UNIVERSITÄT SIEGEN

Amtliche Mitteilungen

Datum **20. April 2022** **Nr. 34/2022**

I n h a l t :

Richtlinie
Klassifizierung von Informationen

der
Universität Siegen

Vom 20. April 2022

Herausgeber: Rektorat der Universität Siegen
Redaktion: Dezernat 3, Adolf-Reichwein-Straße 2 a, 57076 Siegen, Tel. 0271/740-4813

Richtlinie
Klassifizierung von Informationen

der
Universität Siegen

Vom 20. April 2022

Definitionen, Abkürzungen, Verweise

Begriff	Definition
BDSG	Bundesdatenschutzgesetz
BISB	Bereichs-Informationssicherheitsbeauftragte
CD	Compact Disc
CISO	Chief Information Security Officer
DIN	Deutsches Institut für Normung
DVD	Digital Versatile Disc
EU-DSGVO	Datenschutzgrundverordnung der Europäischen Union
ISO	International Organization for Standardization
NDA	Non-Disclosure Agreement (Vertraulichkeitsvereinbarung)
USB	Universal Serial Bus
ZIMT	Zentrum für Informations- und Medientechnologie

Abstimmungstabelle

Empfänger	Organisationseinheit	RACI
Rektor	Universität Siegen	A
Kanzler	Universität Siegen	A
CISO	Universität Siegen	R
Leiter Stabsstelle Datenschutz	Universität Siegen	C
ZIMT-Leitung	Universität Siegen	C
BISB	Universität Siegen	C
Alle Universitätsangehörigen	Universität Siegen	I

Tabelle 1: RACI Abstimmungstabelle[1]

Verbundene Dokumente

Dokumentenname	Ablageort
ISO/IEC 27001:2013	https://www.iso.org/isoiec-27001-information-security.html
BDSG (gültig ab 25. Mai 2018)	https://www.gesetze-im-internet.de/bdsg_2018/
EU-DSGVO (Gültig ab 25. Mai 2018)	https://eu-datenschutz.org/
Leitlinie zur Informationssicherheit der Universität Siegen vom 16. November 2020	Amtliche Mitteilungen Universität Siegen Nr. 83/2020

[1] **Responsible** – verantwortlich (**Durchführungsverantwortung**), zuständig für die eigentliche Durchführung. Die Person, die die Initiative für die Durchführung (durch Andere) gibt oder die die Aktivität selbst durchführt.
Accountable – rechenschaftspflichtig (**Kostenverantwortung**), verantwortlich im Sinne von „genehmigen", „billigen" oder „unterschreiben". Die Person, die im rechtlichen oder kaufmännischen Sinne die Verantwortung trägt.
Consulted – konsultiert (**Fachverantwortung**). Eine Person, deren Rat eingeholt wird. Wird auch als Verantwortung aus fachlicher Sicht interpretiert.
Informed – zu informieren (Informationsrecht)

Inhalt

1 Einleitung

Informationen und Ideen sind der Schlüssel zum Geschäftserfolg. Deshalb ist es essenziell, Informationen zu schützen und sie nur Berechtigten zugänglich zu machen.

2 Zweck des Dokuments

Dieses Dokument dient als Leitfaden für die Einordnung von Informationen in die vorgegebenen Vertraulichkeitsstufen, die Kennzeichnung von sowie den Umgang mit eingestuften Informationen und deren Entsorgung bzw. Vernichtung.

3 Geltungsbereich

Diese Richtlinie gilt für alle Einrichtungen der Universität Siegen (Fakultäten, Zentrale Universitätsverwaltung, Universitätsbibliothek, sowie weitere wissenschaftliche und Service-Einrichtungen), für die gesamte IT-Infrastruktur, einschließlich der in den Einrichtungen betriebenen IT-Systeme und IT-Dienste, sowie für alle Mitglieder, Angehörige und Gäste der Universität Siegen.

Alle bisher existierenden Regelungen bezüglich der Klassifizierung von Informationen, Daten, Dokumenten etc. werden durch diese Richtlinie hinfällig und vollständig ersetzt. Von dieser Richtlinie abweichende interne Regelungen dürfen nur in Abstimmung und mit schriftlicher Zustimmung des CISO erlassen werden.

Soweit besondere Rechtsvorschriften über den Zugang zu Informationen, die Auskunftserteilung oder die Gewährung von Akteneinsicht bestehen, gehen sie den Regelungen dieser Richtlinie vor.

