Philipps Universität Marburg

Informationssicherheitsleitlinie der Philipps-Universität

Inhaltsverzeichnis

Präambel

In der Universität besteht ein hoher Anspruch an die Qualität der Informationstechnologie (IT). Die Mitglieder und Angehörigen[1] der Philipps-Universität sind auf eine fehlerfrei funktionierende IT angewiesen. Das gilt für nahezu alle Anwendungen in der Forschung, dem Studium und der Lehre sowie in der Verwaltung der Philipps-Universität. Eine sichere IT trägt entscheidend dazu bei, dass alle Mitglieder der Philipps-Universität Informationen effizient, fehlerfrei und gemäß den geltenden rechtlichen Rahmenbedingungen austauschen und verarbeiten können. Um dies zu gewährleisten, müssen Informationen im Hinblick auf ihre Verfügbarkeit, Vertraulichkeit und Integrität durch geeignete Sicherheitsmaßnahmen geschützt werden. Dabei soll die Informationssicherheit das Kernprinzip jedes bestehenden und neu entwickelten Dienstes sein. Die vorliegende Leitlinie verdeutlicht durch Ziele und Rahmenbedingungen das Selbstverständnis aller Mitglieder der Philipps-Universität im Hinblick auf Informationssicherheit und sichert die Handlungsfähigkeit von Forschung und Lehre.

§ 1 Geltungsbereich

(1) Die Leitlinie ist für alle Mitglieder der Philipps-Universität verbindlich.

§ 2 Allgemeine Sicherheitsziele und Begriffsbestimmungen

(1) Die Philipps-Universität und all ihre Organisationseinheiten stellen die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen sicher. In Abwägung der Chancen für die Universität, der Werte der zu schützenden Informationen, der dafür bestehenden Risiken sowie des Aufwands an Personal- und Sachmitteln für Informationssicherheit, strebt die Universität hierfür ein angemessenes Sicherheitsniveau an. Informationssicherheit ist eine Momentaufnahme, in der die Risiken, die beim IT-Einsatz aufgrund von Bedrohungen und Schwachstellen für die Vertraulichkeit, die Integrität und die Verfügbarkeit von Daten und IT vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. Die Grundwerte der Informationssicherheit sind:

Verfügbarkeit: Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Nutzern stets wie vorgesehen genutzt werden können.

[1] Im Folgenden Mitglieder genannt. Gemeint sind hiermit diverse, weibliche und männliche Personen.

Integrität: Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Vertraulichkeit: Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.[2]

§ 3 Wesentliche Ziele zur Gewährleistung der Informationssicherheit

(1) Die Mitglieder der Philipps-Universität Universität kennen die für ihre IT-Nutzung relevanten rechtlichen Vorgaben und vertragliche Regelungen zur Informationssicherheit und halten sie ein.

(2) Die IT der Philipps-Universität wird durch koordinierte Maßnahmen widerstandsfähiger gegen Bedrohungen wie Cyberangriffe, Systemausfälle oder Datenverluste gemacht.

(3) Es gibt eine geordnete Vorgehensweise für die Inbetriebnahme und die Änderung von IT-Verfahren. Dabei werden die Belange der Informationssicherheit im erforderlichen Umfang berücksichtigt.

(4) IT-Systeme werden in einer angemessen sicheren Weise und Umgebung betrieben, so dass die Schutzziele der IT-gestützten Geschäftsprozesse nicht gefährdet ist. Hierzu wird die Administration der IT-Systeme nachvollziehbar gestaltet und Software zeitnah auf einem aktuellen Versionsstand gehalten. Hierfür tolerieren die Mitglieder der Philipps-Universität kurzfristige Einschränkungen bei den IT-Diensten (bspw. bei Sicherheitsupdates).

(5) Die Stabsstelle Informationssicherheit bietet regelmäßig anlassbezogene Schulungen zu verschiedenen Themen der Informationssicherheit für die Mitglieder der Philipps-Universität an.

(6) Informationen werden bezüglich ihres Schutzbedarfes im Hinblick auf Verfügbarkeit, Integrität und Vertraulichkeit bewertet. Sicherheitsmaßnahmen für Systeme und Verfahren richten sich nach der Höhe des Schutzbedarfes und werden beispielsweise in Sicherheitskonzepten dokumentiert. Sicherheitskonzepte werden der oder dem Informationssicherheitsbeauftragten vorgelegt.

