Informationssicherheits-leitlinie für die Technische Universität Darmstadt

Informationssicherheit TU Darmstadt
Veröffentlichung: 05. April 2024

TECHNISCHE UNIVERSITÄT DARMSTADT

!nfoSec
TU Darmstadt

Kennzeichnung

Titel (Dokumentenkürzel):	Informationssicherheitsleitlinie für die Technische Universität Darmstadt (ISLL)
Ersteller:	Johannes Braun / Review: Peter Pelz, Jochen Becker, Stefan Tomaszek, Andreas Schönfeld / Anna Schindler
Funktion des Erstellers:	CISO / VP-DNI, Leiter TUDa-CERT, Vertretung IT-SB, Leitung HRZ (ISMT)
Versionsnummer:	v02
Letzte Überarbeitung:	05. April 2024
Nächste geplante Überarbeitung:	Q4 2028
Verabschiedet am / durch:	07. März 2024 / Präsidium der Technischen Universität Darmstadt
Inkrafttreten:	mit Veröffentlichung
Klassifizierung:	öffentlich
Berechtigte Rollen (Verteilerkreis):	alle Personen gemäß *§ 2 Geltungsbereich*
Änderungsübersicht:	v01 → v02: • Schärfung der Zielsetzung • Aufnahme Informationssicherheitsstrategie • Vereinheitlichung der Darstellung der Rollen und Verantwortlichkeiten • Aufnahme Struktur für Regelwerke • Durchgängige Nutzung des Begriffs Informationssicherheit, statt IT-Sicherheit • Verschiedene Umbenennungen

Inhaltsverzeichnis

Präambel

Der Betrieb einer Universität hängt in hohem Maße von der Qualität ihrer IT-Services ab. Dafür ist die Aufrechterhaltung der Informationssicherheit von grundlegender Bedeutung. Dies bedeutet, dass die Integrität, die Vertraulichkeit und die Verfügbarkeit von IT-Verfahren, IT-Systemen, IT-Diensten sowie Informationen jeglicher Art und Daten nachhaltig geschützt werden müssen.

Um dieser Verpflichtung angesichts einer wachsenden Bedrohungslage und der sich weiterentwickelnden Technik nachzukommen, müssen sämtliche Einrichtungen der Universität den Schutz der Informationstechnik als gemeinsame Herausforderung begreifen, die auf der Basis einer einheitlichen und verbindlichen Informationssicherheitsstrategie der Universität in einem kontinuierlichen Informationssicherheitsprozess angegangen wird. Unerlässliche Grundvoraussetzung für den Erfolg ist dabei ein angemessenes Verhältnis zwischen den Anforderungen der akademischen Freiheit und der Erfüllung relevanter Anforderungen der Informationssicherheit.

§ 1 Gegenstand der Leitlinie

Diese Informationssicherheitsleitlinie (ISLL) regelt als führendes Dokument die Informationssicherheit an der Technischen Universität Darmstadt (im Folgenden „TUDa“ genannt) und gibt eine Übersicht über die geltende Sicherheitsstruktur mit allen notwendigen Rollen und Verantwortlichkeiten. Mit dieser ISLL werden die Ziele an die Informationssicherheit sowie deren Einhaltung formuliert, um die Gesamtziele der TUDa zu unterstützen.

Die Umsetzung des Informationssicherheitskonzepts der TUDa basiert u.a. auf den folgenden Rahmenbedingungen, deren Einhaltung maßgeblich für die Umsetzung der eigenen Informationssicherheitsziele sind:

- Informationssicherheitsleitlinie für die Hessische Landesverwaltung
- Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT -Sicherheitsgesetz - HITSiG)
- Hessisches E-Government-Gesetz (HEGovG)
- Sicherheitsstandards, insbesondere den BSI Standards 200-1 bis 200-4 sowie das BSI IT-Grundschutzkompendium
- EU-DSGVO, BDSG-neu, Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG), § 55 Hessisches Hochschulgesetz (HessHG)

§ 2 Geltungsbereich

Die ISLL erstreckt sich auf alle Geschäftsprozesse und die darin verarbeiteten Informationen und Daten der TUDa, von oder für die TUDa betriebenen IT-Komponenten, den gesamten IT-Betrieb sowie alle Arbeitsplätze, die innerhalb und außerhalb der von der TUDa bewirtschafteten Campus liegen.

