Universität Kassel
Das Präsidium

19. Februar 2024
Az. 1.10.01 /E 2

10. Protokoll, 9. Wahlperiode
Anlage 27

B E S C H L U S S

Leitlinie zur Informationssicherheit

P/237

Das Präsidium beschließt die Leitlinie zur Informationssicherheit gemäß Anlage und ersetzt hiermit die Leitlinie gemäß P/687 vom 17. Mai 2019.

UNIKASSEL
VERSITÄT

Leitlinie zur Informationssicherheit

Universität Kassel

Inhaltsverzeichnis

Präambel

Das Präsidium der Universität Kassel betrachtet die Informationssicherheit als einen wichtigen Faktor für die Aufrechterhaltung des Universitätsbetriebs. Es stellt daher sicher, dass Informationssicherheit angemessen behandelt wird und bekennt sich zu seiner Verantwortung für die kontinuierliche Überwachung und Weiterentwicklung der Informationssicherheitsstrategie, des Informationssicherheitsniveaus und der Informationssicherheitsmaßnahmen.

Die Informationssicherheit dient insbesondere der Prävention und Abmilderung von Sicherheitsvorfällen. Dazu zählen alle Ereignisse mit negativen Auswirkungen auf Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen.

Die meisten Prozesse an der Universität werden maßgeblich durch IT unterstützt. Vernetzte IT-Systeme sind angreifbar und können sowohl von innen als auch von außen kompromittiert werden. Die IT-Sicherheit ist daher ein wesentlicher Teilbereich der Informationssicherheit.

Die einzelnen Maßnahmen zur Erhöhung des Informationssicherheitsniveaus sind auf der Basis der vorliegenden Leitlinie zur Informationssicherheit (IS-LL) in einem kontinuierlichen Informationssicherheitsprozess (IS-Prozess) zusammengefasst. Die Maßnahmen und Regeln, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern, werden als Informationssicherheitsmanagementsystem (ISMS) bezeichnet. Das ISMS wird durch den IS-Prozess umgesetzt und weiterentwickelt. Die IS-LL gibt den strategisch-organisatorischen Rahmen für den IS-Prozess und das ISMS vor und baut auf der mit der Satzung zur Ausgestaltung des technischen Informationsmanagements vom 24.04.2020 (Mitt.Bl. Univ. Kassel Nr. 4/2020 vom 15.05.2020, S. 75) geschaffenen Struktur auf. Im Fall einander widersprechender Regelungen im Bereich der Informationssicherheit gehen jedoch die Regelungen der IS-LL jenen der genannten Satzung vor.

Eine zentrale Anforderung der Universität ist dabei die Gewährleistung der akademischen Freiheit bei gleichzeitiger Erfüllung der Anforderungen an die Informationssicherheit gem. dem Hessischen Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG).

§ 1 Gegenstand

Die IS-LL beschreibt allgemein verständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Universität Kassel durch den IS-Prozess und das ISMS hergestellt werden soll. Die IS-LL initiiert den IS-Prozess und ist das zentrale organisatorische Regelwerk des ISMS.

§ 2 Geltungsbereich

Die IS-LL gilt für alle Organisationseinheiten, Mitglieder und Angehörigen der Universität Kassel.

§ 3 Ziele

Die Informationssicherheit umfasst den fortlaufenden und ganzheitlichen Schutz von digitalen und analogen Daten. Folgende grundlegende Schutzziele der Informationssicherheit sind im Rahmen des IS-Prozesses sicherzustellen und fortlaufend aufrechtzuhalten:

- **Vertraulichkeit**: Informationen können nur von autorisierten Personen, Systemen oder Prozessen abgerufen oder bearbeitet werden.
- **Integrität**: Informationen und Systeme sind vor unerlaubten oder unbeabsichtigten Veränderungen zu schützen.

- **Verfügbarkeit**: Informationssysteme und -dienste sind jederzeit für autorisierte Nutzer:innen zugänglich.
- **Authentizität**: Übermittelte Daten können im Rahmen datenschutzrechtlicher Bestimmungen jederzeit ihrem Ursprung zugeordnet werden. Es ist sichergestellt, dass sie von der angegebenen Quelle (einer bestimmten Person, einer IT-Komponente oder einer Anwendung) stammen.

