Grundsätze für die Informationssicherheit an der Universität Heidelberg (Informationssicherheitsleitlinie)

Inhaltsverzeichnis

Präambel

Die Digitalisierung durchdringt sämtliche Prozesse der Universität Heidelberg im Bereich von Forschung, Lehre, Verwaltung sowie Innovation und Transfer. Die Mitglieder und Angehörigen der Universität Heidelberg sind auf zuverlässig funktionierende IT-Dienste angewiesen. Diese sind eine conditio sine qua non zur Gewährleistung sowie zur Effizienzsteigerung von Arbeitsabläufen gemäß den rechtlich geltenden Rahmenbedingungen. Entsprechend ist die Universität auf eine hochqualitative, funktionsfähige und sichere Informationstechnologie (IT) angewiesen, die im Hinblick auf ihre Verfügbarkeit, Vertraulichkeit und Integrität durch geeignete Sicherheitsmaßnahmen geschützt wird.
Die vorliegende Leitlinie erörtert durch die Definition von Zielen und Rahmenbedingungen das Selbstverständnis der Universität Heidelberg bezüglich der Informationssicherheit. Ein Hauptanliegen dabei ist es, die Handlungsfähigkeit der Forschung, Lehre, Verwaltung und des Transfers mit hohen Sicherheitsstandards bereitzustellen.

§ 1 Geltungsbereich

Diese Leitlinie ist für alle Mitglieder, Angehörige und Organisationseinheiten der Universität Heidelberg verbindlich. Darüber hinaus gilt sie für alle externen Nutzer:innen der IT-Infrastruktur und der IT-Dienste der Universität Heidelberg.

§ 2 Allgemeine Grundsätze und Ziele der Informationssicherheit an der Universität Heidelberg

(1) Ein angemessenes Sicherheitsniveau – der aktuellen Technik entsprechend – soll an der an der Universität Heidelberg angestrebt und umgesetzt werden. Dabei werden insbesondere die Grundschutzstandards des BSI (Bundesamt für Sicherheit in der Informationstechnik) sowie die internationalen Normen DIN ISO/IEC 27001 ff. als Grundlage verwendet. Insbesondere für Bereiche, in denen ein höherer Schutzbedarf festgestellt wird (z.B. wegen der Verarbeitung von sensiblen Daten), müssen ggf. ergänzende Sicherheitsmaßnahmen eingeführt und dokumentiert werden.

(2) Die Informationssicherheit ist kein Selbstzweck und muss neben den Sicherheitsstandards auch Informationsoffenheit, Kosten und Nutzerakzeptanz berücksichtigen.

(3) Die Universität und alle ihre Organisationseinheiten schützen ihre verarbeiteten Informationen durch die Sicherung der Grundwerte der Informationssicherheit. Die Grundwerte der Informationssicherheit sind:

Verfügbarkeit: Die Gewährleistung, dass Daten, Informationen, IT-Systeme und Anwendungen für Berechtigte im vorgesehenen Umfang und in angemessener Zeit nutzbar sind.

Vertraulichkeit: Die Gewährleistung, dass Daten und Informationen ausschließlich Befugten zugänglich sind.

Integrität: Die Gewährleistung, dass Unverfälschtheit und Vollständigkeit von Daten, Informationen, IT-Systemen und Anwendungen gegeben sind.

(4) Informationssicherheit wird als strategische Aufgabe begriffen, und Maßnahmen zu ihrer Gewährleistung werden durch das Rektorat unterstützt.

(5) Die Informationssicherheitsleitlinie wird regelmäßig, mindestens jedoch einmal pro Jahr auf ihre Aktualität, Wirksamkeit und Angemessenheit hin überprüft und bei Bedarf weiterentwickelt.

(6) Informationssicherheit kann nur erreicht werden, wenn universitätsweit gültige Sicherheitsstandards definiert werden und diese ggf. gestuft auf Ebene von Arbeitsgruppen, Instituten, Fakultäten erfolgreich umgesetzt werden.

(7) Ein angemessenes Sicherheitsniveau kann nur dann erreicht werden, wenn das IT-Fachpersonal die nötige Kompetenz besitzt. Detaillierte Risikoanalysen zur Erkennung und Abwehr von Sicherheitslücken erfordern qualifiziertes Personal mit hohem Expertenwissen und detaillierten IT-Kenntnissen. Entsprechende Schulungen und Zertifizierungen sollen hierfür regelmäßig wahrgenommen werden. Weiterhin werden IT-nutzende Beschäftigte regelmäßig informiert und sensibilisiert, sodass in der Breite ein Grundverständnis für die Belange der Informationssicherheit gewährleistet werden kann; hinzu kommen aufgabenspezifische Schulungen.