(7) Das Vorgehen bei IT-Notfällen wird in Notfallmanagementplänen konkretisiert.

(8) Durch regelmäßige Revisionen werden die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen überprüft und dokumentiert. Abweichungen werden mit dem Ziel analysiert, das Sicherheitsniveau kontinuierlich zu verbessern[3] und ständig auf dem aktuellen Stand zu halten.

(9) Das Informationssicherheitsmanagement der Philipps-Universität wird in Anlehnung an gängige Standards zum Informationssicherheitsmanagement organisiert.

(10) In Kooperationen mit Dritten wird die Umsetzung des Informationssicherheitsmanagements in erforderlichem Maß durch Vereinbarungen geregelt.

---

[2] Die Definitionen von Verfügbarkeit, Integrität und Vertraulichkeit wurden aus dem Glossar des IT-Grundschutz-Kompendiums des Bundesamtes für Sicherheit in der Informationstechnik entnommen (vgl. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html).

[3] Nach dem sog. PDCA-Modell: Plan – Do – Check – Act

§ 4 Verantwortlichkeiten

(1) Das Präsidium hat die Aufgabe, ein angemessenes Sicherheitsniveau für die Philipps-Universität zu gewährleisten. Dafür trägt das Präsidium die Gesamtverantwortung. Das Präsidium benennt eine/n Informationssicherheitsbeauftragte/n und weist die Zuständigkeit für das Informationssicherheitsmanagement in seinem Geschäftsverteilungsplan aus. Um seiner Verantwortung für ein angemessenes Informationssicherheitsniveau gerecht zu werden, führt das Präsidium der Universität ein organisationsweites Informationssicherheitsmanagementsystem ein und entwickelt dieses kontinuierlich weiter. Das Informationssicherheitsmanagementsystem dient zur Planung, Lenkung und Kontrolle des Prozesses zur Herstellung von Informationssicherheit.

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

(3) Jedes Mitglied der Philipps-Universität ist für die Einhaltung eines angemessenen Sicherheitsniveaus im Bereich der eigenen IT-Nutzung verantwortlich und unterstützt die Erfüllung der in §2 und §3 genannten Ziele und Prinzipien.

§ 5 Organisationsstruktur

(1) Informationssicherheitsmanagement-Team

(a) Um der Verantwortung für Informationssicherheit gerecht zu werden, richtet das Präsidium als zentrales Organ ein Informationssicherheitsmanagement-Team der Universität ein. Es ist für das Informationssicherheitsmanagement sowie den Aufbau und die Weiterentwicklung eines Informationssicherheitsmanagementsystems verantwortlich.

(b) Dem Informationssicherheitsmanagement-Team gehören an:

das für das Informationssicherheitsmanagement zuständige Präsidiumsmitglied,

das Präsidiumsmitglied für Informationsmanagement,

die Kanzlerin oder der Kanzler,

die oder der Informationssicherheitsbeauftragte,

die oder der behördliche Datenschutzbeauftragte,

die Leiterin oder der Leiter des HRZ.

Anlassbezogen kann das Informationssicherheitsmanagement-Team um weitere nicht-ständige Mitglieder ergänzt werden.

(c) Das Präsidiumsmitglied, in dessen Verantwortlichkeit die Informationssicherheit nach dem jeweils geltenden Geschäftsverteilungsplan des Präsidiums fällt, leitet das Informationssicherheitsmanagement-Team.

(d) Das Informationssicherheitsmanagement-Team unterstützt das Präsidium bei IT-bezogenen strategischen und taktischen Entscheidungen, sodass das für Informationsmanagement zuständige Präsidiumsmitglied taktische Vorgaben beschließen kann.

(2) Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter

(a) Die oder der Informationssicherheitsbeauftragte ist unmittelbar dem für Informationssicherheit zuständigen Präsidiumsmitglied unterstellt. Organisatorisch bildet sie oder er mit weiteren Mitarbeiterinnen und Mitarbeitern die Stabsstelle Informationssicherheit.

(b) Die IT-Administrierenden der zentralen und dezentralen IT-Systeme der Universität unterstützen die oder den Informationssicherheitsbeauftragte/n. Der oder die Informationssicherheitsbeauftragte hat ein Recht auf Auskunft sowie Einsichtnahme in informationssicherheitsrelevante Informationen.