Die Universität Kassel verfolgt auf Basis dieser grundlegenden Schutzziele der Informationssicherheit sowie der Vorgaben durch das HITSiG die Umsetzung eigener Sicherheitsziele:

(1) Schärfung des Bewusstseins für Informationssicherheit

Die Mitglieder und Angehörigen der Universität sind über potenzielle Sicherheitsrisiken zu informieren. Ein umfassendes Verständnis und Bewusstsein für Informationssicherheit sind bei allen Mitgliedern und Angehörigen der Universität zu fördern, um eine Kultur der Sicherheit durch regelmäßige Schulungen, Informationsveranstaltungen und einschlägige Kommunikation zu etablieren.

(2) Compliance

Durch die Implementierung von IS-Maßnahmen und Überprüfungsmechanismen ist die Einhaltung von Vorschriften wie jenen der Datenschutz-Grundverordnung (DS-GVO), des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG), des Hessischen IT-Sicherheitsgesetzes (HITSiG) und anderer relevanter Gesetze und Verordnungen zu gewährleisten.

(3) Gewährleistung der funktionalen Aufgabenerledigung

Die Informationstechnik ist so zu betreiben, dass Informationen verlässlich und hinreichend schnell verfügbar sind. Ausfälle, die zu Terminüberschreitungen von mehr als einem Tag bei der Abwicklung von Vorgängen in Verwaltung, Forschung und Lehre führen, sind möglichst zu vermeiden. Netzwerkinfrastruktur und IT-Systeme einschließlich der damit verarbeiteten Informationen sind gegen Missbrauch oder Sabotage von innen und außen zu schützen.

(4) Schadensverhütung

Direkte und indirekte finanzielle Schäden und negative Einflüsse auf die Reputation der Universität, die durch den Verlust der Vertraulichkeit sensibler Daten, Datenänderungen oder Systemausfälle entstehen könnten, sind durch angemessene Maßnahmen tunlichst zu verhindern.

(5) Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen

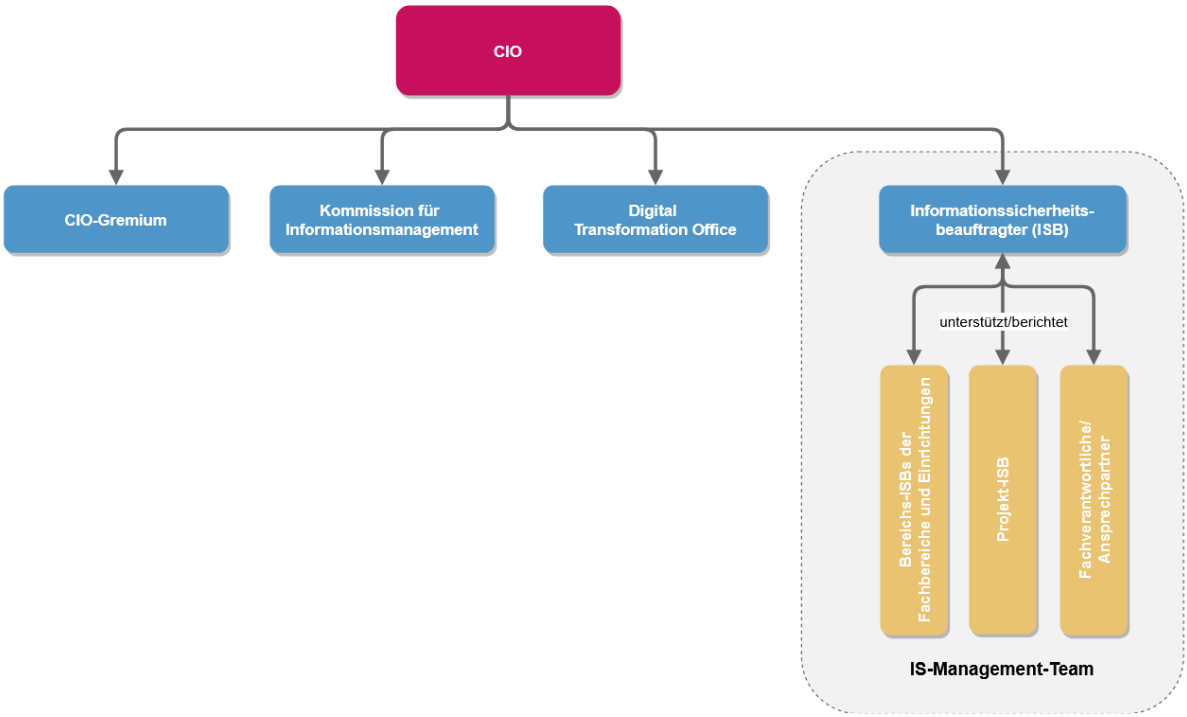
Vertraulichkeit und Integrität der persönlichen und betrieblichen Informationen sind zu schützen, unabhängig davon, in welcher Form sie vorliegen. Dies gilt besonders für die aus den gesetzlichen Vorgaben resultierenden Anforderungen an den Datenschutz. Geheimhaltungspflichten ist Folge zu leisten.

