Leitlinie zur Informationssicherheit an der Carl von Ossietzky Universität Oldenburg

vom 28.05.2019

Das Präsidium der Carl von Ossietzky Universität Oldenburg hat am 21.05.2019 gemäß § 37 Absatz 1 Satz 3 NHG in Verbindung mit Artikel 4 Nummer 7 und Artikel 24 Absatz 1 der Europäischen Datenschutzgrundverordnung (EU-DSGVO) die nachfolgende Leitlinie zur Informationssicherheit an der Universität beschlossen.

Inhaltsverzeichnis

I
Präambel

Die Carl von Ossietzky Universität Oldenburg verarbeitet eine Vielzahl von Informationen, um ihre Aufgaben (vgl. § 3 Abs. 1 Niedersächsisches Hochschulgesetz (NHG)), insbesondere in Forschung, Lehre, Studium sowie Weiterbildung und den damit verbundenen Verwaltungs- und Unterstützungsaufgaben, zu erfüllen und die hierfür erforderlichen Kern- und Unterstützungsprozesse effizient zu gestalten. Dabei verarbeitet sie auch Informationen, die vor der unberechtigten Kenntnisnahme durch Dritte und vor Verlust oder unautorisierter Veränderung besonders zu schützen sind.

Zudem sind Maßnahmen zur Gewährleistung der Sicherheit von Informationen nicht nur gesetzlich vorgeschrieben, sondern auch Teil der Verpflichtungen der Universität gegenüber ihren Mitgliedern und Angehörigen, Gästen sowie Kooperations- und Vertragspartnern.

Das Präsidium der Carl von Ossietzky Universität Oldenburg bekennt sich daher zur Gewährleistung der Informationssicherheit als Managementaufgabe und setzt sich das strategische Ziel, dieser Verantwortung insbesondere durch die Einführung und den Betrieb eines strukturierten Informationssicherheitsmanagementsystems (ISMS) nachzukommen.

II.
Anwendungsbereich

(1) Informationssicherheit bezeichnet einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen auf ein akzeptierbares Maß reduziert sind. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Informationen auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten und Informationen.

(2) Die Regelungen dieser Leitlinie zur Informationssicherheit sind bindend für alle Einrichtungen und Organisationseinheiten der Universität sowie für alle Mitglieder, Angehörige und Gäste der Universität (im Folgenden auch als Nutzerin bzw. Nutzer bezeichnet).

(3) Die Regelungen beziehen sich auf alle informationsverarbeitenden Prozesse. Neben den Schwerpunkten Informations- und Kommunikationstechnologie (digitale Datenverarbeitung) sind auch klassische analoge Informationsträger wie beispielsweise Akten eingeschlossen.

(4) Alle Regelungen sind soweit anwendbar und rechtlich zulässig auch bei Kooperationen, Auftragsverarbeitung und sonstiger Beteiligung Dritter zu berücksichtigen. In der Regel sind in diesen Fällen entsprechende Vereinbarungen zu treffen, die ein angemessenes Sicherheitsniveau gewährleisten.

III.
Sicherheitsziele

(1) Aufgaben der Universität nach § 3 Abs. 1 NHG, insbesondere in Forschung, Lehre, Studium und Weiterbildung, stellen im Rahmen dieser Leitlinie zur Informationssicherheit Kernprozesse der Universität dar.

(2) Diese Kernprozesse werden durch strategische Prozesse (Steuerungsprozesse) gesteuert und durch Prozesse im Personalmanagement, im Finanzmanagement, im Studierendenmanagement, im Gebäudemanagement, im IT-Servicemanagement sowie durch allgemeine administrative und andere Services unterstützt (Unterstützungsprozesse).

(3) Alle diese Geschäftsprozesse (Kern-, Steuerungs- und Unterstützungsprozesse) erfordern für ihren effizienten Ablauf Informationen, Verfahren und Systeme. Deren **Verfügbarkeit**, **Integrität** und **Vertraulichkeit** müssen stets auf dem jeweils erforderlichen und nachfolgend konkretisierten Niveau liegen, um die Kernprozesse vor Störungen und Ausfällen und damit die Universität vor materiellen sowie immateriellen Schäden zu bewahren.