4 Gesetzliche Grundlage

Die Verpflichtung zum Informationsschutz ergibt sich direkt oder indirekt aus einer Vielzahl von gesetzlichen Regelungen und Verordnungen. Exemplarisch dafür sind u.a. die EU-DSGVO und das BDSG.

5 Informationssicherheit

5.1 Informationsarten und Vertraulichkeitsstufen

Informationen jeglicher Art, wie z. B. Dokumente, Bilder, Zeichnungen, Daten und Programme auf Papier oder magnetischen, elektronischen, optischen oder anderen Informationsträgern, sind unabhängig von ihrer Erscheinungsform gleichermaßen zu schützen. Wichtig für den Erfolg von Maßnahmen zur Einhaltung von Vertraulichkeit ist eine klare, abgestufte und eindeutige Einstufung bzw. Klassifizierung von Informationen.

Die Universität Siegen hat für die Vertraulichkeitsklassifizierung von Informationen die folgenden vier Stufen festgelegt:

- **„ÖFFENTLICH“**
- **„NICHT-ÖFFENTLICH“**
- **„VERTRAULICH“'**
- **„STRENG VERTRAULICH“**

5.2 Einstufung von Informationen

Die Einstufung der Vertraulichkeit von Informationen und Dokumenten richtet sich nach den Vorgaben des Chief Information Security Officers (CISO). Informationen werden vom jeweiligen Informationseigner als verantwortliche Person in die entsprechenden vier Kategorien eingestuft.

Die Einstufung der Vertraulichkeit einer Information ist unabhängig von deren Erscheinungsform (schriftlich, digital, gedanklich, sprachlich etc.) immer gleich.

5.2.1 „ÖFFENTLICH“

Eine Einstufung in die Kategorie „ÖFFENTLICH“ erfolgt für Informationen, die insbesondere zur Publikation vorgesehen sind. Dafür ist die Zustimmung bzw. die Freigabe durch die Hochschulleitung oder durch die autorisierten Personen notwendig. Dies dient dem Schutz der Universität Siegen vor ungewollter Veröffentlichung von Informationen und dadurch bedingter Schäden für die Universität Siegen.

Ausgenommen von dieser Regelung sind Informationen, die ohnehin öffentlich bekannt sind oder einer Veröffentlichungspflicht unterliegen.

Eine verbindliche Liste der autorisierten Personen und der Informationsarten, die freigegeben werden können, ist in *Anlage 2* veröffentlicht.

5.2.1.1 Beispiele für Informationen der Stufe „ÖFFENTLICH“

- Informationen zu Lehrveranstaltungen oder hochschulöffentlichen Veranstaltungen
- Informationen zu und Inhalte aus öffentlichen Veranstaltungen
- im Internet öffentlich bereitgestellte Informationen
- Veröffentlichungen der Pressestelle
- Werbematerial
- Amtliche Mitteilungen
- Dissertationsschriften
- Organisationspläne (sofern kein Rückschluss auf Personen möglich)

5.2.1.2 Kennzeichnung von Informationen der Stufe „ÖFFENTLICH“

Bei Dokumenten, die als „ÖFFENTLICH“ eingestuft sind und die offen verwendet werden sollen, ist auf der Titelseite der Vermerk „ÖFFENTLICH“ anzubringen. Auf allen weiteren Seiten des Dokumentes ist der Vermerk „ÖFFENTLICH“ in der Fußzeile einzufügen.

Elektronische Informationen bzw. Dateien sind, wenn technisch möglich, im Dateinamen mit dem Vermerk „OEF“ zu kennzeichnen. Alle Schriften, die ihrer Natur entsprechend zur Veröffentlichung bestimmt sind, müssen nicht gesondert gekennzeichnet werden, insbesondere öffentliche Webseiten. Die Zugehörigkeit zur Universität Siegen muss für den Leser leicht erkennbar sein (z.B. Anbringen des Logos).

5.2.1.3 Verteilung von Informationen der Stufe „ÖFFENTLICH“

Diese Informationen dürfen der Öffentlichkeit zugänglich gemacht werden. Bei der Verteilung in Papierform, mit IT-Unterstützung oder per Sprachkommunikation sind keine besonderen Maßnahmen zu ergreifen.