(6) Kontinuierliche Verbesserung

Die Universität Kassel strebt die kontinuierliche Verbesserung des IS-Prozesses an.

§ 4 Organisationsstruktur

Die Etablierung eines erfolgreichen IS-Prozesses setzt klar definierte Verantwortlichkeiten und die Erfüllung der daraus resultierenden Aufgaben innerhalb der Organisationsstruktur voraus. Die Informationssicherheit wird wie folgt in die bestehende CIO-Governance integriert, wobei unter CIO-Governance der einheitliche Steuerungs- und Koordinationsprozess des technischen Informations–managements zur Gestaltung der Digitalen Transformation der Universität verstanden wird:



Der IS-Prozess wird demnach von folgenden Verantwortlichen getragen:

Beim **Präsidium** liegt die Gesamtverantwortung für die Informationssicherheit. Es bestimmt den Stellenwert der Informationssicherheit, sorgt für deren Integration in die Geschäftsprozesse und stellt dafür angemessene Ressourcen bereit.

Der/Die **Informationssicherheitsbeauftragte(r) (ISB)** ist Mitglied des CIO-Gremiums. Er/Sie implementiert, steuert und koordiniert den IS-Prozess und erarbeitet kontinuierlich gemeinsam mit dem CIO das IS-Konzept sowie weitere zentrale IS-Dokumente. In seinen/ihren Aufgaben als Informationssicherheitsbeautragte/r ist der/die ISB nur an Weisungen der Hochschulleitung gebunden. Er/Sie berät das Präsidium auf dem Gebiet der Informationssicherheit, berichtet über den Status der Informationssicherheit und unterstützt bei der Umsetzung der Ziele der Leitlinie. Der/Die ISB steuert und überprüft die Realisierung von Sicherheitsmaßnahmen, die Umsetzung, den Betrieb und die Weiterentwicklung des ISMS, das Sicherheitsvorfallmanagement, die Schaffung eines Informationssicherheitsbewusstseins in allen Bereichen der Universität sowie die Berichterstattung gegenüber Behörden. Der/Die ISB hat ein Informations- und Vorschlagsrecht gegenüber dem Präsidium.

Das **IS-Management-Team** unterstützt den/die ISB bei der Erarbeitung und Weiterentwicklung der IS-Dokumente und der Koordination der Maßnahmen zur Umsetzung der IS-LL, des IS-Konzepts und des ISMS. Darüber hinaus analysiert das IS-Management-Team die aktuelle Sicherheitslage und bearbeitet die Sicherheitsvorfälle. Mitglieder des IS-Management-Teams sind:

- ISB (Vorsitz),
- Stellvertretung des/der ISB,
- Bereichs-Informationssicherheitsbeauftragte,
- ITS-Leitung,
- Datenschutzbeauftragte(r),
- Personalratsvertretung.

Weitere Personen – z.B. Ansprechpersonen ausgewählter Fachverfahren und sonstige IT-Verantwortliche – können anlassbezogen als Gäste zu den Sitzungen des IS-Management-Teams eingeladen werden.

