IT-Ordnung der Humboldt-Universität zu Berlin

- Entwurf, 02.10.2013 -

Inhalt

Auf der Grundlage des § 2 Abs. 8 Satz 1 des Berliner Hochschulgesetzes (BerlHG) in der ab 02.06.2011 gültigen Fassung (GVBl. S. 378) sowie des § 5 Abs. 1 der Verfassung der Humboldt-Universität zu Berlin hat der Akademische Senat der Humboldt-Universität zu Berlin am XXXXXXXX die nachstehende IT-Ordnung der Humboldt-Universität zu Berlin beschlossen:

Präambel und Zielsetzungen

Der Universitätsbetrieb erfordert in hohem Maß die abgestimmte Integration von Verfahren und Abläufen, die sich auf die Möglichkeiten der Informationstechnologie (IT) stützen. Diese Ordnung dient dem Zweck, die Planung und den Betrieb von IT an der Humboldt-Universität zu Berlin (HU) grundlegend zu regeln. Das Ergreifen von Schutzmaßnahmen zur Sicherstellung aller IT-gestützten

Dienste und Verfahren hat dabei höchste Priorität und nimmt in dieser Ordnung eine zentrale Stelle ein.

§ 1 Gegenstand und Geltungsbereich

(1) Diese IT-Ordnung regelt die Zuständigkeiten, die Verantwortung, die Zuordnung von Aufgaben und Befugnissen sowie die Zusammenarbeit bezüglich der IT-Infrastruktur und der sie betreibenden Institutionen bzw. Personen der HU. Sie bestimmt den Umgang mit IT-Verfahren und IT-Systemen und soll den effizienten IT-Einsatz sowie die Sicherheit der IT-Infrastruktur, der IT-Prozesse und der zu verarbeitenden Daten bestmöglich fördern.

(2) Die IT-Ordnung ist verbindlich für alle Personen und Einrichtungen der HU mit Ausnahme der Charité. Sie umfasst die gesamte IT-Infrastruktur der HU einschließlich aller darin betriebener Hard- und Softwaresysteme.

§ 2 Grundsätze des IT-Betriebes und der IT-Benutzung an der HU

(1) Funktionierende und sichere IT-Prozesse sind eine zentrale Grundlage für die Leistungsfähigkeit der HU in Forschung, Studium, Lehre und Verwaltung.

(2) Der IT-Betrieb an der HU ordnet sich den gesetzlich festgelegten Aufgaben der Hochschulen sowie ihrem Mandat zur Wahrung der akademischen Freiheit unter.

(3) Die Einrichtungen der HU sind grundsätzlich für den Betrieb und die Benutzung ihrer eigenen IT-Infrastruktur zuständig.

(4) Der CMS ist der zentrale IT-Dienstleister der HU.

(5) IT-Sicherheit ist eine notwendige Voraussetzung für die Datensicherheit, d.h. den Schutz von Daten vor Vernichtung, Verfälschung oder Nichtverfügbarkeit.

(6) Datensicherheit ist eine notwendige Voraussetzung für den Datenschutz, den grundrechtlich garantierten Schutz personenbezogener Daten.

(7) Die IT-Sicherheitspolitik an der HU folgt dem Grundsatz, dass der Aufwand für die Schutzmaßnahmen stets in Relation zum erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter zu setzen ist.

(8) Die Benutzung von IT-Technik erfolgt ausschließlich unter Berücksichtigung der Wahrung der Rechte Dritter (z. B. Softwarelizenzen, Auflagen der Netzbetreiber, Datenschutzaspekte).

(9) Die Benutzung von IT-Technik verpflichtet die Betreiber sowie die Benutzerinnen und Benutzer zu korrektem Verhalten im Umgang mit dieser und zu ökonomischem und sparsamem Gebrauch der benutzten Ressourcen.

(10) Beim Einsatz von IT-Technik verpflichtet sich die HU zur sozialen Verantwortung, zur Verantwortung für die Umwelt und zum effizienten Gebrauch von Energie.

(11) Die Benutzung von IT-Ressourcen der HU ist i.d.R. an eine persönliche Anmeldung gebunden bzw. kann auf diese eingeschränkt sein. Die spezifischen Benutzungsbedingungen sind in den jeweiligen Benutzungsordnungen geregelt.

§ 3 IT-Infrastruktur

(1) Die **IT-Infrastruktur** der HU besteht aus technischen, organisatorischen, finanziellen und personellen IT-Ressourcen. Zu den technischen Ressourcen gehören Rechnernetze, Computerhardware, Computersoftware und sonstige IT-Systeme, die an der HU zur Erhebung, Verarbeitung und Speicherung von Daten verwendet werden. Bestandteil der technischen Ressourcen sind außerdem die zum Betrieb benötigten technischen Räume und Anlagen zur Klimatisierung, Stromversorgung, Überwachung und Signalisierung sowie zur Regelung des Zutritts.