5.2.1.4 Versand von Informationen der Stufe „ÖFFENTLICH“

Bei Versand innerhalb der Universität Siegen als „Hauspost“ kann auf einen verschlossenen Umschlag verzichtet werden, beim externen Versand ist ein Umschlag mit korrekter Adressierung und ohne besondere Kennzeichnung zu verwenden.

Eine Übertragung per Fax und E-Mail ist zulässig.

Eine Übertragung per Sprachkommunikation (persönlich, telefonisch) ist zulässig.

5.2.1.5 Aufbewahrung von Informationen der Stufe „ÖFFENTLICH“

Für diese Dokumente in Papierform und Informationen in elektronischer Form sind keine besonderen Maßnahmen bzgl. der Aufbewahrung durchzuführen.

5.2.1.6 Entsorgung von Informationen der Stufe „ÖFFENTLICH“

Dokumente in Papierform können über den normalen Papiermüll entsorgt werden.

Daten in elektronischer Form werden einfach gelöscht.

5.2.2 „NICHT-ÖFFENTLICH“ (ohne Kennzeichnung)

Informationen, die nur für den internen Gebrauch bestimmt sind, bedürfen keiner expliziten Kennzeichnung.

Als Informationen mit der Einstufung “NICHT-ÖFFENTLICH” werden Informationen verstanden, deren Weiterverbreitung einen Schaden für die Universität Siegen nach sich ziehen kann.

5.2.2.1 Beispiele für Informationen der Stufe „NICHT-ÖFFENTLICH“

- Projektakten die keine Informationen der Kategorien „VERTRAULICH“ oder „STRENG VERTRAULICH“ (siehe 5.2.3 und 5.2.4) enthalten
- Wissenschaftliche Daten, die für Dritte nicht interpretierbar sind und für die keine Geheimhaltungsvereinbarungen bestehen
- In der Regel Geschäftsverteilungspläne
- Anweisungen für den täglichen Betrieb, interne Richtlinien und Rundschreiben, interne Berichte
- Interner Schriftverkehr (Mail, Chat usw.) der keine Informationen der Kategorien „VERTRAULICH“ oder „STRENG VERTRAUCHLICH“ (siehe 5.2.3 und 5.2.4) enthält

5.2.2.2 Kennzeichnung von Informationen der Stufe „NICHT-ÖFFENTLICH“

Informationen der Stufe „NICHT-ÖFFENTLICH“ benötigen keine explizite Kennzeichnung. Es muss jedoch auf jeden Fall ersichtlich sein, dass es sich um ein Dokument der Universität Siegen handelt. Es kann auf der Titelseite der Vermerk „NICHT-ÖFFENTLICH“ angebracht werden. In diesem Fall ist auch auf allen weiteren Seiten des Dokumentes der Vermerk „NICHT-ÖFFENTLICH“ in der Fußzeile einzufügen.

Elektronische Informationen bzw. Dateien können, wenn technisch möglich, im Dateinamen mit dem Vermerk „NOE“ gekennzeichnet werden.

5.2.2.3 Verteilung von Informationen der Stufe „NICHT-ÖFFENTLICH“

Diese Informationen dürfen nur innerhalb der Universität Siegen weitergegeben werden. Die Weitergabe an Externe bedarf der Genehmigung durch die zuständige Führungskraft, die diese entweder fallbezogen oder aufgabenbezogen erteilen kann. Wenn der Externe sich vertraglich zur Geheimhaltung zu verpflichten hat (Non Disclosure Agreement/NDA), ist keine weitere Freigabe erforderlich.

Nach Extern weitergegebene Informationen der Stufe „NICHT-ÖFFENTLICH“ müssen unabhängig der vorstehenden Regelung grundsätzlich einen Vermerk enthalten, der den Empfänger darauf hinweist, dass es sich um universitäts-interne (eigene) Informationen handelt, die vertraulich behandelt werden müssen und deren Weitergabe an Dritte untersagt ist. Analog ist bei einer Übertragung per Sprachkommunikation zu verfahren. Der Empfänger muss explizit darauf hingewiesen werden, dass es sich um universitäts-interne Informationen handelt, die vertraulich behandelt werden müssen und deren Weitergabe an Dritte untersagt ist.

5.2.2.4 Versand von Informationen der Stufe „NICHT-ÖFFENTLICH“

Bei Versand innerhalb der Universität Siegen als „Hauspost“ kann auf einen verschlossenen Umschlag verzichtet werden, beim externen Versand ist ein Umschlag mit korrekter Adressierung und ohne besondere Kennzeichnung zu verwenden.

