Amtliches Mitteilungsblatt

Der Vizepräsident für Forschung

Leitlinie
zur Informationssicherheit an der Humboldt-Universität zu Berlin

Herausgeber:	Die Präsidentin der Humboldt-Universität zu Berlin Unter den Linden 6, 10099 Berlin	**Nr. 61/2020**
Satz und Vertrieb:	Abteilung Kommunikation, Marketing und Veranstaltungsmanagement	**29. Jahrgang/30. November 2020**

Leitlinie
zur Informationssicherheit an der Humboldt-Universität zu Berlin

Präambel

Der Universitätsbetrieb erfordert in hohem Maß die abgestimmte Integration von Verfahren und Abläufen, die sich auf die Möglichkeiten der Informationstechnologie (IT) stützen. Funktionierende und sichere IT-Prozesse sind eine zentrale Grundlage für die Leistungsfähigkeit der Humboldt-Universität zu Berlin (HU) in Forschung, Studium, Lehre und Verwaltung. Hieraus erwächst ein hoher Anspruch an die Verfügbarkeit, die Vertraulichkeit und die Integrität der verarbeiteten Informationen, IT-Verfahren und IT-Systeme. Diese Leitlinie zur Informationssicherheit beschreibt die Rahmenbedingungen, um diesen hohen Anspruch an die Informationssicherheit zu erreichen.

1 Geltungsbereich

Diese Leitlinie zur Informationssicherheit an der HU gilt für

- Einrichtungen der HU (Fakultäten, Institute, Verwaltungen, sonstige Einrichtungen),
- Mitarbeiterinnen und Mitarbeiter sowie Gäste der HU,
- Studierende der HU,
- Dritte, die IT-Verfahren, IT-Dienste oder sonstige informationsverarbeitende Verfahren der HU benutzen.

2 Stellenwert

Informationssicherheit ist nicht nur eine Frage der Technik, sondern hängt maßgeblich von den organisatorischen und personellen Rahmenbedingungen ab. Ein funktionierender Betrieb der HU in Forschung, Lehre, Studium und Verwaltung ist ohne IT nicht denkbar. Die Informationssicherheit nimmt daher in Zeiten der fortschreitenden Durchdringung von Prozessen durch IT, der zunehmenden Vernetzung sowie der steigenden Bedrohung durch Angriffe einen immer höheren Stellenwert ein. Die Universitätsleitung erkennt die Informationssicherheit als Schlüsselfaktor für die Aufrechterhaltung eines erfolgreichen Universitätsbetriebes und sichert die dafür nötigen und angemessenen Ressourcen zu.
Aus den Anforderungen, die sich hieraus ergeben, sowie den einzuhaltenden gesetzlichen, regulatorischen und vertraglichen Verpflichtungen leiten sich die Sicherheitsziele hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit der eingesetzten informationsverarbeitenden Systeme und Prozesse ab.

Als Risiko wird die Eintrittswahrscheinlichkeit eines Schadens aufgrund einer Gefährdung verstanden. Entsprechend sollen alle Risiken für die Informationssicherheit erkannt und geeignet behandelt werden, z.B. durch Sicherheitsmaßnahmen (um zu vermeiden bzw. zu reduzieren), durch Akzeptieren oder durch Transferieren der Risiken.
Alle Sicherheitsmaßnahmen müssen angemessen sein und in einem finanziell vertretbaren Verhältnis zum Wert der schützenswerten Informationen, der informationsverarbeitenden Systeme und Prozesse stehen. Ereignisse mit negativen finanziellen, aber auch immateriellen Auswirkungen durch unzureichende Informationssicherheit müssen verhindert werden.

