FRANKFURT UNIVERSITY OF APPLIED SCIENCES

Baustein-Kommentierungen

Dokumentation erstellt von: Bernhard Brandel

Exportiert am: 04.09.2020

Inhaltsverzeichnis

ISMS.1 Sicherheitsmanagement

Versionshinweis	Unverändert in Edition 2020.
Anforderungen	Die Anforderungen zur Basis Absicherung **ISMS.1.A1 – A9** und die Anforderungen **ISMS.1.A10 - A12** müssen umgesetzt werden. Die weiteren Anforderungen zur Standard Absicherung **ISMS.1.A13 – A15** sollten umgesetzt werden. Bei einem erhöhtem Schutzbedarf sollten unbedingt die Empfehlungen zu **1.A16** in Betracht gezogen werden.
Ausnahmen	**ISMS.1.A5** entfällt, wenn kein externe Informationssicherheitsbeauftragter bestellt wird. **ISMS.1.A17** kann nicht umgesetzt werden, weil Universitäten und Hochschulen keine Versicherungen abschließen dürfen.
Priorisierung	**R1 (1.A1 - 1.A9)** Basis-Absicherung **R2 (1.A10 - 1.A12)** **R3 (1.A13 - 1.A15 u. ggf. 1.A16)** Die Erfüllung der weiteren Anforderungen kann auf R2 gesetzt werden, da für die Erreichung eines grundsätzlichen Sicherheitsniveaus nachrangig regelungsrelevant sind.
Allgemeine Empfehlungen zum Baustein	Ein etabliertes Informationssicherheitsmanagement ist die Grundlage für die Erreichung und die Aufrechterhaltung eines angemessenen Sicherheitsniveaus an der Hochschule. Die Managementaufgabe 'Informationssicherheit' an Hochschulen unterscheidet sich grundsätzlich nicht von der Aufgabenstellung in Behörden und Unternehmen. Diffenzen sind in den Empfehlungen zur Umsetzung aufgeführt. Die Verantwortlichkeiten für die Erfüllung der Anforderungen zur Basis-Absicherung (ausser 1.A7 u. 1.A8) liegen bei der **Leitung der Hochschule (/Präsidium)**.
Empfehlungen zur Umsetzung der Anforderung	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 über mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen informieren lassen. Dafür müssen Sicherheitsziele sowie eine Strategie für Informationssicherheit festgelegt und in einer **Leitlinie zur Informationssicherheit** dokumentiert werden.
	Darüber hinaus sollte in einer Ordnung oder einer Richtlinie die Grundsätze der Leitlinie verfeinert werden und u.a. folgende Themenfelder behandeln: • Organisation der Informationssicherheit / Verantwortlichkeiten • Grundsätze für den Einsatz von Informationstechnik • Lenkung von Dokumenten • Identifizierung und Behandlung von Risiken • Umgang mit Sicherheitsvorfällen / Abwehr von Gefahren • Aufrechterhaltung der Informationssicherheit • Berichte zur Informationssicherheit • Planung, Dokumentation und Umsetzung von Fach- und IT-Verfahren
	Als weitere zentrale Dokumente im Sicherheitsprozess einer Hochschule müssen Sicherheitskonzepte erstellt, umgesetzt sowie regelmäßig überprüft werden.
	Besonderheiten an Hochschulen

Umsetzungshinweise:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/ISMS/Umsetzungshinweise_zum_Baustein_ISMS_1_Sicherheitsmanagement.html

https://www.ak-if.de/dokumente/HRK_MV_Empfehlung_Informationssicherheit_06112018.pdf

(ISO 27003 - Entwicklung und die Implementierung eines Information Security Management System (ISMS) - kostenpflichtige Norm)

ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch das Präsidium

Das Präsidium muss sich regelmäßig über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit aufklären lassen (Holschuld!). Dazu ist es empfehlenswert, das Präsidium auf folgende Punkte aufmerksam zu machen:

- Darstellung der Sicherheitsrisiken und der damit verbundenen **Auswirkungen** und **Kosten**
- Auswirkungen von Sicherheitsvorfällen auf die kritischen Geschäftsprozesse
- Gesetzliche und vertragliche Sicherheitsanforderungen
- Übersicht über Standard-Vorgehensweisen zur Informationssicherheit für die Universitäten und Hochschulen

Verbündete mit ins Boot holen. Auf die rechtlichen Konsequenzen eines Nichthandelns hinweisen (analog zu lizenzrechtlichen Fragen).

Die Übernahme der Gesamtverantwortung muss dokumentiert werden (**1.M3**).

ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie [Präsidium]
In Vorabgesprächen sollen die Kronjuwelen und strategischen, kritischen Geschäftsprozesse identifiziert und dokumentiert werden. Die Festlegung von Sicherheitszielen und -strategien hat **nichts** mit Technik zu tun. Die Dokumentation der Sicherheitsziele und -strategie mündet in ISMS.M3. Eine Empfehlung gibt es hier: https://www.ak-if.de/dokumente/HRK_MV_Empfehlung_Informationssicherheit_06112018.pdf

ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit [Präsidium]

Im September 2014 beschloss die Allianz der Wissenschaftsorganisationen eine vom AKIF (Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen) für alle wissenschaftlichen Einrichtungen erarbeiteten IT-Sicherheitsleitlinie. Diese wurde an alle Universitäten und Hochschulen verschickt. Diese Leitlinie ist hier zu finden: https://www.ak-if.de/dokumente/Allianzpapier%20IT-Sicherheit.pdf

ISMS.1.A4 Benennung eines Informationssicherheitsbeauftragten [Präsidium]

Der Text aus M4 sollte nach Möglichkeit 1-zu-1 in der Tätigkeitsbeschreibung / Bestellung des ISB stehen. Der ISB ist ein Manager, kein Techniker (letzteres kann allerdings nicht schaden). Da er die Sicherheitsmaßnahmen durchsetzen und kontrollieren muss, ist hohe Resilienz gegen Frustration ebenfalls eine notwendige Eigenschaft eines ISB. Bei der Benennung muss das Präsidium auch die notwendigen Ressourcen für die erfolgreiche Arbeit des ISB bereitstellen, insbesondere für die Zuhilfenahme Externer.

ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit [Präsidium]

Die zu schaffende Organisationsstruktur für die Informationssicherheit sollte in einer Organisationsrichtlinie dokumentiert werden. Dabei sollte man sich an der Organisationsstruktur der IT ausrichten. Je dezentraler die IT organisiert ist, desto dezentraler muss auch die Organisationsstruktur der Informationssicherheit aufgebaut sein.

Das Management der Informationssicherheit unterliegt einem PDCA Zyklus. Alle Dokumentationen und umgesetzte Maßnahmen müssen in einem vorher festzulegenden Zeitrahmen überprüft werden.

Für die Dokumentation und den Management Zyklus ist die Beschaffung eines Tools sinnvoll.

ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen [Prozessverantwortliche]

Umsetzung des IT- Grundschutz-Profils. Entsprechend des Schutzbedarfs werden konkrete Sicherheitsmaßnahmen festgelegt und im Sicherheitskonzept dokumentiert.

ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse [Präsidium/CIO]

Bei der Planung, Dokumentation und Umsetzung von Fach- und IT-Verfahren muss sichergestellt werden, dass der ISB bzw. die Sicherheitsorganisation beteiligt werden.

Dies muss durch eine Ordnung oder Richtlinie hochschulweit geregelt werden.

ISMS.1.A10 Erstellung eines Sicherheitskonzepts [Prozessverantwortliche]

siehe ISMS.1.M7

ISMS.1.A11 Aufrechterhaltung der Informationssicherheit [ISB / Revision]

Die Gewährleistung und Weiterentwicklung eines entsprechenden Sicherheitsniveaus wird im Rahmen eines iterativen Managementprozesses im PDCA-Zyklus (Plan-Do-Check-Act) durchgeführt

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. Dazu muss der ISB bzw. die Revision ermächtigt werden.

ISMS1.A12 Management-Berichte zur Informationssicherheit [Präsidium]

Das Präsidium/CIO müssen regelmäßig und anlassbezogen 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. Alle Entscheidungen über erforderliche Aktionen, Umgang mit Restrisiken und mit Veränderungen von sicherheitsrelevanten Prozessen müssen dokumentiert werden.

ISMS.1.A13 Dokumentation des Sicherheitsprozesses [Präsidium]

siehe ISMS.1.M12

ISMS.1.A14 Sensibilisierung zur Informationssicherheit

Siehe dazu ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

Maßnahmen für erhöhten Schutzbedarf

ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien

Im Kontext eines ISMS steht hier der Aufbau des Regelwerks im Vordergrund. Dies sollte sich in mehreren Ebenen (z.B. Leitlinie, Richlinien (/Ordnungen), Anweisungen und technische Vorgaben) gliedern, so dass die verschieden Zielgruppen (u.a. Prozessverantwortliche, Betreiber, Nutzer und Administratoren) bedarfsgerecht angesprochen werden (dazu auch **1.M16**).

ORP.1 Organisation

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-UYbRng • Materialien: zki.de/goto/gp-C6qT2g
Anforderungen	**A1 bis A5 Basis-Anforderungen,** **A6 bis A13 Standard-Anforderungen** Die Anforderungen sind in Hinblick auf die an der Hochschule vorhandenen Verfahren und Organisatorischen Rahmenbedingungen unter Beachtung der Schutzzielpriorisierung der betroffenen Informationsverbünde zu prüfen und geeignet umzusetzen. EIn Teil der Anforderungen wird im Baustein OPS 1.1.2 Ordnungsgemäße IT-Administration behandelt.
Ausnahmen	**ORP.1.A4 Funktionstrennung zwischen operativen und kontrollierenden Aufgaben** Diese Anforderung ist der Betriebspraxis an Hochschulen möglicherweise nicht auf allen Ebenen gewährleistbar.
Priorisierung	**R1** Bereitstellung von in der Betriebspraxis nutzbaren Vorgaben und Handlungsempfehlungen für die Betroffenen.
Allgemeine Empfehlungen zum Baustein	An Hochschulen sind typischerweise langjährige Erfahrungen im Zusammenhang mit dem Betrieb von IT vorhanden und zentrale Dienste werden kontinuierlich und institutionalisiert erbracht. Ein Teil der Anforderungen wird grundsätzlich oft schon durch die institutionellen Rahmenbedingungen einer staatlichen Hochschule sichergestellt. Je nach Schutzbedarf der Prozesse dürften sich Differenzierungen in der Intensität der Umsetzung der Anforderungen ergeben. Für bestimmte sensible Bereiche der Hochschulverwaltung können Maßnahmen umfassender und vollständiger umgesetzt werden als zum Beispiel für den wissenschaftlichen Bereich oder den Webauftritt.
Empfehlungen zur Umsetzung der Anforderung	Die Hochschule ist ein öffentlicher Raum, der in weiten Bereichen jeder Person offensteht. Folglich sind Regelungen zu treffen, wie in diesem Spannungsfeld eine Trennung von öffentlichen und nicht oeffentlichen Bereichen (z.B. Büro IT-Betrieb, Serverraum) angemessen umgesetzt werden kann.
	Können Basisanforderungen nicht erfüllt werden, ist eine Risikoanalyse durchzuführen. Es sind Maßnahmen zu definieren, die der Anforderung bestmöglich entsprechen. Die Anforderungen ORP.1.A3 "Beaufsichtigung oder Begleitung von Fremdpersonen" und ORP. 1.A4 "Funktionstrennung zwischen unvereinbaren Aufgaben" sind hier besonders zu erwähnen. Werden Verträge mit Managed Service Providern geschlossen, ist es das Ziel ganze Bereiche aus der eigenen Organisation auszulagern. Kontinuierliche Begleitung und Überwachung würde dem Ziel nicht entsprechen. Ebenso kann in vielen Bereichen die Trennung von Aufgabe und Kontrolle nicht zeitnah umgesetzt werden. Es könnten aber z.B regelmäßige Prüfungen vereinbart werden.

ORP.2 Personal

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-FeZGeg • Materialien: zki.de/goto/gp-w87QKg
Anforderungen	**ORP.2.A1-A10** Die Anforderungen A1 - A10 sind anzuwenden.
Ausnahmen	keine
Priorisierung	**R1**
Allgemeine Empfehlungen zum Baustein	Es ist wichtig von Anfang an neuen Mitarbeiter*innen aufzuzeigen, dass sie eine wesentliche Rolle spielen, wenn es um IT-Sicherheit geht. ORP.3: Sensibilisierung und Schulung ist zu beachten
Empfehlungen zur Umsetzung der Anforderung	**ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeiter [Vorgesetzte]** Es ist ratsam **eine** Checkliste zu erstellen, mit deren Hilfe alle neuen Mitarbeiter*innen über dieselben und jeweils aktuellen Grundlagen informiert werden.
	Folgende Anforderung ORP.2.A2 wurde in Edition 2020 gestrichen, da sie als zentrale Aufgabe im Baustein ORP.4 abgehandelt wird. Dennoch sollte sie im Blick behalten werden: **ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern [Vorgesetzte, IT-Betrieb]** Sinnvoll ist es, einen Prozess zu etablieren, der sicherstellt, dass die IT-Administration rechtzeitig (vorher) informiert wird wenn Mitarbeiter*innen die Hochschule verlassen. Der Einsatz eines Identity und Access Managment System mit Schnittstelle zum stammdatenverwaltenden System (Personalverwaltung) ist hier hilfreich.
	ORP.2.A9 Schulung von Mitarbeitern In-House Schulungen mit Berücksichtigung der Gegebenheiten sollten bevorzugt werden.

ORP.3: Sensibilisierung und Schulung

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-uVkdAA • Materialien: zki.de/goto/gp-UCzpFQ
Anforderungen	**ORP.3.A1-A3 sowie A4 - A8** Die Anforderungen A1 - A8 sind anzuwenden. **ORP.3.A9** Die Anforderung A9 ist bei hohem Schutzbedarf ebenfalls anzuwenden.
Ausnahmen	keine
Priorisierung	**R1 (und innerhalb der R1- Prozesse zeitgleich zu ISMS.1 beginnen)** Sensibilisierung betrifft alle Zielgruppen einer Hochschule, beginnend mit der Hochschulleitung, die die Gesamtverantwortung für den Informationssicherheitsprozess trägt und die Rahmenbedingungen für Informationssicherheit (s. ISMS.1 Sicherheitsmanagement, Leitlinie) setzt und mit gutem Beispiel vorangehen muss. Gleichzeitig betrifft Sensibilisierung auch die Professorenschaft und das mittlere Management sowie die wissenschaftlichen Beschäftigten, Verwaltungspersonal, das IT-Personal und die Studierenden. Die Realisation von ORP.3 sollte zeitgleich mit ISMS.1 beginnen, was die Umsetzung beider Bausteine beschleunigt. Sinnvoll ist es, auch die Standardanforderungen A5 - A8 möglichst von Beginn an umzusetzen.
Allgemeine Empfehlungen zum Baustein	Begrifflichkeiten: "Institution" ist die entsprechende Hochschule (Fachhochschule oder Universität) Hochschulen haben als Zielgruppe nicht nur "Mitarbeiter". Genauso müssen die "Studierenden" und fallweise weitere Nutzergruppen in die Sensibilisierungs- und Schulungsmaßnahmen mit einbezogen werden. In Baustein und Umsetzungshinweisen sind daher i.d.R. unter "Mitarbeitern" "Beschäftigte, Lehrbeauftragte sowie Studierende" zu verstehen. An dualen Hochschulen ist der Begriff noch weiter zu fassen (siehe auch (a) ORP.4 Identitäts- und Berechtigungsmanagement).
Empfehlungen zur Umsetzung der Anforderung	Die Sensibilisierungsmaßnahmen müssen auf die Bedürfnisse der Zielgruppen zugeschnitten werden. Der Unterarbeitskreis Awareness des ZKI sammelt und entwickelt Beispiele für Schulungsmaterialien und Sensibilisierungsmaßnahmen, die bei Bedarf genutzt und gerne ergänzt werden können. **ORP.3.A1** Leitungspersonen benötigen kurze, nicht technik-lastige Informationen über Risiken, Folgen und Lösungsmöglichkeiten, wie sie ihrer Gesamtverantwortung für die Informationssicherheit am besten nachkommen können.
	ORP.3.A2 Es empfiehlt sich, in allen Organisationseinheiten (Fakultäten, zentralen Einrichtungen etc.), Multiplikatoren zu benennen und zu befähigen (festzulegen in ISMS.1, Leitlinie). Bereits existierende Organisationsstrukturen/Kanäle sollten dafür genutzt werden (z.B. Administratorentreffen).

	ORP.3.A3 Wichtig ist die Kontinuität der Maßnahmen. Neue Beschäftigte, Wiedereinsteigende und Studierende sollten gleich zu Beginn sensibilisiert werden.
	ORP.3.A7 Den Sicherheitsverantwortlichen müssen die notwendigen Ressourcen (Zeit, Geld, Personal, Schulungen) zur Verfügung gestellt werden (siehe ISMS.1).
	ORP.3.A6 und ORP.3.A8 Sensibilisierung "im laufenden Geschäftsbetrieb" ist besonders wirkungsvoll. Deshalb ist der Einsatz geeigneter Software, die Angriffssimulationen wie Spear-Phishing-Kampagnen samt Messung und anonymisierter Auswertung des Lernerfolgs ermöglicht, sehr zu empfehlen. Vor der Durchführung ist es notwendig, die Kampagnen mit den Personalvertretungen abzustimmen. Der in Edition 2020 in ORP.3.A6 hinzugefügte Austausch mit anderen Playern (Datenschutz, Gesundheits- und Arbeitsschutz, Brandschutz etc.) über die Effizienz der Aus- und Weiterbildung ist sinnvoll.

ORP.4 Identitäts- und Berechtigungsmanagement

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Yx0dAg • Materialien: zki.de/goto/gp-HoSdSQ
Anforderungen	**ORP.4.A1-A9** Die hier beschriebenen Empfehlungen zur Umsetzung Anforderungen beziehen sich auf die im Grundschutz-Profil genannten Prozesse im Rahmen der Aufgaben des reinen Hochschulbetriebs. Bei Universitätskliniken sind darüberhinaus u.U. weitere Maßnahmen notwendig, dies wird hier nicht betrachtet. Die Anforderungen A1 - A9 sind anzuwenden. Es ist zu beachten, dass Hochschulen einschlägigen Gesetzen unterliegen. In der Festlegung von Benutzergruppen, die in den Anforderungen erwartet werden, sind Hochschulen nicht frei. Obwohl Hochschulen eine Rechtspersönlichkeit sind, bestehen innerhalb einer Hochschule eigenständige IT-Verbünde mit Leitern, Administratoren und Benutzern. Die Anforderungen A1 - A9 müssen in der Umsetzung so erweitert werden, dass die Umsetzung der Anforderungen in den unabhängigen IT-Verbünden dokumentiert ist. **ORP.4.A10-A19** Die Bausteine ORP.4.A10 - A.19 SOLLTEN umgesetzt werden.
Ausnahmen	
Priorisierung	**R1**
Allgemeine Empfehlungen zum Baustein	Es wird der Hochschulleitung empfohlen, eine Übersicht der Personalressourcen einer Hochschule zu erhalten, die mit IT-Aufgaben befasst sind. Die in Edition 2020 modernisierten Passwort-Richtlinien (Streichung von regelmäßigen Änderungen) sind sehr zu begrüßen.
Empfehlungen zur Umsetzung der Anforderung	Die im Abschnitt 3 das Baustein genannten weiteren Verantwortlichen („Administrator, Benutzer, Leiter IT“) sind Funktionsgruppen, die innerhalb einer Hochschule dezentral auf verschiedene Personen übertragen werden. Diese Personen sind je nach anwendbaren Landesgesetzen (Hochschulgesetz etc.) und lokal gültiger Grundordnung in unterschiedlichen Hierarchiezweigen und damit unterschiedlichen Vorgesetzten zugeordnet. Folgende Prüffragen sollten bedacht werden: Welche Benutzergruppen gibt es nach dem anwendbaren Hochschulgesetz? Wie werden die durch das angewendete Hochschulgesetz bestimmten Benutzergruppen in der Hochschule ausdifferenziert (siehe Grundordnung)? In einer Hochschule gibt es unter Umständen formal unabhängig voneinander betriebene IT-Strukturen, die auf einem gemeinsamen IAM aufbauen. Prüffrage: Wie werden zwischen den IT-Leitern der unabhängigen Strukturen die das IAM betreffenden Fragen diskutiert und entschieden? Welche Kooperationen gibt es, die Externen Zugriff auf Ressourcen der Hochschule einräumen?