Eine Übertragung per Fax und E-Mail ist zulässig.

Eine Übertragung per Sprachkommunikation (persönlich, telefonisch) ist zulässig.

5.2.2.5 Aufbewahrung von Informationen der Stufe „NICHT-ÖFFENTLICH“

Innerhalb der Universität Siegen sind keine besonderen Maßnahmen zu treffen, doch ist ebenso wie beim Mitnehmen von Unterlagen darauf zu achten, dass Dritte keinen Zugriff auf diese Informationen bekommen. Datenträger, auf denen Informationen der Kategorie „NICHT-ÖFFENTLICH“ gespeichert werden, sind zu verschlüsseln. Gleiches gilt für mobile Geräte (Smartphones, Tablets, Laptops).

5.2.2.6 Entsorgung von Informationen der Stufe „NICHT-ÖFFENTLICH“

Dokumente in Papierform werden über Aktenvernichter oder Datenschutztonnen mit der jeweils entsprechenden Sicherheitsstufe entsorgt (siehe 5.3).

Daten in elektronischer Form werden sicher gelöscht.

5.2.3 „VERTRAULICH“

Als vertrauliche Informationen werden solche verstanden, deren Weiterverbreitung einen Schaden an Vermögen und/oder Ansehen der Universität Siegen oder rechtliche Konsequenzen nach sich ziehen kann.

5.2.3.1 Beispiele für Informationen der Stufe „VERTRAULICH“

- Vertragsentwürfe und Verträge (Rahmenverträge, Forschungsverträge etc.)
- Konzepte und Layout-Unterlagen (Sicherheitsmaßnahmen, Netzpläne etc.)
- Mediadaten und eigenentwickelte Software aus abgeschlossenen Projekten
- Prüfungsdaten (Notenlisten, Prüfungsprotokolle etc.)
- In der Regel personenbezogene Daten
- Abschlussberichte (Revisionsberichte, Auditberichte etc.)
- Vertrauliche Inhalte aus Gremiensitzungen
- Finanzdaten (Budget etc.)
- Kalkulation von wirtschaftlichen Drittmittelprojekten

5.2.3.2 Kennzeichnung von Informationen der Stufe „VERTRAULICH“

Bei Dokumenten ist auf der Titelseite der Vermerk „VERTRAULICH“ gut sichtbar anzubringen. Auf jeder Seite ist in der Fußzeile ebenso der Vermerk „VERTRAULICH“ anzubringen. Darüber hinaus sollte auf der Titelseite der Vermerk „COPY FORBIDDEN/KOPIEREN VERBOTEN“ angebracht werden.

Nach Möglichkeit sollte die Vertraulichkeit zeitlich beschränkt werden, z.B. durch den Aufdruck auf dem Titelblatt „VERTRAULICH BIS DD.MM.YYYY“ bzw. „CONFIDENTIAL UNTIL DD MMM YYYY“. Es muss vermerkt werden, auf welche Einstufung das Dokument nach dem Ablaufdatum zurückfällt, z.B. „nach Ablauf des Datums ist das Dokument nur für den internen Gebrauch“.

Elektronische Informationen bzw. Dateien sind, wenn technisch möglich, im Dateinamen mit dem Vermerk „VTR“ zu kennzeichnen.

5.2.3.3 Verteilung von Informationen der Stufe „VERTRAULICH“

Diese Informationen dürfen nur innerhalb der Universität Siegen an Mitarbeiterinnen und Mitarbeiter weitergegeben werden, die im Rahmen ihrer Tätigkeit Kenntnis dieser Information haben müssen (Need-to-know-Prinzip). Die Weitergabe an Externe bedarf der Genehmigung durch die zuständige Führungskraft, der Empfänger hat sich zur Geheimhaltung zu verpflichten (z.B. durch ein Non Disclosure Agreement/NDA).

Zur Überwachung der Verteilung sollte ein Verteiler angelegt werden, der regelmäßig geprüft und aktualisiert werden muss.

5.2.3.4 Versand von Informationen der Stufe „VERTRAULICH“

Bei Versand innerhalb der Universität Siegen als „Hauspost“ muss ein verschlossener Umschlag verwendet werden, auf dem die korrekte Anschrift sowie der Adressat angegeben ist. Dieser Umschlag muss undurchsichtig sein und ist so zu verschließen, dass er nicht unbemerkt geöffnet werden kann (z.B. durch Verkleben).