3 Ziele

Ziele der Informationssicherheit sind der angemessene Schutz von Informationen hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität zur Bewahrung der verfassungsmäßigen Ordnung, zum Schutz des informationellen Selbstbestimmungsrechts und die Gewährleistung der Ordnungsmäßigkeit der dienstlichen oder studentischen Tätigkeiten, unabhängig davon, ob Informationen mit oder ohne Unterstützung von IT verarbeitet werden.
Folgende Ziele liegen dieser Leitlinie zur Informationssicherheit zu Grunde:

- Die Verfügbarkeit der IT, die für die ordnungsgemäße Durchführung insbesondere von Forschung, Lehre, Studium und Verwaltung erforderlich ist, ist gewährleistet.
- Bei der Verarbeitung von Informationen werden die Grundanforderungen der Informationssicherheit eingehalten. Entsprechend ihres Schutzbedarfs werden Informationen angemessen und sicher verarbeitet und adäquat vor unberechtigten Zugriffen geschützt.
- Die vorrangigen Kriterien für geeignete Sicherheitsmaßnahmen sind deren Wirksamkeit im Hinblick auf das zu tragende Restrisiko und die wirtschaftliche Angemessenheit.
- Es gibt eine geordnete Vorgehensweise für die Inbetriebnahme und die Änderung von IT-Verfahren. In diesem werden die Belange der Informationssicherheit in angemessenem Umfang berücksichtigt.

- Alle Nutzenden haben ein Grundverständnis für Belange der Informationssicherheit und sind zu einem zweckmäßigen und verantwortungsvollen Umgang mit der IT angehalten.
- IT-Systeme werden durch Personal betreut, welches über die erforderliche Fachkunde verfügt.
- Das Angebot regelmäßiger und anlassbezogener Schulungen ist Bestandteil eines geordneten Informationssicherheitsprozesses.
- Die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen wird regelmäßig überprüft und dokumentiert.
- Verletzungen der Informationssicherheit werden kommuniziert und dokumentiert, so dass schnell, angemessen und nachhaltig auf sie reagiert werden kann.

4 Informationssicherheitsmanagement

Grundlage des Managements der Informationssicherheit an der HU sind die Standards 200-1 „Managementsysteme für Informationssicherheit (ISMS)" und 200-2 „IT-Grundschutz-Methodik" des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Hier werden die Verfahren zum Planen, Implementieren, Betreiben und Aufrechterhalten eines Systems zum Informationssicherheitsmanagement definiert.
Die Zuständigkeiten und Verantwortlichkeiten im Informationssicherheitsmanagement an der HU sind wie folgt festgelegt:

- Die Präsidentin/der Präsident trägt die Gesamtverantwortung für Informationssicherheit an der HU.
- Das oberste Gremium für Belange der IT und der Informationssicherheit ist die Lenkungsgruppe Informationsprozesse (LGI).
- Die/der Informationssicherheitsbeauftragte (ISB) der HU wird von der Präsidentin/dem Präsidenten der HU bestellt. Sie/er ist einrichtungsübergreifend in Fragen der Informationssicherheit zuständig.
- Die/der IT-Sicherheitsbeauftragte (IT-SiBe) der HU wird von der Präsidentin/dem Präsidenten der HU bestellt. Sie/er ist am CMS angesiedelt und für alle Belange der IT-Sicherheit insbesondere im Zusammenhang mit den vom CMS betriebenen Verfahren zuständig. Sie/er arbeitet eng mit der/dem Informationssicherheitsbeauftragten der HU zusammen und wird durch sie/ihn unterstützt.
- Die Verantwortlichkeiten der/des behDSB der HU ergibt sich aus deren/dessen rechtlicher Zuständigkeit.
- Die Verantwortlichkeiten der Personalvertretungen der HU ergeben sich aus deren rechtlicher Zuständigkeit.
- Weitere Zuständigkeiten und Verantwortlichkeiten sind in der „Satzung zur IT-Organisation der Humboldt-Universität zu Berlin" geregelt.

5 Inkrafttreten und Aktualisierung

Das IT-Board erarbeitet unter Beteiligung der AG Informationssicherheit (und evtl. anderer Gremien) Entwürfe für neue Versionen der Leitlinie zur Informationssicherheit (IS-Leitlinie). Die Lenkungsgruppe Informationsprozesse (LGI) ist das CIO-Gremium und beschließt die IS-Leitlinie auf Basis dieser Entwürfe. Bei bedeutenden Veränderungen des ISMS ist die IS-Leitlinie anzupassen. Spätestens nach zwei Jahren sollen eine Überprüfung und ggf. eine Anpassung bzw. Fortschreibung erfolgen.

Die IS-Leitlinie tritt mit ihrer Veröffentlichung im *Amtlichen Mitteilungsblatt der Humboldt-Universität zu Berlin* in Kraft.