Sie ist verbindlich für das Präsidium, alle Einrichtungen, Mitglieder und Angehörige der Universität sowie sonstige Akteure und Personen, die für und im Auftrag der TUDa mit informationssicherheitsrelevanten Tätigkeiten beauftragt sind oder aus anderen Gründen innerhalb des Informationsverbundes der TUDa IT-Infrastruktur betreiben und / oder nutzen. Gleiches gilt für alle in vorstehender Aufzählung nicht genannten Partner der TUDa, deren Handeln die Informationssicherheitsinteressen der TUDa berühren.

§ 3 Ziele der Informationssicherheit

Als übergeordnete Ziele gelten die Umsetzung sowie die Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus, welche sich aus gesetzlichen und regulatorischen Anforderungen und der eigenen Verpflichtung gegenüber den Mitgliedern und Angehörigen der Universität sowie ihrer Partner ergeben. Das umfasst den Schutz von jeglichen Informationen und Daten in Hinblick auf deren Vertraulichkeit, Integrität und Verfügbarkeit. Dies gilt insbesondere auch für Forschung und Lehre und den Schutz von Forschungsdaten und -ergebnissen. Darüber hinaus ergeben sich für die TUDa folgende Sicherheitsziele:

- Einhaltung der gesetzlichen, vertraglichen und regulatorischen Anforderungen, welchen die TUDa unterliegt
- Etablierung von klaren Verantwortlichkeiten für festgelegte Informationssicherheitsprozesse
- Schaffung und Aufrechterhaltung eines Sicherheitsbewusstseins bei allen Personen gemäß *§ 2 Geltungsbereich*
- Etablieren einer Organisationsstruktur für die Umsetzung von Informationssicherheitsprozessen
- Etablieren eines Prozesses zum Erkennen und Behandeln von Sicherheitsvorfällen sowie die Umsetzung eines angemessenen Notfallmanagements
- Verpflichtung zur kontinuierlichen Verbesserung der bestehenden Informationssicherheitsorganisation und -prozesse sowie dem Umgang mit Abweichungen und Ausnahmen

§ 4 Informationssicherheitsstrategie

Zur Sicherstellung der Aufgabenerfüllung und Sicherstellung der Geschäfts- und Sicherheitsziele der TUDa wird ein Informationssicherheitsmanagement-System (ISMS) nach dem Stand der Technik gemäß den BSI-Standards 200-1 bis 200-4 (BSI Grundschutz) umgesetzt. Sicherheitsmaßnahmen werden hinsichtlich des festgestellten Schutzbedarfs für alle Prozesse, Verfahren sowie die benötigten IT-Komponenten umgesetzt, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten. Mögliche Sicherheitsrisiken zu den Informationswerten werden identifiziert, analysiert, bewertet und hinsichtlich notwendiger Maßnahmen beurteilt und ggf. umgesetzt. Alle sicherheitsrelevanten Vorgabe- und Nachweisdokumente unterliegen einem Revisionszyklus.

Das Präsidium ist als oberste Leitungsebene gesamtverantwortlich für die Umsetzung, Weiterentwicklung und kontinuierliche Verbesserung des ISMS. Für die interne Steuerung werden die Aufgaben auf mehrere Rollen und Verantwortlichkeiten sowie Gremien verteilt. Die Verantwortlichkeiten sind zu regelmäßigen Weiterbildungen sowie der Benennung einer vertretenden Person verpflichtet. Dadurch soll eine kontinuierliche Aufrechterhaltung der Informationssicherheitsprozesse sowie eines angemessenen Sicherheitsniveaus gewährleistet werden.