Beim externen Versand ist ein Umschlag mit korrekter Adressierung und ohne besondere Kennzeichnung zu verwenden. Der Versand als Einschreiben (mit Rückantwort) ist zu bevorzugen.

Eine Übertragung ist extern nur verschlüsselt zulässig, z.B. per E-Mail oder über eine gesicherte Austauschplattform. Hierbei ist ein Verschlüsselungsverfahren nach dem aktuellen Stand der Technik zu verwenden. Intern ist die Verschlüsselung sichergestellt.

Eine Übertragung per Sprachkommunikation ist nur persönlich und nur in ausschließlicher Anwesenheit der Personen, die auf dem Verteiler vermerkt sind, zulässig. Bei einer telefonischen oder anderen fernmündlichen Übertragung muss sich der Versender versichern, dass auf Empfängerseite keine unberechtigten Personen anwesend sind. Dies kann er tun, indem er den Versender darauf hinweist, dass ab jetzt vertrauliche Informationen ausgetauscht werden und daher nur die auf dem Verteiler vermerkten Personen beim jeweiligen Empfänger anwesend sein dürfen. Eine Übertragung in der Öffentlichkeit (z.B. Bahn, Flugzeug, Café, Restaurant) ist unzulässig, da nicht sichergestellt werden kann, dass kein unberechtigter Dritter mithört.

5.2.3.5 Aufbewahrung von Informationen der Stufe „VERTRAULICH“

Informationen der Stufe „VERTRAULICH“ sind dauernd unter Verschluss zu halten. Bei Informationen, die auf IT-Systemen gespeichert werden, ist ein zusätzlicher Schutz über erweiterte Zugriffskontrolle oder Verschlüsselung erforderlich. Die Mitnahme von Dokumenten erfolgt nur unter dem Gebot erhöhter Vorsicht. Datenträger, auf denen Informationen der Kategorie „VERTRAULICH“ gespeichert werden, sind zu verschlüsseln. Gleiches gilt für mobile Geräte (Smartphones, Tablets, Laptops).

5.2.3.6 Entsorgung von Informationen der Stufe „VERTRAULICH“

Dokumente in Papierform werden über Aktenvernichter oder Datenschutztonnen mit der jeweils entsprechenden Sicherheitsstufe entsorgt (siehe 5.3).

Daten in elektronischer Form werden sicher gelöscht.

5.2.4 „STRENG VERTRAULICH“

Als streng vertrauliche Informationen werden solche klassifiziert, deren allgemeine Offenlegung die vitalen Interessen der Universität Siegen bedrohen, weil sie etwa einen schweren Schaden an Vermögen und/oder Image der Universität Siegen oder massive rechtliche Konsequenzen nach sich ziehen können.

Sofern in der Vergangenheit solche Informationen mit der Kennzeichnung „Secret“ klassifiziert wurden, gelten die hier festgelegten Regelungen entsprechend. Die Klassifizierung „Secret“ ist für neue Informationen nicht mehr zu verwenden und bei Bearbeitung bestehender Informationen entsprechend in „STRENG VERTRAULICH“ zu ändern.

5.2.4.1 Beispiele für Informationen der Stufe „STRENG VERTRAULICH“

- Informationen über bestehende Sicherheitsmaßnahmen (Konfiguration von Sicherheitseinrichtungen, Schlüsselverteilungsplan etc.)
- Informationen zu schwerwiegenden Schwachstellen (Software, Zutrittssteuerung etc.)
- Strategiepapiere vor Veröffentlichung
- besondere personenbezogene Daten nach DSGVO (Gesundheitsdaten, Religionszugehörigkeit etc.)
- besondere wissenschaftliche Daten (Patentunterlagen vor ihrer Offenlegung)

5.2.4.2 Kennzeichnung von Informationen der Stufe „STRENG VERTRAULICH“

Auf der Titelseite ist der Vermerk „STRENG VERTRAULICH“ gut sichtbar anzubringen. Auf jeder Seite in der Fußzeile ist ebenso der Vermerk „STRENG VERTRAULICH“ anzubringen. Darüber hinaus muss auf der Titelseite der Vermerk „COPYING WILL LEAD AUTOMATICALLY TO LEGAL CONSEQUENCES AND IS FORMALLY FORBIDDEN“ bzw. „KOPIEREN FÜHRT AUTOMATISCH ZU RECHTLICHEN KONSEQUENZEN UND IST AUSDRÜCKLICH VERBOTEN“ angebracht werden.

