Universität Leipzig

Ordnung zur Informationssicherheit an der Universität Leipzig

Vom 6. März 2020

§ 1
Präambel

Die Universität Leipzig hat mit Beschluss der Grundsätze zur Informationssicherheit vom 21. Januar 2014 den hohen Stellenwert einer ordnungsgemäßen Verarbeitung von Informationen und eines sicheren Betriebes der Informationstechnik zum Ausdruck gebracht. Die Abläufe in Studium, Lehre, Forschung, Transfer und Verwaltung sind auf funktionierende und sichere Informationsverarbeitung angewiesen. Darüber hinaus ist die Informationssicherheit auch eine zwingende Voraussetzung für das Gelingen der weiteren Digitalisierung. Mit dieser Ordnung werden wesentliche Anforderungen aus dem Sächsischen Informationssicherheitsgesetz (SächsISichG) an der Universität Leipzig umgesetzt.
Informationssicherheit muss sich nach den gesetzlich festgelegten Aufgaben der Hochschulen sowie deren Mandat zur Wahrung der akademischen Freiheit richten. Das ist nur innerhalb geregelter Strukturen und klar definierter Maßstäbe zu erreichen. Daher orientiert sich die Universität Leipzig an den IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Soweit weitere Standards durch den Freistaat Sachsen gem. § 4 Abs. 2 SächsISichG, durch den IT-Planungsrat gem. Art. 91 c GG bzw. gem. § 5 Onlinezugangsgesetz (OLZ) vorgegeben werden, sind diese verbindlich einzuhalten.

§ 2
Gegenstand dieser Ordnung

(1) Diese Ordnung legt den Aufbau der Informationssicherheitsorganisation der Universität Leipzig fest. Inhalte dieser Ordnung sind die Regelungen zum hochschulweiten Managementsystem für Informationssicherheit (Informations-Sicherheits-Management-System - ISMS). Dazu gehören

die erforderlichen organisatorischen Strukturen, eine Aufgabenzuordnung sowie die Zusammenarbeit der Beteiligten.

(2) Weiterhin sind in dieser Ordnung allgemeine Grundsätze der Informationssicherheit und Bedingungen definiert, unter denen informations- und kommunikationstechnische Systeme an der Universität Leipzig betrieben und genutzt werden können.

§ 3
Geltungsbereich

Die Ordnung zur Informationssicherheit an der Universität Leipzig gilt für alle Organe, Fakultäten, Einrichtungen, Mitglieder, Angehörige und Gäste der Universität Leipzig sowie für Dritte, die IT der Universität Leipzig benutzen oder betreiben.

§ 4
Beteiligte am Informationssicherheitsprozess

(1) Die Gesamtverantwortung für die Informationssicherheit trägt das Rektorat. Das CIO-Gremium ist als beauftragtes Organ des Rektorats für die zentralen Steuerungsaufgaben des Informationsmanagements und damit auch für die Informationssicherheit verantwortlich. Es bindet alle Fakultäten und Einrichtungen, insbesondere das Universitätsrechenzentrum, in den Informationssicherheitsprozess ein.

(2) Grundsätzlich ist jedes Mitglied der Universität für die in seinem Verantwortungs- und Aufgabenbereich liegenden Daten und Informationen und damit für die Gewährleistung der Schutzziele sowie die Umsetzung von Sicherheitsmaßnahmen zuständig. Die Leitungen der Fakultäten und Einrichtungen sind verantwortlich für die Informationssicherheit ihrer Organisationseinheit.

(3) Darüber hinaus besteht die Informationssicherheitsorganisation aus den folgenden Funktionsträger_innen:

- Informationssicherheitsmanagement-Team (ISMT)
- Informationssicherheitsbeauftragte_r (ISB) und seine_ihre Vertretung
- Dezentrale Ansprechpersonen für Informationssicherheit

(4) Mitglieder des Informationssicherheitsmanagement-Teams sind:

- der_die Beauftragte für Informationssicherheit
- ein_e Vertreter_in der Universitätsverwaltung
- ein_e Vertreter_in der dezentralen Ansprechpersonen für Informationssicherheit
- ein_e Vertreter_in des Universitätsrechenzentrums
- ein_e Vertreter_in aus Forschung und Lehre.