Das IS-Management-Team hält regelmäßige, mindestens zweimal pro Kalenderjahr, Sitzungen ab.

Das IS-Management-Team setzt die Sicherheitsmaßnahmen nach IS-Konzept gem. § 6 IS-LL um und prüft deren Wirksamkeit.

Ein/Eine **Bereichs-ISB** wird in jedem Fachbereich und in jeder zentralen Einrichtung sowie in jeder Abteilung und in der Regel auch in jeder Stabsstelle der zentralen Verwaltung der Universität benannt. Weitere Organisationseinheiten der Universität können eine/einen Bereichs-ISB vorsehen. Er/Sie ist innerhalb der Organisationseinheit für die Umsetzung, Einhaltung und Kommunikation der IS-LL, des IS-Konzepts und des ISMS verantwortlich. Bereichs-ISB unterstützen den/die ISB bei der Erfüllung der Berichtspflichten sowie bei der Erfassung und Bearbeitung von Sicherheits-/Verdachtsvorfällen.

In besonderen Fällen wird für einzelne Projekte oder Systeme ein **Projekt-/System-ISB** benannt. Der/Die Projekt-/System-ISB ist für die Umsetzung der Maßnahmen zur Verbesserung der Informationssicherheit und die Meldung von Sicherheits-/Verdachtsvorfällen an den/die zuständige(n) Bereichs-ISB oder den/die ISB verantwortlich.

Alle **Mitglieder und Angehörigen** der Universität Kassel leisten durch die Teilnahme an dem Schulungsangebot sowie den Sensibilisierungsmaßnahmen zur Informationssicherheit und durch die Meldung von Sicherheits-/Verdachtsvorfällen ihren Beitrag zur Erreichung der Sicherheitsziele.

§ 5 Strategie

Um die gesetzten Sicherheitsziele und damit ein angemessenes Sicherheitsniveau zu erreichen, ist ein systematisches Vorgehen erforderlich. Durch die am BSI IT-Grundschutz orientierte Vorgehensweise (§ 3 Abs. 1, letzter Satz HITSiG) in Kombination mit den Bausteinen des BSI IT-Grundschutz-Kompendiums und dem ZKI IT-Grundschutz Profil für Hochschulen wird im IS-Prozess eine systematische Methodik zur Implementierung, Aufrechterhaltung und kontinuierlichen Verbesserung eines ISMS an der Universität Kassel angewendet. Im Rahmen des ISMS werden Bewertungen des hochschulweiten Risikomanagements berücksichtigt. Der/Die ISB trägt dafür Sorge, dass Aspekte des IS-Managements, insbesondere des IS-bezogenen Risikomanagements, in das hochschulweite Risikomanagement einfließen.

(1) Erstellung des IS-Konzepts

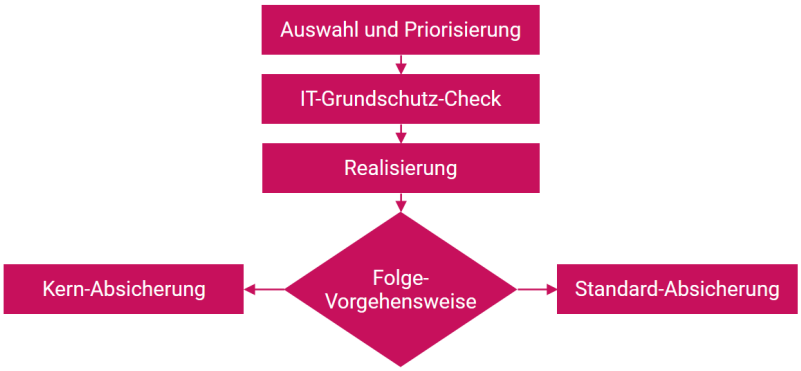
Der/Die ISB entwickelt in Abstimmung mit dem CIO und dem IS-Management-Team das IS-Konzept für die Universität Kassel, das mit Beschluss des Präsidiums in Kraft gesetzt wird. Es beschreibt die Maßnahmen, mit denen die in der IS-LL festgelegten Ziele und Strategien verfolgt werden sollen und definiert deren Umfang sowie die Priorisierung der zu schützenden Werte (Assets). Das IS-Konzept wird parallel zu den nachfolgend beschriebenen Schritten der Strategie gem. § 5 IS-LL kontinuierlich weiterentwickelt.