Nach Möglichkeit sollte die Vertraulichkeit zeitlich beschränkt werden, z.B. durch den Aufdruck auf dem Titelblatt „STRENG VERTRAULICH BIS DD.MM.YYYY“ bzw. „STRICLY CONFIDENTIAL UNTIL DD MMM YYYY“. Es muss vermerkt werden, auf welche Einstufung das Dokument nach dem Ablaufdatum zurückfällt, z.B. „nach Ablauf des Datums ist das Dokument nur für den internen Gebrauch“.

Elektronische Informationen bzw. Dateien sind im Dateinamen, wenn technisch möglich, mit dem Vermerk „SVT“ zu kennzeichnen.

5.2.4.3 Verteilung von Informationen der Stufe „STRENG VERTRAULICH“

Diese Informationen sind nur einem stark beschränkten, namentlich bekannten Personenkreis zugänglich. Die Weitergabe an Externe bedarf der Genehmigung durch die Hochschulleitung oder beauftragte Personen**,** der Empfänger hat sich zur vertraglichen Geheimhaltung zu verpflichten (Non Disclosure Agreement/NDA). Zur Überwachung der Verteilung muss ein Verteiler angelegt werden, der regelmäßig geprüft und aktualisiert werden muss.

5.2.4.4 Versand von Informationen der Stufe „STRENG VERTRAULICH“

Die persönliche Überbringung ist die beste Möglichkeit, Dokumente mit dieser Einstufung auszuliefern. Beim Einsatz von Boten müssen diese persönlich bekannt sein und als zuverlässig gelten. Grundsätzlich sind die Annahme und Übergabe der Unterlagen zu quittieren.

Der Versender kann in Ausnahmefällen von einer Quittierung absehen, wie z.B. in Fällen persönlicher direkter Übergabe durch den Versender an den Empfänger oder beim Einsatz von Vertrauenspersonen des Versenders wie persönlichen Assistenten.

Bei Versand innerhalb der Universität Siegen per Hauspost muss ein verschlossener und undurchsichtiger Umschlag verwendet werden, der mittels Versiegelung gegen unberechtigtes Öffnen gesichert ist. Eine Versiegelung im Sinne dieser Richtlinie kann z.B. ein Stempel oder eine Paraphe an der verklebten Stelle des verschlossenen Umschlags sowie eine Verklebung mit nichtablösbarem Klebestreifen sein. Zudem ist auf dem Umschlag die korrekte Anschrift zwingend mit dem Vermerk „persönlich“ zu versehen.

Beim externen Versand ist ein Umschlag ohne besondere Kennzeichnung zu verwenden, jedoch mit dem Hinweis „nur persönliche Übergabe“. Der Versand muss als Einschreiben mit Rückschein erfolgen.

Auf die korrekte Adressierung ist bei externem Versand besonderer Wert zu legen, ebenfalls auf die Überwachung des unversehrten Eingangs beim Adressaten.

Eine Übertragung per Fax und E-Mail ist nur nach Freigabe durch den jeweils verantwortlichen Vorgesetzten zulässig. Die genehmigte Übertragung ist in jedem Falle nur verschlüsselt zulässig, egal ob intern oder extern. Hierbei ist ein Verschlüsselungsverfahren nach dem aktuellen Stand der Technik zu verwenden.

Eine Übertragung per Sprachkommunikation ist nur von Angesicht zu Angesicht und nur in ausschließlicher Anwesenheit der Personen, die auf dem Verteiler vermerkt sind, zulässig. Eine telefonische oder andere fernmündliche Übertragung sowie eine Übertragung in der Öffentlichkeit (z.B. Bahn, Flugzeug, Café, Restaurant) ist unzulässig, da nicht sichergestellt werden kann, dass kein unberechtigter Dritter mithört. In jedem Falle ist vom Versender sorgfältig sicherzustellen, dass es für unberechtigte Personen keinerlei Möglichkeiten gibt mitzuhören.