Die Mitglieder des ISMT werden vom CIO benannt.

(5) Informationssicherheit ist integraler Bestandteil aller Arbeitsabläufe der Universität. Innerhalb der Ablauforganisation der UL sind IT-Verfahrens- und Prozessverantwortliche zu benennen.

§ 5
Aufgaben im Informationssicherheitsprozess

(1) Das **ISMT** ist das zentrale Organ der Universität für die Informationssicherheit. Es ist für die Entwicklung, Fortschreibung, Umsetzung und Überwachung des Informationssicherheitsmanagementsystems verantwortlich. Zu den Aufgaben des ISMT gehören außerdem die Erstellung bzw. Überarbeitung von Richtlinien zur Informationssicherheit und die Erstellung eines jährlichen Berichts zur Informationssicherheit für das Rektorat. Die verbindliche Beschlussfassung der Richtlinien obliegt dem Rektorat nach Zustimmung des CIO-Gremiums. Das ISMT soll regelmäßig zur kontinuierlichen Weiterentwicklung des ISMS und der Richtlinien zur Informationssicherheit beraten. Den Vorsitz im ISMT hat der_die ISB.

(2) Der_Die **ISB** berät die Hochschulleitung in Fragen der Informationssicherheit und berichtet zu aktuellen Sicherheitsvorfällen. Er_Sie hat unmittelbares Vortragsrecht beim Rektorat und ist bei der Ausübung seiner_ihrer Aufgaben weisungsfrei. Ihm_Ihr dürfen durch die Wahrnehmung seiner_ihrer Aufgaben keine Nachteile entstehen.
Der_Die ISB dokumentiert sicherheitsrelevante Vorfälle und koordiniert die Meldepflichten gem. § 17 SächsISichG. Er_Sie entwickelt ein Sensibilisierungskonzept zur Informationssicherheit.
Der_Die ISB koordiniert und steuert die Umsetzung des Informationssicherheitsprozesses und wird dabei vom ISMT und den dezentralen Ansprechpersonen für Informationssicherheit unterstützt. Der_Die ISB ist

Ansprechperson in allen Fragen zur Informationssicherheit. Er_Sie ist berechtigt, die Umsetzung des Informationssicherheitsprozesses und die Einhaltung der Richtlinien zu prüfen und Audits in den einzelnen Einrichtungen durchzuführen. Die Prozess- und IT-Verfahrensverantwortlichen unterstützen den_die ISB bei seinen_ihren Aufgaben und gewähren ihm_ihr Zugang zu allen erforderlichen Informationen, insb. auch Protokolldaten. Vor wesentlichen Änderungen an Informationssystemen ist das Benehmen mit dem_der ISB herzustellen. Er_Sie ist rechtzeitig an IT-Vorhaben zu beteiligen.

(3) Die **dezentralen Ansprechpersonen** koordinieren und begleiten die Umsetzung des Informationssicherheitsprozesses in ihren Einrichtungen und unterstützen die Prozess- und die IT-Verfahrensverantwortlichen bei der Erstellung von Sicherheitskonzepten. In den Sicherheitskonzepten sind alle Sicherheitsmaßnahmen und deren Umsetzung dokumentiert. Sie werden regelmäßig aktualisiert. Die dezentralen Ansprechpersonen informieren die Leitung ihrer Organisationseinheit und den_die ISB regelmäßig über den Stand der Umsetzung und über aktuelle Problemfälle.
Die Benennung der dezentralen Ansprechpersonen entlässt die Leitung der Fakultäten sowie der wissenschaftlichen, zentralen und sonstigen Einrichtungen der Universität Leipzig nicht aus ihrer Verantwortung für die Informationssicherheit in ihrem Bereich.