§ 5 Rollen und Verantwortlichkeiten in der Informationssicherheitsorganisation

Die Gesamtverantwortung für die Umsetzung der Informationssicherheit liegt beim Präsidium. Zur Erreichung aller Informationssicherheitsziele wurde durch das Präsidium eine Organisationsstruktur für die Sicherheitsorganisation an der TUDa festgelegt. Maßgeblich für den Erfolg von Informationssicherheitsmaßnahmen ist, dass alle Rollen und Gremien mit genügend Ressourcen für ihre Aufgaben ausgestattet sind. Für jede Rolle ist eine stellvertretende Person zu benennen, welche die Aufgaben und die Verantwortlichkeit in einem notwendigen Vertretungsfall wahrnehmen kann.

Am Informationssicherheitsprozess der TUDa sind folgende Rollen beteiligt und in Abbildung 1 dargestellt:

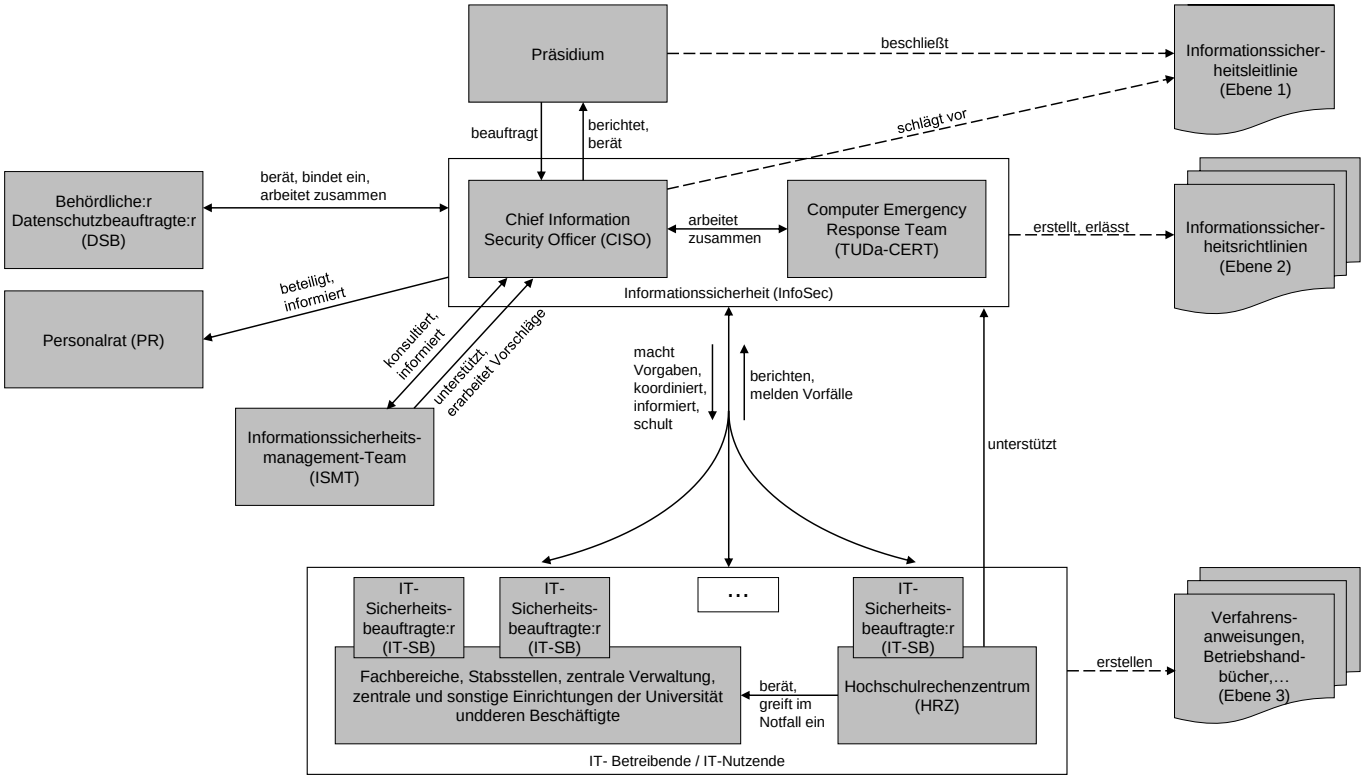

Abbildung 1: Rollen und Verantwortlichkeiten in der Informationssicherheitsorganisation. Bezüglich ISMS Dokumentenstruktur siehe auch *§ 6 Regelungsstruktur Informationssicherheit*.