	ORP.4.A1 Regelung für die Einrichtung von Benutzern und Benutzergruppen Die Benutzergruppen sind weitestgehend durch einschlägige Gesetze vorgegeben (Hochschulgesetze usw.). Hochschulen können diese Gruppen innerhalb ihrer Selbstverwaltung weiter ausdifferenzieren. Über die Zuordnung von Benutzern zu Gruppen entscheiden innerhalb einer Hochschule verschiedene Zuständigkeiten. Die in A1 geforderten „separate administrative Rollen“ sind in dieser Anforderung zu nennen. Beispiele können sein *Personalabteilung der zentralen Verwaltung*, Verwaltung einer *Fakultät*, Verwaltung einer *Projektgruppe* oder *Forschungsgruppe* etc. **ORP.4.A2 Regelung für Einrichtung, Änderung und Entzug von Berechtigungen** Die Bedarfe, auf Ressourcen zugreifen zu dürfen, ergeben sich aus verschiedenen Quellen. Studierende: Der Zugriff auf Lehrveranstaltungen in E-Learning-Systemen ergibt sich aus Prüfungsordnungen, -ergebnissen. Eine Bestimmung des Bedarfs ergibt sich nicht aus der Beschreibung von Prozessen, sondern aus fachwissenschaftlichen Erwägungen. Dezentrale Verwaltung in Fakultäten: Der Zugriff auf Verwaltungsdaten ergibt sich aus den Anforderungen eines Fachbereichs, der autonom von der zentralen Verwaltung geführt wird. Daraus ergibt sich, dass die technische Umsetzung von Berechtigungen verschiedenen anderen Erwägungen nachgeordnet ist. **ORP.4.A4 Aufgabenverteilung und Funktionstrennung** Die Aufgabenverteilung innerhalb des Verbundes einer Hochschule ergibt sich aus technikfernen Strukturen einer sich selbst verwaltenden Organisation. (…)
	ORP.4.A16 Für den Baustein ORP.4.A16 ist zu beachten, dass Personen verschiedenen Benutzergruppen angehören können (Bsp. studentische Hilfskräfte, die studieren und angestellt sind)

ORP.5 Compliance Management (Anforderungsmanagement)

Anforderungen	Die Anforderungen sind in Hinblick auf die vorhandenen Verfahren und Rahmenbedingungen der jeweiligen Hochschule zu prüfen.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-5ePImw • Materialien: zki.de/goto/gp-rLXVsQ
Ausnahmen	
Priorisierung	**R3** Bereitstellung von in der Betriebspraxis nutzbaren Handlungsempfehlungen für die Betroffenen.
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen. Ein Teil der Anforderungen wird grundsätzlich oft schon durch die institutionellen Rahmenbedingungen einer staatlichen Hochschule sichergestellt. Die Umsetzung gesetzlicher Anforderungen ist im IT- Betrieb einer Hochschule allerdings hochgradig interpretationsbedürftig und oft auch kaum idealtypisch und vollständig möglich. Diese Problematik wird in der Praxis durch das Vorhandensein etablierter hochschulübergreifender Kooperationsstrukturen relativiert. Relevante Themen und aktuelle Entwicklungen können hier angemessen und auf breiterer Basis behandelt werden. Beispiele für Kooperationsstrukturen im IT-Bereich sind der DFN-Verein, mit seinen verschiedenen Untergliederungen (insbesondere die Forschungsstelle Recht), der zki.ev mit seinen verschiedenen Arbeitskreisen. Über den IT-Betrieb hinaus existieren zusätzlich überregionale Gremien für CIOs, DSBs und die Leitungsebene der Hochschulen. Möglicherweise besteht ein besonderer, abweichender Regelungsbedarf bei Kooperationen mit externen Partnern wie Zum Beispiel Auftragsforschung.
Empfehlungen zur Umsetzung der Anforderung	Eine in der Hochschulpraxis besonders zu beachtende Compliance-Anforderung dürfte das Lizenzmanagement sein.

CON.1 Kryptokonzept

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-ko-KdA • Materialien: zki.de/goto/gp-Y4UO1A
Anforderungen	**CON.1.A1-A2** Die Anforderungen A1 - A2 sind anzuwenden. **CON.1.A3-A6** Die Anforderungen sind in der Regel umzusetzen, siehe Umsetzungshinweise **CON.1.A7-A18** Siehe Hinweise
Ausnahmen	Für gesetzlich vorgesehene Methoden zu Identifikation und Kommunikation, etwa eID, DE-Mail, beBPo oder qualifizierte elektronische Signaturen können gesetzliche Vorgaben für die Verschlüsselung bestehen. Gleiches gilt für elektronische Bezahlungsvorgänge.
Priorisierung	
Allgemeine Empfehlungen zum Baustein	Als Stand der Technik für Verschlüsselung solte BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen herangezogen werden. Funkverbindungen sollten bei der Verarbeitung von Geheimnissen und personenbezogenen Daten nicht das einzig eingesetzte kryptografische Verfahren sein. Auf proprietäre kryptografische Konzepte sollte abseits der Festplattenverschlüsselung der Betriebssysteme von Microsoft und Apple verzichtet werden. Für Kassensicherheit sind bei öffentlichen Stellen die Vorgaben der Haushaltsrechts zu beachten und für alle Stellen die GoBD.
Empfehlungen zur Umsetzung der Anforderung	**CON.1.A1 Auswahl geeigneter kryptografischer Verfahren [Fachverantwortliche](B)** Entscheidungsgrundlage für die Wahl kryptografischer Verfahren und Schlüssellängen sollte BSI TR-02102-1 sein.
	CON.1.A2 Datensicherung bei Einsatz kryptografischer Verfahren [IT-Betrieb] (B) Windows: Die Speicherung der Schlüssel für Bitlocker zu einem Computerobjekt im AD sollte mit einem Monitoring des AD verbunden werden. Entwicklungsumgebungen: Eine in der Praxis bewährte Lösung ist Vault von HashiCorp.
	CON.1.A3 Verschlüsselung der Kommunikationsverbindungen (S) Zur Verschlüsselung von Kommunikationsverbindungen sollte ein System gewählt werden, dass
	CON.1.A4 Geeignetes Schlüsselmanagement (S) Im Hinblick auf die fehlerhafte Implementierungen von Verschlüsslungen sollte bei der Prüfung (insbesondere bei Rechtsgeschäften
	CON.1.A5 Sicheres Löschen und Vernichten von kryptografischen Schlüsseln [IT-Betrieb] (S) Siehe CON.6
	CON.1.A6 Bedarfserhebung für kryptografische Verfahren und Produkte [IT-Betrieb, Fachverantwortliche] (S) -

	CON.1.A7 Erstellung einer Sicherheitsrichtlinie für den Einsatz kryptografischer Verfahren und Produkte (H) Siehe 4.1 Wissenswertes
	CON.1.A8 Erhebung der Einflussfaktoren für kryptografische Verfahren und Produkte (H) -
	CON.1.A9 Auswahl eines geeigneten kryptografischen Produkts [IT-Betrieb, Fachverantwortliche] (H) Neben der Zertifizierung von IT-Produkten und IT-Systemen im Hinblick auf deren Sicherheitsfunktionalitäten bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine sogenannte Zertifizierung nach Technischen Richtlinien (TR) an.
	CON.1.A10 Entwicklung eines Kryptokonzepts (H) Siehe 4.1 Wissenswertes
	CON.1.A11 Sichere Konfiguration der Kryptomodule [IT-Betrieb] (H) -
	CON.1.A12 Sichere Rollenteilung beim Einsatz von Kryptomodulen [IT-Betrieb] (H) Diese Anforderungen müssen im Rahmen der Beschaffung abgebildet werden.
	CON.1.A13 Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen (H) Diese Anforderungen müssen im Rahmen der Beschaffung abgebildet werden.
	CON.1.A14 Schulung von Benutzern und Administratoren [Vorgesetzte, Fachverantwortliche, Leiter IT] (H) -
	CON.1.A15 Reaktion auf praktische Schwächung eines Kryptoverfahrens (H) -
	CON.1.A16 Physische Absicherung von Kryptomodulen [Leiter IT] (H) -
	CON.1.A17 Abstrahlsicherheit [Leiter IT] (H) Es sollte grundsätzlich auf die Nutzung von Funktechnologien verzichtet werden.
	CON.1.A18 Kryptografische Ersatzmodule [IT-Betrieb] (H) Für öffentliche Stellen sollte im Hinblick aus das Haushaltsrecht über eine gemeinsame Beschaffung mit ggf. mehreren gemeinsamen Lagerstandorte nachgedacht werden.

CON.2 Datenschutz

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-410McQ • Materialien: zki.de/goto/gp-ZXdi9g
Anforderungen	**CON.2.A1** Die Basis-Anforderung A1 ist anzuwenden. Es sind keine Standard-Anforderungen und Anforderungen für einen erhöhten Schutzbedarf definiert. Die konkrete Festlegung der Anforderungen, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten, erfolgt im Rahmen einer Risikoanalyse.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Verwendung des Standard-Datenschutzmodells – Version 2.0b (SDM-V2b)
Empfehlungen zur Umsetzung der Anforderung	Referenzmaßnahmen-Katalog des SDM und ISO/IEC 27701

CON.3 Datensicherungskonzept

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-ePii1g • Materialien: zki.de/goto/gp-CU6WgA
Anforderungen	**CON.3.A1-A12** Die Anforderungen A1 - A12 sind anzuwenden. **CON.3.A13** Die Anforderung A13 ist bei erhöhtem Schutzbedarf anzuwenden.
Ausnahmen	*[Die Begründung ist von großer Bedeutung]*
Priorisierung	**R1**
Allgemeine Empfehlungen zum Baustein	Die Konkretisierungen in Edition 2020 sind hilfreich.
Empfehlungen zur Umsetzung der Anforderung	**CON.3.A6** Obwohl die Bereitstellung zentraler Strukturen für Datensicherung angestrebt werden sollte, sollte aufgrund der dezentralen Hochschulstrukturen beachtet werden, dass es u.U. mehrere solche Datensicherungskonzepte geben kann. Hinzu kommen spezielle Anforderungen aus dem Bereich Archivierung von Forschungsrohdaten. **CON.3.A9** Hier sind ggf. Datenschutzaspekte und ggf. Anforderungen für einen erhöhten Schutzbedarf mit zu berücksichtigen **CON.3.A10** Aufgrund der dezentralen Administration und eines ggf. verteilten technischen Angebots im Umfeld einer Hochschule wird die umfassende Sensibilisierung der Mitarbeiter bezüglich Vorgaben und Umsetzung einer Datensicherung im Rahmen der Anwendung des Bausteins ORP.3 empfohlen. Siehe diesbezüglich auch CON.3.M6.
	CON3.A13 (erhöhter Schutzbedarf) Sofern es die Backup-Software zulässt, sollten die gesicherten Daten standardmäßig verschlüsselt werden.

CON.4 Auswahl und Einsatz von Standardsoftware

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-fioBsw • Materialien: zki.de/goto/gp-iVM0uQ
Anforderungen	Basis und Standard Absicherung: Die Anforderungen **CON.4 A1-A9** müssen umgesetzt werden. Maßnahmen bei erhöhtem Schutzbedarf sollten die Maßnahmen **CON.4 A10-A11 umgesetzt werden.**
Ausnahmen	Es werden keine Ausnahmen definiert.
Priorisierung	**R1 A1-A4. A8. A9** **R2 A5, A6, A7,**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen sind allgemein gehalten und daher grundsätzlich auch auf Hochschulen übertragbar. Es gilt diesen Baustein eng mit OPS 1.1.2 (Ordnungsgemäße IT-Administration), OPS 1.1.4 (Schutz vor Schadprogrammen) und OPS 1.1.6 (Software-Tests und -Freigaben) zu verknüpfen. Dieser Baustein ist essentiell für die Etablierung eines ISMS für die Einführung von neuer Software und sollte auch hinsichtlich der Awareness durch die Hochschulleitung verpflichtend für die Organisation definiert werden. Ergänzend sollten für die Umsetzung des Bausteins auch die Empfehlungen des BSI berücksichtigt werden: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/CON/Umsetzungshinweise_zum_Baustein_CON_4_Auswahl_und_Einsatz_von_Standardsoftware.html?nn=10027602
Empfehlungen zur Umsetzung der Anforderung	**CON.4.M1 Sicherstellen der Integrität von Standardsoftware** Die Integrität muss sowohl beim Erhalt der Software, als auch bei der weiteren Bereitstellung intern sichergestellt werden. Es sollte wenn möglich ein Verfahren zur Checksummenprüfung der Softwarepakete genutzt werden. Bei der direkten Bereitstellung von Software über externe Portale sollten Nutzende in die Lage versetzt werden, die Integrität der Quelle als auch des Paketes selbst zu verifizieren.

CON.5 Einsatz von Individualsoftware

Versionshinweis	Bereits auf Stand Edition 2020. Neuer Name in Edition 2020: CON.9 Informationsaustausch. Alter Name in Edition 2019: CON.5 Einsatz von allgemeinen Anwendungen.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Ug1ibg • Materialien: zki.de/goto/gp-CZgzrw
Anforderungen	**CON.5.A1, A3-A4 sowie A6, A8-A9, A11** Die Anforderungen A1, A3 - A4 sowie A6, A8 - A9, A11 sind anzuwenden. **OPS.3.1.A12-A13** Bei erhöhtem Schutzbedarf sollte eine Risikoanalyse erfolgen und die Anforderungsvorschläge A12 und A13 in Betracht gezogen werden.
Ausnahmen	
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

CON.6 Löschen und Vernichten

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-lxHI4w • Materialien: zki.de/goto/gp-pt-62Q
Anforderungen	**CON.6.A1-A2** Die Anforderungen sind anzuwenden. **CON.6.A3-A8** Die Anforderungen sind in der Regel umzusetzen, siehe Umsetzungshinweise **CON.6.A9-A11** Siehe Hinweise
Ausnahmen	Archivrechtliche Regelungen sind vorrangig.
Priorisierung	
Allgemeine Empfehlungen zum Baustein	Komplexität ist zu vermeiden. Eine Abstimmung mit Haushaltsverantwortlichen (und Archiv (bei öffentlichen Hochschulen) und Abfallentsorgung ist essentiell. Insbesondere das Haushaltsrecht (z.B. VV zu Art. 71 BayHO, § 71) gibt für öffentliche Stellen bereits Teile des Konzeptes vor. Zum Vorgehen empfiehlt sich DIN 66398.
Empfehlungen zur Umsetzung der Anforderung	**CON.6.A1 Regelung der Vorgehensweise für die Löschung und Vernichtung von Informationen** Soweit bereits Verwaltungsvorschriften (insbesondere aus dem Haushaltsrecht) gelten, bedarf es keiner zusätzlichen Regelung. Eine gute Orientierung bietet der Beschluss des Rats der IT-Beauftragten der Ressorts vom 6. Dezember 2013. Die Vorgaben des Archivrechts sind für öffentliche Stellen zu integrieren.
	CON.6.A2 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln und Informationen Veröffentlichte Informationen (z.B. Publikationen oder Statistiken) sind in der Regel nicht schutzwürdige Informationen im Sinne von CON.6. Entsorgungs- und Vernichtungseinrichtungen sollten leicht erreichbar sein.
	CON.6.A3 Löschen der Datenträger vor und nach dem Austausch -
	CON.6.A4 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern -
	CON.6.A5 Geregelte Außerbetriebnahme von IT-Systemen und Datenträgern Es bietet sich für öffentliche Stellen eine Integration in den Prozess zu Aussonderung nach Haushaltsrecht an.
	CON.6.A6 Einweisung aller Mitarbeiter in die Methoden zur Löschung oder Vernichtung von Informationen Es bietet sich eine Kombination mit der Unterweisung nach § 12 ArbSchG an.

	CON.6.A7 Beseitigung von Restinformationen Der Weitergabe steht auch eine gemeinsame Nutzung von Ressourcen (z.B: Gruppendrucker, Pool-PCs oder virtuelle Arbeitsplätze gleich). Bei einem Nutzerwechsel muss sichergestellt sein, dass insbesondere Verlaufshistorien oder temporäre Dateeiablagen) gelöscht werden.
	CON.6.A8 Richtlinie für die Löschung und Vernichtung von Informationen Der Richtlinie sollte die Methodik der DIN 66398 erstellt werden.
	CON.6.A9 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Datenträgern bei erhöhtem Schutzbedarf Insbesondere im Hinblick auf Implementierungsfehler bei modernen Speichertechnologien, ist eine Vernichtung der Löschung vorzuziehen. Zur Umsetzung der Vernichtung bei erhöhtem Schutzbedarf empfiehlt sich gemäß DIN 66398 nach Sicherheitsstufe 5 oder höher festzulegen.
	CON.6.A10 Beschaffung geeigneter Geräte zur Löschung oder Vernichtung von Daten Diese Vorgaben ergeben sich für öffentliche Stellen und Zuwendungsempfänger bereits aus dem Vergaberecht.
	CON.6.A11 Vernichtung von Datenträgern durch externe Dienstleister Erfolgt eine Vernichtung bereits unter durchgehender Aufsicht vor Ort geprüft gemäß DIN 66398 nach Sicherheitsstufe 5 oder höher, ist der Abtransport der vernichteten Daten nicht zu kontrollieren.
	Weitere Anforderung Ein Weitergabe von gelöschten Datenträgnern nach CON.6.A7 Beseitigung von Restinformationen sollte in Regelungen nach CON.6.A1 bei erhöhtem Schutzbedarf untersagt sein.

CON.7 Informationssicherheit auf Auslandsreisen

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-CSyovg • Materialien: zki.de/goto/gp-TbPj-A
Anforderungen	**CON.7.A1-A12** Die Anforderungen A1 - A12 sind anzuwenden.
Ausnahmen	keine
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	**CON.7.A1** Für Auslandsreisen ist zu unterscheiden, ob sie im Rahmen der Verwaltung/Steuerung (typischerweise Reisen des Rektorats oder des Präsidiums) oder als Forschungsreise angetreten werden. Für diese Einsatzzwecke sind eigene Richtlinien notwendig, weil die Anforderung aus CON.7.A1 unterschiedlich anzuwenden sind. Die Unterschiede ergeben sich aus der Klassifizierung der mitgeführten Informationen und der Verantwortlichkeit. **CON.7.A1** Bei Forschungsreisen, die durch eine Professur oder eine Fakultät durchgeführt werden, muss die Verantwortung des Leiter dieser Professur oder Fakultät dokumentiert und übernommen werden. Die Sammlung und Bereitstellung von Forschungsdaten unterliegen weiteren Regelwerken, die außerhalb der Zuständigkeit einzelner Hochschulen liegen (Horizon2020-Projekte mit mindestens drei Partner aus zwei Ländern, Forschung an Großanlagen wie CERN, HPC-Cluster). In diesen Fällen sind die Richtlinien externer Organisationen zu beachten.
	CON.7.A2 Sensibilisierung der Mitarbeiter zur Informationssicherheit auf Auslandsreisen (B) Die jeweiligen Behörden der Verfassungsschutzes der Länder bieten oft Vorträge und Sensibilisierungen an.
	CON.7.A3 Forschungsreisen bringen je nach Fachrichtung besondere Anforderungen an die Widerstandfähigkeit von Hardware (Feldforschung). Die Verantwortlichkeit ist auf die Abteilung auszudehnen, die für die Bereitstellung von Hardware verantwortlich ist.
	CON.7.A4 Verwendung von Sichtschutz-Folien [Benutzer] (B) Die Benutzer sind auf die Grenzen der Schutzwirkung der Blickschutzfilter hinzuweisen. Die Blickschutz muss in Ausgleich mit den Maßnahmen zur Arbeitssicherheit gebracht werden.
	CON.7.A5 Verwendung der Bildschirm-/Code-Sperre [Benutzer] (B) Es sollten Richtlinien für den Bildschirm-/Code-Sperre vorgegeben werden, damit diese nicht leicht erraten werden können. Bei der Beschaffung sollte sichergestellt werden, dass die Bildschirm-/Code-Sperre widerstandsfähig gegen Bruteforce-Angriffe sind.
	CON.7.A6 Zeitnahe Verlustmeldung [Benutzer] (B) Es bietet sich für öffentliche Stellen eine Verknüpfung mit den haushaltsrechtlichen Vorgaben an. Auch der DSB und ISB sollten über den Verlust in Kenntnis gesetzt werden.

	CON.7.A7 Sicherer Remote-Zugriff auf das Netz der Institution [IT-Betrieb, Benutzer] (B) Umsetzungshinweise
	CON.7.A8 Sichere Nutzung von öffentlichen WLANs [Benutzer] (B) Bei ordnungsgemäßer Konfiguration ist das eduroam WLAN anderen WLAN bei der Nutzung vorzuziehen.
	CON.7.A9 Sicherer Umgang mit mobilen Datenträgern [Benutzer] (B) Synergien mit CON.6 möglich.
	CON.7.A10 Verschlüsselung tragbarer IT-Systeme und Datenträger [Benutzer, IT-Betrieb] (B) Synergien mit CON.6 möglich.
	CON.7.A11 Einsatz von Diebstahl-Sicherungen [Benutzer] (B) Synergien mit CON.6 möglich.
	CON.7.A12 Sicheres Vernichten von schutzbedürftigen Materialien und Dokumenten [Benutzer] (B) Synergien mit CON.6 möglich.
	CON.7.A13 Mitnahme notwendiger Daten und Datenträger [Benutzer] (S) Umsetzungshinweise
	CON.7.A14 Kryptografisch abgesicherte E-Mail-Kommunikation [Benutzer, IT-Betrieb] (S) Die DFN-PKI bietet eine einfache Lösung für verschlüsselte Kommunikation. Je nach Zielland sollten die Auswirkungen des Verlusts der privaten Schlüssels mit die Risikobetrachtung eingestellt werden. Bei der Nutzung inhaltsverschlüsselter Kommunikation ist auf die Gewährleistung der ordnungsgemäßen Aktenführung besonders bei der Ablage zu beachten.
	CON.7.A15 Abstrahlsicherheit tragbarer IT-Systeme (H) Umsetzungshinweise
	CON.7.A16 Integritätsschutz durch Check-Summen oder digitale Signaturen [Benutzer] (H) Umsetzungshinweise
	CON.7.A17 Verwendung vorkonfigurierter Reise-Hardware [IT-Betrieb] (H) Anstelle eines Notebooks kann auch ein Tablet ausreichend sein.
	CON.7.A18 Eingeschränkte Berechtigungen auf Auslandsreisen [IT-Betrieb] (H) Umsetzungshinweise

CON.9 Informationsaustausch

Versionshinweis	Bereits auf Stand Edition 2020. Neuer Name in Edition 2020: CON.9 Informationsaustausch. Alter Name in Edition 2019: OPS. 1.2.3 Informations- und Datenträgeraustausch.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-qQEYMA • Materialien: zki.de/goto/gp-uLG4xQ
Anforderungen	Die Anforderungen zur Basis Absicherung **CON.9. A1 - A3** müssen umgesetzt werden. Die Anforderungen zur Standard Absicherung **CON.9.A4 - A8** sollten umgesetzt werden. Für erhöhtem Schutzbedarf hat das BSI keine Anforderungen definiert. In diesem Fall sollte eine Risikoanalyse erfolgen.
Ausnahmen	Keine Ausnahmen.
Priorisierung	**R3** Umsetzungsreihenfolge wie im Grundschutz empfohlen.
Allgemeine Empfehlungen zum Baustein	Hochschulen haben in der Regel eine sehr hohe Zahl an Kommunikationspartnern und entsprechende Anforderungen, die zwischen den zentralen und dezentralen Einrichtungen variieren können. Dazu kommt, dass Institute, Forschungsbereiche, Professuren und die jeweiligen zentralen Einrichtungen eigenständig mit Datenträgern arbeiten, weshalb die zentrale Verwaltung von Datenträgern häufig nicht oder nur schwer etabliert werden kann. Der neue Baustein CON.9 konzentriert sich auf den Informationsauastausch. Der in OPS.1.2.3 (alt) mit enthaltene Datenträgeraustausch wurde zusammen mit SYS.3.4 (alt) Mobile Datenträger ausgegliedert nach SYS.4.5 Wechseldatenträger. Die im alten Baustein noch vorhandenen Anforderungen für erhöhten Schutzbedarf, die thematisch zu CON.9 gehören (OPS.1.2.3 A13 und A18), wurden sinnvollerweise als CON.9.A7 und A8 für normalen Schutzbedarf (s.o.) vorgeschrieben.
Empfehlungen zur Umsetzung der Anforderung	**CON.9.A1 (entspricht altem Baustein OPS.1.2.3.A1 / M1) Festlegung zulässiger Kommunikationspartner** Es könnte hilfreich sein, zentrale Regelungen bereichsweise zu ergänzen. Bei der Umsetzung von **CON.9.A2** sind das TLP-Protokoll und die Datenklassifizierung sehr hilfreich bzw. unumgänglich .