(4) Die dezentralen Ansprechpersonen für Informationssicherheit unterstützen das ISMT bei der Erarbeitung von Richtlinien und übergreifenden, hochschulweit relevanten Konzepten. Das ISMT kann anlassbezogene Arbeitsgruppen einrichten, beispielsweise zur Unterstützung von operativen Aufgaben. Die Auswahl der Mitglieder einer Arbeitsgruppe obliegt dem_der ISB.

(5) Das **Universitätsrechenzentrum** (URZ) ist als Betreiber der grundlegenden IT-Infrastruktur und IT-Basisdienste von zentraler Bedeutung für die Informationssicherheit. Es unterstützt den ISB, die dezentralen Ansprechpersonen und das ISMT in technischen Fragen.

(6) Der_Die ISB konzipiert in Zusammenarbeit mit dem URZ ein hochschulweites Informations- und Kommunikationssystem, über das alle Beteiligten am Informationssicherheitsprozess in Kontakt stehen und Informationen austauschen können.

(7) Bei der Benennung der im Informationssicherheitsprozess aktiven Personen ist die erforderliche personelle Kontinuität zu berücksichtigen. Deshalb sollen die Personen möglichst zum hauptamtlichen Personal der Hochschule gehören oder über langfristige Verträge verfügen.

(8) Alle Mitglieder und Angehörigen der Universität Leipzig sowie Benutzer_innen der IT-Infrastruktur sind verantwortlich für den ordnungsgemäßen und sorgsamen Umgang mit verarbeiteten Informationen und verwendeten IT-Systemen. Sie sind zur Meldung sicherheitsrelevanter Ereignisse an die dezentralen Ansprechpersonen ihrer Einrichtung und den_die ISB verpflichtet.

§ 6
Gefahrenintervention

(1) Bei Gefahr im Verzug können der_die ISB oder die dezentralen Ansprechpersonen in ihren Zuständigkeitsbereichen die sofortige vorübergehende Stilllegung betroffener IT-Systeme anordnen, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden nicht anders abzuwenden ist. Der_Die ISB ist unverzüglich zu informieren.

(2) Soweit das URZ Gefahr im Verzug feststellt, kann es Netzanschlüsse auch ohne vorherige Benachrichtigung der Betroffenen vorübergehend sperren, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden für die IT-Infrastruktur der Universität Leipzig nicht anders abzuwenden ist. Der_Die ISB ist unverzüglich ggf. nachträglich zu informieren.

(3) Die Wiederinbetriebnahme erfolgt erst nach der Durchführung hinreichender Sicherheitsmaßnahmen in Abstimmung mit dem_der ISB.

(4) Für kritische IT-Ressourcen der Universität sind Notfallpläne durch die IT-Verfahrensverantwortlichen zu erarbeiten, die Handlungsanweisungen und Verhaltensregeln für bestimmte Gefahrensituationen und Schadensereignisse beinhalten. Die Zielsetzung ist, Gefahren soweit wie möglich abzuwenden und eine möglichst schnelle Wiederherstellung der Verfügbarkeit der IT-Ressourcen in Krisensituationen zu erreichen.

(5) Systembetreiber_innen sind berechtigt nach den Maßgaben der §§ 12, 13 und 14 SächsISichG Protokolldaten zur Abwehr und Erkennung von Gefahren zu erheben und auszuwerten. Das Referat für Datenschutz und Informationssicherheit und der_die Leiter_in der Einrichtung sind zu beteiligen.

§ 7
Betrieb von IT-Verfahren

(1) Voraussetzung für die Inbetriebnahme von IT-Verfahren an der Universität Leipzig ist, dass davon keine, nach dem Stand der Technik vermeidbaren Gefährdungen für die Informations- und Kommunikationsinfrastruktur ausgehen. Wenn die Risiken für die Informationssicherheit nicht durch angemessene Maßnahmen beherrscht werden können, ist auf den Einsatz informationstechnischer Systeme zu verzichten.

(2) Für jedes IT-Verfahren ist ein_e Verfahrensverantwortliche_r zu benennen. Der_Die IT-Verfahrensverantwortliche ist verpflichtet, den_die ISB an wesentlichen Entscheidungen und Planungen mit grundsätzlichen Bezug zur Informationssicherheit zu beteiligen. Er_Sie ist verantwortlich für die fortlaufende Umsetzung von Sicherungsmaßnahmen seines_ihres Verfahrens.