(4) Die Rahmenbedingungen und Kernziele der Informationssicherheit der Universität werden daher wie folgt zusammengefasst:

a. Die Informationssicherheit wird durch den Aufbau und den Betrieb eines strukturierenden ISMS sichergestellt

b. Die **Verfügbarkeit** der Informationen und IT-Systeme der Universität wird auf ein so hohes Niveau gebracht und gehalten, dass die noch verbleibenden Ausfallzeiten toleriert werden können. Für alle IT-Verfahren oder Kategorien von Verfahren sind die Zeiten, in denen sie verfügbar sein sollen, festzulegen.

c. Informationen sind gegen unbeabsichtigte Veränderungen und vorsätzliche Verfälschung zu schützen. Die **Integrität** der Daten, also ihre Vollständigkeit und Korrektheit, wird dadurch sichergestellt. Fehlfunktionen und Unregelmäßigkeiten in Daten, Anwendungen und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel.

d. Die Anforderungen an **Vertraulichkeit** liegen auf einem Niveau, das sich an den einschlägigen rechtlichen Bestimmungen sowie an dem jeweils festzulegenden Schutzbedarf orientiert. Der physische und logische Zugang zu Informationen wird ausschließlich den Zugriffsberechtigten in zulässiger Weise gewährt. Jede Nutzerin bzw. jeder Nutzer erhält eine Zugriffsberechtigung nur auf die Informationen, die er zur Erfüllung seiner Aufgaben benötigt.

e. Alle Nutzerinnen und Nutzer der Universität sind gehalten, die einschlägigen Gesetze sowie Regelungen zur Informationssicherheit und Datenschutz, sonstige rechtliche Bestimmungen und vertraglichen Regelungen einzuhalten und werden hierauf hingewiesen und verpflichtet.

f. Schadensfälle mit hohen finanziellen Auswirkungen oder negativen Folgen für die Reputation der Universität müssen verhindert werden.