5.2.4.5 Aufbewahrung von Informationen der Stufe „STRENG VERTRAULICH“

Die Unterlagen sind dauernd und sicher unter Verschluss (vorzugsweise Tresor oder vergleichbare Sicherstufe) zu halten. Bei Unterlagen, die auf IT-Systemen gespeichert werden, ist ein zusätzlicher

Schutz (z. B. Dokumentenschutz, Freigabeschutz) über erweiterte Zugriffskontrolle oder Verschlüsselung erforderlich. Die Mitnahme der Dokumente erfolgt nur in extremen Ausnahmefällen unter dem Gebot äußerster Vorsicht. Datenträger, auf denen Informationen der Kategorie „STRENG VERTRAULICH“ gespeichert werden, sind zu verschlüsseln. Gleiches gilt für mobile Geräte (Smartphones, Tablets, Laptops).

5.2.4.6 Vernichtung von Informationen der Stufe „STRENG VERTRAULICH“

Dokumente in Papierform werden über Aktenvernichter oder Datenschutztonnen mit der jeweils entsprechenden Sicherheitsstufe entsorgt (siehe 5.3)

Daten in elektronischer Form werden sicher gelöscht.

5.3 Löschung und Entsorgung von Dokumenten und Datenträgern

5.3.1 Entsorgung von Dokumenten in Papierform

Die Entsorgung von Dokumenten in Papierform mit der Einstufung “ÖFFENTLICH“ kann über den normalen Papiermüll erfolgen.

Die Entsorgung von Dokumenten in Papierform mit der Einstufung “NICHT-ÖFFENTLICH“ erfolgt entweder über die vorhandenen Datenschutzbehälter oder über Aktenvernichter mit mindestens der Sicherheitsstufe 2 entsprechend der Klassifizierung nach ISO 21964-1 (DIN 66399).

Die Entsorgung von Dokumenten in Papierform mit der Einstufung “VERTRAULICH“ oder “STRENG VERTRAULICH“ erfolgt entweder über höherwertige Aktenvernichter mit mindestens der Sicherheitsstufe 5 entsprechend der Klassifizierung nach ISO 21964-1 (DIN 66399) oder über spezielle und gekennzeichnete bereitgestellte Datenschutzbehälter.

Dabei ist die Richtlinie über die Aufbewahrung, Aussonderung, Archivierung und Vernichtung von Unterlagen vom 03.06.2019 der Universität Siegen (Amtliche Mitteilung 14/2019) zu beachten.

5.3.2 Sicheres Löschen von Datenträgern

Sowohl aus der Sicht des Datenschutzes als auch der Informationssicherheit ist beim Löschen von sensiblen oder personenbezogenen Daten auf Datenträgern zu gewährleisten, dass die Daten sicher, d.h. vollständig und unumkehrbar, gelöscht (z.B. 7-faches Überschreiben über WIPE, etc.) werden.

5.3.3 Entsorgung von Datenträgern

Disketten, CDs, DVDs, USB-Sticks, externe Festplatten, Magnetbänder, Speicherkarten und sonstige digitale Datenträger müssen über die von Dienstleistern zur Verfügung gestellten Datenschutzbehälter vernichtet werden. Festplatten werden über einen vom ZIMT bereitgestellten Festplattenvernichter der Kategorie H-5 (dies entspricht der Schutzklasse 2 / Sicherheitsstufe 5 gemäß DIN 66399) entsorgt.

6 Verteilung und Gültigkeit

Diese Richtlinie tritt am Tage nach ihrer Veröffentlichung in Kraft. Sie wird in dem Verkündungsblatt „Amtliche Mitteilungen der Universität Siegen“ veröffentlicht.

Ausgefertigt aufgrund des Beschlusses des Rektorats vom 10. Februar 2022.

Siegen, den 20. April 2022

Der Rektor

gez.

(Universitätsprofessor Dr. Holger Burckhart)