OPS.1.1.2 Ordnungsgemäße IT-Administration

Versionshinweis	Version basiert auf Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-AKiyOw • Materialien: zki.de/goto/gp-NT4FNg
Anforderungen	**Anforderungen A1-A6** Die Anforderungen sind in Hinblick auf die vorhandenen Möglichkeiten und Schutzzielpriorisierungen umzusetzen. **Anforderungen A7-A12** Die Anforderungen sind in Hinblick auf die vorhandenen Möglichkeiten und Schutzzielpriorisierungen umzusetzen.
Ausnahmen	
Priorisierung	**R1**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen vereinbaren lassen. An Hochschulen sind typischerweise langjährige Erfahrungen im Zusammenhang mit dem Betrieb von IT vorhanden und zentrale Dienste werden kontinuierlich und institutionalisiert erbracht. Der IT-Betrieb ist unter Umständen aber auch gekennzeichnet durch einen Best-Effort- Ansatz, Dienste werden erbracht so gut als möglich. Mit den zur Verfügung stehenden Ressourcen wird darüber hinaus oft ein möglichst breites und dynamisch angepasstes Dienst-Portfolio angestrebt. Im Unterschied zu anderen Branchen könnte der Schwerpunkt eher in Richtung Flexibilität und weniger in Richtung Vollständigkeit gesetzt sein. Je nach Schutzbedarf der Prozesse können sich Differenzierungen in der Umsetzung der Anforderungen ergeben. Für bestimmte sensible Bereiche der Hochschulverwaltung können Maßnahmen umfassender und vollständiger umgesetzt werden als zum Beispiel für den wissenschaftlichen Bereich oder den Webauftritt.
Empfehlungen zur Umsetzung der Anforderung	**A5 Administrationskennungen** Anforderung "Administratoren DÜRFEN unter diesen Kennungen nur administrative Arbeiten durchführen" Ein leicht umzusetzendes Verfahren ist das standardmäßige Anlegen eines zweiten persönlichen Hochschul-Benutzerkontos für alle im IT-Betrieb tätigen Personen. Es können dann die normalen Lifecycle-Verfahren Anwendung finden, manche Hochschulen haben für Admin-Kennungen spezielle Namensschemata z.B. "-adm" am Ende.
	A6 Schutz administrativer Kennungen • "Jeder Anmeldevorgang über eine Administrationskennung (Login) MUSS protokolliert werden, sodass nachvollziehbar ist, wann, auf welchem Weg und unter welcher Nutzerkennung auf das System zugegriffen wurde." • Keine Nutzung von Kennungen durch mehrere Personen Dies ist bei manchen In der Hochschulpraxis verbreiteten Produkten nicht nativ unterstützt. Z.B. gibt es nur einen einzigen administrativen Nutzer.

OPS.1.1.3 Patch- und Änderungsmanagement

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-4e0xtQ • Materialien: zki.de/goto/gp-mnaaaw
Anforderungen	Die Anforderungen sind in Hinblick auf die vorhandenen Verfahren und Rahmenbedingungen der jeweiligen Hochschule zu prüfen.
Ausnahmen	
Priorisierung	**R1**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen. An Hochschulen sind typischerweise langjährige Erfahrungen zum Thema Patch- und Änderungsmanagement vorhanden. Hochschulspezifische Herausforderungen bestehen bei • dezentralem Systembetrieb in Lehre und Forschung • und der oft üblichen Unterstützung nutzereigener Geräte (BYOD)
Empfehlungen zur Umsetzung der Anforderung	

OPS.1.1.4 Schutz vor Schadprogrammen

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-kGncSg • Materialien: zki.de/goto/gp-1Oolbg
Anforderungen	**OPS.1.1.4.A1-A7 (Basisanforderungen)** Die Anforderungen A1 - A7 sind anzuwenden. **OPS.1.1.4.A8-A9 (Standard-Anforderungen)** Die Anforderungen A8 - A9 sind anzuwenden. **OPS.1.1.4.A10-A15 (Anforderungen bei erhöhtem Schutzbedarf)** Die Anforderungen A10 - A15 sind anzuwenden.
Ausnahmen	Keine Ausnahmen.
Priorisierung	**R1 Umsetzungsreihenfolge wie im IT-Grundschutz empfohlen.**
Allgemeine Empfehlungen zum Baustein	Das BSI empfiehlt den Einsatz von cloudbasierten AV-Lösungen zur Verbesserung der Detektionsleistung (s. **OPS.1.1.4.A8)**
	OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen Wenn eine zentrale Meldung technisch nicht möglich ist, kann es hilfreich sein, die Nutzer darüber in Kenntnis zu setzen und nochmal insbesondere dafür zu sensibilisieren, die Meldungen an die Ansprechpartner durchzuführen. Dafür kann eine feste Definition der weiteren Meldewege über die Ansprechpartner an die entsprechende zentrale Stelle (RZ, ISB etc.) sinnvoll sein.

OPS.1.1.5 Protokollierung

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-d1Xy-A • Materialien: zki.de/goto/gp-kUvRdQ
Anforderungen	**A1 bis A5 (Basisanforderungen)** Die Anforderungen sind unter Berücksichtigung der Schutzzielpriorisierung der betroffenen Informationsverbünde und Anwendungen umzusetzen. **A6 bis A10 (Standardanforderungen)** Die Umsetzung der Anforderungen ist unter Berücksichtigung der Schutzzielpriorisierung der betroffenen Informationsverbünde zu prüfen.
Ausnahmen	
Priorisierung	**R1**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen.
Empfehlungen zur Umsetzung der Anforderung	

OPS.1.1.6 Software-Tests und -Freigaben

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-niAG7Q • Materialien: zki.de/goto/gp-X9QWmw
Anforderungen	**A1 bis A5 (Basisanforderungen)** Die Anforderungen sind in Hinblick auf die an der Hochschule vorhandenen Verfahren und Rahmenbedingungen unter Beachtung der Schutzzielpriorisierung zu prüfen. **A6 bis A13 (Standardanforderungen)** Die Anforderungen sind in Hinblick auf die an der Hochschule vorhandenen Verfahren und Rahmenbedingungen unter Beachtung der Schutzzielpriorisierung zu prüfen.
Ausnahmen	
Priorisierung	**R1**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen vereinbaren lassen. Es bestehen keine Zielwidersprüche der Schutzzieldimensionen (CIA). Die Hochschulpraxis ist allerdings auch gekennzeichnet durch kleinteiligere Test- und Freigabeverfahren, bei denen das im Baustein angenommene Prozedere und Instrumentarium nicht vorkommt (z.B. dedizierte Testpersonen mit spezieller Ausbildung, schriftlich zu bestätigende Freigabeerklärungen und explizite Pflichtenhefte). Ein Beispiel für solches Test- und Freigabeverfahren wäre das Upgrade des zentralen E-Elearning-Systems einer Hochschule oder des zentralen Webauftritts. Die Anforderungsanalyse, Entwicklung, Implementierung und die Tests erfolgen im Extremfall durch ein- und dieselbe Person. Die zu testende Funktionalität und mögliche Anforderungen sind unter Umständen im Vorfeld gar nicht benennbar sondern Ergebnis eines iterativen Entwicklungs- und Freigabe- und Umsetzungsprozesses. Test- und Freigabeverfahren können in einem solchen Szenario durch Akzeptanz seitens der Stakeholder umgesetzt werden. (z.B. betroffene Fachabteilung wie Prüfungsamt, Kommunikationsabteilung etc., zusätzlich auch über Change-Management-Strukturen im IT-Betrieb).
Empfehlungen zur Umsetzung der Anforderung	

OPS.1.2.2 Archivierung

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-BM4-Xg • Materialien: zki.de/goto/gp-JHvogQ
Anforderungen	**OPS 1.2.2 A1-A9** Die Anforderungen zur Basis Absicherung **OPS.1.2.2 A1 - A9** müssen umgesetzt werden. **OPS 1.2.2 A7-A19** Die Anforderungen zur Standard Absicherung **OPS.1.2.2 A7 - A19** sollten umgesetzt werden. **OPS 1.2.2 A20-A21** Bei einem erhöhtem Schutzbedarf sollten unbedingt die Empfehlungen zu **OPS.1.2.3 A20 und A21** in Betracht gezogen werden.
Ausnahmen	Keine
Priorisierung	**R3,** Umsetzungsreihenfolge wie im IT-Grundschutz empfohlen:
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

OPS.1.2.4 Telearbeit

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-mXc2FQ • Materialien: zki.de/goto/gp-xydnwQ
Anforderungen	**OSP.1.2.4.A1-A5** Die Anforderungen A1 - A5 sind anzuwenden. **OSP.1.2.4.A6-A10** Die Anforderungen A1 - A5 sind anzuwenden.
Ausnahmen	Uneingeschränkt für Verwaltungsarbeitsplätze oder Nutzung von Verwaltungssystemen auf mobilen Arbeitsplätzen in F&L. Für F&L sind A7, A8, A10 strikte Empfehlungen, d.h. Information ist notwendig, Arbeitsweisen müssen unter den Geischtpunkt der Geheimhaltung der Forschungsergebnisse betrachtetet werden.
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	Es ist zwischen Telearbeit und Mobiler Arbeit zu unterscheiden. Dies betrifft insbesonder alle auf Regelungen der Arbeitszeit beruhenden Umsetzungsanweisungen aber auch die Regelungen für die Kommunikation- insbesondere VPN, E-Mail-Verschlüsselung, Verschlüsselung von Festplatten etc.

OPS.1.2.5 Fernwartung

Versionshinweis	Bereits auf Stand Edition 2020. Neuer Name in Edition 2020: OPS.1.2.5 Fernwartung. Alter Name in Edition 2019: OPS.2.4 Fernwartung.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-uO60RA • Materialien: zki.de/goto/gp-W7xitQ
Anforderungen	Die Anforderungen sind in Hinblick auf die vorhandenen Verfahren und Rahmenbedingungen der jeweiligen Hochschule zu prüfen. Es erscheint empfehlenswert für Fernwartung die gleichen Verfahrensweisen und Grundsätze anzuwenden wie für andere Abläufe im IT-Betrieb.
Ausnahmen	
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	Bei der Fernwartung durch / mit Externen können die Anforderungen und Verfahrensweisen wie für die eigene IT- Dokumentation der Hochschule Anwendung finden (Wer, Wann, Was, Warum, Wo wird dokumentiert). **OPS.2.4.A6 Erstellung einer Richtlinie für die Fernwartung** Beispiele finden sich im Anhang.
Empfehlungen zur Umsetzung der Anforderung	

OPS.2.1 Outsourcing für Kunden

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-MEy5GA • Materialien: zki.de/goto/gp-5NusSA
Anforderungen	**OPS.2.1.A1** Die Anforderung A1 ist anzuwenden. **OPS.2.1.A2 Beteiligung Personalvertretung** Diese Anforderung wird unabhängig vom Schutzbedarf als MUSS-Anforderung anzusehen sein.
Ausnahmen	
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	**OPS.2.1.A1** Im Rahmen der allgemeinen Strategie der Hochschule muss eine *Outsourcing-Strategie* entwickelt werden. Dies ist für Hochschulen ein komplexes Unterfangen, besonders wenn Kooperationen im Rahmen von geförderten Forschungsprojekten stattfinden oder spezielle Gesetze eine gemeinsame Datenhaltung erzwingen. Das Outsourcing ist für Hochschulen mit rechtlichen Risiken verbunden (Mehrwertsteuerproblematik, Forschungsprivileg in Datenschutzgesetzen und weitere). Siehe auch Anforderung **OPS.2.1.A5 Festlegung Outsourcing-Strategie**.
Empfehlungen zur Umsetzung der Anforderung	**OPS.2.1.A2 Beteiligung Personalvertretung** Diese Anforderung wird unabhängig vom Schutzbedarf als MUSS-Anforderung anzusehen sein. Die Notwendigkeit ergibt sich nicht aus Überlegungen der Informationssicherheit, sondern aus dienstrechtlichen Erwägungen, die auf dem Persönlichkeitsrecht im öffentlichen Dienst beruhen.

OPS.2.2 Cloud-Nutzung

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-itYTNQ • Materialien: zki.de/goto/gp-WBIkTw
Anforderungen	Besondere Bedeutung in der Betriebssituation Hochschule haben A1 Cloud-Nutzungs-Strategie: Die Hochschule sollte für sich ihre Rahmenbedingungen formulieren. Beispiele finden sich im Anhang A2 Sicherheitsrichtlinie für die Cloud-Nutzung. Die Hochschule sollte für sich ihre Rahmenbedingungen formulieren. Beispiele finden sich im Anhang
Ausnahmen	*[Die Begründung ist von großer Bedeutung]*
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen. Werden Cloud-Angebote anderer Hochschulen oder ähnlicher staatlicher Einrichtungen genutzt, entfallen tendenziell Prüferfordernisse, da von gleichwertigen Rahmenbedingungen (z.B. gesetzliche Verpflichtungen) ausgegangen werden kann.
Empfehlungen zur Umsetzung der Anforderung	A1 und A2 können in einem "Leitfaden"-Dokument zusammengefasst werden.

OPS.3.1 Outsourcing für Dienstleister

Versionshinweis	Unverändert in Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1 sowie für A2-A15 und Vorschlag A16.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Ug1ibg • Materialien: zki.de/goto/gp-CZgzrw
Anforderungen	**OPS.3.1.A1 sowie A2-A15** Die Anforderungen A1 - A15 sind anzuwenden. **OPS.3.1.A16** Die Anforderung A16 ist bei hohem Schutzbedarf ebenfalls anzuwenden.
Ausnahmen	
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

DER.1 Detektion von sicherheitsrelevanten Ereignissen

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-GHiJ8A • Materialien: zki.de/goto/gp-dtZM8g
Anforderungen	Die Anforderungen zur Basis Absicherung **1.A1-A5** und die Anforderungen **1.A6 - 1.A13** müssen umgesetzt werden. Bei einem erhöhten Schutzbedarf sind müssen die Anforderungen **1.A14 - 1.A18** in Betracht gezogen werden.
Ausnahmen	Problematisch: 1.A10
Priorisierung	**R1 (1.A1 - 1.A5)** **R2 (1.A6 - 1.A8, 1.A11 - 1.A12)** **R3 (1.A9, 1.A10, 1.A13, 1.A14 - 1.A18)**
Allgemeine Empfehlungen zum Baustein	Bedingt durch die Bedrohungslage im Cyberraum gab es eim Bereich der Informationssicherheit einen Paradigmenwechsel, der sich auch im neuen IT-Grundschutz niedergeschlagen hat (Schicht DER). Es geht insbesondere um die Verbesserung der Fähigkeiten zur Erkennung von Angriffen, die Sicherstellung einer zeitnahen Reaktion und eine bessere Kooperation zum Austausch sicherheitsrelevanter Informationen. Die Anforderungen sind allgemein gehalten und daher grundsätzlich auch auf Hochschulen übertragbar. Es gilt diesen Baustein eng mit DER.2.1 (Behandlung von Sicherheitsvorfällen) und OPS.1.3-4 (Protokollierung und Schwachstellenmanagemen) zu verknüpfen. Für Mitglieder des DFN-Vereins können sich Vorteile bei der Erfüllung der Anforderungen ergeben, diese werden bei den Umsetzungsempfehlungen thematisiert.
Empfehlungen zur Umsetzung der Anforderung	**1.M1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen** **1.M2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokolldaten** **1.M3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse** **1.M4 Sensibilisierung der Mitarbeiter** **1.M5 Einsatz von mitgelieferten Systemfunktionen zur Detektion** Die Anforderungen zur Basis-Absicherung sind allgemein gültig. Zentrales Element ist die Erstellung einer Richtlinie zu diesem Themenbereich. Es ist zu empfehlen diese Richtlinie zusammen mit der Richtlinie für die Protokollierung anzugehen. Detektion und Protokollierung sind zwar nicht identisch, jedoch ist in beiden Fällen eine Beteiligung des Datenschutzbeauftragten und der Personalvertretung erforderlich. Dies gilt auch für die rechtlichen Rahmenbedingungen. Es müssen zunächst keine spezifischen Meldewege festgelegt werden, diese Aspekte sollten zusammen mit dem Baustein DER 2.1 Behandlung von Sicherheitsvorfällen angegangen werden. Hochschulangehörige über aktuelle Bedrohungen und über die Vorgehensweisen von Cyberkriminellen zu informieren, sollte nicht als spezifische Maßnahme anzusehen, sondern als Bestandteil der allgemeinen Sensibilisierung und Schulung (ORP.3.1) betrachtet werden.
	Weitere Empfehlungen folgen in Kürze.

DER.2.1 Behandlung von Sicherheitsvorfällen

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-J1ICow • Materialien: zki.de/goto/gp-IhCubg
Anforderungen	**DER.2.1.A1 bis A6; DER.2.1.A7 bis A18** Die Anforderungen A1 bis A18 sind umzusetzen. **DER.2.1.A19 bis A22** Die Anforderungen A19 bis A22 sollten bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.
Ausnahmen	Keine Ausnahmen.
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Eine zentrale Meldung von Sicherheitsvorfällen an ein CERT ist wichtig, da die Gesamtsituation (Verbreitung, generelle Auswirkungen) dort am besten eingeschätzt werden kann. DFN-Mitgliedseinrichtungen können Sicherheitsvorfälle an das DFN-CERT melden. Besonders kleinere Hochschulen ohne eigenes CERT profitieren davon. Eine gute Vernetzung der ISBs der Hochschulen bei Sicherheitsvorfällen untereinander (wie z.B. in Bayern) ist von Vorteil. Ein guter Kontakt zu den Behörden (Polizei, BSI, LSI, Verfassungsschutz, Datenschutz) ist ebenso wichtig. Es empfiehlt sich, den Erstkontakt schon VOR dem ersten Sicherheitsvorfall - in nicht stressgetriebener Atmosphäre - aufzunehmen. Aus Sicht der Hochschul-CERTs wäre eine Anpassung dieses Bausteins im Rahmen dieses Profils wünschenswert (Aktualität, Struktur, einzelne Inhalte sollten ergänzt werden). Falls besondere Anforderungen, die sich aus Struktur und Betrieb einer Hochschule ergeben, mit dem vorhandenen Baustein nicht vollständig abgedeckt werden können, sind Hochschulen, die den Baustein bereits geeiget angepasst haben, aufgerufen, ihre Erfahrungen mit dem ZKI zu teilen, damit sie in das Profil mit aufgenommen werden können.
Empfehlungen zur Umsetzung der Anforderung	**DER.2.1.A21 Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen (CIA)** Die Vernetzung von Hochschul-CERTs und Experten aus den Hochschulen zum Gedanken- und Wissensaustausch sowie zur gegenseitigen Unterstützung bei aktuellen Problemen und dem Entwurf und der Umsetzung von technisch-organisatorischen Maßnahmen hat sich bewährt und sollte weiter auf allen Ebenen ausgebaut werden.

DER.2.2 Vorsorge für die IT-Forensik

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-UTImuA • Materialien: zki.de/goto/gp-XlnxIA
Anforderungen	Die folgenden Anforderungen sind anzuwenden. **DER.2.2.A1 - A3** **DER.2.2.A4 - A12** *zusätzlich bei Verfahren mit erhöhtem Schutzbedarf* **DER.2.2.A13 - A15**
Ausnahmen	Es sind keine Ausnahmen zulässig
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	
Weitere Hinweise zur Umsetzung	BSI: Leitfaden „IT-Forensik“ Version 1.0.1 (März 2011) An der Universität der Bundeswehr München entsteht aktuell eine Seminararbeit zum Thema.

DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-vQsn0Q • Materialien: zki.de/goto/gp-l6c7Qg
Anforderungen	Die folgenden Anforderungen sind anzuwenden: **DER.2.3.A1 - A8** zusätzlich bei Verfahren mit erhöhtem Schutzbedarf **DER.2.3.A9 - A10**
Ausnahmen	Keine
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

DER.3.1 Audits und Revisionen

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-cTDtpg • Materialien: zki.de/goto/gp-ogexOw
Anforderungen	**DER.3.1.A1-A4** Die Anforderungen A1 - A4 sind anzuwenden. **DER.3.1.A7-A27** sind anzuwenden. erhöhter Schutzbedarf **DER.3.1.A28** sind anzuwenden.
Ausnahmen	
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	Vorbedingung: Die Einrichtung einer Innenrevision/internen Revision wird empfohlen
Empfehlungen zur Umsetzung der Anforderung	

DER.4 Notfallmanagement

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-0hp9Ow • Materialien: zki.de/goto/gp-WrYp1g
Anforderungen	**Basisanforderungen:** gibt es nicht und sind daher auch nicht umzusetzen. **Standardanforderungen:** DER.4.A1 und A2 sind anzuwenden. **erhöhter Schutzbedarf:** DER.4.A3 - A16 sollten angewendet werden.
Ausnahmen	
Priorisierung	**R3**
Allgemeine Empfehlungen zum Baustein	Trotz nicht vorhandener Basisanforderungen sollte man die Notfallplanung immer im Blick haben. Sie ist auch eng mit dem Risikomanagement verknüpft. Einige Hochschulen (z.B. Univ. Bayreuth, s.u.) beginnen mit dem Notfallmanagement, um basierend auf den dort gewonnenen Erkenntnissen IT-Grundschutz durchzuführen.
Empfehlungen zur Umsetzung der Anforderung	Umsetzungshinweise seitens des BSI wären wünschenswert. **Best Practise-Beispiel IT-Notfallmanagement (Vorgehensweise Univ. Bayreuth, Ralf Stöber)** 1. Erfassen der Prozesse der Hochschule in einem geeigneten Detaillierungsgrad. Beispiele: Bewerbungen von Studieninteressierten, Prüfungen, Personalverwaltung). Helfen kann hier der Geschäftsverteilungsplan. 2. Erfassen der IT-Services der Hochschule in einem geeigneten Detaillierungsgrad. Beispiele: Fileservice, Mailservice, Medientechnik im Hörsaal. 3. Bestimmung der Abhängigkeiten der IT-Services untereinander. Beispiel: Emailservice benötigt das Netzwerk. 4. Ermittlung, welcher Prozess der Hochschule welche IT-Services benötigt. 5. Ermitteln des Schutzbedarfs (hinsichtlich C, I, A) aller Prozesse der Hochschule. Zu empfehlen ist die Definition einer geeigneten Skala für jedes der drei Schutzziele zur einheitlichen Bewertung wie von 1 (sehr niedrig) bis 6 (sehr hoch). 6. Zuordnung des Schutzbedarfs aus den Prozessen zu den IT-Services nach dem Prinzip: „Der höchste Schutzbedarf zählt“ (Maximum-Prinzip). 7. Erstellung von Wiederanlaufplänen für jeden IT-Service mit Verantwortlichen, Wiederanlaufzeiten und Feststellung, welche anderen Services schon vorher laufen müssen, beispielsweise das Netzwerk vor dem Starten des Emailservice. 8. Zusammenstellung der Wiederanlaufpläne mit einem geeigneten Programm zu einem elektronischen oder gedruckten Notfallhandbuch. Als Werkzeug kann beispielsweise eine Textverarbeitung dienen. 9. Aufstellung der Leitlinie und Richtlinien: Dies erfolgt am besten zusammen mit einem Informationssicherheitsmanagementsystem.

APP.1.1 Office Produkte

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-MPVckg • Materialien: zki.de/goto/gp-fr6cZQ
Anforderungen	**APP1.1.A1-A4** Die Anforderungen A1 - A4 sind anzuwenden. **APP1.1.A5-A14** Die Anforderungen sind in der Regel umzusetzen, siehe Umsetzungshinweise **APP1.1.A15-A16** Siehe Hinweise
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Für eine verwaltbare Umsetzung der Anforderungen ist folgende Infrastruktur sinnvoll: 1. eine zentrale Richtlinienvergabe (Bsp.: AD - GPO)(APP1.1.A2, A3 A7, A10, A12, A13) 2. eine Softwareverteilung (APP1.1.A1, A6, A7, A8) 3. ein CMS (APP.1.1.A14, A15)
Empfehlungen zur Umsetzung der Anforderung	**APP1.1.A2** Eine Verteilung der Einstellung via GPO ist zu empfehlen.
	APP1.1.A6 Die Anforderung ist je nach Officeprodukt unterschiedlich komplex umzusetzen. z. B. unterstützen Microsoft Office 2019 Prof. und niedriger kein staging. Bei anderen Produkten ist der Einsatz eines Updateservers oder einer zentralen Softwareverteilung ist sinnvoll.
	APP1.1.A10 Eine Verteilung der Einstellung via GPO ist zu empfehlen.
	APP1.1.A14 Hier wird der Einsatz eines CMS mit Möglichkeit einer Versionierung (und damit Nachvollziehbarkeit von Änderungen) empfohlen. Alternativ bzw. zusätzlich wird empfohlen, solche Dokumente mit beschränkten Zugriffsrechten zu speichern.

	APP1.1.A15 Verschlüsselung: Bei lokaler Datenspeicherung ist der Einsatz von TPM Modulen auf Rechnern notwendig, bei zentraler Speicherung von Daten wird der Einsatz von entsprechenden Laufwerken mit Verschlüsselung (z.B. Teamdrive) erforderlich. Bei Verwendung eigener Nutzerzertifikate und Schlüssel ist organisatorisch sicherzustellen, dass ggf. erforderlicher Dokumentenzugriff durch Dritte bei Schlüsselverlust oder Ausscheiden des Mitarbeiters erfolgen kann (siehe Gefährdung 2.10) Signatur: Hier wird der Einsatz von Nutzerzertifikaten erforderlich, die im Mailprogramm hinterlegt werden müssen. Im Umgang mit Zertifikaten müssen die Anwender geschult werden, zudem muss der Mechanismus zur Verlängerung von Zertifikaten etabliert sein.
	APP1.1.A16 Hier ist der Einsatz externer Tools zur Sicherung der Daten vor Manipulation erforderlich.

APP.1.2 Web-Browser

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-TlLjYA • Materialien: zki.de/goto/gp-VSqzxg
Anforderungen	Die Anforderungen sind im Hinblick auf die vorhandenen Möglichkeiten und Schutzzielpriorisierungen anzuwenden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen. Die technischen Anforderungen sind in einem Gesamtkonzept der Hochschule mit anderen Bausteinen wie z.B. „ORP.3: Sensibilisierung und Schulung“ zu betrachten.
Empfehlungen zur Umsetzung der Anforderung	Es wird davon ausgegangen, dass ältere Browser üblicherweise weniger sicher sind als neue. Neue Sicherheitsfeatures werden integriert und veraltete Protokolle werden nicht mehr unterstützt. Im Hinblick auf die an Hochschulen bereitgestellten Webanwendungen dürfte es aus Sicherheitsabwägungen deshalb üblicherweise angemessen sein, keine besondere Abwärtskompatibilität mit älteren Browsern anzustreben (Insbesondere bei Anwendungen mit Authentifizierung). **APP.1.2.A6 Kennwortmanagement im Webbrowser [Benutzer] (S)** Ältere Masterpasswortverfahren (Mozilla verwendete über 10 Jahre "SHA-1 ohne Wiederholung") bieten keinen genügenden Schutz und sollten nicht verwendet werden. APP.1.2.A3 Verwendung von vertrauenswürdigen Zertifikaten Firefox: Firefox nutzt seinen eigenen Zertifikatsspeicher und nicht den Windows-Zertifikatsspeicher. Zertifikate müssen daher extra importiert werden. Das kann bei Bedarf per Richtlinie (Firefox eigene ADMX) auf den Windows-Zertifikatsspeicher umgestellt werden: https://support.umbrella.com/hc/en-us/articles/115000669728-Configuring-Firefox-to-use-the-Windows-Certificate-Store https://github.com/mozilla/policy-templates/blob/3c0d7fcf4ce4aaa7be5f5a3d66fa7c3e2b8487ad/README.md#certificates–importenterpriseroots

APP.2.1 Allgemeiner Verzeichnisdienst

APP2.1 Allgmeiner Verzeichnisdienst (Hauptseite)

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-6DSGgQ • Materialien: zki.de/goto/gp-agA4lQ
Anforderungen	**APP.2.1.A1-A15** Die Anforderungen A1 - A15 sind anzuwenden. **APP.2.1.A16** Es wird im Falle erhöhten Schutzbedarfs dringend empfohlen, den Baustein umzusetzen
Ausnahmen	
Priorisierung	**R1**
Allgemeine Empfehlungen zum Baustein	Die folgende Literatur kann zusätzliche Informationen enthalten (aus älterer Version des Bausteins) [ISFTM12] The Standard of Good Practice for Information Security Area TM 1.2 Security Event Logging, Information Security Forum (ISF), June 2018 [NISTSP800123] Guide to General Server Security NIST Special Publication 800-123, Juli 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , zuletzt abgerufen am 05.09.2018 [TKOM1] Privacy and Security Assesment Verfahren: Sicherheitsanforderungen Proxyserver Deutsche Telekom, Oktober 2016, https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/sicherheit/privacy-and-security-assessment-verfahren-342724, zuletzt abgerufen am 05.10.2018
Empfehlungen zur Umsetzung der Anforderung	**BSP.2.4.A1 Beispielanforderung A** "Informationssicherheit ist Chefsache!" Dies bedeutet, dass ... . **Umsetzungshinweise siehe BSP.2.4.M1**
	BSP.2.4.A2 Beispielanforderung B ...
	BSP.2.4.A3 Beispielanforderung C In der Zielgruppe X gilt die verpflichtende Regelung Y. Die Umsetzung der Regelung impliziert die Umsetzung dieser Anforderung.
	BSP.2.4.A8 Anforderung für besonders schützenswerte Zielobjekte X Zusätzlich zu der Anforderung besteht für die Zielgruppe dieses Profils im Allgemeinen die Verpflichtung Y. Daraus ergibt sich, dass zusätzlich folgende Anforderung umgesetzt werden muss: ... . Die Umsetzung kann wie folgt stattfinden: ...

APP.2.2 Active Directory

APP.2.2 Active Directory

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-C2gJwQ • Materialien: zki.de/goto/gp-ctJr7g
Anforderungen	**APP.2.2.A1-A12** Die Maßnahmen sind wie im Standard vorgesehen umzusetzen. **APP.2.2.A13-A15** Die Maßnahmen sollten gemäß Ergebnis der Risikoanalyse in Betracht gezogen werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	**APP.2.2.A1-A5,A8** Dabei ist zu berücksichtigen (A3), dass an Hochschulen auch System mit anderen Betriebssystemen eingesetzt werden (Linux/Unix, MacOS, Großrechnersysteme) Unter Umständen kann die folgende Literatur Grundlageninformationen geben. Bitte stets daraufachten, dass jede Information, die Server älter als 2016 betreffen, veraltet ist. [ADRL] AD Reading Library (Active Directory Security), mit weiterführender Literatur des AD Security Blogs, https://adsecurity.org/page_id=41, zuletzt abgerufen am 24.08.2018 [ESAE] Enhanced Security Administrative Environment Microsoft TechNet https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access, zuletzt abgerufen am 09.08.2018 [PAW] Privileged Access Workstations Microsoft TechNet, April 2016, http://download.microsoft.com/download/9/3/9/9392A4D2-D530-4344-8447-4A7CF1C01AEE/Privileged%20Access%20Workstation_Datasheet.pdf, zuletzt abgerufen am 09.08.2018
Empfehlungen zur Umsetzung der Anforderung	Für diesen Baustein sind Umsetzungsempfehlungen des BSI vorhanden, siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/APP/Umsetzungshinweise_zum_Baustein_APP_2_2_Active_Directory.html

APP.2.3 OpenLDAP

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Kfargw • Materialien: zki.de/goto/gp-sYwvsA
Anforderungen	**APP.2.3.A1-A6** Die Anforderungen A1 - A6 sind anzuwenden. **APP.2.3.A7-A13** Die Anforderungen A7 - A13 sind gemäß Empfehlungen anzuwenden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	**A6:** Dies ist eine Anforderung, die auch bei anderen Systemen sinnvollerweise verwendet wird. Ohne sichere Authentisierung ist das System mit hoher Wahrscheinlichkeit sehr leicht zu brechen. **A7:** OpenLDAP kann z.B. mit geeigneten Werkzeuge (ApacheDirectory Studio) verwaltete werden. Das Einspielen von Overlays und Anpassung ist nicht immer gradlinig und widerspruchsfrei, inbesondere wenn unterschiedliche Lösungen für dasselbe Thema existieren z.B. "memberOf". Daher sin genaue Kenntnisse der Arbeitsweise von OpenLdap notwendig. **A8:** Bedarf geeigneter Kenntnisse von OpenLDAP, Bei der Übernahme von Overlay ist zu prüfen, ob diese Regeln gegebenenfalls verletzt wird. **A9:** ist "größenabhängig": Beispiel Instituts-Partitionieren, Standort-Partitionierung **A13:** Sollte im "BCM (Business-Continuity-Management) Konzept mit berücksichtigt werden

APP.3.1 Webanwendungen

Versionshinweis	Version basiert auf Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-jroWgQ • Materialien: zki.de/goto/gp-5UrNLA
Anforderungen	Die Basis- und Standardanforderungen sind im Hinblick auf die vorhandenen Möglichkeiten und Schutzzielpriorisierungen anzuwenden. Werden Standardprodukte eingesetzt, kann die Erfüllung der Anforderungen oft nur im Produkt selbst erreicht werden (Angabe "[Entwickler]" im Namen der Anforderung). In der Referenzmodellierung dieses Grundschutz-Profils sind die im folgenden aufgelisteten Anwendungen und Produkte betroffen. Weitere Informationen zur produktspezifischen Umsetzung der Anforderungen und sonstigen Aspekten der einzelnen Produkte werden nach Verfügbarkeit bereitgestellt. Weitere Informationen unter zki.de/goto/gp-L4WZdA • A17 EvaExam (Evaluationen) • A26 Ilias (E-Learning) • A27 Stud.IP (E-Learning) • A28 Chat /Messenger Produkt rocketchat • A32 Produkt OTRS (Ticketsystem), Produkt kix, Produkt zammad • A33 Webserver (Webauftritt) • A34 CMS (Webauftritt) Produkt TYPO3 • A37 Moodle (E-Learning)
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen.
Empfehlungen zur Umsetzung der Anforderung	Anmerkungen zu einzelnen Anforderungen **A7 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen** kann teilweise auch über Funktionaltäten der DFN-Anbindung abgedeckt werden **A9 Beschaffung, Entwicklung und Erweiterung von Webanwendungen** Bei der Beauftragung von Dienstleistern können EVB-IT Vertragsvorlagen mitsamt den zugehörigen ABGs zuverlässige Rahmenbedingungen bieten. So ist es zum Beispiel möglich, bei Arbeiten an Open Source Produkten die Weiternutzung der beauftragten Ergebnisse ohne Rückfrage im Vertrag zu spezifizieren. Beispiele für EVB-IT Verträge zu Webanwendungen finden sich im Anhang. **A18 Kontrolle der Protokollierungsdaten** Hochschul- und anwendungsspezifisch angemessene Regelungen zu Art und Umfang der Protokollierung sowie zur Sicherstellung der systematischen Auswertung sollten festgelegt werden.

APP.3.2 Webserver

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-XYMTrQ • Materialien: zki.de/goto/gp-9LbFEQ
Anforderungen	Alle im Baustein genannten Anforderungen sind anzuwenden. **APP.3.2.A18** Sofern A18 in Anbetracht des Schutzbedarfs Anwendung finden soll, können hier eventuell Dienstleistungen des DFN als Provider in Anspruch genommen werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen.
Empfehlungen zur Umsetzung der Anforderung	

APP.3.3 Fileserver

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-TH8bkA • Materialien: zki.de/goto/gp-r6Q4CA
Anforderungen	**APP.3.3.A2 - A7; A15** Es ist empfohlen bei der Basisabsicherung neben den Basis-Anforderungen A2 - A5 sowie A15 auch schon die Standardanforderungen A6 und A7 anzuwenden. **APP.3.3.A8-A9, A11, A14** Diese Anforderungen sollten ebenfalls umgesetzt werden. **APP.3.3.A12, A13** Bei höherem Schutzbedarf sollte eine Risikoanalyse erfolgen und die Anforderungsvorschläge A12 und A13 in Betracht gezogen werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	**APP.3.3.A2** Der Einsatz der Festplatten im RAID-Verbund ist zu empfehlen. Es sollten kompatible Hotspare-Festplatten vorgehalten werden. Im Falle von virtuellen Fileservern ist die Anforderung für die Virtualisierung zu berücksichtigen (siehe SYS.1.5 Virtualisierung)
	APP.3.3.A3 OPS.1.1.4 Schutz vor Schadprogrammen sollte beachtet werden. Auf dem Fileserver muss eine aktuelle Antiviren-Software eingesetzt werden. Die meisten Anbieter bieten dedizierte Serverversionen der Antiviren-Software an. Diese sind zu bevorzugen.
	APP.3.3.A5 Die Berechtigungen sollten über AD-Gruppen zentral verwaltet werden. Zugriffsrechte dürfen nicht "auf Zuruf" vergeben werden. Ein Formular, das durch definierte "Antragsberechtigte" wie Fachbereichsleitungen oder Dezernatsleitungen oder von Ihnen benannte berechtigte Personen ausgefüllt wird erleichtert den Prozess. Die automatisierte Vergabe von Berechtigungen durch ein Script unter Berücksichtigung von Stammdaten wie Fachbereiszugehörigkeit ist zu bevorzugen.

	APP.3.3.A8 Strukturierte Datenhaltung [Benutzer] Bewährt hat sich die Erstellung von "Gruppenordnern" für Arbeits- oder Projektgruppen, Fachbereichen, Instituten, Dezernaten, Abteilungen, etc.. "Persönliche Order" der Benutzer sollten sich auch gesammelt an einem Ort finden. Programminstallationen gehören nicht auf den Fileserver.

APP.3.6 DNS-Server

APP.3.6: DNS-Server

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-tDO6GQ • Materialien: zki.de/goto/gp-6mPrzQ
Anforderungen	**APP.3.6.A1-A4, A6-A9 sind Basismassnahmen und MÜSSEN umgesetzt werden (A5 ist in Edition 2020 entfallen, s.u.)** **APP.3.6.A10-A18 sind Standardmassnahmen und SOLLEN umgesetzt werden** **APP.3.6.A19-A22 sind für erhöhten Schutzbedarf anzuwenden**
Ausnahmen	keine
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	DNS Server werden im Allgemeinen von den Netzwerk Spezialisten einer Institution betrieben. In größeren Einrichtungen ist der Einsatz eines mandantenfähigen IP-Adress Manangement Systems (IPAM) empfehlenswert.
Empfehlungen zur Umsetzung der Anforderung	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/APP/Umsetzungshinweise_zum_Baustein_APP_3_6_DNS-Server.html
	APP.3.6.A1 Planung des DNS-Einsatzes Konzept für den Einsatz von DNS schreiben. Gegebenenfalls mit dem Konzept zur Verteilung von IP Adressen in der Institution verknüpfen
	APP.3.6.A2 Einsatz redundanter DNS-Server Zusätzlich zum Primary Advertising Server in der Institution mehrere Secondary Advertising Server beim DFN betrieben. Damit werden DOS Angriffe auf DNS Server beträchtlich erschwert.
	APP.3.6.A3 Verwendung von separaten DNS-Servern für interne und externe Anfragen Die Advertising DNS Server, die Anfragen aus dem Internet entgegennehmen, sollten ausschließlich die IP Adressen von Servern auflösen, die aus dem Internet erreichbar sind. Resolving DNS Server intern für interne Abfragen.
	APP.3.6.A4 Sichere Grundkonfiguration eines DNS-Servers z.B. in der named.conf für den ISC BIND festlegen, welche IP Adressbereiche rekursive DNS Anfragen stellen dürfen
	APP.3.6.A5 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates Dies sollte ein Selbstverständlichkeit sein (APP.3.6.A5 ist deshalb in Edition 2020 entfallen). Sicherheitslücken beim BIND z.B. über die Dienste des DFN-CERT beziehen.
	APP.3.6.A6 Absicherung von dynamischen DNS-Updates Absicherung über IP Adressbereiche
	APP.3.6.A7 Überwachung von DNS-Servern Im Monitoring aktive DNS Abfragen an die eigenen DNS Server durchführen, CPU Auslastung, Platten Auslastung und Server Prozess monitoren.

