HCU | HafenCity Universität Hamburg

HochschulAnzeiger

Nr. 04/2018 vom 22. Juni 2018

Herausgeber: Präsidium
Redaktion: Präsidium

Bekanntmachung gemäß § 108 Absatz 5 Satz 2 des Hamburgischen Hochschulgesetzes (HmbHG) vom 18. Juli 2001 (HmbGVBl., S. 171), in der jeweils geltenden Fassung.

Im Hochschulanzeiger der HafenCity Universität Hamburg, dem hochschulinternen Verkündungsblatt, werden Satzungen, Ordnungen und Richtlinien sowie andere Mitteilungen der Hochschule, die nicht im Amtlichen Anzeiger der Freien und Hansestadt Hamburg gemäß § 108 Abs. 5 Satz 1 HmbHG veröffentlicht werden müssen, in geeigneter Weise bekannt gegeben.

Der Hochschulanzeiger wird ausschließlich auf der Internetseite der HCU Hamburg veröffentlicht.

Die in dieser Ausgabe veröffentlichten Satzungen, Ordnungen und Richtlinien sowie andere Mitteilungen der Hochschule, werden durch diesen Hochschulanzeiger bekannt gegeben und treten am Tag dessen Veröffentlichung in Kraft.

Eine Druckversion des Hochschulanzeigers steht im Präsidium der HCU Hamburg sowie in der Bibliothek der HCU zu Einsichtnahme zu Verfügung.

Inhaltsverzeichnis:

48 Informationssicherheits- und Datenschutzleitlinie der HafenCity Universität Hamburg (HCU) vom 24. Mai 2018

Informationssicherheits- und Datenschutzleitlinie der HafenCity Universität Hamburg (HCU) Vom 24. Mai 2018

Beschlossen durch das Präsidium der HCU am 24. Mai. 2018.

Inhalt:

Präambel
§ 1 Geltungsbereich
§ 2 Ziele
§ 3 Verantwortung
§ 4 Aufgaben der bzw. des Informationssicherheitsbeauftragten (InSiBe)
§ 5 Aufgaben der bzw. des Datenschutzbeauftragten (DSB)
§ 6 Ansprechpartnerin bzw. Ansprechpartner für Informationssicherheit (AIS) bei eigenständigen Organisationseinheiten
§ 7 Gefahrenintervention
§ 8 Verstöße gegen die Informationssicherheits- und Datenschutzleitlinie
§ 9 Schlussbemerkung
§ 10 Inkrafttreten

Präambel

Die Informationstechnik hat sich zu einem der wichtigsten Arbeitsmittel für eine moderne Universität entwickelt. Dabei sind die Möglichkeiten, die eine Vernetzung der Computer untereinander bieten, unverzichtbar geworden. Ohne diese Techniken wäre der Auftrag zur Forschung und Lehre für die HCU kaum erfüllbar. Leider haben zahlreiche Vorfälle weltweit gezeigt, dass vernetzte Computersysteme sowohl von innen als auch von außen generell angreifbar sind und kompromittiert werden können.

Ein solcher Sicherheitsvorfall

- kann zu hohen Kosten bei der Beseitigung von Schäden führen, weil dadurch die Betroffenen an ihren eigentlichen Aufgaben gehindert und personelle Ressourcen gebunden werden,
- beeinträchtigt oder verhindert unter Umständen die bestimmungsgemäße Nutzung,
- erhöht möglicherweise die Kosten für den Betrieb des Universitätsnetzwerkes und der Anbindung an das Internet,
- verletzt eventuell die Vertraulichkeit von Informationen und personenbezogenen Daten, die nicht für Dritte bestimmt sind,
- kann gegen geltendes Recht verstoßen und
- schädigt gegebenenfalls das Ansehen der HCU in der Öffentlichkeit.

Ziel muss es deshalb sein, Missbrauch und Gefahren einzudämmen, damit die Vertraulichkeit und Integrität der Daten und die aufgabengemäße Verfügbarkeit der IT-Systeme gewährleistet sind. IT-Sicherheit ist hierbei jedoch nur ein Teilbereich der Aufgaben eines weitergehenden Informationssicherheits- und Datenschutzmanagements. Informationssicherheit und Datenschutz umfassen im Allgemeinen eine Vielzahl von Aspekten, neben technischen und infrastrukturellen Rahmenbedingungen vor allem auch organisatorische Maßnahmen und Regelungen. Dies kann im Einzelfall eine Einschränkung für die Bedienbarkeit und Funktionalität bedeuten, so dass zwischen den verschiedenen Interessen abgewogen werden muss. Die Kompromisse, die dabei einzugehen sind, müssen von jeder Nutzerin bzw. jedem Nutzer der HCU-Infrastruktur akzeptiert und mitgetragen werden. Dies gilt auch für Gäste, die nur vorübergehend an der HCU anwesend sind.