(1) **Präsidium der Universität**

Zu den Aufgaben des Präsidiums zählen das Beschließen und Steuern der Informationssicherheitsstrategie und -ziele sowie der Digitalisierungsstrategie. Aufgaben zur Umsetzung und Einhaltung dieser können durch das Präsidium an nachgeordnete Verantwortlichkeiten delegiert werden.
Die Informationssicherheit liegt im Verantwortungsbereich des zuständigen Präsidiumsmitglieds. Insbesondere obliegt ihr/ihm die Qualitätskontrolle und Aufsicht der Informationssicherheitsorganisation.

Das Präsidium und alle Führungsverantwortlichkeiten leben aktiv die Umsetzung von Informationssicherheit in der TUDa vor und dienen damit als motivierendes Vorbild für alle Beschäftigten. Das Präsidium lässt sich regelmäßig über den Stand der Informationssicherheit durch die/den zuständigen Chief Information Security Officer berichten und entscheidet über notwendige Maßnahmen. Die Gesamtverantwortung und mögliche Risikoübernahme liegen beim Präsidium.

(2) **Chief Information Security Officer (CISO)**

Die/der CISO wird durch das Präsidium bestimmt und berichtet direkt an das Präsidium. Die/der CISO ist Leiter:in der zentralen Informationssicherheit der TUDa (InfoSec), welche organisatorisch als Stabsstelle dem zuständigen Präsidiumsmitglied zugeordnet ist. Sie/er steht den IT-Sicherheitsbeauftragten (IT-SB) und dem Computer Emergency Response Team (TUDa-CERT, siehe (4)) vor und vertritt die Interessen des Präsidiums gegenüber allen nachgeordneten Verantwortlichkeiten und Gremien im Informationssicherheitsprozess.

Die/der CISO verantwortet den Aufbau, den Betrieb und die Weiterentwicklung der Informationssicherheitsorganisation in der TUDa, erstellt und erlässt übergeordnete Informationssicherheitsvorgaben, berät das Präsidium sowie den Datenschutz und das Business Continuity Management und koordiniert die Umsetzung des übergreifenden IT-Notfall- und IT-Krisenmanagements der TUDa. Sie/er ist zentrale:r Ansprechpartner:in in allen informationssicherheitsrelevanten Fragen nach innen und nach außen und verantwortet das hochschulweite Informations- und Kommunikationssystem, über das alle am Informationssicherheitsprozess Beteiligten in Kontakt stehen.

Die/der CISO berichtet regelmäßig zum aktuellen Stand der Informationssicherheit an das Präsidium, koordiniert die Umsetzung und Wirksamkeit von Informationssicherheitsmaßnahmen, Sensibilisierungs- und Schulungsmaßnahmen und berät bei internen und externen Projekten in Informationssicherheitsfragen. Insbesondere trägt sie/er für das Verfassen und Versenden des jährlichen IT-Sicherheitsberichts an die hessische Landesregierung die Verantwortung und stimmt diesen mit dem zuständigen Präsidiumsmitglied ab.

Für die Erfüllung der Funktion und Umsetzung notwendiger Aufgaben werden durch das Präsidium die erforderlichen Ressourcen bereitgestellt und eine regelmäßige Weiterbildung der/des CISO sichergestellt. Die/der CISO hat ein situatives Mitsprache-, Weisungs- und Vetorecht bei allen Entscheidungen, die den verantworteten Bereich der Informationssicherheit betreffen und muss bei allen anhängigen Vorhaben (z.B. neue Projekte oder der Änderungen der IT-Infrastruktur) mit einbezogen werden.

Die/der CISO ist befugt sämtliche für den Informationssicherheitsprozess relevanten Informationen bei den einzelnen Einrichtungen einzuholen[1] und ist in Bezug auf die Informationssicherheit weisungsbefugt.

Die/der CISO ist in ihren/seinen fachlichen Themen weisungsfrei und unabhängig.

Die Aufgaben, Rechte und Pflichten gelten analog für die vertretende Person.