7 Anlagen

7.1 Anlage 1: Übersicht „Einstufung bzw. Klassifizierung von Informationen“

Klassifizierungsstufe	**ÖFFENTLICH**	**NICHT-ÖFFENTLICH**	**VERTRAULICH**	**STRENG VERTRAULICH**
Kennzeichnung	**Jede Seite: „ÖFFENTLICH“** **Im Dateinamen: „OEF“**	**Optional jede Seite: „NICHT-ÖFFENTLICH“** **Optional im Dateinamen: „NOE“**	**Jede Seite: „VERTRAULICH“** **Im Dateinamen: „VTR“**	**Jede Seite: „STRENG VERTRAULICH“** **Im Dateinamen: „SVT“**
Aufbewahrung	• Keine besonderen Maßnahmen	• Unter Aufsicht	• **Physisch**: im Mobiliar abgeschlossen • **Elektronisch**: Passwortschutz	• **Physisch**: vorzugsweise Tresor/Sicherheitsmobiliar • **Elektronisch**: verschlüsselt, entsprechend Benutzerberechtigungskonzept
Übermittlung	• Keine besonderen Maßnahmen	• Keine besonderen Maßnahmen	• **Physisch**: in verschlossenem und undurchsichtigem Umschlag • **Elektronisch**: verschlüsselt mit aktuellem Verschlüsselungsverfahren	• **Physisch**: direkte Übergabe oder Versand in verschlossenem, undurchsichtigem und versiegeltem Umschlag, Unversehrtheit prüfen • **Elektronisch**: ausschließlich verschlüsselt mit aktuellem Verschlüsselungsverfahren
Rückzug und Vernichtung	• Keine besonderen Maßnahmen	• **Physisch**: Datentonnen • **Elektronisch**: gesichertes Löschen	• **Physisch**: Datentonnen • **Elektronisch**: gesichertes Löschen	• **Physisch**: Aktenvernichter mit Klassifizierung nach ISO 21964-1 (DIN 66399) • **Elektronisch**: gesichertes Löschen (7x wipe oder schreddern)
Beispiele	• Informationen zu Lehrveranstaltungen oder hochschulöffentlichen Veranstaltungen • Informationen zu und Inhalte aus öffentlichen	• Projektakten die keine Informationen der Kategorien „VERTRAULICH“ oder „STRENG VERTRAULICH“ (siehe 5.2.3 und 5.2.4) enthalten.	• Vertragsentwürfe und Verträge (Rahmenverträge, Forschungsverträge etc.) • Konzepte und Layout-Unterlagen (Sicher-	• Informationen über bestehende Sicherheitsmaßnahmen (Konfiguration von Sicherheitseinrichtungen, Schlüsselverteilungsplan etc.) • Informationen zu schwerwiegenden Schwachstellen

	Veranstaltungen • im Internet öffentlich bereitgestellte Informationen • Veröffentlichungen der Pressestelle • Werbematerial • Amtliche Mitteilungen • Dissertationsschriften • Organisationspläne (sofern kein Rückschluss auf Personen möglich)	• Wissenschaftliche Daten, die für Dritte nicht interpretierbar sind und für die keine Geheimhaltungsvereinbarungen bestehen • In der Regel Geschäftsverteilungspläne • Anweisungen für den täglichen Betrieb, interne Richtlinien und Rundschreiben, interne Berichte. • Interner Schriftverkehr (Mail, Chat usw.) der keine Informationen der Kategorien „VERTRAULICH“ oder „STRENG VERTRAUCHLICH“ (siehe 5.2.3 und 5.2.4) enthält.	heitsmaßnahmen, Netzpläne etc.) • Mediadaten und eigenentwickelte Software aus abgeschlossenen Projekten • Prüfungsdaten (Notenlisten, Prüfungsprotokolle etc.) • In der Regel personenbezogene Daten • Abschlussberichte (Revisionsberichte, Auditberichte etc.) • Vertrauliche Inhalte aus Gremiensitzungen • Finanzdaten (Budget etc.) • Kalkulation von wirtschaftlichen Drittmittelprojekten	(Software, Zutrittssteuerung etc.) • Strategiepapiere vor Veröffentlichung • besondere personenbezogene Daten nach DSGVO (Gesundheitsdaten, Religionszugehörigkeit etc.) • besondere wissenschaftliche Daten (Patentunterlagen vor ihrer Offenlegung)

7.2 Anlage 2: Übersicht „Personen, die Informationen als „ÖFFENTLICH“ freigeben dürfen“

Informationsart	Bereich	Name	Gültig ab	Bemerkung
Informationen zu Lehrveranstaltungen	Dezentrale	Professorinnen und Professoren /Lehrende	21.04.2022	
Inhalte aus öffentlichen Veranstaltungen	Pressestelle	Leiterin oder Leiter der Stabsstelle für Presse, Kommunikation und Marketing	21.04.2022	
Im Internet öffentlich bereitgestellte Informationen	Homepage-Verantwortliche	Verantwortliche der Homepage	21.04.2022	