§ 1
Geltungsbereich

Diese Leitlinie gilt für alle angegliederten, sowie eigenständigen Organisationseinheiten, die zur HCU gehören oder in deren Netzinfrastruktur integriert sind. Betroffen sind sowohl digitale Informationen sowie die Geräte, mit denen Informationen (inklusive personenbezogener Daten) verarbeitet werden, als auch analoge Medien (zum Beispiel Ausdrucke), die ebenfalls schützenswerte Informationen enthalten können.

§ 2
Ziele

Aus den allgemein anzustrebenden Schutzzielen der Informationssicherheit und den geltenden Datenschutzgesetzen werden die folgenden Ziele für die HCU abgeleitet:

1. Aufbau und Pflege eines Informationssicherheits- und Datenschutzmanagementsystems;
2. Schutz der Verfügbarkeit von IT-Systemen, Diensten und Daten;
3. Sicherstellung der Vertraulichkeit bei der Verarbeitung von Informationen und Daten;
4. Schutz der Integrität der IT-Systeme, Dienste und Daten;
5. Schutz vor unberechtigtem Zugriff auf Daten und Systeme;
6. Sensibilisierung der Hochschulangehörigen für einen sicheren Umgang mit IT;
7. Aufbau eines Notfallmanagements;
8. Ermittlung von Sicherheitsrisiken mit anschließender Definition von geeigneten Gegenmaßnahmen;
9. Einhaltung der einschlägigen Gesetze und sonstigen rechtlichen Bestimmungen zur Wahrung der Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter sowie der Studierenden, sowie weiterer Angehöriger der Universität.

Um dies zu erreichen, werden technische und organisatorische Maßnahmen ergriffen, die dem jeweiligen Schutzbedarf der Informationen angemessen sind.

§ 3
Verantwortung

(1) Die Gesamtverantwortung für Informationssicherheit und Datenschutz liegt beim Präsidium der HCU, vertreten durch die Präsidentin bzw. den Präsidenten der HCU.

(2) Die bzw. der Informationssicherheitsbeauftragte (InSiBe) und die bzw. der Datenschutzbeauftragte (DSB) koordinieren, ggf. in Personalunion, die übergreifenden Informationssicherheits- und Datenschutzprozesse und beraten das Präsidium.

(3) Die Verantwortung, alle definierten Informationssicherheitsprozesse und -richtlinien in die Praxis umzusetzen, liegt bei der Leitung der einzelnen Organisationseinheiten (OE). Die dazugehörigen Aufgaben können an eine Ansprechpartnerin bzw. einen Ansprechpartner für Informationssicherheit (AIS) für die OE delegiert werden. Die Benennung einer bzw. eines AIS entlässt die Leitung der OE aber nicht aus ihrer Verantwortung für die Informationssicherheit und den Datenschutz in ihrem Bereich.

(4) Die AIS bzw. die OE-Leitung ist der Kontakt für die bzw. den InSiBe und DSB.

(5) Zentrale Infrastrukturkomponenten werden durch die HCU-Informationstechnik (HCU-IT) bereitgestellt und betrieben.

§ 4
Aufgaben der bzw. des Informationssicherheitsbeauftragten (InSiBe)

Die bzw. der InSiBe koordiniert den übergreifenden Informationssicherheitsprozess und unterstützt die AIS in ihrer Arbeit. Die Aufgaben der bzw. des InSiBe sind

1. Aufbau und Pflege eines Informationssicherheitsmanagementsystems,
2. die Analyse übergreifender, HCU-weiter Bedrohungen,
3. die Empfehlung und Ausarbeitung von übergreifenden, HCU-weiten Schutzmaßnahmen und Prozessen in Zusammenarbeit mit dem Präsidium und der HCU-IT,
4. die technische Umsetzung der übergreifenden Maßnahmen in Zusammenarbeit mit der HCU-IT,
5. die Beratung, Information und Weiterbildung der AIS,
6. Entwicklung von Sicherheitskonzepten für die HCU,
7. Begleitung bei Sicherheitsvorfällen, Weitermeldung etc.