(3) **Informationssicherheitsmanagement-Team (ISMT)**

Aufgrund der engen Verzahnung der Themen und der übergreifenden Ziele der TU Darmstadt wird ein ISMT gebildet. Gemäß BSI Standard 200-2 unterstützt das ISMT den CISO, indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.

Aktuell besteht das ISMT aus

- einer Vertretung des Präsidiums (das zuständige Präsidiumsmitglied),
- der/dem CISO,
- der TUDa-CERT-Leitung,
- einer Vertretung der IT-Sicherheitsbeauftragten und
- einer Vertretung der Leitung des HRZ.

Auf Beschluss des ISMT kann es bei Bedarf um zusätzliche Personen erweitert werden (wie zum Beispiel den Datenschutzbeauftragten (DSB, siehe (8)) der Universität, beratende Expert:innen (z.B. für Betriebssysteme wie Unix, Linux oder Microsoft- Windows), fachlich Verantwortliche (z. B. für E-Mail-, Netzwerk- oder Nutzeradministration) oder eine Vertretung des Personalrats.

Die Mitglieder des ISMT unterstützen die folgenden Aufgaben in ihren jeweiligen Wirkungskreisen:

- Die Informationssicherheitsziele und -strategien zu bestimmen und die Leitlinie zur Informationssicherheit weiterzuentwickeln.

[1] Erfolgt die Einholung in Form von datenschutzrechtlich geschützten Informationen, ist dies zu dokumentieren. Wenn wiederkehrende Prozesse entstehen, in denen regelmäßig personenbezogene Daten verwendet werden, sind diese Prozesse in einem Verzeichnis von Verarbeitungstätigkeiten zu beschreiben. Ferner sind die betroffenen Benutzenden in den gesetzlich vorgeschriebenen Fällen zu benachrichtigen. Werden arbeitsplatz- und das Beschäftigungsverhältnis betreffende Daten von Hochschulbeschäftigten benötigt, ist der Personalrat darüber in Kenntnis zu setzen. Sollte, etwa im Kontext eines Notfalls, situationsbezogen schnelles Handeln erforderlich sein, ist dies im Nachgang ausreichend.

- Die Umsetzung der Sicherheitsrichtlinien zu überprüfen.
- Die Informationssicherheitsprozesse zu initiieren, steuern und kontrollieren.
- Bei der Erstellung von Informationssicherheitskonzepten mitzuwirken.
- Die Wirksamkeit und Eignung der in den Sicherheitskonzepten geplanten Sicherheitsmaßnahmen zu überprüfen.
- Die Sensibilisierungs- und Schulungsprogramme für die Informationssicherheit zu konzipieren.

Das ISMT bildet für die TU Darmstadt das zentrale Kontrollorgan für die Informationssicherheit und wird durch die Vertretung des Präsidiums geleitet. Das ISMT ist für die Umsetzung der ISLL verantwortlich, tagt regelmäßig und soll Vorschläge zur Weiterentwicklung der Informationssicherheitsregularien erarbeiten. Die Beteiligten am Informationssicherheitsprozess können dem ISMT Vorschläge unterbreiten.

(4) **Computer Emergency Response Team (TUDa-CERT)**

Das TUDa-CERT ist organisatorisch der/dem CISO unterstellt und ist Teil von InfoSec. Das TUDa-CERT arbeitet vertraulich und unmittelbar mit der/dem CISO zusammen, stimmt sich bei zentralen Fragen ab und berichtet der/dem CISO in regelmäßigen Abständen über seine Tätigkeiten.

Das TUDa-CERT besteht aus der Leitung des TUDa-CERT und weiteren Mitarbeiter:innen – Informationssicherheitsexpert:innen z.B. in den Bereichen: Netz, Identity-Management, E-Mail-Server und Gateway, kritische Infrastruktur.