(c) Die oder der Informationssicherheitsbeauftragte berät das Informationssicherheitsmanagement-Team in Fragen des Informationssicherheitsmanagements und setzt die strategischen Vorgaben des Informationssicherheitsmanagement-Teams um.

(3) Ansprechperson zur dezentralen Informationssicherheitskoordination

(a) Die Fachbereiche stellen eine Ansprechperson zur Verfügung, die sich um die dezentrale Veranlassung von Informationssicherheitsmaßnahmen kümmert. Die Ansprechperson ist zu dokumentieren und der oder dem Informationssicherheitsbeauftragen mitzuteilen.

(b) Die Ansprechperson zur dezentralen Informationssicherheitskoordination unterstützen die oder den Informationssicherheitsbeauftragten. Der oder die Informationssicherheitsbeauftragte hat ein Recht auf Auskunft sowie Einsichtnahme in informationssicherheitsrelevante Informationen.

(4) Leitungen der Einrichtungen und Bereiche

(a) Die Fachbereiche, die Einrichtungen und die Universitätsverwaltung haben die Aufgabe ein angemessenes Informationssicherheitsniveau zu gewährleisten. Dafür tragen die Leitungen der Einrichtungen und Bereiche (z. B. Dekaninnen und Dekane) die Verantwortung in ihrem Zuständigkeitsbereich im Rahmen der Festlegungen des Präsidiums und der einschlägigen Richtlinien.

(b) Die Ansprechpersonen zur dezentralen Informationssicherheitskoordination unterstützen die Leitungen der Einrichtungen und Bereiche.

(5) Hochschulrechenzentrum (HRZ)

(a) Das HRZ hat eine besondere Verantwortung im Bereich der IT-Sicherheit, da es die Grundversorgung mit Einrichtungen zur Kommunikation und zur Informationsverarbeitung, beispielsweise dem universitären Datennetz oder der TK-Anlage, betreibt.

(b) Das HRZ unterstützt die Mitarbeiter der Stabsstelle Informationssicherheit bei der Beratung der Fachbereiche, der Einrichtungen und der Universitätsverwaltung sowie die Fachverfahrensverantwortlichen bei der Begutachtung von Informationssicherheitsrisiken und der Umsetzung von Maßnahmen zur Reduktion von Informationssicherheitsrisiken.

§ 6 Vorgehensweise zum Umgang mit Sicherheitsvorfällen

(1) Sicherheitsvorfälle werden in geeigneter Form der oder dem Informationssicherheitsbeauftragten gemeldet und dokumentiert, sodass zeitnah angemessen reagiert werden kann. Die Stabsstelle Informationssicherheit leitet in Zusammenarbeit mit dem HRZ und wenn nötig den Ansprechpersonen zur dezentralen Informationssicherheitskoordination geeignete Maßnahmen zur Abwehr der Gefährdungen ein, koordiniert diese, prüft sie auf ihre Wirksamkeit, informiert erforderlichenfalls die zuständigen Stellen und dokumentiert den Vorfall. Die oder der Informationssicherheitsbeauftragte informiert das Präsidium und die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten unverzüglich über größere Sicherheitsvorfälle.

§ 7 Regelwerke

(1) Diese Leitlinie zur Informationssicherheit wird durch weitere Richtlinien ergänzt und präzisiert. Das Präsidium beschließt diese Richtlinien auf Empfehlung des Informationssicherheitsmanagement-Teams und nach Erörterung durch die Universitätskonferenz sowie den IT-Beirat. Zentrale untergeordnete Richtlinien zur Informationssicherheitsleitlinie sind:

Richtlinie zum Informationssicherheitsmanagement inklusive einer Struktur der Sicherheitsorganisation sowie allgemeinen Richtlinien für Informationssicherheit,

Richtlinie zum IT-Betrieb mit verbindlichen Vorgaben und Hinweisen zur Erstellung von Sicherheitskonzepten für alle Betreiber von Informationstechnik.

§ 8 Inkrafttreten

Die Informationssicherheitsleitline tritt nach ihrer Bekanntmachung in den Amtlichen Mitteilungen in Kraft und ersetzt die die IT-Sicherheitsrichtlinie der Philipps-Universität Marburg vom 24.04.2012. Sie wird spätestens fünf Jahre nach Inkrafttreten evaluiert.