§ 5
Aufgaben der bzw. des Datenschutzbeauftragten (DSB)

Die bzw. der DSB ist Ansprechpartnerin bzw. Ansprechpartner in allen Fragen des Datenschutzes an der HCU, egal ob diese bzw. dieser intern oder extern tätig ist. Die Aufgaben der bzw. des DSB sind:

1. Aufbau und Pflege eines Datenschutzmanagementsystems,
2. Beratung der datenverarbeitenden Stellen bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten,
3. Frühzeitige Mitwirkung bei der Erarbeitung interner Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten,
4. Überwachung der Einhaltung datenschutzrechtlicher Vorschriften,
5. alle betroffenen Personen über gültige Bestimmungen des Gesetzes sowie sonstige Vorschriften über den Datenschutz aufklären und schulen.

§ 6
Ansprechpartnerin bzw. Ansprechpartner für Informationssicherheit (AIS) bei eigenständigen Organisationseinheiten

Organisationseinheiten und Gremien, die nicht unmittelbar der Weisung des Präsidiums der HCU unterstellt sind, obwohl sie gänzlich oder zumindest teilweise in die Infrastruktur der HCU integriert und durch diese mit IT-Dienstleistungen versorgt sind, müssen einen AIS und mindestens eine Vertreterin bzw. einen Vertreter gegenüber der bzw. dem InSiBe benennen, die bzw. der die Bereiche innerhalb der HCU-Infrastruktur vertritt.

Sollte eine Zusammenarbeit mit den eigenständigen Organisationseinheiten bei Sicherheitsvorfällen nicht möglich sein und eine akute Gefährdung der Infrastruktur bestehen, so werden die Organisationseinheiten zum Schutz der übrigen Teilnehmenden temporär getrennt, bis die Probleme behoben oder ein Konsens mit dem Präsidium über die weitere Kooperation hergestellt wurde. Für die bzw. den AIS der eigenständigen Organisationseinheit gelten dieselben Aufgaben und Kompetenzen wie für die übrigen AIS.

§ 7
Gefahrenintervention

(1) Bei Gefahr im Verzuge veranlasst die bzw. der InSiBe oder die bzw. der AIS entsprechend des Zuständigkeitsbereichs die sofortige vorübergehende Stilllegung betroffener IT-Systeme seitens der HCU-IT, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden nicht anders abzuwenden ist. Die bzw. der InSiBe ist unverzüglich zu informieren.

(2) Soweit die HCU-IT Gefahr im Verzuge feststellt, kann sie Netzanschlüsse (ggf. auch ohne vorherige Benachrichtigung der Betroffenen) vorübergehend sperren, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden für die IT-Infrastruktur der HCU nicht anders abzuwenden ist. Die bzw. der InSiBe ist unverzüglich gegebenenfalls nachträglich zu informieren.

(3) Die Wiederinbetriebnahme erfolgt erst nach der Durchführung hinreichender Sicherheitsmaßnahmen in Abstimmung mit der bzw. dem InSiBe.

§ 8
Verstöße gegen die Informationssicherheits- und Datenschutzleitlinie

Als Verstöße werden folgende Handlungen verstanden:

1. die Planung, Beauftragung oder Durchführung von nicht erlaubten Aktivitäten, die zu einer Kompromittierung von IT-Systemen, Anwendungen oder Daten führen oder führen könnten,
2. der unberechtigte Zugriff auf Informationen und IT-Systeme und die unberechtigte Änderung, Nutzung und / oder Veröffentlichung von vertraulichen Informationen.

Verstöße gegen die Informationssicherheits- und Datenschutzleitlinie und die jeweils gültige Benutzerordnung können nach den geltenden Regelungen und gesetzlichen Bestimmungen geahndet werden.

§ 9
Schlussbemerkung

Sicherheitsmaßnahmen müssen im Rahmen eines kontinuierlichen Prozesses formuliert, kommuniziert, realisiert, überwacht und fortentwickelt werden. Letztendlich liegt dies immer in der Verantwortung des Präsidiums bzw. der Leitung der Organisationseinheit, auch wenn die faktische Zuarbeit durch die bzw. den InSiBe, die bzw. den DSB und die AIS erfolgt. Sofern einzelne Maßnahmen oder Regelungen einen gravierenden Einfluss auf die Arbeitsabläufe haben, sollten diese der Leitung zur abschließenden Entscheidung vorgelegt werden. Ausnahmen von solchen bindenden Maßnahmen und Regelungen bedürfen der schriftlichen Zustimmung.

§ 10
Inkrafttreten

Diese Informationssicherheits- und Datenschutzleitlinie tritt mit ihrer Bekanntmachung im Hochschulanzeiger in Kraft.

Hamburg, den 22. Juni 2018

HafenCity Universität Hamburg