Aufgaben des TUDa-CERT sind die übergreifende Koordinierung und auf operativer Ebene die zeitnahe Reaktion auf Informationssicherheitsvorfälle sowie Missbrauch und unsachgemäße Nutzung der Informationsinfrastruktur. Das TUDa-CERT sorgt für die Konzeption und Einführung von Maßnahmen, um Sicherheitsvorfälle präventiv zu verhindern und eintretende Schäden auf ein Minimum zu begrenzen. Das TUDa-CERT unterstützt den CISO, die IT-SB und das ISMT in technischen Fragen und greift zur Gefahrenabwehr im IT-Notfall selbstständig ein und koordiniert die übergreifenden Gegenmaßnahmen auf operativer Ebene. Es erstellt für das ISMT regelmäßig ein Lagebild über die IT-Sicherheitssituation der TU Darmstadt. Die Leitung des TUDa-CERT berichtet regelmäßig dem ISMT und der/dem CISO über die operativen Maßnahmen. Ferner berichtet sie/er in akuten Fällen unverzüglich an die/den CISO.

TUDa-CERT Mitglieder sind gegenüber IT-Nutzenden und IT-Betreibenden in IT-Notfällen und IT-Stör- und Krisensituationen weisungsbefugt. Insbesondere können bei Verstoß gegen die geltenden Richtlinien und zur Gefahrenabwehr die Mitglieder des TUDa-CERT die sofortige, vorübergehende Stilllegung des betroffenen IT-Systems anordnen sowie die verantwortlichen Nutzenden vorübergehend von der Nutzung der Informationstechnik ausschließen.

(5) **IT-Sicherheitsbeauftragte (IT-SB)**

Alle Bereiche, d.h. Fachbereiche, Stabsstellen, zentrale Verwaltung, zentrale und sonstige Einrichtungen der Universität, die IT-Systeme betreiben, benennen eine:n IT- Sicherheitsbeauftragte:n. Die Zuständigkeit kann sich dabei auf mehrere Einrichtungen und Fachbereiche beziehen. Die Benennung der/des IT-SB erfolgt ausschließlich aus dem hauptamtlichen Personal der Universität. Benennt eine Einrichtung keine:n IT-SB, kann das Präsidium, eine:n kommissarische:n IT-SB bestellen. Bis dahin nimmt die Leitung der Einrichtung diese Aufgaben wahr. Weitere Aufgaben und Befugnisse der IT-SB werden in den nachgeordneten ISMS-Dokumenten (siehe *§ 6 Regelungsstruktur Informationssicherheit*) beschrieben.

Die Rollen sind für die Durchführung des Informationssicherheitsprozesses in ihrer Einrichtung zuständig. Sie sind verpflichtet, sich aktuelle sicherheitsrelevante Informationen zu beschaffen und werden darin von der/dem CISO unterstützt. Darüber hinaus stellen die Systembetreibenden den IT-SB alle angefragten Informationen zur Verfügung, die zur Meldung an interne und externe übergeordnete Stellen notwendig sind, und stellen diese der/dem CISO vollständig und strukturiert zur Verfügung. Die IT-SB veranlassen in ihrem Bereich die erforderlichen IT- Sicherheitsmaßnahmen zur Gefahrenabwehr. Hierzu müssen sie von der Leitung ihrer Einrichtung mit den notwendigen Kompetenzen ausgestattet werden. Die Bereitstellung von Informationen ist auch gegenüber dem TUDa-CERT sicherzustellen.

(6) **Das Hochschulrechenzentrum (HRZ)**

Das Hochschulrechenzentrums (HRZ) unterstützt maßgeblich die Sicherstellung von Informationssicherheit und

verantwortet das IT-Notfallmanagement für die vom HRZ bereitgestellten Services. Die Mitarbeitenden des HRZ unterstützen den CISO, die IT-SB, das TUDa-CERT und das ISMT in technischen Fragen.

(7) **Fachbereiche, Stabsstellen, zentrale Verwaltung, zentrale und sonstige Einrichtungen der Universität und deren Beschäftigte**

Trotz der Benennung der IT-SB bleibt die Verantwortung der Leitungen der Fachbereiche, der Stabsstellen, der zentralen Verwaltung, der zentralen und sonstigen Einrichtungen sowie der angeschlossenen Einrichtungen der Universität für die Informationssicherheit in ihren Bereichen unberührt. Sie sind verpflichtet, an allen Planungen, Verfahren und Entscheidungen, die in Bezug zur Informationssicherheit stehen, die zuständigen IT-SB und die/den CISO zu beteiligen. Die ihnen zugeordneten Nutzenden der IT-Infrastruktur sind an die Regelungen und Vorgaben aus den ISMS-Dokumenten (siehe *§ 6 Regelungsstruktur Informationssicherheit*), der Benutzungsordnung der TU Darmstadt sowie an Anweisungen durch weisungsbefugte Informtionssicherheitsrollen gebunden.