(2) Aufbau der IS-Organisation

Den in § 4 definierten Verantwortlichen sind Aufgaben sowie Verantwortungsbereiche zuzuordnen und, sofern erforderlich, im Rahmen der Strukturplanung der Bereiche und/oder in Tätigkeitsbeschreibungen von Beschäftigten – den hierfür vorgesehenen Verfahren folgend – festzulegen. Die Informationssicherheit ist in die Abläufe und Prozesse der Universität zu integrieren. Der IS-Prozess und gegebenenfalls weitere zur Erfüllung der Aufgaben benötigte Prozesse sind einzurichten, und die IS-Organisation einschließlich der genannten Prozesse ist im ISMS zu dokumentieren.

(3) Umsetzung der Basis-Absicherung nach BSI IT-Grundschutz

Die am BSI IT-Grundschutz orientierte Basis-Absicherung umfasst auf Komponenten von Geschäftsprozessen, Anwendungen und IT-Systemen bezogene organisatorische, personelle, infrastrukturelle und technische Anforderungen, die im Rahmen des IS-Prozesses zu erfüllen sind und wie folgt in Aktionsfelder zusammengefasst werden:



Auswahl und Priorisierung: Die im IS-Konzept definierten Informationsverbünde (Geltungsbereiche) werden gemäß IT-Grundschutz-Kompendium system- und prozessbezogen modelliert. Auf dieser Grundlage erfolgt eine systematische Auswahl und Priorisierung abzuleitender IS-Maßnahmen.

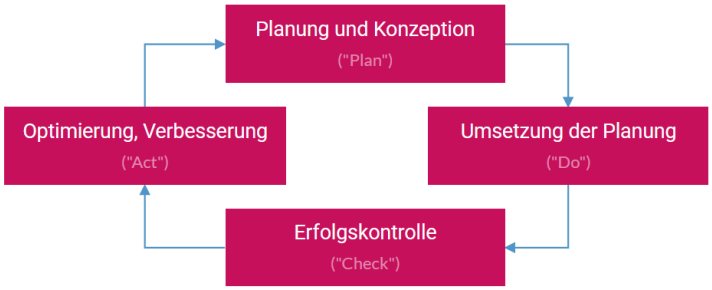
IT-Grundschutz-Check: Nach den im IS-Konzept definierten Prioritäten werden einzelne Bereiche, Prozesse oder Assets dahingehend überprüft, ob oder inwieweit die in den Basisanforderungen nach IT-Grundschutz formulierten Vorgaben bereits erfüllt sind und welche Sicherheitsmaßnahmen noch fehlen.

Realisierung: Für die bisher nicht erfüllten Basisanforderungen werden geeignete Sicherheitsmaßnahmen festgelegt und umgesetzt.

Folge-Vorgehensweise: Die Basis-Absicherung dient als Einstiegsvorgehensweise. Es ist daher rechtzeitig festzulegen, zu welchem Zeitpunkt und mit welcher IT-Grundschutz-Vorgehensweise das Sicherheitsniveau weiter angehoben werden soll.

(4) Erfolgskontrolle

Der IS-Prozess, das ISMS, das IS-Konzept und die IS-Organisation unterliegen einem PDCA-Lebenszyklus („Plan – Do – Check – Act“) und werden von dem/der ISB in regelmäßigen Abständen auf Aktualität und Wirksamkeit überprüft.



„Erfolgskontrolle (Check)“ schließt auch die umgehende Beseitigung kleinerer Mängel ein. Vor grundlegenden oder umfangreichen Veränderungen ist erneut mit der Planungsphase zu beginnen.

§ 6 Dokumente / Regelwerk

Die IS-LL gibt den strategisch-organisatorischen Rahmen des ISMS vor. Sie wird vom Präsidium erlassen und regelmäßig, jedoch spätestens alle vier Jahre einer Revision unterzogen.