	APP.3.6.A8 Verwaltung von Domainnamen [Leiter IT] DNS Domains nach Möglichkeit beim DFN Verein registrieren.
	APP.3.6.A9 Erstellen eines Notfallplans für DNS-Server Organisatorische Maßnahme

APP.4.2 SAP-ERP-System

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Hh5VFw • Materialien: zki.de/goto/gp-huXxkQ
Anforderungen	**APP.4.2.A1-A10** Die Anforderungen A1 - A10 sind anzuwenden. **APP.4.2.A11-A31** (Standard) Die Anforderungen A11 - A31 sollten angewendet werden, darunter A17 nur bei UNIX Installationen. Alle anderen bei produktiven Systemen beibehalten. **APP.4.2.A32** Bei hohem Schutzbedarf wie typischerweise bei besonders sensiblen Krankendaten, besonders sensiblen Sozialdaten, Steuerdaten, strafbaren Handlungen, Verwaltungsdaten entsprechend der „VS-Vertraulich“ sollte eine Risikoalalyse erfolgen und der Anwendungsvorschlag A32 in Betracht gezogen werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	SAP-ERP Systeme werden in Forschung und Demonstration benötigt (Training). Diese Systeme sind in eigenständigen Netzen zu betreiben unnterliegen den gleichen Anforderungen falls mehr als nur dummy Daten verwendet werden. Dies gilt insbesondere für die Nutzerdaten. Oft werden auch diese Systeme an ein AD oder LDAP angeschlossen.
Empfehlungen zur Umsetzung der Anforderung	**Siehe Umsetzungshinweise**

APP.4.3 Relationale Datenbanksysteme

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-543AxQ • Materialien: zki.de/goto/gp-exbFsQ
Anforderungen	Die Anforderungen sind Im Hinblick auf den Kontext der Datenbankinstallation anzuwenden (s. Ausnahmen)
Ausnahmen	Datenbanken die nicht direkt erreichbar sind, sondern nur durch Anwendungen, welche die Schutzanforderungen bereits gewährleisten. Bei Standardsoftware oder Webanwendungen sind Datenbanken gemäß dieses Bausteins manchmal bereits enthalten oder es werden Datenbanken separat installiert. Der Zugriff auf die Datenbank erfolgt aber ausschließlich und systemintern über eine andere Anwendung. Beispiele für solche Fälle wären MSSQL-Server oder SQLite-Dantenbanken die in Installationspaketen integral enthalten sind oder eine MariaDB-Datenbank aus den Standardquellen des Betriebssystems, auf die aber nur über eine Webanwendung zugegriffen werden kann. In solchen Fällen muss ein Großteil der Schutzanforderungen in anderen Bausteinen thematisiert werden. Die Anforderungen aus dem Baustein APP.4.3 Datenbanksysteme sind in solchen Fällen trotzdem anzuwenden, wenn die Datenbank von außen direkt genutzt werden kann oder anderweitig exponiert ist. Dies wäre zum Beispiel der Fall, wenn der Zugriff nicht alleine über ein Web-LMS (z.B.moodle) erfolgt, sondern bestimmte (auch technische) Nutzer direkt auf die verwendete Datenbank von außerhalb zugreifen.
Priorisierung	**R2** **APP.4.3.A1** Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme Die Sicherheitsrichtlinie kann auf anderen Regelungen zum Beispiel zur Nutzerverwaltung basieren. **APP.4.3.A9** Datensicherung eines Datenbanksystems Datenbanken erfordern oft spezielle Verfahren zur Datensicherung. Im Hochschulbetrieb zentral angebotene Sicherungsverfahren, die auf Dateisystemebene arbeiten sind oft nicht ausreichend. Geeignete Sicherungsverfahren sind ggf. einzurichten und deren Funktionsfähigkeit ist zu überprüfen.
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen.
Empfehlungen zur Umsetzung der Anforderung	

APP.4.6 ABAP-Programmierung

Versionshinweis	Unverändert in Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden. Daher gelten die Vorgaben des BSI für A1-A4 sowie für A5-A21 und Vorschlag A22.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-TrgWeQ • Materialien: zki.de/goto/gp-U6Ecpg
Anforderungen	**APP.4.6.A1-A4 sowie A5-A21** Die Anforderungen A1 - A21 (BSI) sind somit anzuwenden. **APP.4.6.A22** Bei erhöhtem Schutzbedarf ist der Einsatz eines ABAP-Codeanalyse-Werkzeugs sinnvoll.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	Noch keine hochschulspezifischen Empfehlungen vorhanden.

APP.5.1 Allgemeine Groupware

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Ihco8A • Materialien: zki.de/goto/gp-oBvyIQ
Anforderungen	**Die Anforderungen APP.5.1.A1-A4, A7, A22 sowie APP.5.1.A6, A8, A12, A16-A18 sind anzuwenden.** **Die Anforderung APP.5.1.A21 ist bei hohem Schutzbedarf anzuwenden.**
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen. Der Schwerpunkt der Anforderungen in diesem Baustein liegt bei E-Mail
Empfehlungen zur Umsetzung der Anforderung	

APP.5.2 Microsoft Exchange und Outlook

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-xLbDYA • Materialien: zki.de/goto/gp-Z4Zt8g
Anforderungen	**APP.5.2.A1-A5 sowie A6-A16 und A19 (neu in Edition 2020)** Die Anforderungen A1 - A16 und A19 sind anzuwenden. **APP.5.2.A17** Die Anforderungen A17 ist bei erhöhtem Sicherheitsbedarf anzuwenden
Ausnahmen	Hinweis: Gegenüber Edition 2019 sind einige Anforderungen entfallen.
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Dabei sind ALLE im Einsatz befindlichen System zu prüfen. Ein Ausschluss von Client/ Konnektoren scheint nicht möglich zu sein.
Empfehlungen zur Umsetzung der Anforderung	Der Entfall von A4, A6, A13, A16, A18 in Edition 2020 (da allgemeiner Art und nicht nur für diesen Baustein spezifisch) entbindet nicht davon, diese Anforderungen für Microsoft Exchange und Outlook umzusetzen. Gerade diei Hinwendung von Cloud Installationen macht es schwieriger dies zu überprüfen aber dennoch zwingend erforderlich.

SYS.1.1 Allgemeiner Server

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Aytcsw • Materialien: zki.de/goto/gp-WL4Ncg
Anforderungen	**SYS.1.1.A1-A10** Die Anforderungen A1-A10 sind anzuwenden. **SYS.1.1.A11-A25** Die Standardanforderungen A11-A25 sind anzuwenden. **SYS.1.1.A26-A34** Bei erhöhtem Schutzbedarf muss eine Risikoanalyse durchgeführt werden. Die Anforderungen A26-A34 sind gute Vorschläge zur Umsetzung. Die fogenden Anforderungen erscheinen im HS-Kontext je nach Anwendung insbesondere relevant: • SYS.1.1.A1 Geeignete Aufstellung [Haustechnik] • SYS.1.1.A2 Benutzerauthentisierung • SYS.1.1.A5 Schutz der Administrationsschnittstellen • SYS.1.1.A7 Updates und Patches für Firmware, Betriebssystem und Anwendungen • SYS.1.1.A8 **Regelmäßige Datensicherung** • SYS.1.1.A11 **Festlegung einer Sicherheitsrichtlinie für Server** • SYS.1.1.A15 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] • SYS.1.1.A16 Sichere Installation und Grundkonfiguration von Servern • SYS.1.1.A18 Verschlüsselung der Kommunikationsverbindungen • SYS.1.1.A20 Beschränkung des Zugangs über Netze • SYS.1.1.A21 Betriebsdokumentation • SYS.1.1.A23 Systemüberwachung • SYS.1.1.A24 Sicherheitsprüfungen • SYS.1.1.A25 Geregelte Außerbetriebnahme eines Servers • SYS.1.1.A27 Hostbasierte Angriffserkennung(IA) • SYS.1.1.A29 Einrichtung einer Testumgebung(CIA) Materialien und Beispiele zu diesem Baustein unter: zki.de/goto/gp-SdnG1g

Ausnahmen	Alle Anforderungen erscheinen grundsätzlich plausibel es bestehen keine Zielwidersprüche. Allerdings können in der Praxis die Ziele möglicherweise durch andere Maßnahmen wirtschaftlicher erreicht werden. Z.B. SYS.1.1.A6 "Alle nicht benötigten Dienste und Anwendungen MÜSSEN von Servern deaktiviert oder deinstalliert werden". So enthält beispielsweise die Grundinstallation von Ubuntu-Server viele möglicherweise nicht benötigte Anwendungen und Dienste. Es muss im Einzelfall entschieden werden, ob eine vielleicht fehlerträchtige Deaktivierung dieser Dienste notwendig ist oder die notwendigen Schutzziele nicht auch durch anderweitige Maßnahmen wie z.B. Isolierung in dedizierte virtuelle Maschinen pro Rechtekreis erreicht werden können. Ein Kriterium in diesem Zusammenhang ist die Erreichbarkeit dieser Dienste von außen.
Priorisierung	**R2** SYS.1.1.A11 Festlegung einer Sicherheitsrichtlinie für Server. Beispiele hierfür unter: zki.de/goto/gp-SdnG1g
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen. Siehe auch Umsetzungshinweise des BSI (Link unter zki.de/goto/gp-SdnG1g).
Empfehlungen zur Umsetzung der Anforderung	

SYS.1.2.2 Windows Server 2012

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-I6s67A • Materialien: zki.de/goto/gp-wPe1rA
Anforderungen	**SYS.1.2.2.A1-A3** Die Anforderungen A1-A3 sind anzuwenden. Zu A2 und A3 gibt es Empfehlungen zur Umsetzung, welche leicht von der Vorlage abweichen, siehe Umsetzungsempfehlungen **SYS.1.2.2.A4-A9** Die Standardanforderungen A4 und A5 sollten abweichend von dem BSI-Original-Baustein schon zu den Basis-Anforderungen gezählt werden und frühestmöglich umgesetzt werden. Die Anforderungen A6-A9 sollten ebenfalls vollständig umgesetzt werden. **SYS.1.2.2.A10-A14** Bei erhöhtem Schutzbedarf sind A10-A14 ebenfalls umzusetzen. Voraussichtlich wird es keinen offiziellen Baustein *Windows Server 2016* geben, weil schon ein Baustein *SYS.1.2.3 Windows Server 2019* in Planung ist, der inzwischen als Community Draft unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Drafts/Community_Draft/SYS_1_2_3_Win_Server_2019_CD.pdf?__blob=publicationFile&v=5 zur Verfügung steht. Für Windows Server 2016 steht ein benutzerdefinierter Baustein SYS.bd.1 zur Verfügung, näheres siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Benutzerdefinierte_BS/WindowsServer2016.html Bei Einsatz von Windows Server 2016 • sind die Basis-Anforderungen des benutzerspezifischen Bausteins **A3.1.1 -A3.1.5** umzusetzen. • Ergänzend sollten die Standardanforderungen **A3.2.1 - A3.2.13** umgesetzt werden, wenn die im benutzerdefinierten Baustein SYS.bd.1 (Windows Server 2016) genannten Funktionen eingesetzt werden. Abweichend vom Baustein SYS.bd.1 wird hier die Anforderung A.3.1.6 als Standardanforderung betrachtet. • Bei erhöhtem Schutzbedarf sind **A3.3.1 - A3.3.3** ebenfalls in Betracht zu ziehen. Bei EInsatz von Windows Server 2019 • sind noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1-A5 (B), A6-A9 (S) sowie A10-A12 - A21.
Ausnahmen	Einige Anforderungen müssen ggf. über lokale Gruppenrichtlinien oder Konfiguration erfüllt werden, wenn sich die Server beispielsweise nicht, wie im Baustein vorausgesetzt, in einer Domäne befinden.
Priorisierung	**R2**

Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein lassen sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren, jedoch soll auf folgende Punkte hingewiesen werden: • An Hochschulen gibt es sehr oft dezentrale IT-Strukturen, welche unabhängig voneinander betrieben werden und verschiedene Verantwortlichkeiten haben. Durch das Fehlen von Vertrauensstellungen und/oder einer gemeinsamen Domäne ist es daher oft nicht möglich Konfigurationsvorgaben für Windows Server hochschulweit und zentral gesteuert zu etablieren. Bei den Anforderungen im Originalbaustein des BSI wird jedoch von einer "Standardeinbindung in eine Active-Directory-Domäne ausgegangen". • Bei Vernetzung mit dezentralen Servern darf das Schutzniveau nicht verringert werden. Es ist daher empfehlenswert Vertrauensstellungen zwischen Active-Directory Domänen mit der Anforderung einer möglichst homogenen Systemlandschaft oder höheren Versionen (Windows Server 2016-2019) zu verbinden. Alternativ sollte man sich auf kryptographische Mindeststandards einigen, damit die Anforderungen erfüllt werden können. • In dem benutzerdefinierten Baustein SYS.bd.1 zu Windows Server 2016 werden einige zusätzliche Anforderungen den Basisanforderungen zugerechnet. Für den sicheren Betrieb von Windows Server 2012 müssen daher analog auch die Punkte A4 und A5 umgesetzt sein. Siehe auch Umsetzungshinweise des BSI unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.pdf
Empfehlungen zur Umsetzung der Anforderung	**SYS.1.2.2.A2** fordert den Einsatz der Server-Core-Variante - in der Praxis ist dies oft nicht empfehlenswert, da vielen Windows-Administratoren die entsprechende Ausbildung zur Administration mittels CLI oder Powershell fehlt und es dadurch zu sicherheitsproblematischen Betrieb kommen kann. Es ist daher abzuwägen, ob die Befähigung zum Betrieb der Server-Core oder Nano vorhanden ist. **SYS.1.2.2.A3** fordert eine Schulung der Administratoren zu sicherheitsrelevanten Aspekten. Es ist nicht klar zu welcher Windows Version diese Schulung benötigt wird und welcher Umfang oder welche Zertifizierung erwartet wird. Daher, Schulung sollte vorhanden sein, aber eine Windows Server 2012 Schulung (ggf. mit MCSA Zertifizierung bzw. gleichwertigen Kenntnissen durch Berufserfahrung) kann zum Erfüllen der Basis und Standardanforderungen auch bei Windows Server 2016 ausreichen. Insgesamt birgt die Umsetzungsempfehlung zu A3 die Gefahr, dass durch den Zwang zur Benutzung der Konsole (Server-Core-Version) ein deutlich höherer Schulungsaufwand und Erfahrung der Administratoren benötigt wird.

SYS.bd.1 Windows Server 2016

SYS.1.2.3 Windows Server

Versionshinweis	Benutzerdefinierter Baustein vom 08.05.2019.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-i7zhbw • Materialien: zki.de/goto/gp-6mVBlw
Anforderungen	**A1.1-A1.5** Die Anforderungen A1.1 - A1.5 sind umzusetzen. **A2.2-A2.3** Die Standardanforderungen **A2.1 - A2.13** sollten umgesetzt werden, insofern die hier im benutzerdefinierten Baustein SYS.bd.1 Windows Server 2016 genannten Funktionen eingesetzt werden. **A3.3.1 - A3.3.3** Bei erhöhtem Schutzbedarf sind A3.3.1 - A3.3.3 ebenfalls in Betracht zu ziehen.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

SYS.1.2.3 Windows Server 2019

Versionshinweis	Version basiert auf Community Draft SYS.1.2.3 Windows Server 2019 vom 19.03.2020. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Drafts/Community_Draft/SYS_1_2_3_Win_Server_2019_CD.pdf?__blob=publicationFile&v=5 Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1 - A5 sowie für A6-A9 und Vorschläge A10-A12.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-YskVeg • Materialien: zki.de/goto/gp-bwIRfg
Anforderungen	**SYS.1.2.3.A1-A5 sowie SYS.1.2.3.A6-A9** Die Anforderungen A1 - A9 (BSI) sind somit anzuwenden. **SYS.1.2.3.A10-A12** Bei erhöhtem Schutzbedarf sollte eine Risikoanalyse erfolgen und die Umsetzung der Vorschläge A10-A12 geprüft werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

SYS.1.3 Server unter Linux und Unix

Versionshinweis	Bereits auf Stand Edition 2020. Neuer Name in Edition 2020: SYS.1.3 Server unter Linux und Unix. Alter Name in Edition 2019: SYS.1.3 Server unter Unix.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-p8qxnQ • Materialien: zki.de/goto/gp-305s7w
Anforderungen	Alle Anforderungen sind anzuwenden. Materialien und Beispiele zu diesem Baustein unter: zki.de/goto/gp-H4XBew
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die Anforderungen in diesem Baustein dürften sich grundsätzlich mit der gängigen Betriebspraxis im zentralen IT-Betrieb von Hochschulen gut vereinbaren lassen. Beim Einsatz von Virtualisierung hat die Gewährleistung der Anforderungen durch die Virtualiserungshosts besondere Bedeutung. In den einzelnen virtualisierten Servern erübrigen sich möglicherweise Anforderungen, da die Abschottung bereits auf Ebene der Virtualisierung erfolgen kann (Abschottung auf Ebene von Servern nicht innerhalb eines Servers).
Empfehlungen zur Umsetzung der Anforderung	

SYS.1.5 Virtualisierung

Versionshinweis	Bereits auf Stand Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden. Daher gelten die Vorgaben des BSI für A1-A7 sowie für A8-A19 und Vorschläge A20-A28.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-ix3JeA • Materialien: zki.de/goto/gp-hE56JQ
Anforderungen	**SYS.1.5.A1-A7 sowie A8-A19** Die Anforderungen A1 - A19 (BSI) sind somit anzuwenden. **APP.4.6.A20-A28** Bei erhöhtem Schutzbedarf muss eine Risikoanalyse erfolgen. DIe Umsetzungsvorschläge A20-A28 sind sinnvoll.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

SYS.1.6 Container

Versionshinweis	Version basiert auf Community Draft SYS.1.6 Container vom 19.03.2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Y9XKNQ • Materialien: zki.de/goto/gp-XOPzBA
Anforderungen	Es sind die Anforderungen des Bausteins Container so umzusetzen, dass die Anforderungen aus den Bausteinen SYS.1.1 Allgemeiner Server und SYS.1.3 Server unter Unix sowie SYS.1.2.2 Windows Server unvermindert auch bei Nutzung von Containern Gewährleistet werden können.
Ausnahmen	**SYS.1.6.A3 Härtung des Host-Systems,** **SYS.1.6.A4 Härtung der Software im Container** Bei Isolation auf Ebene von Hosts sind die entsprechenden Anforderungen aus den Server-Bausteinen SYS.1.1, SYS.1.3 SYS.1.2.2. und ggf. Bausteinen zu Anwendungen grundsätzlich ausreichend. Dies ist der Fall, wenn durch die Containerisierung keine Eskalation der Freiheitsgrade im Vergleich zum Betrieb auf einem Host erfolgt. Die Anforderungen erhöhen sich nicht, wenn eine Anwendung statt direkt auf einem Host zusätzlich abgeschottet in einem Container auf diesem Host betrieben wird. **SYS.1.6.A9 Separierung der Netze,** **SYS.1.6.A10 Einbinden von Volumes** Wenn die Separierung auf Ebene der Hosts stattfindet, ist es möglich, die Anforderungen dieser Maßnahmen auch über den Host zu gewährleisten. Beispiel: eine Anwendung, ein Server und zur Anwendung zugehörige Container auf diesem Server. In diesem Fall müssen nicht zwangsweise striktere Regelungen für die Verwendung von Containern gelten als für denselben Dienst ohne Container. **SYS.1.6.A11 Administrativer Fernzugriff auf Container** Text im Baustein: "Es MUSS sichergestellt sein, dass der administrative Fernzugriff nur auf den Container-Host und nicht auf die Dienste innerhalb der Container erfolgen kann." Wenn der administrative Zugriff auf einen Host gemäß der einschlägigen Bausteine zulässig ist wenn dieser ohne den Einsatz von Containern betrieben wird, kann dieser auch bei Verwendung von Containern zulässig sein. Die fehlende Persistenz muss dabei berücksichtigt werden, sie kann in Hinblick auf die Schutzziele ein Nachteil (Gefahr des Datenverlusts) aber auch ein Vorteil (Reversibilität von Änderungen) sein.
Priorisierung	**R2**

Allgemeine Empfehlungen zum Baustein	Der Einsatz von Containern bietet in der Hochschulpraxis einerseits die Chance, eine in sich abgeschlossene und sorgfältig vorkonfigurierte Anwendungsumgebung zu erhalten. Andererseits reduziert der Einsatz von Containern die Kontrolle und auch das Wissen über die enthaltenen Komponenten. Dies erhöht die Gefährdungslage durch zwei Bedrohungen: 1. Unbehandelte Schwachstellen in Images / Abhängigkeit von externen Quellen mit unbekannter Verfügbarkeit zur bloßen Sicherstellung des laufenden Systembetriebs 2. Unerwünschte oder unerlaubte Funktionalitäten in den Containern (z.B. Datensammlung zu externen Quellen). Diese Gefährdungslage führt zu einem einem Zielkonflikt beim wirtschaftlichen Nutzen des Einsatzes von durch externe gepflegten Containern. Der Nutzen besteht oft gerade darin, sich nicht mit dem Innenleben beschäftigen zu müssen, sondern es unbesehen von extern übernehmen zu können. Die konzeptbedingt gekapselten abstrahierten Interna müssten verstanden werden um gegebenenfalls handlungsfähig zu sein. Build- und Deployprozesse müssten bei Bedarf durch die Hochschule bei mangelhaft gepflegten Images selbst betrieben werden können. Dies erscheint in typischen Anwendungsfällen unrealistisch, da ja gerade zur Bewältigung der Komplexität auf extern gepflegte Images zurückgegriffen wird. Die Anforderungen, die für den Betrieb von Server-Betriebssystem gelten (z.B. zum Einspielen von Sicherheitspatches) müssen auch auf von extern bezogene Images, welche oft ein komplettes Betriebssystem enthalten, Anwendung finden um das Schutzniveau des Gesamtverbunds nicht zu schwächen. Im Rahmen der Modellierung der Anwendung des Hochschulprofils sind als vom Hersteller bereitgestellte fertige Container z.B. ubuntu-server, mariadb, rocketchat oder gitlab zu nennen.
Empfehlungen zur Umsetzung der Anforderung	