(8) **Behördliche:r Datenschutzbeauftragte:r der Universität (DSB)**

Die/der behördliche Datenschutzbeauftragte übernimmt die Aufgaben gem. Art. 39 DSGVO. Durch die Verantwortlichkeit werden alle notwendigen Maßnahmen zur Einhaltung des HDSIG, BDSG-neu sowie der EU-DSGVO überwacht. Weiterhin erfolgt die Unterstützung der/des CISO und der IT-SB zur Gewährleistung des Datenschutzes von personenbezogenen Daten in allen IT-gestützten Prozessen und Verfahren.

Sofern im Rahmen des Informationssicherheitsmanagements datenschutzrechtliche Belange betroffen sind, wird die/der behördliche Datenschutzbeauftragte der Universität hinzugezogen.

Die/der behördliche Datenschutzbeauftragte der Universität soll auf schriftlichen Antrag von beeinträchtigten Nutzenden überprüfen, ob die Informationseinholung für den Informationssicherheitsprozess relevant und notwendig war. Die/der behördliche Datenschutzbeauftragte informiert die antragstellende Person, das ISMT und ggf. den Hessischen Beauftragten für Datenschutz und Informationsfreiheit über die Ergebnisse der Überprüfung und kann Empfehlungen für die zukünftige Informationseinholung aussprechen.

(9) **Personalrat der Universität (PR)**

Die Beteiligung des Personalrats der Universität erfolgt nach Maßgabe des § 69 Hessisches Personalvertretungsgesetz. Werden im Rahmen des Informationssicherheitsmanagements arbeitsplatz- und personalbezogene Daten von Hochschulbeschäftigten benötigt, ist der Personalrat darüber in Kenntnis zu setzen. Sollte, etwa im Kontext eines Notfalls, situationsbezogen schnelles Handeln erforderlich sein, ist dies im Nachgang ausreichend.

Die am Informationssicherheitsprozess beteiligten Rollen und Verantwortlichkeiten arbeiten in allen Belangen der IT-Sicherheit konstruktiv und lösungsorientiert zusammen. Bei Bedarf können externe Fachleute beratend hinzugezogen werden. Die Konkretisierung der Aufgaben und Befugnisse der am Informationssicherheitsprozess beteiligten Rollen und Verantwortlichkeiten werden in den nachgeordneten ISMS-Dokumenten (siehe *§ 6 Regelungsstruktur Informationssicherheit*), beschrieben.

Informationssicherheitsvorfälle und -notfälle jeder Art sind meldepflichtig. Bei sicherheitsrelevanten Ereignissen erfolgt gegenüber allen Beteiligten eine gegenseitige, unverzügliche, umfassende und vollständige Information. Die Systembetreibenden sind verantwortlich dafür, dass die Meldungen der Ereignisse durch die Nutzenden selbst oder durch die Systembetreibenden erfolgen. Erfolgt die Meldung an die IT-SB, so haben diese die Information umgehend an das TUDa-CERT und – insofern personenbezogene Daten betroffen sind – an den behördlichen Datenschutzbeauftragten weiterzuleiten.

§ 6 Regelungsstruktur Informationssicherheit

(1) Für die Umsetzung aller getroffenen Maßnahmen und der notwendigen dokumentierten Informationen, ist in der TUDa eine hierarchische Regelungsstruktur getroffen worden. Diese Dokumente unterliegen einem regelmäßigen Revisionszyklus. Die Ebene 1 umfasst die Informationssicherheitsleitlinie der TUDa. Sie wird vom Präsidium verabschiedet und spätestens alle fünf Jahren in dessen Auftrag überprüft.