Der IS-LL nachgeordnet ist das IS-Konzept. Darin dokumentiert der/die ISB gemeinsam mit dem IS-Management-Team und in Absprache mit dem CIO identifizierte Risiken und die zu deren Minimierung geeigneten technischen und organisatorischen Maßnahmen. Das IS-Konzept ist vor jeder wesentlichen Veränderung der eingesetzten technischen Systeme zu aktualisieren und alle zwei Jahre einer Revision zu unterziehen.

Die Erstellung und Fortschreibung von als Richtlinien für Informationssicherheit (IS-Richtlinien) bezeichneten besonderen organisatorischen und/oder technischen Regelungen und Maßnahmen wird von dem/der ISB koordiniert, im IS-Management-Team und im CIO-Gremium abgestimmt und in geeigneter bzw. vorzusehender Form (z.B. als Dienstvereinbarung oder Dienstanweisung für Beschäftigte, im Rahmen der IT-Benutzungsordnung, als Handreichung, als standardisierter Passus in Verträgen und Vereinbarungen) umgesetzt. Hierbei ist ein möglichst hohes Maß an Verbindlichkeit für den Geltungsbereich gemäß § 2 IS-LL vorgesehen. Die Richtlinien werden regelmäßig, jedoch spätestens jährlich auf Aktualität und Wirksamkeit überprüft.

§ 7 Sicherheitsrelevante Ereignisse

Als sicherheitsrelevantes Ereignis wird ein Ereignis bezeichnet, das die Grundwerte Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität beeinträchtigen kann (s. Punkt 5.8 der Informationssicherheitsleitlinie für die hessische Landesverwaltung [2021]).

(1) Definition

Verdachtsfall: liegt vor, wenn in der fachlichen Bewertung eines sicherheitsrelevanten Ereignisses festgestellt wird, dass die Möglichkeit eines Sicherheitsvorfalls besteht oder dieses Ereignis sich zu einem Sicherheitsvorfall entwickeln kann.

Sicherheitsvorfall: jedes Ereignis, das die Informationssicherheit in mindestens einem ihrer Grundwerte Vertraulichkeit, Verfügbarkeit, Integrität oder Authentizität nicht nur unerheblich beeinträchtigt.

(2) Abgrenzung

Störung: ist eine Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen. Störungen werden in der Regel innerhalb des Normalbetriebs durch den IT-Betreiber behoben. Störungen können jedoch zu einem Sicherheitsvorfall eskalieren.

(3) Umgang mit Sicherheitsvorfällen

Mitglieder und Angehörigen der Universität Kassel sind verpflichtet, Sicherheits-/Verdachtsvorfälle unverzüglich dem/der zuständigen Bereichs-ISB oder dem/der ISB zu melden. Sicherheits-/Verdachtsvorfälle, die eine Verletzung personenbezogener Daten zur Folge haben, sind zusätzlich unverzüglich der/dem Datenschutzbeauftragten zu melden. Die Meldewege sind in allen Bereichen zu kommunizieren.

Eine Eskalationsstrategie (eindeutige Handlungsanweisungen, wer auf welchem Weg bei welcher Art von erkennbaren oder vermuteten Sicherheitsstörungen wann einzubeziehen ist) und Verantwortlichkeiten für den Fall eines Sicherheitsvorfalls sind festzulegen.

Alle Sicherheitsvorfälle sind zu dokumentieren und gemäß den gesetzlichen und regulatorischen Anforderungen an zuständige Behörden zu melden.

Der Prozessablauf zur Behandlung von Sicherheitsvorfällen ist in einem Folgedokument (Richtlinie) zu definieren.

§ 8 Inkrafttreten

Die Leitlinie zur Informationssicherheit der Universität Kassel tritt nach Beschlussfassung durch das Präsidium der Universität Kassel am Tag nach ihrer Bekanntmachung in Kraft.

Die Informationssicherheitsleitlinie der Universität Kassel (Mitt.Bl. Univ. Kassel Nr. 6/2019 vom 28.05.2019, S. 332) tritt gleichzeitig außer Kraft.