IV.
Informationssicherheitsmanagement, Rollen und Verantwortlichkeiten

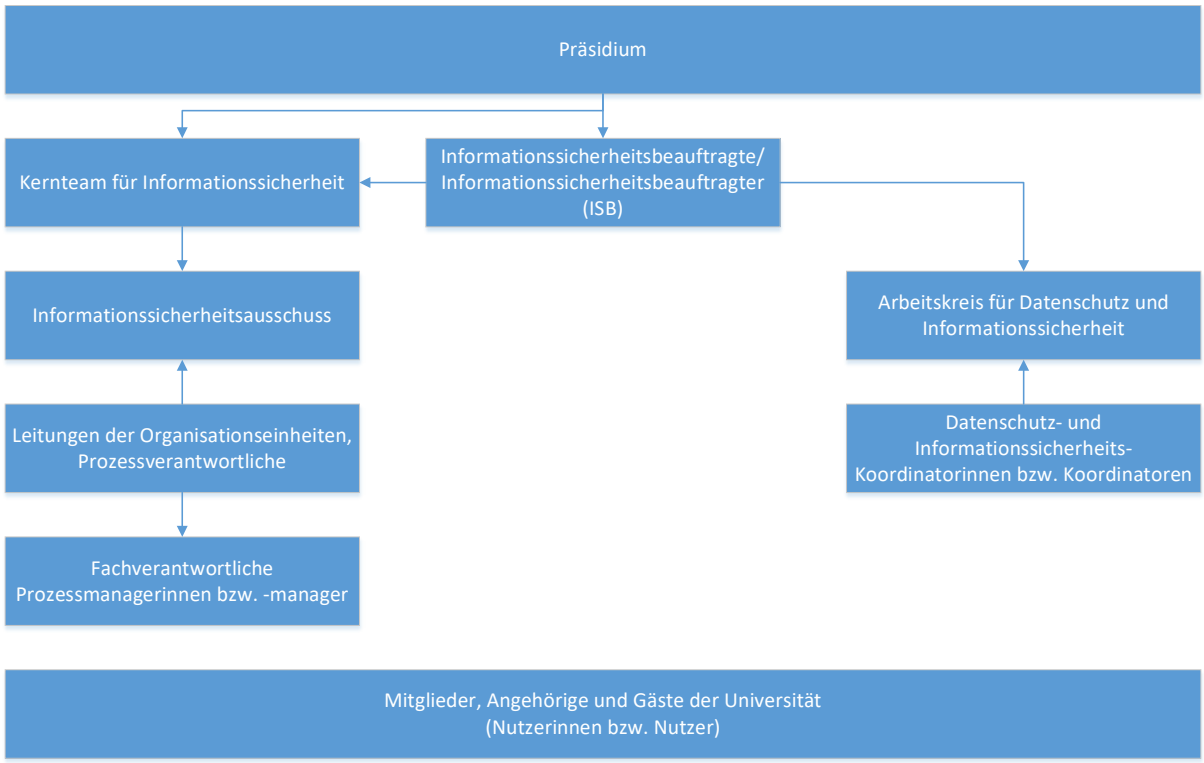

Abbildung: Organisation des Informationssicherheitsmanagements

(1) Die Verantwortung für die rechtskonforme und ordnungsgemäße Aufgabenerfüllung der Universität und damit auch für die Informationssicherheit insgesamt trägt das **Präsidium** der Universität. Um dieser Verantwortung gerecht zu werden benennt das Präsidium **eine Informationssicherheitsbeauftragte bzw. einen Informationssicherheitsbeauftragten** (siehe Absatz 2), richtet **ein Kernteam für die Informationssicherheit** (siehe Absatz 3) ein und beteiligt alle Organisationseinheiten (insbesondere

auch die Fakultäten) in angemessener Weise im Rahmen eines **Informationssicherheitsausschusses** (siehe Absatz 4) und eines **Arbeitskreises für Datenschutz- und Informationssicherheit** (siehe Absatz 5). Bei Bedarf kann das Präsidium dauerhaft oder befristet weitere Arbeits- oder Projektgruppen einrichten.

(2) Die **Informationssicherheitsbeauftragte** bzw. der **Informationssicherheitsbeauftragte (ISB)** ist in der Ausübung direkt der bzw. dem Vizepräsidenten für Verwaltung und Finanzen, unterstellt. Sie bzw. er vertritt in Fragen der Informationssicherheit die Belange des Präsidiums und kann in diesem Zusammenhang bzgl. Prozessen, die in der direkten Verantwortung des Präsidiums liegen, bei dringendem, kurzfristigen Bedarf auch fachliche Weisungen erteilen. Sie bzw. er hat insbesondere die folgenden Aufgaben:

a. Überwachung und Kontrolle der Umsetzung dieser Leitlinie

b. Verantwortlichkeit für den Aufbau und Betrieb eines ISMS

c. Weiterentwicklung der Sicherheitsziele und -strategien sowie dieser Leitlinie

d. Unterstützung bei der ressortübergreifenden Erstellung und Entwicklung von Sicherheitsmaßnahmen und –strategien

e. Mitwirkung bei der Erarbeitung von Vorgaben für organisatorische Maßnahmen zur Informationssicherheit sowie für Hard- und Software, die der Gewährleistung oder Verbesserung der IT-Sicherheit von zentral betriebenen Querschnittsverfahren dienen, wie beispielsweise Firewall-Lösungen, Virenschutzsoftware, Verschlüsselungssoftware oder VPN-Lösungen

f. Überprüfung der Eignung, Funktion und Wirksamkeit der technischen und organisatorischen Maßnahmen zur Informationssicherheit und der in den IT-Systemrichtlinien vorgesehenen Sicherheitsmaßnahmen

g. Erstellung der jährlichen Informationssicherheitsberichte und Umsetzungspläne zur Informationssicherheit

h. Konzeption und der Ausführung von Schulungs- und Sensibilisierungsprogrammen

i. Erster Ansprechpartner für die Meldung von schwerwiegenden Vorfällen/Verstößen und unverzügliche Information des Kernteams

j. Untersuchung von Sicherheitsvorfällen

k. Ansprechpartner in Fragen der Informationssicherheit

l. Organisation der Sitzungen des Kernteams sowie des Arbeitskreises für Datenschutz und Informationssicherheit

(3) Das **Kernteam für Informationssicherheit** berät sich in regelmäßigen Abständen sowie bei akutem Bedarf und setzt sich grundsätzlich aus folgenden Mitgliedern zusammen:

- Vizepräsidentin bzw. Vizepräsident für Verwaltung und Finanzen oder deren bzw. dessen Vertretung

- Ggf. die mit der Rolle einer bzw. eines Chief Information Officer (CIO) betraute Person

- Informationssicherheitsbeauftragte bzw. Informationssicherheitsbeauftragter

- Leitung der IT-Dienste oder deren Vertretung

- Leitung des Gebäudemanagements (Dezernat 4) oder deren Vertretung

- Leitung des Organisationsmanagements (Dezernat 1) oder deren Vertretung

- Datenschutzbeauftragte bzw. Datenschutzbeauftragter

- Referentin bzw. Referent für Datenschutzmanagement

Das Kernteam für Informationssicherheit kann zu den Sitzungen weitere Funktionsträgerinnen bzw. Funktionsträger oder andere Personen als Gäste hinzuziehen soweit dies im Einzelfall erforderlich ist.