(8) Informationssicherheit umfasst nicht nur die Verhinderung von inneren und äußeren Angriffen auf die Universität, sondern auch die Verhinderung von Angriffen, die aus der Universität auf externe Institutionen ausgehen.

(9) Informationssicherheitsvorfälle werden in dem vom Universitätsrechenzentrum betriebenen ISMS (Informationssicherheits-Managementsystem) dokumentiert und regelmäßig an den CIO kommuniziert.

(10) Das Vorgehen bei IT-Notfällen wird in Notfallmanagement-Plänen, die das Zusammenwirken mit den zuständigen Behörden (u.a. Polizei, MWK, CSBW, BSI) abbilden, konkretisiert.

(11) In Kooperationen mit Dritten wird die Umsetzung des Informationssicherheits-Managements in erforderlichem Maß durch Vereinbarungen geregelt.

§ 3 Verantwortlichkeiten

(1) Das Rektorat und der Senat beschließen die Informationssicherheitsleitlinie, die die Hauptziele und die Verantwortungsstrukturen der Universität festlegt.

(2) Die Gestaltung und Koordinierung der Informationssicherheitsprozesse an der Universität Heidelberg liegen in der Verantwortung des CIO (Chief Information Officer). In dieser Funktion berichtet der CIO regelmäßig an das Rektorat. Weiterhin fungiert der CIO als Schnittstelle zu den Aktivitäten des Kernteams Informationssicherheit auf Landesebene sowie zu weiteren CERTs (Computer Emergency Response Teams) auf Bundesebene. Auf Basis der vom CIO festgelegten strategischen Ausrichtung koordiniert der CISO (Chief Information Security Officer) die operative Umsetzung der notwendigen Maßnahmen. Allgemein werden die entsprechenden Sicherheitsmaßnahmen im Rahmen von festgelegten Sicherheitsrichtlinien (s. § 4) definiert.

(3) Die Leitung der jeweiligen Organisationseinheit trägt die Verantwortung für die Organisation der Informationssicherheit im jeweiligen Bereich.

(4) Jedes Mitglied der Universität ist für die Einhaltung eines angemessenen Sicherheitsniveaus im Bereich der eigenen IT-Nutzung, auch unter Berücksichtigung der geltenden Informationssicherheitsrichtlinien, verantwortlich und unterstützt die Erfüllung der in §2 genannten Grundsätze und Ziele.

§ 4 Erörterung des Prozesses zur Bereitstellung von Richtlinien

Die Bereitstellung von Informationssicherheitsrichtlinien setzt voraus, dass eine regelmäßige und grundlegende Überprüfung des Sicherheitsstatus und des Schutzbedarfs bezüglich der IT der Universität erfolgt. Dazu sollen regelmäßig eine Bestandsaufnahme und Strukturanalyse der IT-Prozesse, IT-Geräte, Software, Anwendungen und Daten erfolgen. Daraus resultiert eine Zuordnung der IT-gestützten Prozesse und Informationen in eine der folgenden Schutzbedarfskategorien.

- **Schutzbedarf Niedrig bis Mittel**
  Der Schaden wirkt sich in geringem bis mittlerem Maße auf die Handlungsfähigkeit der Universität aus und ist auf einzelne Personengruppen beschränkt.
- **Schutzbedarf Hoch**
  Der Schaden wirkt sich in beträchtlichem Maße aus und kann mehrere Organisationseinheiten der Universität umfassen.
- **Schutzbedarf Sehr hoch**
  Der Schaden wirkt sich in höchstem Maße aus und kritische Prozesse werden so beeinträchtigt, dass die Universität teilweise oder als ganze nicht mehr handlungsfähig ist.

Im Falle von universitären IT-Bestandteilen und -Bereichen, die der obenstehenden Einteilung zufolge in die Bereiche "Schutzbedarf Hoch" oder "Schutzbedarf Sehr hoch" fallen, muss zudem eine Risikoanalyse vorgenommen werden. Die aus dieser Analyse resultierenden Ergebnisse werden in Zusammenarbeit mit den jeweiligen IT-Nutzer:innen und den jeweiligen Leitungsebenen der betroffenen Einrichtungen und Organisationseinheiten abgestimmt.
Auf Basis der gewonnenen Erkenntnisse sollen Sicherheitsrichtlinien seitens des Universitätsrechenzentrums abgeleitet und definiert werden. Diese sollen die Konkretisierung der Maßnahmen beinhalten, die zur Erfüllung der in den Leitlinien definierten Ziele beitragen. Bei der Definition der Sicherheitsrichtlinien wird zwischen proaktiven (vorsorglichen) und reaktiven (nach Eintreten eines Vorfalls) Richtlinien unterschieden.