SYS.1.8 Speicherlösungen

Versionshinweis	Version basiert auf Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1 - A5 sowie für A6-A20 und Vorschläge A21-26.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-dnEHPw • Materialien: zki.de/goto/gp-GEJQ6g
Anforderungen	**SYS.1.8.A1-A5** sowie **SYS.1.8.A6-A20** Die Anforderungen A1 - A20 (BSI) sind somit anzuwenden. **SYS.1.8.A21-A26** Bei erhöhtem Schutzbedarf sollte eine Risikoanalyse durchgeführt sowie die Umsetzung der Vorschläge A21-A26 geprüft werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

SYS.2.1 Allgemeiner Client

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-LeyDIg • Materialien: zki.de/goto/gp-TISydg
Anforderungen	Basis und Standard Anforderungen: **SYS.2.1.A1-A27** Anforderungen bei erhöhtem Schutzbedarf: **SYS.2.1.A28-A41**
Ausnahmen	keine.
Priorisierung	**R2** SYS.2.1.A1-A27
Allgemeine Empfehlungen zum Baustein	**Grundsätzliches** Es ist nicht unüblich, dass in Forschung und Lehre selbst administrierte Geräte eingesetzt werden. Sollte das in ihrer Hochschule zutreffen, müssen die Nutzenden solcher Geräte durch organisatorische Maßnahmen zur Einhaltung der Maßnahmen verpflichtet werden. Die Einhaltung sollte in angemessener Art und Weise geprüft werden. Die weiteren Maßnahmen und Betrachtung in diesem Baustein bezieht sich auf Clients, die durch die Hochschule bereit gestellt und betrieben werden. Richtlinien für den Betrieb von eigenen Clients in Netzwerken der Hochschule müssen davon separat zu beschrieben werden.
Empfehlungen zur Umsetzung der Anforderung	BSI Umsetzungshinweise

SYS.2.2.3 Clients unter Windows 10

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-bR0wJw • Materialien: zki.de/goto/gp-sf5zPw
Anforderungen	**SYS.2.2.3.A1- A6** Die Anforderungen zur Basis Absicherung müssen umgesetzt werden **SYS.2.2.3.A7 - A20** Die Anforderungen zur Standard Absicherung müssen umgesetzt werden **SYS.2.2.3.A21 - A25** Maßnahmen zur Umsetzung sollten bei Anforderung für erhöhten Schutzbedarf in Betracht gezogen werden
Ausnahmen	**SYS.2.2.3.A12 Datei- und Freigabeberechtigungen unter Windows 10 (S)** Einige hochschulspezifische Anwendungen (HIS-FSV bzw. RKS) funktionieren nur mit für Benutzer aktiven Schreibrechten für die jeweiligen Programmordner. Hier müssen Schreibrechte eingeräumt und das Programm für jeden Nutzer separat abgelegt werden um Änderungen des Programmes nicht an andere Nutzer weiter zu geben. Diese Anforderung ist in diesem Profil daher teilweise nicht anwendbar, solange diese Programme im Einsatz sind.
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	**SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem** Sofern in der Hochschule eine Richtlinie zum Einsatz von Online Diensten des Anbieters Microsoft gibt, sollte eine Integration von Online Konten dahingehend geprüft werden.
	SYS.2.2.3.A14 Einsatz des Sprachassistenten Cortana [Benutzer] (S) Ab Windows 10 2004 (20H1) wird Cortana als App bereit gestellt und kann via Powershell entfernt werden: • `Get-AppxPackage *Microsoft.549981C3F5F10* -AllUsers| Remove-AppxPackage`

SYS.2.3 Clients unter Linux und Unix

Versionshinweis	Bereits auf Stand Edition 2020. Neuer Name in Edition 2020: SYS.2.3 Clients unter Linux und Unix. Alter Name in Edition 2019: SYS.2.3 Clients unter Unix.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-dc9jXA • Materialien: zki.de/goto/gp-qSwgRA
Anforderungen	**SYS.2.3.A1- A5** Die Anforderungen zur Basis Absicherung müssen umgesetzt werden **SYS.2.3.A6 - A12** Die Anforderungen zur Standard Absicherung sollten umgesetzt werden **SYS.2.3.A13 - A20** Maßnahmen zur Umsetzung sollten bei Anforderung für erhöhten Schutzbedarf in Betracht gezogen werden
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Alle Anforderungen in diesem Baustein dürften sich mit der gängigen Betriebspraxis von Hochschulen gut vereinbaren lassen.
Empfehlungen zur Umsetzung der Anforderung	

SYS.2.4 Clients unter macOS

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-8gjgKQ • Materialien: zki.de/goto/gp-mXHO7Q
Anforderungen	**SYS.2.4.A1-A3** Die Anforderungen sind anzuwenden, siehe Hinweise **SYS.2.4.A4-A11** Die Anforderungen sind in der Regel umzusetzen, siehe Hinweise **SYS.2.4.A12** Umsetzung sollte bei Vorliegen erhöhten Schutzbedarfs geprüft werden
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Siehe Umsetzungshinweise zum BSI gemäß Grundschutz-Kompendium 2019: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.pdf
Empfehlungen zur Umsetzung der Anforderung	**SYS.2.4.A2 Nutzung der integrierten Sicherheitsfunktionen von macOS (B)** Einige hochschuleigene Programme und Programme, die für Hochschulen entwickelt werden, sind nicht digital signiert. Hier muss überprüft werden ob und wie weit Ausnahmen beim Gatekeeper zugelassen werden, ohne ihn komplett auszuhebeln. **SYS.2.4.A3 Verwendung geeigneter Benutzerkonten [Benutzer] (B)** Anmeldung von Domänennutzern ist nur gegen die eigene Domäne möglich, nicht aber als Nutzer eine Trusted Domain anmelden. Der Zugriff auf die Trusted Domain oder ggf. direkt das IDM muss dann über andere Protokolle, z.B. LDAP, erfolgen.
	SYS.2.4.A5 Deaktivierung sicherheitskritischer Funktionen von macOS (S) Deaktiviert die "Wo ist..."-Suchfunktion bei Geräteverlust

SYS.3.1 Laptops

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-1zoOGg • Materialien: zki.de/goto/gp-ZWs6Yg
Anforderungen	Basis Anforderungen **A1 - A5 sind anzuwenden** Standard Anforderungen **A6 - A15 sind anzuwenden** Anforderungen bei erhöhtem Schutzbedarf **A16 -A18 sollten angewendet werden**
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Evtl. muss **INF.9** Mobiler Arbeitsplatz berücksichtigt werden. Bezügl. **INF.7.A5** sollte eine Blickschutzfolie zur Verfügung stehen.
Empfehlungen zur Umsetzung der Anforderung	**A3 Bei Einsatz von Client Windows 10:** Wenn möglich sollte die Einstellung der Windows Defender Firewall für alle drei Profile über die Gruppenrichtlinien vorgegeben werden. Zusätzlich wird auf SYS.2.2.3.A.4 verwiesen, da evtl. die Regelung bezüglich Telemetriedaten berücksichtigt werden müssen. **A7** Damit Sichergestellt wird, wie sensible Daten sicher gelöscht werden, müssen Beschäftigte in anzuwendende Programme eingewiesen werden. (z.B. dass unter Windows mit sein eigenes "On Board" sicheres Löschprogramm "Cipher"). **A8** Aktivierung von Schnittstellen (z.B. Bluetooth, W-Lan) nur bei Bedarf.

SYS.3.2.1 Allgemeine Smartphones und Tablets

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-7U6b5g • Materialien: zki.de/goto/gp-hje1Ig
Anforderungen	**SYS.3.2.1.A1-A8** Die Anforderungen A1 - A8 sind anzuwenden. **SYS.3.2.1.A9-A22, A28** Die Anforderungen A9 - A22 sowie A28 sollten angewendet werden. **SYS.3.2.1.A23-A27, A29-A30** Die Anforderungen A23 - A27 sowie A29 - A30 sollten bei erhöhtem Schutzbedarf angewendet werden.
Ausnahmen	Die Anforderung A9 ist gegebenfalls neu auszulegen, wenn Apps für die Forschung entwickelt werden.
Priorisierung	**R2** Die Priorisierung zu R2 sollte erfolgen, um mit den Basisentscheidungen aus diesem Baustein die Umsetzung der Bausteine SYS.3.2.2, SYS.3.2.3 und SYS.3.2.4 zu ermöglichen.
Allgemeine Empfehlungen zum Baustein	Wenn eigene Apps für die Forschung entwickelt werden, muss die Anforderung A8 dahingehend geändert werden, dass diese eigenen Apps installiert werden dürfen. Die Anforderung A9 mit der Empfehlung zur restriktiven Nutzung von Funktionen muss dahingehend geändert werden, dass die Erweiterung von Funktionen zum Forschungsinteresse werden kann. Die Grundordnungen von Hochschulen sehen in der Regel eine Arbeitsteilung zentraler Aufgaben vor. Die Beschaffung allgemeiner Smartphones und Tablets ist nicht systematisch oder strategisch geregelt. Es ist ein Bewusstsein dafür zu schaffen, dass solche Geräte als Informationstechnologie anzusehen sind und von daher erstens zentral beschafft werden sollten und zweitens durch den IT-Betrieb zu managen sind. Zu den Nutzungsszenarien siehe Kategorisierung im Baustein SYS.3.2.2 (MDM). Auf strategischer Ebene sollte dieser Baustein mit den Bausteinen OPS.2.1 Outsourcing und OPS.2.2 Cloud-Nutzung bearbeitet werden. Ein datenschutzkonformer Umgang wird nur bei sehr disziplinierter Nutzung von iCloud oder Google-Diensten möglich sein, es sei denn, es gibt praktisch anwendbare alternative Cloud-Dienste.
Empfehlungen zur Umsetzung der Anforderung	**SYS.3.2.1.A2** Im Wissenschaftsbetrieb etablieren sich alternative Cloud-Dienste für E-Learning, Dateiablage und hochschulübergreifende Projektarbeit. Diese überschreiten die Grenze einer Hochschule, sind dennoch auf den akademischen Bedarf zugeschnitten. Bei der Formulierung einer Strategie für die Cloud-Nutzung sollten diese Dienste bevorzugt werden.
	SYS.3.2.1.A8 Wenn im Rahmen der Forschung eigene Apps installiert werden, sollten diese in einem eigenen App-Store mit Zertifikaten nach Industriestandards angeboten werden. In Deutschland bietet das DFN solche Zertifikate an. Solche Apps dürfen nur auf vorher definierte Netzbereiche zugreifen. Es ist zu berücksichtigen, dass die von mobilen Endgeräten gesammelten Forschungsdaten als Teil eines umfassenderen Forschungsdatenmanagements gesehen werden müssen.

	SYS.3.2.1.A9 Wenn für die Forschung eigene Apps entwickelt werden, sollte die Funktionalität von mobilen Geräten kreativ genutzt werden. Die erhöhte Angriffsfläche muss beherrschbar gemacht werden, indem solchermaßen modifizierten Endgeräten kein Zugriff auf Bereiche mit erhöhtem Schutzbedarf gestattet wird. Diese Apps müssen, sofern sie relevant für Forschungsergebnisse werden, einem Forschungsdatenmanagement zugänglich sein (Open-Access, Software-Repositories, Langzeitarchivierung).

SYS.3.2.2 Mobile Device Management (MDM)

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-JZqJZw • Materialien: zki.de/goto/gp-IFHQww
Anforderungen	In Hochschulen existieren für die verschiedenen Nutzungsszenarien mobiler Endgeräte unterschiedliche Ebenen des Informationszugangs. Die vollständige Anwendbarkeit des Bausteins ist auf nur einen Teil der möglichen Nutzungsszenarien beschränkt. Details zu den verwendeten Kategorien sind unter "Allgemeine Empfehlungen zum Baustein" aufgeführt. **SYS.3.2.2.A1 bis A6, A20; A7 bis 12, A21, A22** Geräte, die unter die Nutzungsszenarien VHME1 und VHME2 fallen: Die Anforderungen SYS. 3.2.2.A1 bis A6, A20; A7 bis 12, A21, A22 sind zu erfüllen. Geräte, die unter Nutzungsszenario VHME3 fallen: Die Anforderungen SYS.3.2.2.A1, A2, A3, A5, A6, A20; A7 bis 12, A21, A22 sind zu erfüllen. Für die Bausteine A4, A7, A8, A9, A21, A22 können Ausnahmen notwendig sein. Geräte, die unter Nutzungsszenario UHME und Betriebsmodell BYOD fallen: Die Geräte sind nicht in MDM-Systemen zu verwalten. Die Anforderungen SYS.3.2.2.A1 und A2, mit Ausnahme von Satz 2, sind zu erfüllen. **SYS.3.2.2.A14, A17, A19, A23** Geräte im Betriebsmodell 'verwaltete hochschuleigene mobile Endgeräte' (VHME): Die Anforderungen SYS.3.2.2.A14, A17, A19, A23 sind umzusetzen. Es besteht die Notwendigkeit weiterer interner Regelungen.
Ausnahmen	Ausnahme für A2 Satz 2: SYS.3.2.2 betrachtet die Nutzung eines MDM mit dem Ziel der Verwaltung aller Mobilgeräte, die im Netzwerk der Organisation verwendet werden. Die gegenwärtige Situation an den Hochschulen lässt nicht darauf schließen, dass jedes mobile Endgerät, das einen Zugang zum Campusnetzwerks erhält, in einem MDM verwaltet werden wird. Dagegen spricht die nicht bestimmbare Zahl mobiler Endgeräte mit einer großen Bandbreite an unterschiedlichen Betriebssystemen, die Studierende und Gastwissenschaftler auf dem Campus einsetzen. Ein begrenzter Informationszugang zur Einrichtung, der sich vom öffentlichen Zugang (Internet) unterscheidet, ist für dieses Geräte dennoch üblich. Ausnahme für A4: Für die wissenschaftliche Nutzung kann die Einbindung in ein MDM ausgeschlossen sein, wenn keine Vereinbarung mit den Nutzern der Geräte vorliegt. Dennoch wird in diesem Nutzungsszenario der Zugriff auf Informationen der Hochschule zuzulassen sein. Hierfür muss die MDM-Strategie Vorkehrungen treffen. Ausnahmen A7, A8, A9, A21, A22: Der administrative Einwirkung auf die Mobilgeräte ohne Kontrolle durch die Gerätenutzer kann im wissenschaftlichen Kontext einen Eingriff in Rechte auslösen, die sich aus Art. 5 Abs. 3 S. 1 GG begründen. Die wissenschaftliche Nutzung kann es beispielsweise erforderlich machen, die Aktualisierung von Apps nicht zu erzwingen oder nicht zertifizierte Apps zu nutzen bzw. Zertifikate selbst zu erstellen. Der Informationszugang innerhalb der Hochschule muss für diese Ausnahmen in der Mobilgerätestrategie spezifiziert werden.
Priorisierung	**R2**

Allgemeine Empfehlungen zum Baustein	Der Einsatz von MDM-Systemen zur Verwaltung von mobilen Endgeräten kann nur erfolgen, wenn die Maßnahmen zur Umsetzung der Bausteinanforderungen relevante gesetzliche und interne Regelungen berücksichtigen. Darüber hinaus ist zu erwarten, dass eine Notwendigkeit an zusätzlicher interner Regelung durch dienstliche Anweisungen oder Vereinbarungen entsteht. Mit dem Begriff Vereinbarung sind hier entweder freiwillige oder in der betrieblichen Mitbestimmungsvorschrift festgelegte Formen von Vereinbarungen zwischen der Vertretung einer Hochschulstatusgruppe und der Dienststelle gemeint. In den Umsetzungshinweisen des BSI werden zwei mögliche Betriebsmodelle genannt (BSI1 2019: Abschnitt 2.1 Basismaßnahmen): • institutionseigene (hier: hochschuleigene) mobile Endgeräte • private mobile Endgeräte (BYOD) Nach Vorgabe von SYS.3.2.2.A1 muss im Rahmen der Mobilgerätestrategie für diese Betriebsmodelle definiert werden, welcher Zugriff auf die IT-Ressourcen der Hochschule bestehen soll. Für den Hochschulkontext muss das Betriebsmodell hochschuleigene mobile Endgeräte weiter differenziert werden, weil die Wirksamkeit von Art. 5 Abs. 3 S. 1 GG ("Kunst- und Wissenschaftsfreiheit") Einfluss auf die Administrationsfähigkeit von Geräten in wissenschaftlichem oder künstlereichen Einsatzbedingungen hat. **<u>Unterteilung des Betriebsmodells hochschuleigene mobile Endgeräte (HME)</u>** Die Verwaltung „hochschuleigener mobiler Endgeräte“ in MDM-Systemen sollte im allgemeinen angestrebt werden. Eine Verwaltung durch ein MDM-System nach den Anforderungen dieses Bausteins kann jedoch dem Einsatz eines Geräts als Arbeits- oder Hilfsmittel zur wissenschaftlichen Betätigung aus verschiedenen Gründen entgegenstehen. Es wird empfohlen, die private Nutzung hochschuleigener mobiler Endgeräte zu untersagen, um die Umsetzsetzbarkeit der Bausteinanforderungen zu verbessern. Ist die private Nutzung nicht ausgeschlossen, müssen für diese Geräte Compliance-Aufgaben wie für private Geräte bearbeitet werden. Interne Regelungen, die Einschränkungen zu übergeordneten Vorschriften festlegen sollen, können dadurch unwirksam sein. **VHME** Verwaltete hochschuleigene mobile Endgeräte, die in ein MDM eingebunden oder zur Einbindung in ein MDM vorgesehen sind. Diese Gerätegruppe wird für verschiedene Nutzungsszenarien weiter unterteilt. **VHME1** Hochschuleigene mobile Endgeräte ohne Nutzung zu wissenschaftlichen Zwecken Beispiel: Mobile Geräte in der Hochschulverwaltung. Es besteht weitgehend die Möglichkeit, den Einsatz von MDM-Systemen durch dienstliche Anweisungen und Dienstvereinbarungen zu regeln. **VHME2** Hochschuleigene mobile Endgeräte zur kurzzeitigen Überlassung an Hochschulangehörige, auch zur wissenschaftlichen Nutzung Beispiel: Mobile Geräte für zeitlich begrenzte Einsatzzwecke in Forschung, Lehre, Wissenschaftstransfer, Verwaltung oder in der Weiterbildung (Laborgeräte, Leihgeräte). Es sollten Informationen zur Nutzung ausgehändigt werden. Vor jeder Nutzung ist die Zustimmung zu den Nutzungsbedingungen einzuholen. Zugriffsmöglichkeiten auf Informationen der Hochschule dürfen nur nach einem nutzerbezogenen Berechtigungsverfahren bestehen. Die Geräte sind nach jeder Nutzung und vor der Übergabe an neue Nutzer in den Ausgangszustand zurückzusetzen.

	VHME3 Hochschuleigene mobile Endgeräte mit dauerhafter Überlassung an wissenschaftlich arbeitende Hochschulangehörige mit Einbindung in ein MDM, wobei die Nutzenden einem freiwilligen, teilweisen Verzicht auf Grundrechte, die sich aus Art. 5 Abs. 3 S. 1 GG ergeben, zustimmen müssen. Zur Umsetzbarkeit einiger Anforderungen des Bausteins sind daher Vereinbarungen zwischen Dienststelle und Nutzer zu treffen. Beispiele: Dienst-Smartphones, Tabletcomputer der Wissenschaftler **UHME** Hochschuleigene mobile Endgeräte, die nicht in einem MDM-verwaltet werden (unmanaged). Der Betrieb von unverwalteten hochschuleigenen mobilen Endgeräte ergibt sich, wenn Vereinbarungen zur MDM-Verwaltung nicht getroffen wurden, aber hochschuleigene Geräte beschafft und genutzt werden. Die Beschaffung sollte dennoch so stattfinden, dass diese Geräte den Anforderungen zum MDM genügen (A2). Für hochschuleigene mobile Endgeräte ohne MDM-Einbindung finden somit nur die strategischen Anforderungen des Bausteins SYS. 3.2.2 Anwendung. **Betriebsmodell BYOD** Nicht-hochschuleigene mobile Endgeräte, die in der Hochschule genutzt werden. Beispiele: Mobile Endgeräte von Studierenden, Gastwissenschaftlern und anderen Nicht-Hochschulangehörigen Es finden nur die strategischen Anforderungen des Bausteins SYS.3.2.2 Anwendung. Nicht-hochschuleigene mobile Endgeräte sind als nicht vertrauenswürdig einzustufen und es wird empfohlen, sie nur für eingeschränkte, in der MDM-Strategie festgelegte Informationszugänge zuzulassen. Für das Betriebsmodell BYOD werden in den Umsetzungshinweisen im Abschnitt "Welche[s] Betriebsmodell soll für mobile Endgeräte in Betracht kommen?" sieben Ausschlusskriterien für ein Zulassen von BYOD genannt. Die Wahrscheinlichkeit, dass in Hochschulen eine dieser Fragen mit Nein beantwortet wird ist hoch. Als Beispiel sei die Frage nach der Vereinbarung zur Löschung des Gerätedatenbestands in Notfällen genannt. Die Hürde zur Einbindung in ein MDM-System wird durch Compliance-Anforderungen weiter erhöht. Wenn private Geräte in ein MDM einbezogen würden, ergäben sich umfassende Anforderungen im Bereich der Persönlichkeitsrechte, u.a. im Kontext des Datenschutzes (Studierende, Hochschullehrer) und der betrieblichen Mitbestimmung (Mitarbeitende).
Empfehlungen zur Umsetzung der Anforderung Umsetzungshinweise des BSI	Mehrere Bausteinanforderungen und Umsetzungshinweise enthalten bereits Formulierungen, die auf eine Notwendigkeit zur internen Regelung enthalten. Im Hochschulkontext sind vor allem zusätzliche Compliance-Aufgaben, die für die Hochschulstatusgruppen jeweils verschiedenen ausfallen können, zu berücksichtigen. **SYS.3.2.2.A1, A2, A3** Eine MDM-Strategie ist durch die Leitung der Hochschule zu formulieren. Unter MDM-Strategie ist hier weniger in Bezug zu einem Softwaresystem zu sehen, als zum generellen Umgang mit mobilen Endgeräten an der Hochschule. Die darauffolgenden Anforderungen thematisieren vornehmlich das Management eines MDM-Systems. Eine hochschulweite Verpflichtung zur zentralen Beschaffung mobiler Endgeräte kann die Bandbreite verschiedner Endgeräte minimieren und die technische Kompatibilität zum MDM sichern. Die Umsetzbarkeit von A2 verbessert sich.
	SYS.3.2.2.A4 Aus der MDM-Strategie sowie den technischen und organisatorischen Anforderungen der Hochschule sind Richtlinien zu erstellen. Wird für bestimmte Gruppen mobiler Endgeräte die Einbindung in ein MDM ausgeschlossen, muss der Umfang des Informationszugangs für diese Geräte durch Richtlinien bestimmt werden, die auch außerhalb des MDM-Systems gelten.