Das Kernteam für Informationssicherheit hat die folgenden Aufgaben:

a. Unterstützung der bzw. des ISB bei wesentlichen Fragen zum Aufbau und Betrieb des ISMS

b. Beratung von Änderungen dieser Leitlinie sowie weiterer Richtlinien und Regelungen zur Informationssicherheit bevor diese dem Präsidium zum Beschluss vorgeschlagen werden

c. Abstimmung zum Vorgehen bei akuten und schwerwiegenden Vorfällen bzw. Verstößen bezüglich der Informationssicherheit sowie Vorbereitung entsprechender Empfehlungen an das Präsidium

d. Information und Beratung des Präsidiums und des Informationssicherheitsausschusses

Die Sitzungen des Kernteams werden grundsätzlich durch die Vizepräsidentin bzw. den Vizepräsidenten für Verwaltung und Finanzen geleitet, welcher bzw. welchem im Rahmen ihrer bzw. seiner Verantwortung auch die Letztentscheidungsbefugnis obliegt.

(4) Der **Informationssicherheitsausschuss** wird in regelmäßigen Abständen (mindestens eine Sitzung pro Semester) sowie bei Bedarf durch die Vizepräsidentin bzw. den Vizepräsidenten für Verwaltung und Finanzen einberufen und setzt sich aus folgenden Mitgliedern zusammen:

- Mitglieder des Kernteams für Informationssicherheit

- Dezernatsleitungen, Referatsleitungen sowie Leitungen der Stabsstellen oder deren jeweilige benannte Vertretungen

- jeweils eine von der Fakultät benannte und bevollmächtige Vertretung je Fakultät

- einer Vertretung des Personalrats

- einer Vertretung der Studierendenschaft

- der Gleichstellungsbeauftragten

Es können weitere Funktionsträgerinnen bzw. Funktionsträger oder andere Personen als Gäste in den Informationssicherheitsausschuss hinzugezogen werden, soweit dies im Einzelfall erforderlich ist.

Die Sitzungen des Informationssicherheitsausschusses werden durch die Vizepräsidentin bzw. den Vizepräsidenten für Verwaltung und Finanzen geleitet.

Der ISB und die weiteren Mitglieder des Kernteams für Informationssicherheit informieren den Informationssicherheitsausschuss über wichtige Vorgänge und Planungen bzgl. der Informationssicherheit.

Der Informationssicherheitsausschuss hat ausschließlich beratende Funktion sowie die wichtige Aufgabe relevante Informationen in die jeweiligen Organisationseinheiten weiterzugeben. Empfehlungen des Informationssicherheitsausschusses sollen vom Kernteam für Informationssicherheit aufgenommen und nach Möglichkeit berücksichtigt werden.

(5) In, vor allem größeren, Organisationseinheiten werden von den jeweiligen Leitungen **Datenschutz- und Informationssicherheits-Koordinatoren** benannt. Sie haben für Ihren Wirkungsbereich die folgenden Aufgaben:

a. Förderung der Sensibilisierung für Datenschutz und Informationssicherheit

b. Erhebung des spezifischen Schulungsbedarfs

c. Meldung von sicherheitsrelevanten Ereignissen an den ISB

d. Mitwirkung bei der Erstellung und Pflege von Sicherheitskonzepten

e. Prüfung der Wirksamkeit der eingesetzten Sicherheitsmaßnahmen

f. Bildung eines Informations- und Wissensforums zum Thema Datenschutz und Informationssicherheit

Die Datenschutz- und Informationssicherheits-Koordinatoren treffen sich regelmäßig, (mindestens eine Sitzung pro Semester) im **Arbeitskreis für Datenschutz und Informationssicherheit**, der durch die bzw. den ISB und die Datenschutzmanagerin bzw. den Datenschutzmanager organisiert wird. Die Treffen des Arbeitskreises sollen vor allem dem fachlichen Austausch untereinander und als Schnittstelle des zentralen Informationssicherheitsmanagements und Datenschutzmanagements in die Organisationseinheiten dienen.

(6) Für alle Geschäftsprozesse sind die **Prozessverantwortlichen** bzw. die Leitungen der Organisationseinheiten verantwortlich. Sofern die Aufgaben nicht selbst wahrgenommen werden, ist jeweils eine **fachverantwortliche Prozessmanagerin bzw. ein fachverantwortlicher Prozessmanager** zu benennen. Prozessmanager haben die folgenden Aufgaben:

a. Festlegung der verarbeiteten Informationen und deren Schutzbedarf

b. Definition von Verantwortlichkeiten im Rahmen der Datenverarbeitung

c. Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz der im Verantwortungsbereich befindlichen Informationen implementieren bzw. entsprechende Anforderungen kommunizieren

d. Ggf. Durchführung einer Risikoanalyse

Für die Umsetzung dieser Aufgaben steht den Prozessmanagern die bzw. der Informationssicherheitsbeauftragte und ggf. die bzw. der für den Bereich zuständigen Datenschutz- und Informationssicherheits-Koordinatorin bzw. Koordinator beratend zur Seite.