(3) Für jedes IT-Verfahren ist eine Verfahrensdokumentation zu erstellen. Der Inhalt und Umfang der Dokumentation ist abhängig von der Art der im IT-Verfahren erfassten Geschäftsprozesse, der eingesetzten IT-Systeme und der damit verarbeiteten Informationen. Zu den unverzichtbaren Bestandteilen der IT-Verfahrensdokumentation gehören:

- Beschreibung des IT-Verfahrens
  Darin enthalten sind Begründung, Zweck und Zielsetzung des IT-Verfahrens. Ebenso sind die Arbeitsabläufe und die betroffenen Einrichtungen der Universität Leipzig aufzuführen.
- Umsetzungskonzept
  Darin enthalten sind Angaben über Anzahl und Art der technischen Einrichtungen und IT-Systeme sowie Angaben zu Schnittstellen mit anderen IT-Verfahren und Diensten.
- Betriebs- und Sicherheitskonzept
  Wesentliche Bestandteile sind die Schutzbedarfsanalyse, bei erhöhtem Schutzbedarf eine Risikoanalyse, die Beschreibung der getroffenen Sicherheitsmaßnahmen und alle für den Betrieb notwendigen Angaben über die im Umsetzungskonzept enthaltenen technischen Systeme.

(4) Beim Betrieb von IT-Systemen in Forschungsprojekten und für IT-Systeme mit kurzer Betriebsdauer (weniger als zwölf Monate) besteht keine Pflicht zur ausführlichen Verfahrensbeschreibung. Es muss dennoch die Sicherheit der eingesetzten IT-Systeme sowie der zugrundeliegenden Infrastruktur gewährleistet werden.

(5) Werden in dem IT-Verfahren personenbezogene Daten verarbeitet, ist der_die IT-Verfahrensverantwortliche verpflichtet, den_die Datenschutzbeauftragte_n zu beteiligen. Weitere Rechte und Pflichten sind in einer Ordnung zum Datenschutz geregelt. Ausnahmen nach Absatz 4 sind in diesen Fällen nicht statthaft.

(6) Werden Daten an staatliche Stellen des Freistaates übermittelt sind die Bestimmungen in § 11 des SächsISichG zu beachten.

§ 8
Ressourcenabsicherung

(1) Informationssicherheit ist integraler und untrennbarer Bestandteil jeder Ablauforganisation, jedes IT-Verfahrens und jedes Projektes. Die personellen und finanziellen Ressourcen für angemessene Maßnahmen zur Gewährleistung der Informationssicherheit sind durch die Verantwortlichen nach § 4 Absatz 5 mit zu planen.

(2) Die personellen und finanziellen Ressourcen aller hochschulweiten, zentralen Maßnahmen zur Informationssicherheit werden aus zentralen Ansätzen finanziert.

§ 9
Inkrafttreten und Überprüfung

Die Ordnung zur Informationssicherheit wurde am 19. Dezember 2019 vom Rektorat und am 21. Januar 2020 vom Senat beschlossen und tritt mit der Veröffentlichung in den Amtlichen Bekanntmachungen der Universität Leipzig in Kraft. Sie soll alle zwei Jahre überprüft und gegebenenfalls angepasst werden.

Leipzig, den 6. März 2020

Prof. Dr. med. Beate Schücking
Rektorin

Anhang / Glossar / Definitionen

Audit
Unter einem Audit versteht man ein systematisches Untersuchungsverfahren, mit dem überprüft wird, dass Richtlinien und Sicherheitsmaßnahmen, z.B. bei einem IT-Verfahren, umgesetzt und eingehalten werden.

