (2.2.4, 2.4.2, 0, 0, 2.6.9, 2.7.5, 2.7.6.1)
* Schutz vor äußeren Einflüssen (2.5)
* Umsetzung von Reparaturstrategien und Ausweichprozessen (2.3.13.3, 2.4.5)
* Vertretungsregelungen (2.3.1, 2.3.9)

## Transparenz

*„Das in Art. 5 Abs. 1 lit. a DS-GVO genannte Gewährleistungsziel Transparenz bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Be-treiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck bei einer Verarbeitungstätigkeit erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.“[[13]](#footnote-13)*

*Maßnahmen:*

* Dokumentation von Verarbeitungstätigkeiten (2.4.5 und Zusammenspiel mit anderen Verarbeitungstätigkeiten)
* Dokumentation von Test und der Freigabe (2.4.4, 2.4.5 und ggf. der Vorabkontrolle von neuen oder geänderten Verarbeitungstätigkeiten)
* Dokumentation der Verträge mit internen Mitarbeitenden, mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden (2.3.1, 2.4.5, 2.16.2)
* Protokollierung von Zugriffen und Änderungen (2.4.5, 2.6.9, 2.16.3)
* Dokumentation der Verarbeitungsprozesse auf der Basis eines Protokollierungs- und Auswertungskonzepts (2.4.5, 2.6.9, 2.16.3)
* Versionierung (2.4.4)

Nicht abgedeckte Anforderungen:

* Nachweis der Quellen von Daten
* Auskunftsrechte von Betroffenen
* Dokumentation von Einwilligungen und Widersprüchen

## Intervenierbarkeit

*„Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen. Dazu müssen die für die Verarbeitungsprozesse verantwortlichen Stellen jederzeit in der Lage sein, in die Datenverarbeitung vom Erheben bis zum Löschen der Daten einzugreifen.“[[14]](#footnote-14)*

Maßnahmen:

* Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen (2.4.3, 2.4.4, 2.4.5)
* Dokumentierte Bearbeitung von Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes (2.2.2, 2.2.4, 2.4.5)
* Deaktivierungsmöglichkeit einzelner Funktionalitäten (2.4.3, 2.4.4, 2.4.5)
* Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte (2.6.9, 2.16.3)

Nicht abgedeckte Anforderungen:

* Differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
* Einrichtung eines Single Point of Contact (SPoC) für Betroffene
* Dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verarbeitungstätigkeiten
* Operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten
* Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen

## Nichtverkettung

*„Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden dürfen. Eine Zusammenführung darf nur dann erfolgen, wenn die in Art. 5 Abs. 1 lit. b DS-GVO normierte Anforderung beachtet wird, dass Daten nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben werden.“[[15]](#footnote-15)*

Maßnahmen*:*

* Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten (2.3.2, 2.3.3)
* Programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten (2.4.5, 2.6.2)
* Regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung (2.4.3, 2.4.4)
* Trennung nach Organisations-/Abteilungsgrenzen (2.3.2, 2.3.3)
* Trennung mittels Rollenkonzepten und sichere Authentisierungsverfahren (2.3.2, 2.3.3)
* Einsatz von zweckspezifischen Pseudonymen und Anonymisierungsdiensten (2.16.1)

Nicht abgedeckte Anforderungen:

* Zulassung von nutzerkontrolliertem Identitätsmanagement
* Geregelte Zweckänderungsverfahren

## Weitere Maßnahmen

### Pseudonymisierung und Anonymisierung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Prozessverantwortliche |
| Verantwortlich für die Umsetzung |  | IT-Verfahrensverantwortliche |
| Nach der EU-DSGVO kann die Pseudonymisierung eine geeignete Maßnahme sein, die Rechte der Betroffen bei der Verarbeitung von personenbezogenen Daten zu wahren. Bei einer Pseudonymisierung von personenbezogenen Daten, können diese bei der Verarbeitung ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden. Im Gegensatz zu einer Pseudonymisierung können bei der Anonymisierung ursprünglichen Informationen nicht wiederhergestellt werden.  Sofern die für die Verarbeitung verwendete Software diese Funktionalität nicht bietet, müssen geeignete Verfahren bereitgestellt werden (beispielsweise durch ein Update oder separates Werkzeug). | | |
| Umsetzung / Dokumentation |  | Fach- und Umsetzungskonzepte |