(7) Alle **Mitglieder und Angehörige sowie Gäste der Universität (Nutzerinnen bzw. Nutzer universitärer Infrastruktur)**, insbesondere **Leitungen von Organisationseinheiten**, gewährleisten die Informationssicherheit durch verantwortungsbewusstes Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Sie gehen korrekt und verantwortungsvoll mit den von ihnen genutzten IT-Systemen, Daten und Informationen um. Insbesondere die Leitungen von Organisationseinheiten und die Beschäftigten sind angehalten, mögliche Verbesserungen oder Schwachstellen über die jeweiligen Prozessverantwortlichen, die bzw. den fachverantwortliche/n Prozessmanagerin bzw. Prozessmanager oder andere definierte Ansprechpersonen weiterzugeben. Sicherheitsvorfälle bzw. Sicherheitsverstöße mit schwerwiegender Verletzung der Verfügbarkeit, Vertraulichkeit oder Integrität der Informationen sind unverzüglich an die Informationssicherheitsbeauftragte bzw. den Informationssicherheitsbeauftragten zu melden.

V.
Sicherheitsstrategie

(1) Das Präsidium der Universität und alle ihre Mitglieder, Angehörige und Gäste sind sich ihrer Verantwortung beim Umgang mit der Informationshaltung, Informationsweitergabe und Informationstechnik bewusst und unterstützen die Sicherheitsziele und -strategien hinsichtlich der Informationssicherheit nach besten Kräften.

(2) Zu treffende Sicherheitsmaßnahmen sollen sich grundsätzlich am Stand der Technik orientieren und müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen.

(3) Die Informationssicherheit an der Universität soll durch den Aufbau und Betrieb eines ISMS, welches sich grundsätzlich an Vorgaben einschlägiger Normen (insbesondere ISO/IEC 27001 und BSI IT-Grundschutz) orientieren soll, gewährleistet werden.

(4) Die Sicherheitsstrategie basiert auf folgenden grundsätzlichen Prinzipien und Rahmenbedingungen:

a. Personenbezogene, passwortgesicherte Zugänge zu allen Systemen und Daten Verwendung sicherer Authentifizierungsverfahren und Beschränkung der Zugriffsrechte auf die zur Aufgabenerfüllung notwendigen Rechte (**Minimalprinzip**)

b. **Prävention** von sowie kontrollierter Umgang mit sicherheitsrelevanten Ereignissen und Vorkommnissen

c. Regelmäßige **Überprüfung** der Sicherheitsleit- und Richtlinien sowie deren Umsetzung durch interne und unabhängige, externe Auditierung

d. Schutzbedarfsorientierte **Segmentierung** des Netzes

e. **Redundante, hochverfügbare Systeme** in allen kritischen Bereichen

f. Regelmäßige **Datensicherung**, **Passwortschutz** für Sicherungsmedien und Aufbewahrung von Sicherungsmedien an getrennten Orten

g. **Sichere Aufbewahrung** und **sensibler Umgang** mit vertraulichen und personenbezogenen Informationen und deren Weitergabe durch entsprechende Sicherungsmaßnahmen

h. **Verschlüsselte Datenübertragung** und Datenspeicherung vertraulicher und personenbezogener Informationen soweit erforderlich

i. **Schulung und Sensibilisierung**

j. **Vertraulichkeits- und Verpflichtungserklärung** aller Beschäftigten - insbesondere in Bezug auf personenbezogene Daten

(5) Diese Leitlinie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Informationssicherheitskonzepte, detaillierter Regelungen und Dienstanweisungen zur Informationssicherheit.

(6) Der Informationssicherheitsprozess ist regelmäßig auf seine Aktualität und Wirksamkeit zu überprüfen. Darüber hinaus sind die getroffenen Maßnahmen regelmäßig daraufhin zu untersuchen, ob sie den betroffenen Nutzerinnen und Nutzern bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

(7) Die Leitungsebenen unterstützen die ständige Verbesserung des Sicherheitsniveaus.

VI.
Inkrafttreten

Diese Leitlinie tritt am Tage nach der Veröffentlichung in den Amtlichen Mitteilungen der Carl von Ossietzky Universität Oldenburg in Kraft.