Beauftragte_r für Informationssicherheit / Informationssicherheitsbeauftragte_r (ISB)
Der_Die ISB ist verantwortlich für die Entwicklung des Regelwerks der Informationssicherheit, dessen Veröffentlichung und Fortschreibung und die Sicherstellung, dass dieses in den Fakultäten und Einrichtungen der Universität Leipzig umgesetzt wird. Der_Die ISB wird unterstützt durch das ISMT und die dezentralen Ansprechpersonen für Informationssicherheit. Darüber hinaus berät er_sie die Fakultäten und Einrichtungen der Universität Leipzig und führt Schulungs- und Sensibilisierungsmaßnahmen durch.

Chief Information Office (CIO)
Das CIO Gremium ist als beauftragtes Organ des Rektorats verantwortlich für die zentralen Steuerungsaufgaben des Informationsmanagements und verfügt zu diesem Zweck über ein eigenes Budget. Seine Aufgaben, Kompetenzen und Zuständigkeiten regelt eine Geschäftsordnung. Änderungen an der IT-Strategie beschließt das Rektorat auf Antrag des CIO und nach Stellungnahme durch den Senat.

Datenschutz
Datenschutz regelt die Verarbeitung personenbezogener Daten, um das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht). Die datenschutzkonforme Informationsverarbeitung ist in einer Ordnung zum Datenschutz geregelt.

Datenschutzbeauftragte
Der_Die Datenschutzbeauftragte überwacht an der Universität Leipzig die Einhaltung datenschutzrechtlicher Bestimmungen, die in der EU-Datenschutzgrundverordnung geregelt sind. Eine wesentliche Aufgabe ist die Kontrolle und Überwachung der ordnungsgemäßen Anwendung von IT-Verfahren, mit denen personenbezogene Daten verarbeitet werden.

Dezentrale Ansprechpersonen für Informationssicherheit
Die **dezentralen Ansprechpersonen** einer Fakultät oder Einrichtung der Universität Leipzig sind für die Umsetzung der Vorgaben zur Informationssicherheit in ihrer Organisationseinheit verantwortlich. Sie arbeiten in sicherheitsrelevanten Fragestellungen eng mit dem_der ISB zusammen und werden durch ihn_sie unterstützt. Diese Ansprechpersonen sollten bestenfalls Kenntnisse zur IT und zum Stand der Informationssicherheit, mindestens jedoch einen organisatorischen Überblick zu Strukturen und weiteren Ansprechpersonen ihrer Fakultät oder Einrichtung haben. Die dezentralen Ansprechpersonen für Informationssicherheit sollten von dem_der Leiter_in der jeweiligen Fakultät oder Einrichtung benannt werden.

Integrität
Integrität bezeichnet die Sicherstellung der Korrektheit von Informationen und der korrekten Funktionsweise von IT-Systemen. Integrität ist gewährleistet, wenn IT-Systeme und die durch sie verarbeiteten Informationen nicht unbefugt bzw. unzulässig verändert werden können.

Informationssicherheit
Als Informationssicherheit bezeichnet man Eigenschaften von technischen oder nicht-technischen informationsverarbeitenden Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient zur Einhaltung rechtlicher Rahmenbedingungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.

InformationsSicherheitsManagementSystem (ISMS)
Das Managementsystem für Informationssicherheit ist eine Aufstellung von Prozessen und Regeln der Universität Leipzig, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Informationsverbund
Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei die gesamte Universität Leipzig, einzelne organisatorische Strukturen oder ein oder mehrere IT-Verfahren umfassen.

IT-Beauftragte_r
Der_Die IT-Beauftragte ist für die inhaltliche und strategische Planung des IT-Einsatzes in einem Fachbereich oder einer Einrichtung verantwortlich. Er_Sie stellt sicher, dass eine permanente bedarfsorientierte Versorgung mit IT-Dienstleistungen sichergestellt wird. Darüber hinaus ist der_die IT-Beauftragte

für die Umsetzung der im IT-Sicherheitskonzept formulierten Anforderungen verantwortlich. Er_Sie sollte sich dazu mit der Ansprechperson für Informationssicherheit seiner_ihrer Einrichtung abstimmen.