	SYS.3.2.2.A5 Die Zulässigkeit der Eingriffe durch den MDM-Client in die Autonomie der Gerätebesitzer ist bei wissenschaftlicher Nutzung durch Vereinbarungen zu regeln, anderenfalls ist die Anforderung nicht umsetzbar.
	SYS.3.2.2.A6 und bei erhöhtem Schutzbedarf **A17** Die Zulässigkeit der Protokollierung sicherheitsrelevanter Ereignisse, wodurch personenbeziehbare Daten gespeichert werden, muss explizit geregelt werden. Umfassende Protokollierung könnte zu einer nicht zulässigen Überwachung von Hochschulangehörigen eingesetzt werden. Die regelmäßige ‚befugte' Prüfung der Protokolleinträge (A6) und somit Einsichtnahme durch Angehörige der Universität bedarf aus gleichem Grund der Regelung.
	SYS.3.2.2.A11, A20 Ein Zugriffsberechtigungskonzept (Datenschutzerfordernis) muss erstellt werden, damit die Anforderungen umgesetzt werden können.
	SYS.3.2.2.A22 und bei erhöhtem Schutzbedarf **A19** Die Fernlöschung auf dienstlichen Geräten muss Gegenstand einer internen Vereinbarung sein. Administratives Wiping kann auch bei dienstlicher Nutzung u.a. Urheberrechte und Grundrechte (Stichwort Wissenschaftsfreiheit) berühren. (BGH, Urteil vom 21.02.2019, Az. I ZR 15/18) Geeignet sind Lösungen, die es dem Nutzer ermöglichen, die Fernlöschung selbst durchzuführen oder dies nachvollziehbar zu autorisieren.

SYS.3.2.3 iOS (for Enterprise)

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-GqLp5w • Materialien: zki.de/goto/gp-FfFaug
Anforderungen	**SYS.3.2.3.A1,A2,A5** Die Anforderungen A1, A2, A5 sind anzuwenden. Die Anforderungen A3-A6 sowie A8 werden im Baustein mit Stand Febr. 2020 als „entfallen“ deklariert. Die Anforderung A1 („Strategie für iOS-Nutzung“) muss von der Hochschulleitung als entscheidend verstanden werden, um alle weiteren Richtlinien dieses Bausteins in zentralen und dezentralen Untereinrichtungen durchzusetzen. Für die Anforderung A2 sind Cloud-Dienste zu entwickeln, die geeignet sind, Apple-Dienste zu ersetzen. **SYS.3.2.3.A10-A15,A17-A18,A20-A21** Die Anforderungen A9, A16, A19, A22, A24, A27 werden im Baustein als „entfallen“ deklariert.
Ausnahmen	n.a.
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die hochschulspezifische Umsetzung dieses Bausteins SYS.3.2.3 muss sich an Entscheidungen des Bausteines SYS.3.2.1 und SYS.3.2.2 orientieren. Im Rahmen dieser Bausteine MÜSSEN Entscheidungen getroffen werden, aus denen sich Konkretisierungen in diesem Baustein SYS. 3.2.3 ableiten (Betriebsmodelle VHME1-3, UHME oder BYOD). Das betrifft A1 und weitere. Hierbei ist besonders zu prüfen, ob die „General Terms & Conditions“ von Apple akzeptierbar sind. An Hochschulen hat sich besonders im Bereich der Lehre und der Forschung großflächig der Einsatz von BYOD durchgesetzt, weil es keine Regelungen oder Richtlinien gibt. Der Verweis auf Art. 5 Abs. 3 S. 1 GG wird verwendet (Freiheit der Forschung) wird verwendet, um den Einsatz trotz Regulierungslücke zu begründen und aufrechtzuerhalten. Regulierungen werden als Eingriff in eingeführte Arbeitsabläufe interpretiert werden und müssen entsprechend gemanagt werden. Um die Zahl unautorisierter iOS-Geräte zu vermindern, sollte eine zentrale Beschaffung etabliert werden. Mit ihr können Prozesse zu einem MDM etabliert werden, die alle Dienstgeräte unter iOS erfassen (A1, A11, A12, A13, A14, A20, A21, A23, A25, A26). Dazu bedarf es einer Zustimmung der Hochschulleitung, iOS-Geräte beschaffen zu dürfen. Falls diese vorliegt, muss das gemäß Baustein SYS.3.2.2 eingesetzte MDM die Plattform iOS unterstützen. Zur Ersetzung von kommerziellen Cloud-Diensten durch Apple müssen gleichwertige Dienste entwickelt werden. Diese sind gegebenfalls hochschulübergreifend zu entwickeln, wenn sie die Ressourcen einzelner Hochschulen übersteigen (Anforderung A2). Je nach Bundesland gibt es landesweite Lizenzgemeinschaften. Volumenlizenzen für Apps und Cloudlizenzen sind gegebenenfalls über diese abzuwickeln (A12).
Empfehlungen zur Umsetzung der Anforderung	**SYS.3.2.3.A1** Der bereits breit etablierte Einsatz von iOS als BYOD muss zwischen Wissenschaftsfreiheit und notwendiger Regulierung abgewogen werden. Dazu ist entweder eine entschiedene Durchsetzung einer Entscheidung der Hochschulleitung oder ein hochschulweiter Konsens notwendig.

	SYS.3.2.3.A2 Cloud-Diensten von Apple, deren „General Terms & Conditions“ anzwendenden Gesetzen oder hochschuleigenen Regelungen widersprechen, müssen alternative Cloud-Dienste entgegengestellt werden. Sie müssen verpflichtend oder eindeutig über Richtlinien reguliert sein, aber gleichzeitig als praktikable Alternative angeboten werden.

SYS.3.2.4 Android

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-dsRG8w • Materialien: zki.de/goto/gp-eZf1rg
Anforderungen	**SYS.3.2.4.A1** Die Anforderungen A1 MUSS angewendet werden. **SYS.3.2.4.A2-A7** Die Anforderungen A2-A5 sollten angewendet werden.
Ausnahmen	Im Fall des Betriebsmodells VHME2 (siehe SYS.3.2.2) ist die Anforderung A3 (Entsprechung der Geräte-ID zu einer natürlichen Person) nicht anwendbar.
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Baustein muss unbedingt zusammen mit Bausteinen SYS.3.2.1 und SYS.3.2.2 bearbeitet werden.
Empfehlungen zur Umsetzung der Anforderung	**SYS.3.2.4.A1** Die Wahl für ein Smartphone, Phablet oder Tablet unter Android darf sich nicht in erster Linie am Beschaffungspreis orientieren. Erfahrungsgemäß fallen günstigere Geräte schnell aus den Programmen zur Versorgung mit Sicherheitsupdates. Es ist zu prüfen, ob die „General Terms & Conditions“ des Anbieters oder des Lieferanten akzeptabel sind. Diese Anforderung MUSS umgesetzt werden.
	In Anlehnung an die Anforderung A4 des Bausteins SYS.3.2.2.A4 (Verteilung einer Grundkonfiguration auf mobile Geräte) sollte dieser Baustein SYS.3.2.4 Android ergänzt werden, dass über einen zentralen Beschaffungsprozess auch eine flächendeckende Grundkonfiguration von Android-Geräten angestrebt wird.
	Bei der Wahl des Betriebsmodells BYOD sollten Android-Geräten ohne eine Konfiguration durch ein MDM Zugriff nur zu bestimmten Netzbereichen gestattet werden. Netzbereiche mit höherem Schutzbedarf (zentrale Verwaltung, patentwürdige Forschungsdaten) MÜSSEN so konfiguriert werden, dass nur berechtigte Geräte zugreifen können. Der Nachweis sollte über Zertifikate erfolgen, die über MDM in einem protokollierten Prozess eingespielt wurden.
	Für Hochschulen können mobile Geräte unter Android interessant werden, weil sie folgende Bedingungen erfüllen: • Es können eigene Apps für die Feldforschung entwickelt werden, weil keine Herstellerprüfung die Installation eigener Software unterbindet und die Hardware eigener Forschung zugänglich ist. • Im Fall des Einsatzes in der Forschung muss der Einsatz von Mobilgeräten zum Bestandteil des Forschungsdatenmanagements werden. • Für technische Dienste der Universität (Computer Aided Facility Management oder CAFM, weitere Dienste) bieten Android-Geräte eine Plattform, mit der ihre Aufgaben effizienter erledigt werden können. Es ist zu prüfen, ob der wirtschaftliche Nutzen in der Abwägung höher eingeschätzt wird als das potenzielle zusätzliche Risiko. • Für Android-Geräte gibt es alternative Betriebssysteme.
	Für Android-Geräte sollten Dienste entwickelt werden, die der Zwangsaktivierung mittels einer Google-ID eine praktikable Alternative entgegenstellen.

SYS.3.3 Mobiltelefon

Versionshinweis	Bereits auf Stand Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1-A4 sowie A5-A12 und Vorschläge A13-A15.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-n49aTg • Materialien: zki.de/goto/gp-rlPDpw
Anforderungen	**SYS.3.3.A1-A4** sowie **SYS.3.3.A5-A12** Die Anforderungen A1 - A12 (BSI) sind somit anzuwenden. **SYS.3.3.A13-A15** Bei erhöhtem Schutzbedarf sollte eine Risikoanalyse erfolgen und die Umsetzung der Vorschläge A13-A18 geprüft werden.
Ausnahmen	Diese Anforderung ist in diesem Profil nicht anwendbar, weil ...
Priorisierung	**R1**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-yv7y5g • Materialien: zki.de/goto/gp-3W35Ew
Anforderungen	**SYS.4.1.A1-A2, A12, A22** sowie **A4-A5, A7, A11, A15, A17-A19** Alle Basis- und Standardanforderungen sind umzusetzen. **SYS.4.1.A14** Umzusetzen bei öffentlich zugänglichen Druckern, z. B. Druckstationen für Studierende. **SYS.4.1.A20** In den Geschäftsprozessen G01, G03 und G04 sollte die Notwendigkeit einer verschlüsselten Übertragung geprüft und die Entscheidung dokumentiert werden.
Ausnahmen	Keine
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	**SYS.4.1.A1 Erstellung eines Basis-Konzepts für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten [Leiter IT]** → Umsetzungshinweise siehe SYS.4.1.M1
	SYS.4.1.A2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte → Umsetzungshinweise siehe SYS.4.1.M2 Insbesondere in offenen Hochschulen sollte bei Druckern für Büroarbeitsplätze auf die Aufstellung in zutrittsgeschützten Bereichen geachtet werden.
	SYS.4.1.A12 Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln → Umsetzungshinweise siehe SYS.4.1.M12
	SYS.4.1.A4 Erstellung eines Sicherheitskonzeptes für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten [Leiter IT] → Umsetzungshinweise siehe SYS.4.1.M4
	SYS.4.1.A5 Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten [ISB] → Umsetzungshinweise siehe SYS.4.1.M5
	SYS.4.1.A7 Beschränkung der Administrationszugriffe auf Drucker, Kopierer und Multifunktionsgeräte → Umsetzungshinweise siehe SYS.4.1.M7
	SYS.4.1.A11 Netztrennung beim Einsatz von Multifunktionsgeräten → Umsetzungshinweise siehe SYS.4.1.M11

	SYS.4.1.A15 Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten(CI) → Umsetzungshinweise siehe SYS.4.1.M15

SYS.4.5 Wechseldatenträger

Versionshinweis	Bereits auf Stand Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1-A2, A12 sowie für A4-A7, A13 und Vorschläge A10-A11, A14-A16. Neuer Name in Edition 2020: SYS.4.5 Wechseldatenträger. Alter Name in Edition 2019: SYS.3.4 Mobile Datenträger.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Dlqljg • Materialien: zki.de/goto/gp-PjF2Uw
Anforderungen	**SYS.4.5.A1-A2, A12** sowie für **SYS.4.5.A4-A7, A13** Die Anforderungen A1-A2, A12 und A4-A7, A13 sind somit anzuwenden. **SYS.4.5.A10-A11, A14-A16** Bei erhöhtem Schutzbedarf sollte eine Risikoanalyse erfolgen und die Umsetzung der Vorschläge A10-A11, A14-A16 geprüft werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

NET.1.1 Netzarchitektur und -design

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-jGBCKw • Materialien: zki.de/goto/gp-FKOCaA
Anforderungen	**NET.1.1.A1-A27** Die Anforderungen A1 - A15 (Basis) und A 16 - A 27 (Standard) sind grundsätzlich anzuwenden. Für spezifische Anforderungen (siehe Ausnahmen) können eigenen Netzsegmente gebildet werden. **NET.1.1.A28 - A36** Die Anforderungen A28 - A36 (erhöhter Schutzbedarf) sind in Abhängigkeit sehr hoher Schutzbedarfe (Hochverfügbarkeit etc.) anzuwenden.
Ausnahmen	Die Anforderungen A 4 (Firewall + Whitelisting), A 5 (Client-Server-Segmentierung), A 10 (DMZ-Segmentierung), A 11/ A12 (Absicherung ein und ausgehender Kommunikation) sind für einzelne Teilbereiche einer Hochschule (insbesondere Forschung an und mit IT) problematisch. Ein starke Einschränkung der techn. Kommunikationswege könnte im Widerspruch mit den wissenschaftlichen Anforderungen IT-naher Forschungsbereiche (Bspw. Einrichtung eines Honeypots für IT-Sicherheitsforschung) stehen.
Priorisierung	**R2** zusammen mit den Bausteinen NET.1.2 (Netzmanagement) und NET.3 (Netzkomponenten, insb. Firewall) sinnvoll.
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	**NET.1.1.A4 Netztrennung in Sicherheitszonen** Zur Umsetzung der Anforderung A 4 (Netztrennung in Sicherheitszonen) könnten spezifische Netzsegmente für IT-Forschung eingerichtet werden, in der die o.g. Ausnahmen abgebildet werden.

NET.1.2 Netzmanagement

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-EWjbzA • Materialien: zki.de/goto/gp-MKnKLA
Anforderungen	**NET.1.2.A1-A29** Die Anforderungen A1 - A10 (Basis) und A11 - A 29 (Standard) sind anzuwenden. **NET.1.2.A30 - A38** Die Anforderungen A30 - A 38 sind bei besonderen Sicherheitsanforderungen, z.B. Hochverfügbarkeit oder Anbindung kritischer Systeme, anzuwenden.
Ausnahmen	
Priorisierung	**R2,** zusammen mit den Bausteinen NET.1.1 (Netzarchitektur) und NET.3 (Netzkomponenten) sinnvoll.
Allgemeine Empfehlungen zum Baustein	Der inhaltliche Wegfall der „regelmäßigen Änderung von Passwörtern“ sowie die Behandlung der Passwortsicherheit in ORP.4.A8 in Edition 2020 ist hilfreich.
Empfehlungen zur Umsetzung der Anforderung	

NET.2.1 WLAN-Betrieb

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-ltMdrw • Materialien: zki.de/goto/gp-RW20Ww
Anforderungen	**NET.2.1.A1-A14** Die Anforderungen A1 - A8 (Basis) und A9 - A14 (Standard) sind anzuwenden. **NET.2.1.A15 - A18** Die Anforderungen A15 - A18 sind bei besonderen Sicherheitsanforderungen, z.B. Hochverfügbarkeit oder Anbindung kritischer Systeme, anzuwenden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	In Hochschulen ist es sinnvoll unterschiedlich gesicherte WLAN zu betreiben bspw.: 1. eduroam für Mitarbeitende und Studierende 2. WLAN-Gästeportal für Gäste mit bekannter Identität 3. WLAN mit WPA2 mit Pre-Shared Keys für spezielle Veranstaltungen/Tagungen bei denen die Teilnehmer im Vorfeld nicht bekannt sind.
Empfehlungen zur Umsetzung der Anforderung	**NET.2.1.A12 Einsatz einer geeigneten WLAN-Management-Lösung** Die Management-Lösung SOLLTE den eduroam-Dienst unterstützen. eduroam bietet weltweit und aus unsicheren Netzen heraus einen sicheren und zugleich komfortablen WLAN-Zugang zum Wissenschaftsnetz und zum Netz der eigenen Hochschule.

NET.2.2 WLAN-Nutzung

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-qet9Lw • Materialien: zki.de/goto/gp-9ixUtQ
Anforderungen	**APP.5.2.A1-A3 sowie A4** Die Anforderungen A1 - A4 sind anzuwenden. Für einen erhöhten Schutzbedarf sind keine Anforderungen des BSI definiert. In diesem Fall sollte eine Risikoanalyse erfolgen.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Bei Hochschulen spielt die Verfügbarkeit von Wissenschaftnetzen (eduroam), eingeschränkt offenen Netzen für Studierende und öffentlichen Netze eine Rolle bei der Nutzung.
Empfehlungen zur Umsetzung der Anforderung	

NET.3.1 Router und Switches

Versionshinweis	Unverändert in Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1 - A9 sowie für A10-A23 und Vorschläge A24-A28.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Ks8XrQ • Materialien: zki.de/goto/gp-FXDb9Q
Anforderungen	**NET.3.1.A1-A9 sowie A10-A23** Die Anforderungen A1 - A23 (BSI) sind somit anzuwenden. **NET.3.1.A24-A28** Bei erhöhtem Schutzbedarf sollte eine Risikoanalyse erfolgen und die Umsetzung des Vorschläge A24-A28 geprüft werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

NET.3.2 Firewall

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-fgn1MQ • Materialien: zki.de/goto/gp-iHhCEg
Anforderungen	**NET.3.2.A1 - A15 Basisanforderungen** Die Anforderungen A1 - A15 sind grundsätzlich anzuwenden. **NET.3.2.A16 - A24** Die Anforderungen A16 - A24 sind anzuwenden, ggf. eingeschränkt auf bestimmte Netzsegmente (Vgl. NET.1.1) . **NET.3.2.A25 - A31** Die Anforderungen A25 - A31 sind für besondere, höhere Schutzbedarfe anzuwenden. Dazu sollten geeignete Netzsegmente in Abhängigkeit der Schutzbedarfe (Vgl. NET.1.1) definiert werden.
Ausnahmen	Die Anforderung "NET.3.2.A2: die gesammte Kommunikation ist über die Firewall zu leiten" kann für Daten intensive Forschung Kapazitätsprobleme verursachen.
Priorisierung	**R2,** zusammen mit den Bausteinen NET1.1 (Netzarchitektur) und NET.1.2 (Netzmanagement) sinnvoll.
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	**NET.3.2.A2 Festlegen der Firewall-Regeln** Einrichtung von "Performance-Bypässen" neben der Firewall für spezifische (bekannt und definiert) datenintensive Verbindungen auf Anforderung.

NET.3.3 VPN

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-4wFs1g • Materialien: zki.de/goto/gp-uBtEEw
Anforderungen	**NET.3.3.A1 - A5 Basisanforderungen** Die Anforderungen A1 - A5 sind anzuwenden. **NET.3.2.A6 - A13** Die Anforderungen A16 - A24 sind anzuwenden, ggf. eingeschränkt auf bestimmte Netzsegmente (Vgl. NET.1.1) .
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Problematisch ist die Verwendung im F&L Bereich. Die Systeme werden mobil genutzt, System ausserhalb des Zugriffs der Hochschule werden verwendet z.B. Drucker, Netzwerkspeicher. Der Rechner spielt einen Mittler. Der Zugriff per VPN auf Verwaltungssysteme ist **zwingend**.
Empfehlungen zur Umsetzung der Anforderung	

NET.4.1 TK-Anlagen

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-3LZ1Ug • Materialien: zki.de/goto/gp-pqYUoA
Anforderungen	**NET.4.1.A1-A17** Die Anforderungen A1 - A17 sind anzuwenden. **NET.4.1.A18-A19** Die Anforderungen A18 und A19 sind für für erhöhten Schutzbedarf anzuwenden.
Ausnahmen	keine
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die Umsetzungshinweise zum Baustein NET.4.1 TK-Anlagen des BSI IT-Grundschutz-Kataloges enthalten eine sehr umfangreiche Sammlung an Umsetzungshinweisen. Hinweis: Bei der Erweiterung einer existierenden TK-Anlage mit VoIP-Technik (Voice over IP) oder der Neuinstallation einer VoIP-TK-Anlage sind die Anforderungen des Bausteins NET.4.2 - explizit auch die Anforderungen bei erhöhtem Schutzbedarf - zu beachten.
Empfehlungen zur Umsetzung der Anforderung	**NET.4.1.A1 Anforderungsanalyse und Planung für TK-Anlagen** **NET.4.1.A2 Auswahl von TK-Diensteanbietern** **NET.4.1.A13 Beschaffung von TK-Anlagen** Bei der Erweiterung einer bestehenden TK-Anlage auf VoIP-Technik (Voice over IP) sollte die Möglichkeit zum Umwandeln von Zugriffslizenzen von "klassischen Endpunkten / Endgeräten" auf "VoIP Endpunkte / Endgeräte" geprüft werden. Es ist nicht ausgeschlossen, dass Zugriffslizenzen im Rahmen eines Erweiterungsprojektes umgewandelt werden können. Werden die Anzahl der Endgeräte Lizenzen zur Berechnung der Wartungsgebühren herangezogen gibt es hier doppeltes Potential.
	NET.4.1.A10 Dokumentation und Revision der TK-Anlagenkonfiguration Auf vollständige Dokumentation aller Komponenten und Konfigurationen - auch vom Hersteller der TK-Anlage - muss bestanden werden. Es ist nicht unüblich dass Herstellerdokumente - interne Konfigurationshinweise, Workarounds, Sicherheits-Patches, u.s.w. nicht ausgehändigt werden.