### Auftragsverarbeitung

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Datenschutzbeauftragte |
| Verantwortlich für die Umsetzung |  | Justiziariat |
| Eine Auftragsdatenverarbeitung bzw. Auftragsverarbeitung nach EU-DSGVO liegt vor, wenn die Hochschule (Auftraggeber) externe Dienstleister (Auftragnehmer) damit beauftragt, weisungsgebunden personenbezogene Daten zu verarbeiten. Dieser Sachverhalt liegt vor, wenn beispielsweise externe Unternehmen die Buchhaltung/ Gehaltsabrechnung durchführen, Wartung u. Reparatur an IT-Systemen vornehmen, Fernwartungssysteme einsetzen oder Akten vernichten. Da die Verantwortung für die ordnungsgemäße Datenverarbeitung beim Auftraggeber verbleibt, muss der Auftragnehmer auf die Einhaltung des Datenschutzes vertraglich verpflichtet werden (Art. 28 EU-DSGVO).  Zudem muss der Auftraggeber in regelmäßigen Abständen kontrollieren, ob der Auftragnehmer die rechtlichen Vorgaben einhält. | | |
| Umsetzung / Dokumentation |  | Vertrag |

### Durchführung von Datenschutzaudits

|  |  |  |
| --- | --- | --- |
| Verantwortlich für die Initiierung |  | Datenschutzbeauftragte |
| Verantwortlich für die Umsetzung |  | Datenschutzbeauftragte |
| Neben den technischen Sicherheitsprüfungen der IT-Systeme, mit denen IT-Verfahren umgesetzt werden, müssen auch die Geschäftsprozesse regelmäßig überprüft werden. Der Fokus liegt dabei auf der Einhaltung der Gewährleistungsziele Transparenz, Intervenierbarkeit und Nichtverkettung. | | |
| Umsetzung / Dokumentation |  | Auditbericht |

1. Beispiel:

   Leitlinie zur Informationssicherheit’aus Projekt PRISMA.

   **Pr**ogramm für ein gemeinsames **I**nformations**S**icherheits**Ma**nagement

   Gegenstand des Projektes war die Einführung eines Information Security Management Systems (ISMS) in der jeweiligen Fachhochschule. Auf Basis von gemeinsamen Zielen sollte eine Verbesserung und Harmonisierung der Informationssicherheit verbunden mit Synergieeffekten erreicht werden. Das Projekt zielte außerdem von Anfang an darauf ab, eine langfristige Kooperation für Informationssicherheit (ISKo) zwischen den Fachhochschulen zu etablieren. [↑](#footnote-ref-1)
2. Weitere Informationen beim DFN-CERT, https://www.cert.dfn.de/ueberblick/ [↑](#footnote-ref-2)
3. Es ist zielführend, allen Mitarbeiterinnen und Mitarbeitern einen Leitfaden zur sicheren Nutzung der Informationstechnik an die Hand zu geben. Neben den bereits genannten Punkten, sollen u.a. auch die Themen E-Mail u. Internet-Nutzung, Umgang mit sensiblen Informationen, aktuelle Bedrohungen und Handlungsanweisen zum Verhalten bei Sicherheitsvorfällen enthalten sein. [↑](#footnote-ref-3)
4. https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index\_htm.html [↑](#footnote-ref-4)
5. „ *…insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung, …“* [↑](#footnote-ref-5)
6. Mit dem DFN-Dienst „Netzwerkprüfer“ können Netzbereiche der Hochschule von außen selbst geprüft werden; https://www.cert.dfn.de/nwp/ [↑](#footnote-ref-6)
7. Über den AW-Dienst (Automatische Warnmeldungen) können Warnmeldungen bezogen werden, wenn beim DFN-CERT Auffälligkeiten im Zusammenhang mit IP-Adressen der Hochschule bekannt geworden sind; https://www.cert.dfn.de/autowarn/ [↑](#footnote-ref-7)
8. https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode\_V1.1.pdf [↑](#footnote-ref-8)
9. Aus SDM V1.1 - Abschnitt 5.3 [↑](#footnote-ref-9)
10. Aus SDM V1.1 – Abschnitt 5.4.1(3) [↑](#footnote-ref-10)
11. Aus SDM V1.1 – Abschnitt 5.4.1(2) [↑](#footnote-ref-11)
12. Aus SDM V1.1 – Abschnitt 5.4.1(1) [↑](#footnote-ref-12)
13. Aus SDM V1.1 – Abschnitt 5.4.2(5) [↑](#footnote-ref-13)
14. Aus SDM V1.1 5.4.2(6) [↑](#footnote-ref-14)
15. Aus SDM V1-1 – Abschnitt 5.4.2(4) [↑](#footnote-ref-15)