IT-Verfahren
Ein IT-Verfahren besteht aus einem oder mehreren IT-gestützten Arbeitsprozessen, die eine arbeitsorganisatorisch abgeschlossene Einheit mit einem gemeinsamen Ziel bilden. Hierzu zählen beispielsweise die Studierenden- oder Prüfungsverwaltung, eine Haushaltsmittelbewirtschaftung oder sonstige IT-Fachverfahren. Ein einzelner Arbeitsplatzrechner stellt kein IT-Verfahren dar.
Die Einführung von IT-Verfahren oder deren Veränderung ist fast immer mitbestimmungspflichtig, da sich häufig auch die Arbeitsprozesse der Beschäftigten verändern. Werden in einem IT-Verfahren personenbezogene Daten verarbeitet, muss der Datenschutzbeauftragte vor dem erstmaligen Einsatz des IT-Verfahrens nach dem Sächsischen DSG prüfen, ob die Datenverarbeitung zulässig ist und die vorgesehenen Sicherheitsmaßnahmen nach ausreichend sind (Vorabkontrolle).

IT-Verfahrensverantwortliche
Der_Die IT-Verfahrensverantwortliche trägt die Gesamtverantwortung für ein IT-Verfahren und ist für den korrekten Ablauf verantwortlich. Er_Sie ist der_die Besitzer_in (Informationseigner_in) der in dem IT-Verfahren verarbeiteten Informationen und bestimmt deren Schutzbedarf.

Informationssicherheitsmanagement-Team (ISMT)
Das Informationssicherheitsmanagement-Team berät und unterstützt den_die ISB bei der Umsetzung und Steuerung der Informationssicherheitsprozesse. Dem ISMT fällt keine operative Kompetenz zu. Das ISMT besteht aus Mitgliedern der Universität Leipzig. Den Vorsitz führt der_die ISB.

Informationssicherheitsprozess
Der Informationssicherheitsprozess ist eine zentrale Komponente des ISMS und wird in die folgenden Phasen (PDCA-Zyklus) unterteilt:

Planung und Konzeption (Plan)
Diese Phase beinhaltet die Aufnahme des Ist-Zustands, die Definition von Anforderungen, die Durchführung einer Schutzbedarfsanalyse und ggf. einer Risikoanalyse. Auf Grundlage der Resultate ist eine angemessene Schutzstrategie festzulegen, die in einem Sicherheitskonzept dokumentiert wird.

Umsetzung (Do)
Die im Sicherheitskonzept beschriebenen Sicherheitsmaßnahmen sind anschließend umzusetzen. Die Steuerung und Kontrolle der Umsetzung angemessen zu dokumentieren.

Erfolgskontrolle und Überwachung (Check)
Zur Aufrechterhaltung der Informationssicherheit muss regelmäßig überprüft werden, ob die Sicherheitsmaßnahmen korrekt angewendet, eingehalten werden und wirksam sind. Darüber hinaus müssen Sicherheitsvorfälle rechtzeitig entdeckt und schnell und angemessen auf diese reagiert werden. Dies ist durch geeignete Überwachungsmaßnahmen und Audits sicherzustellen.

Optimierung und Verbesserung (Act)
Das Rektorat der Universität Leipzig und die IT-Verantwortlichen müssen regelmäßig und in angemessener Form über die Ergebnisse von Audits und über den aktuellen Status des Sicherheitsprozesses informiert werden, um die Steuerungsaufgaben wahrnehmen und Verbesserungen durchzuführen zu können.

Personenbezogene Daten
Der Begriff wird im Sächsischen Datenschutzgesetz definiert und bezieht sich auf alle Daten bzw. Informationen, die einer natürlichen Person zugeordnet werden können.

Prozessverantwortliche_r
Die Prozessverantwortlichen tragen die Gesamtverantwortung für die Informationsverarbeitung innerhalb der Ablauforganisation ihrer Geschäftsprozesse. Sie stimmen sich mit den IT-Verfahrensverantwortlichen der in ihren Geschäftsprozessen verwendeten IT-Verfahren über den Schutzbedarf der verarbeiteten Daten und die Umsetzung von Sicherheitsmaßnahmen ab.

Revision
Eine Revision ist ähnlich wie ein Audit eine regelmäßige Überprüfung von Maßnahmen auf ihre Angemessenheit und Wirksamkeit, die beispielsweise zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit umgesetzt worden sind.