(2) Die Ebene 2 umfasst detaillierte Vorgaben in Form von Richtlinien, die entweder für alle oder einen spezifischen Kreis von Personen gemäß *§ 2 Geltungsbereich* verbindliche Rahmenbedingungen festlegen. In Informationssicherheitsrichtlinien werden übergreifende Anforderungen für die Umsetzung von Informationssicherheit dokumen-

tiert. Die Verantwortlichkeit der Erstellung und Pflege der Dokumente obliegt dem CISO. Revisionszyklus: alle 3 Jahre oder anlassbezogen.

(3) Die Ebene 3 umfasst die konkrete Umsetzung der Vorgaben aus der Ebene 1 und der Ebene 2. Die Dokumente dieser Ebene regeln die Umsetzung von spezifischen Informationssicherheitsanforderungen für einzelne Bereiche und Themen. Diese sind im Allgemeinen Verfahrensanweisungen, Betriebshandbücher o.ä. Sofern ergänzende Dokumentationen notwendig sind, können erweitert Handlungshilfen, Leitfäden o.ä. erstellt werden. Zuständig für die Erstellung, Pflege und Kommunikation der Informationen sind die System- bzw. Verfahrensverantwortlichen. Revisionszyklus: jährlich oder anlassbezogen.

Neben den Regelungsdokumenten existieren zusätzliche Nachweisdokumente, wie beispielsweise Sicherheitskonzepte, Reports, Dokumentationen, Auditberichte, Protokolle o.ä. Zuständig für die Erstellung, Pflege und Kommunikation der Informationen sind die System- bzw. Verfahrensverantwortlichen oder die Prozessverantwortlichen. Diese Dokumente sind nicht Teil der Dokumentenpyramide und dienen der erweiterten Dokumentation sowie als Nachweis für die Umsetzung von Sicherheitsmaßnahmen des Informationssicherheitsmanagementsystems.

Ebene	**Dokumentenart/-typen**	**Detaillierungsgrad und Inhalt**
Ebene 1	Leitlinien	Verbindliche Vorgaben für alle Personen gemäß *§ 2 Geltungsbereich*. Gibt den strategisch-organisatorischen Rahmen des Informationssicherheitsmanagements vor.
Ebene 2	Informationsicherheitsrichtlinien	Verbindlich Vorgaben für alle oder einen spezifischen Kreis von Personen gemäß *§ 2 Geltungsbereich*.
Ebene 3	Verfahrensanweisungen, Betriebshandbücher, …	Verbindliche Vorgaben für spezifische/themengebundene Bereiche, die teilweise einen dokumentierenden Charakter haben.
	Handlungshilfen, Leitfäden, Sicherheitskonzepte, …	Empfehlungen, Konfigurationshilfen, Detailbeschreibungen

Tabelle 1: Dokumentenpyramide

§ 7 Kontinuierliche Verbesserung

Das ISMS ist regelmäßig, mindestens jährlich, auf seine Aktualität und Wirksamkeit zu prüfen. Zur Aufrechterhaltung und Weiterentwicklung werden regelmäßig Wirksamkeits- und Erfolgskontrollen durchgeführt sowie mögliche Nicht-Konformitäten behoben. Dieser Prozess dient der Analyse der Angemessenheit, der Eignung und der Wirksamkeit von umgesetzten Maßnahmen und wird zur Steigerung der Effizienz sowie Verbesserung des Informationssicherheitsniveaus durch das Präsidium unterstützt.

Die Umsetzung erfolgt u.a. durch interne Audits, Durchführung von Übungen und Sensibilisierungsmaßnahmen und technische Schwachstellenscans. Gefundene Abweichungen werden im Rahmen des kontinuierlichen Verbesserungsprozesses dokumentiert und anhand von geeigneten Maßnahmen oder Anpassungen in einem angemessenen zeitlichen Rahmen behoben. Die Ergebnisse der Wirksamkeitsprüfungen werden in einem Managementbericht dokumentiert und dem Präsidium berichtet.

§ 8 Inkrafttreten

Die ISLL tritt nach Beschlussfassung des Präsidiums mit ihrer Veröffentlichung auf der Webseite von InfoSec und auf TUprints in Kraft.