NET.4.2 VoIP

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-IUVBcg • Materialien: zki.de/goto/gp-UmfJpA
Anforderungen	**NET.4.2.A1-A13** Die Anforderungen A1 - A13 sind anzuwenden. **NET.4.2.A14-A16** Die Anforderungen A14 - A16 sind für für erhöhten Schutzbedarf empfohlen. Siehe **Allgemeine Empfehlungen zum Baustein** in den folgenden Abschnitten.
Ausnahmen	keine
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die Umsetzungshinweise zum Baustein NET.4.2 VoIP des BSI IT-Grundschutz-Kataloges enthalten eine sehr umfangreiche Sammlung an Umsetzungshinweisen. Die Anforderungen **NET.4.2.A14 Verschlüsselung der Signalisierung (H)** **NET.4.2.A15 Sicherer Medientransport mit SRTP (H)** sollten bei einer bei der Erweiterung einer existierenden TK-Anlage mit VoIP-Technik (Voice over IP) oder der Neuinstallation einer VoIP-TK-Anlage bei der Planung / Auslegung als Standard-Anforderungen betrachtet werden.
Empfehlungen zur Umsetzung der Anforderung	

INF.1 Allgemeines Gebäude

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-OZcSCQ • Materialien: zki.de/goto/gp-gV7MiA
Anforderungen	**INF.1.A1-A8, A9-A20** Die Anforderungen A1 - A8 sind für Basisschutz anzuwenden. die Anforderungen A9 - A20 sind für normalen Schutzbedarf anzuwenden. **INF.1.A21-A34** sind bei erhöhtem Schutzbedarf anzuwenden
Ausnahmen	
	R2
Allgemeine Empfehlungen zum Baustein	Die Anforderungen aus INF.1 richten sich hauptsächlich an die Liegenschaftsverwaltung (Objektmanagmenet/Facilitymanagement) und die Haustechnik. Bei Neubauten sollte der ISB frühzeitig in die Planungen eingebunden werden. **INF.1.A19** wird zu wenig beachtet. Oft werden jahrelang keine Übungen durchgeführt. **INF.1.A20** ist zu beachten, gerade bei Studierenden besteht hohe Fluktuation (jährlich viele Neu-Mitglieder).
Umsetzungshinweise	**INF1.A1** Informationssicherheit fängt bereits bei der Planung eines Gebäudes an. Als gutes Werkzeug hat sich in der Planungsphase die Unterteilung eines Gebäudes in verschiedene Sicherheitszonen erwiesen (siehe auch INF1.M23). Obwohl diese Maßnahme eigentlich nur bei erhöhtem Schutzbedarf anzuwenden ist, sensibilisiert der Einteilung in Schutzzonen die Planer bei der Einrichtung von Fluchtwegen, bei der Planung eines Schließkonzeptes etc.
	INF1.A2 Eine gleichmäßige Verteilung der zu erwartenden Lasten bei der Stromaufnahme auf alle Phasen der Niederspannungsanlage sollte allen Elektrikern klar sein. Eine Sensibilisierung kann aber nicht schaden...
	INF1.A3 Die Einhaltung des Brandschutzes sollte klar sein. Gelegentlich wird aber vergessen, IT-Räume so zu schützen, dass ein externer Brandherd nicht auf diese Räume übergreift.
	INF1.A4 Die Vermeidung unnötiger Brandlasten sollte ebenfalls klar sein. In der Realität trifft man aber häufig auf Netzwerk Verteilerräume, die aufgrund von planerischen Mängeln in Lagernräumen etc. untergerbracht sind. Hier ist Sensibilisierung bereits in der Planungsphase gefragt.
	INF1.A5 und **INF1.A6** Diese Maßnahmen sind beim Brandschutzbeauftragten meist in guten Händen
	INF1.A7 die organisatorische Maßnahme der Zutrittsregelung und -kontrolle fällt deutlich leichter, wenn man eine Konzept der Sicherheitszonen für ein Gebäude erstellt hat. Zutrittskontrolle in nicht öffentlichen Teilen eines Gebäudes kann man durch Autorisierung durch Ausweise oder (RFID)-Chips erreichen.
	INF1.A8 In öffentlichen Gebäuden gilt grundsätzlich Rauchverbot!
	INF1.A9 Lassen Sie ein Sicherheitskonzept für die Gebäudenutzung gleich während der Planungsphase eines Gebäudes erstellen. Bei Bestandsgebäuden muss der ISB leider selbst ran...
	INF.1.A12 Ein Schließplan ist von der Liegenschaftsabteilung zu erstellen. Der Schließplan fällt leichter, wenn man einen Plan der Sicherheitszonen hat.
	INF1.A13 Liegenschaftsabteilung und IT-Abteilung sollten einen Zutrittsplan für Verteilerräume (Elekro-Unterverteilungen, Netzwerk Verteiler) erstellen. Hier sollte man auch darauf achten, wie mit Wartungsmaßnahmen durch Fremdfirmen umgegangen wird.

	INF1.A15 Lagepläne für Versorgungsleitungen sollten schon beim Bau eines Gebäudes dokumentiert werden. Nachträglich ist eine solche Maßnahme extrem aufwändig. Zu Versorgungsleitungen gehören auch die Trassen der LWL Verkabelung zwischen Gebäuden und die Trassen der Tretiärverkabelungen...
	INF1.A18 bis A20 Brandschutzbegehungen, die Information des Brandschutzbeauftragten sowie Bandschutzübungen gehören zu organisatorischen und Awareness Maßnahmen des Brandschutzbeauftragten

INF.2 Rechenzentrum sowie Serverraum

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-69wDPg • Materialien: zki.de/goto/gp-sYCgKg
Anforderungen	**INF.2.A1-A11, A17, A29 Basisanforderungen** Die Anforderungen A1 - A11, A17, A29 sind anzuwenden. **INF.2.A12-A16, A19-A20, A30 Standardanforderungen** Die Anforderungen A12 - A16, A19 - A20, A30 sind anzuwenden. **INF.2.A21 - A28 erhöhte Schutzanforderungen** Die Anforderungen A21 - A28 sind anzuwenden, wenn spezifische Anforderungen definiert wurden (Bspw. Hochverfügbare Systeme im Serverraum).
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Für die Anwendung des Bausteins zu beachten ist die Definition RZ/ Serverraum in Abhängigkeit des Umfangs der betriebenen IT-Dienstleistungen bzw. der versorgten Nutzer.
Empfehlungen zur Umsetzung der Anforderung	Anforderungen für die im Hochschulumfeld häufig vorkommenden, kleineren dezentralen Technikräume/-schränke ist die Umsetzung des Bausteines INF.5 Raum sowie Schrank für technische Infrastruktur zu empfehlen.

INF.3 Elektronische Verkabelung

Versionshinweis	Version basiert auf Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1 - A3 sowie für A4-A12 und Vorschläge A13-A18.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-4Aq3yg • Materialien: zki.de/goto/gp-wL9hFQ
Anforderungen	**INF.3.A1-A3 sowie A4-A12** Die Anforderungen A1 - A12 (BSI) sind somit anzuwenden. **INF.3.A13-A18** Bei erhöhtem Schutzbedarf sollte die Umsetzung der Vorschläge A13-A18 geprüft werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

INF.4 IT-Verkabelung

Versionshinweis	Bereits auf Stand Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-TcTePg • Materialien: zki.de/goto/gp-hQInbA
Anforderungen	**INF.4.A1-A3 sowie A4 - A11** Die Anforderungen A1 - A11 sind anzuwenden. **INF.4.A12 -A15** Die Anforderungen A12 - A15 sind bei hohem Schutzbedarf ebenfalls anzuwenden. Insbesonder gilt: A12, A14 und A15 sind bei Neubauten anzuwenden und sollten wenn möglich auch im Bestand umgesetzt werden. Für öffentlich zugängliche Bereiche (Flur, Hörsäle etc.) ist A13 anzuwenden.
Ausnahmen	A10: Wenn die Verteiler nur für autorisiertes Personal zugänglich sind, kann bei normalem Schutzbedarf auch der ungefähre Verwendungszweck dokumentiert werden (z.B. Datennetz/ Telefon), um im Störungsfall bessere Informationen zur Verfügung zu haben. Details, die sich häufig ändern, sollten aber nicht dokumentiert werden, um ein vorzeitiges Veralten der Dokumentation zu vermeiden.
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Die IT-Verkabelung ist die Grundlage für das Hochschulnetz und die Verbindungen zu anderen Institutionen und zum Internet, die
Empfehlungen zur Umsetzung der Anforderung	**A1 Auswahl geeigneter Kabeltypen** Da Multimode-Fasern bei Bandbreiten ab 10 Gb/s häufig keinen Preisvorteil mehr bieten und die Reichweite bei höheren Bandbreiten begrenzt ist, sollte überlegt werden, die Sekundär- und ggf. die Tertiärverkabelung auch in Single Mode auszuführen. Dabei ist jedoch zu berücksichtigen, ob dies mit den eingesetzten oder geplanten Geräten möglich ist.
	A4 Anforderungsanalyse • Eine nicht ausreichend dimensionierte Verkabelung führt in Hochschulen besonders leicht zu "fliegender Verkabelung" oder Installation zusätzlicher (i.d.R. nicht managebarer) Switches durch die Anwender. Häufig werden Räume außerdem bereits nach kurzer Zeit einer anderen Nutzung zugeführt. Daher sollte wenn möglich bei der Festlegung der Anzahl der Netzanschlüsse eine Reserve für zukünftige Nutzungsänderungen eingeplant werden bzw. die Kabeltrassen für ein späteres Nachziehen von Kabeln ausreichend dimensioniert und zugänglich sein. • Bei Bauprojekten muss die Hochschul-IT frühzeitig beteiligt werden, um eine ausreichende Dimensionierung der Verkabelung sicherzustellen.
	A12 Redundanzen für die Verkabelung Bei bestehender Gebäudeinfrastruktur sollte dieses Ziel langfristig verfolgt werden, z.B. können Tiefbauarbeiten auf dem Hochschulgelände zur Verlegung von Kabeltrassen genutzt werden, auch wenn diese nicht sofort verwendet werden können.

INF.5 Raum sowie Schrank für technische Infrastruktur

Versionshinweis	Version basiert auf Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1 - A7 sowie für A8-A17 und Vorschläge A18-A26.
Anforderungen	**INF.5.A1-A7** sowie **INF.5.A8-A17** Die Anforderungen A1 - A17 (BSI) sind somit anzuwenden. **INF.5.A18-A26** Bei erhöhtem Schutzbedarf sollte eine Risikoanalyse erfolgen und die Umsetzung der Vorschläge A18-A26 geprüft werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

INF.6 Datenträgerarchiv

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-ujQeXQ • Materialien: zki.de/goto/gp-cecszw
Anforderungen	**INF.6.A1-A4** Die Anforderungen A1 - A4 sind anzuwenden. **INF.6.A5-A9** Die Anforderungen A5 - A9 sollten angewendet werden.
Ausnahmen	Keine Ausnahmen.
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Hochschulen haben in der Regel nicht ein zentrales Datenträgerarchiv, weil Institute, Forschungsbereiche und Professuren eigenständig Archive führen. In der Organisation einer Hochschule müssen die Beteiligten, die zentral agieren (Brandschutzbeauftragter, Haustechnik, ISB), über geeignete Strukturen mit dezentral Agierenden (Mitarbeiter) kooperieren. Informationen aus Datenträgerarchiven können Bestandteil der Lehre und der Forschung sein, in die sehr viele Beteiligte (Studierende, Gaststudierende, Gastwissenschaftlerinnen) eingebunden sind. Die Einschränkung von Zutrittsberechtigungen wird mit Anforderungen durch die Aufgaben einer Hochschule abzuwägen sein.
Empfehlungen zur Umsetzung der Anforderung	**INF.6** Es ist zu erwarten, dass neue Anforderungen entstehen durch die Neuorganisation des *Forschungsdatenmanagements*. Damit wird die Menge digitaler Daten deutlich steigen. Weitere Einflussfaktoren: • Zugriffssteuerung (Open-Access, Lizenzmanagement, fluktuierende Forschungs- und Arbeitsgruppen, externe „persistent identifier“) • Datenkuratierung über Geltungsbereiche von Informationsverbünden, Big-Data-Auswertungen in Forschungsprojekten, Machine-Learning • Datenschutz bei Auswertung von personenbeziehbaren Forschungsdaten Es ist zu bestimmen, wie diese Anforderungen (Dezentralität innerhalb einer Hochschule, virtuelle Organisationen über Hochschulgrenzen, komplexe Rechtslagen) in die Verantwortlichkeit für physische Sicherheitsstrukturen abgebildet werden kann.

INF.7 Büroarbeitsplatz

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-9h5HEg • Materialien: zki.de/goto/gp-SxKZhg
Anforderungen	**INF.7.A1 - A7** Die Anforderungen A1 - A7 sind anzuwenden. **INF.7.A8** Bei erhöhtem Schutzbedarf oder in Bereichen mit Publikumsverkehr ist die Anforderung INF.7.A8 ebenfalls anzuwenden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	Zentrale Anforderungen des Bausteins, insbesondere das in INF.7.A4 refrenzierte Sicherheitskonzept, SOLLEN in Dienstanweisungen oder in Fällen mitbestimmungspflichtiger Aspekte in Dienstvereinbarungen geregelt werden, um die in der Dienststelle geltenden Regelungen transparent zu machen. In diesen SOLLTE zusätzlich ein verantwortlicher Ansprechpartner für die Organisationseinheit benannt und die Aus- bzw. Rückgabe beschrieben werden. Die Regelungen SOLLEN auf den üblichen Dienstbetrieb, die Aufgaben und die bauliche Situation anwendbar sein; ggf. zu berücksichtigende Aspekte: Umgang mit Informationen vs. Umgang mit vertraulichen oder personenbezogenen Informationen; vorübergehende Abwesenheit vs. Dienstende; Einzelbüro vs. Mehrpersonenbüro; Einsicht- vs. Zugriffsnahme; Bildschirmsperren auf verschiedenen Geräteklassen - PC, Laptop, Smartphone uä. Türen und Fenster sind gleichartig zu behandeln, d.h. sie MÜSSEN beim Verlassen des Büroraumes je nach Schutzbedarf geschlossen oder verschlossen gehalten werden. Vertraulichkeitsvereinbarungen mit externem Reinigungspersonal MÜSSEN in Auftragsverarbeitungsverträgen berücksichtigt werden.

Empfehlungen zur Umsetzung der Anforderung	**INF.7.A6 Aufgeräumter Arbeitsplatz** Um den unbefugten Zugriff auf IT-Anwendungen oder Daten in zu verhindern, kann am Client-Computer beim Verlassen des Arbeitsplatzes je nach Abwesenheitsdauer die Bildschirmsperre aktiviert werden, die Abmeldung vom Client erfolgen oder der Client ausgeschaltet werden (vgl. SYS.2.1.A22). Der Zeitraum einer automatisch einsetzenden Bildschirmsperre SOLLTE in Client-Management-Systemen administrativ festgelegt werden. Die Beschäftigten SOLLTEN verpflichtet werden, auch beimkurzzeitigen Verlassen eines Clients diesen manuell zu sperren. **INF.7.A6 Aufgeräumter Arbeitsplatz, INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger** Lehrumgebungen - Hörsäle, Seminarräume u.ä. - sollten den Anforderungen A6 und A7 unterliegen, wenn durch die Tätigkeit an diesen Orten vertrauliche Informationen verfügbar werden. **INF.7.A8 Einsatz von Diebstahlsicherungen** In Lehr- und Lernumgebungen - Hörsäle, Seminarräume uä. - MÜSSEN für alle IT-Systeme Diebstahlsicherungen eingesetzt werden, weil diese oftmals 24/7 dem Publikumsverkehr offen stehen. Ausnahmen gelten für IT-Systeme, die nur vorübergehend und unter Aufsicht eingesetzt werden. **Bei erhöhtem Schutzbedarf** Die Bereiche, in denen sich Büroarbeitsplätze mit erhöhtem Schutzbedarf befinden, SOLLTEN durch bauliche Maßnahmen - Flurtüren, die einen "Sicherheitsbereich" definieren und geschlossen gehalten werden uä. - oder technische Maßnahmen - protokollierende Schließzylinder uä. - ertüchtigt werden. An Büroarbeitsplätzen, bei denen eine unbefugte Einsichtnahme in den Bildschirm oder in Dokumente verhindert werden soll, SOLLEN Sichtschutzfolien- und/oder Sichtschutzwände angebracht werden. Gleiches gilt, wenn die Einsicht durch (Klarglas-)Fenster möglich ist.

INF.8 Häuslicher Arbeitsplatz

Versionshinweis	Unverändert in Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1 - A3 sowie für A4-A5 und Vorschlag A6.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-ZHNQ3A • Materialien: zki.de/goto/gp-XpKCKw
Anforderungen	**INF.8.A1-A3 sowie A4-A5** Die Anforderungen A1 - A5 (BSI) sind somit anzuwenden. **INF.8.A6** Bei erhöhtem Schutzbedarf sollte eine Risikoanalyse erfolgen und die Umsetzung des Vorschlags A6 geprüft werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

INF.9 Mobiler Arbeitsplatz

Versionshinweis	Unverändert in Edition 2020. Noch keine hochschulspezifischen Empfehlungen vorhanden, daher gelten die Vorgaben des BSI für A1 - A4 sowie für A5-A9 und Vorschläge A10-A11.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-Neus7w • Materialien: zki.de/goto/gp-zfcXzA
Anforderungen	**INF.9.A1-A4 sowie A5-A9** Die Anforderungen A1 - A9 (BSI) sind somit anzuwenden. **INF.9.A10-A11** Bei erhöhtem Schutzbedarf sollte eine Risikoanalyse erfolgen und die Umsetzung des Vorschläge A10-A11 geprüft werden.
Ausnahmen	
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	
Empfehlungen zur Umsetzung der Anforderung	

INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum

Versionshinweis	Unverändert in Edition 2020.
Weiterführende Links	• Aktuelle Version dieses Bausteins: zki.de/goto/gp-JD1t0g • Materialien: zki.de/goto/gp-rRSqog
Anforderungen	**INF.10.A1 - A3 sowie A4 - A8** Die Anforderungen A1 - A8 sind anzuwenden. **INF.10.A9, A10** Bei erhöhtem Schutzbedarf sind die Anforderungen A9 - A10 ebenfalls anzuwenden.
Ausnahmen	A2 ist im Hochschulumfeld nicht umsetzbar! Dieser Punkt wäre nur für Räume außerhalb des studentischen Betriebs anwendbar (wie Personalbüro, IT, Haushalt) und für Hörsäle passend. Der öffentliche Charakter einer Hochschule macht die Begleitung von Besuchern nur in definierten sensiblen Bereichen notwendig. Sensible Bereiche sind derart zu gestalten, dass der öffentliche Besucherverkehr möglichst nicht angrenzt und durch entsprechende bauliche Maßnahmen oder kontrollierbare Übergangsbereiche getrennt wird. Für sensible Räume ist eine umfassende Risikoanalyse unter Einbezug der Umweltfaktoren und technischen Möglichkeiten durchzuführen.
Priorisierung	**R2**
Allgemeine Empfehlungen zum Baustein	In die Kategorie Besprechungs-,Veranstaltungs-, Schulungsraum fallen ebenfalls alle Räumlichkeiten, die zur Wissensvermittlung zur Verfügung stehen: Hörsäle, Seminarräume, Übungsräume, Bibliotheksräumlichkeiten und Computerarbeitsräume mit dem möglichen Nutzungsszenario 'studentischer Arbeitsplatz'.
Empfehlungen zur Umsetzung der Anforderung	**INF10.A6 Einrichtung sicherer Netzzugänge** Typische Nutzungsszenarios in Seminarräumen und Hörsälen können die wechselweise Nutzung möglicherweise interner Netzwerkangebote (etwa hochschulöffentliches E-Learning, Simulationsumgebungen) und Internetinhalte einschließen. Eine Trennung nach Verbindungsart Intranet/Internet wird im Lehrveranstaltungskontext nicht in jedem Fall umsetzbar sein. Verbindungen zu SMB-Freigaben z.Bsp. oder anderen Diensten, die im aktuellen Kontext nicht benötigt werden, sollten jedoch ausgeschlossen werden. Mögliche Mittel hierzu sind dedizierte WLAN-Dienste wie eduroam oder logische Teilnetze (VLAN). Wenn diese Mittel nicht zur Verfügung stehen, können nach Abwägung der Umsetzunghinweise INF. 10.M6 entsprechend gering autorisierte Identitäten für den Veranstaltungskontext zum Einsatz kommen.