Risikoanalyse
Eine Risikoanalyse wird allgemein zur Identifikation und Bewertung von Risiken eingesetzt, damit mögliche negative Ereignisse mit Präventionsmaßnahmen vermieden, reduziert oder verlagert werden können. Das Restrisiko muss durch den_die IT-Verfahrensverantwortliche_n getragen werden.
Bei quantitativen Risikoanalysen wird dabei das Risiko, dem ein Objekt ausgesetzt ist, in Abhängigkeit von der Eintrittswahrscheinlichkeit eines Schadensereignisses und der möglichen Schadenshöhe definiert.

Schutzbedarf
Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Der tatsächliche Schutzbedarf von Daten

wird durch eine Schutzbedarfsfeststellung ermittelt. Abhängig von dem Ergebnis müssen entsprechende Sicherheitsmaßnahmen ergriffen werden, um die Informationen angemessen zu schützen.

Schutzbedarfsfeststellung
Bei der Schutzbedarfsfeststellung wird für jeden Geschäftsprozess bzw. IT-Verfahren und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der Grundwerte der Informationssicherheit - Vertraulichkeit, Integrität oder Verfügbarkeit - entstehen können. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch". Bei einem hohen oder sehr hohen Schutzbedarf wird ergänzend eine Risikoanalyse durchgeführt.

Sicherheitsmaßnahme
Eine Sicherheitsmaßnahme schützt ein Objekt, wenn es durch eine Bedrohung einer Gefährdung ausgesetzt ist. Im Kontext Informationssicherheit sind dies Gefährdungen hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Es wird üblicherweise zwischen organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsmaßnahmen unterschieden.

Sicherheitskonzept
Sicherheitskonzepte sind zentrale Dokumente im Informationssicherheitsprozess und enthalten die Herleitung der Sicherheitsstrategie und beschreiben die geplante Vorgehensweise, um die gesetzten Sicherheitsziele für ein oder mehrere IT-Verfahren zu erreichen.
Aufbauend auf den Anforderungen, den Ergebnissen der Analyse, der Schutzbedarfsfeststellung und ggf. einer Risikoanalyse, werden die erforderlichen Sicherheitsmaßnahmen identifiziert und im Sicherheitskonzept dokumentiert.

Transparenz
Im Kontext Informationsverarbeitung ist Transparenz gegeben, wenn ein IT-Verfahren für die jeweils Beteiligten in zumutbarer Zeit mit zumutbarem Aufwand nachvollziehbar ist. Dies setzt eine aktuelle und angemessene Dokumentation voraus.
Für Betroffene muss die Verarbeitung ihrer persönlichen Daten vollständig nachvollziehbar sein, d.h. er soll wissen, welche Daten zu welchem Zweck bei welcher Stelle für wie lange und aus welchem Grund gespeichert werden. Entsprechende Rechte und Pflichten sind in der Datenschutzgrundverordnung (DSGVO) geregelt.

Verfahrensverzeichnis
Der Begriff Verfahrensverzeichnis stammt aus dem Datenschutz und beschreibt unter anderem die Dokumentation der im Rahmen eines IT-Verfahrens verarbeiteten personenbezogene Daten.

Verfügbarkeit
Verfügbarkeit ist gewährleistet, wenn IT-Verfahren, ihre Komponenten und die damit verarbeiteten Informationen zu jedem Zeitpunkt wie vorgesehen genutzt werden können.

Vertrauliche Daten
Vertrauliche Daten sind Informationen, die nicht für die Öffentlichkeit, sondern ausschließlich für einen eingeschränkten Personenkreis bestimmt sind. Beispiele sind Personaldaten, Finanzdaten, allgemein Daten mit Personenbezug (personenbezogene Daten) und Forschungsdaten die nicht bzw. noch nicht publiziert worden sind.

Vertraulichkeit
Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertraulichkeit ist gewährleistet, wenn Informationen ausschließlich durch die dafür autorisierten Personen eingesehen bzw. abgerufen werden können.