(2) Arbeitsprozesse, die eine arbeitsorganisatorisch abgeschlossene Einheit bilden und ein gemeinsames Ziel haben, bilden ein Verfahren. Ein durch IT unterstütztes Verfahren wird als **IT-Verfahren** bezeichnet. In den IT-Verfahren wird festgelegt, welche Daten wie und zu welchen Zwecken verarbeitet werden.

(3) Ein **IT-System** ist die Gesamtheit von IT-Infrastruktur, die IT-Verfahren informationstechnisch realisieren. Dazu gehören u. a. IT-Anwendungen und ihre Daten, Server, Arbeitsplatzcomputer, mobile Computer, Client-Server-Systeme, Datennetze, Speichersysteme, Voice-over-IP-Systeme, vernetzte Computer in Steuerungs- und Regelungssystemen sowie virtualisierte Systeme.

§ 4 IT-Organisationsstruktur

(1) Die **IT-Organisationsstruktur** der HU besteht aus Gremien, Einrichtungen, Personen und Funktionsträgern. Zu diesen gehören

- Leitungsgruppe Informationsprozesse (LGI)
- IT-Sicherheitsbeauftragte(r) der HU
- Behördliche(r) Datenschutzbeauftragte(r) (behDSB)
- Personalvertretungen
- Leiterinnen und Leiter der Einrichtungen
- Datenverarbeitungs-Beauftragte(r) der Einrichtungen
- IT-Sicherheitsbeauftragte(r) der Einrichtungen
- IT-Verfahrensverantwortliche(r)
- IT-Betreiber
- IT-Systemverantwortliche(r)

§ 5 Leitungsgruppe Informationsprozesse

(1) Die Leitungsgruppe Informationsprozesse (LGI) erarbeitet die Rahmenbedingungen für die Strategie, die Entwicklung und die Kontrolle grundlegender und einrichtungsübergreifender Informationsprozesse der HU.

(2) Die LGI wird durch die Präsidentin oder den Präsidenten der HU eingesetzt.

(3) Zu ihren Aufgaben gehören:

- strategische Empfehlungen zur Gestaltung der Informationsinfrastruktur der HU,
- die grundlegende Koordination der Informationsverarbeitung,
- richtungweisende Empfehlungen bzw. Entscheidungen zur Verteilung und zum Einsatz finanzieller und personeller Ressourcen bezogen auf die Informationsprozesse der HU,
- die Einsetzung der oder des IT-Sicherheitsbeauftragten der HU,
- die Einbeziehung der Medienkommission des Akademischen Senats in Prozesse der IT-Planung und IT-Organisation der HU.

§ 6 IT-Sicherheitsbeauftragte(r) der HU

(1) Die oder der hauptamtliche IT-Sicherheitsbeauftragte der HU koordiniert und kontrolliert die Maßnahmen zur IT-Sicherheit innerhalb der HU. Sie oder er ist einer Vizepräsidentin oder einem Vizepräsidenten der HU direkt unterstellt. Das Unterstellungsverhältnis wird auf Vorschlag der LGI durch das Präsidium festgelegt.

(2) In Datenschutzbelangen stimmt sich die oder der IT-Sicherheitsbeauftragte jeweils mit der/dem behDSB der HU ab.

(3) Zu ihren/seinen Aufgaben gehören:

- Beratung zu hochschulinternen technischen Standards, Ordnungen und Notfallplänen zur IT-Sicherheit und Kontrolle ihrer Umsetzung und Einhaltung,
- Koordinierung und Kontrolle sicherheitsrelevanter IT-Projekte,

- Auswertung von Problemen und Vorfällen hinsichtlich der IT-Sicherheit, Abstimmung von Gegenmaßnahmen mit den IT-Betreibern,
- Unterstützung der IT-Sicherheitsbeauftragten der Einrichtungen bei ihren Aufgaben und bei ihrer Weiterbildung,
- Information der LGI über besondere Probleme und Vorfälle hinsichtlich der IT-Sicherheit an der HU und Abstimmung von Gegenmaßnahmen,
- Erstellung eines jährlichen IT-Sicherheitsberichts,
- Unterrichtung der Personalvertretungen über Maßnahmen zur Gewährleistung der IT-Sicherheit, von denen Mitbestimmungsangelegenheiten berührt werden,
- Koordinierung der Maßnahmen zur IT-Sicherheit mit der/dem behDSB der HU,
- Meldung sicherheitsrelevanter Vorfälle und der Maßnahmen zu ihrer Behebung bei der Verarbeitung personenbezogener Daten an die/den behDSB der HU,
- Erfüllung der Mitwirkungspflichten bei Außenkontrollen der IT-Sicherheit im Bereich der Verarbeitung personenbezogener Daten.

(4) HU-spezifische Maßnahmenkataloge zur Gewährleistung der IT-Sicherheit sind vom IT-Sicherheitsbeauftragten der HU zu veröffentlichen und regelmäßig fortzuschreiben.

§ 7 Behördliche(r) Datenschutzbeauftragte(r)

(1) Die HU bestellt eine/n Behördliche/n Datenschutzbeauftragte/n (behDSB) sowie eine/n Vertreter/in. Die/der behDSB ist weisungsfrei, zur Verschwiegenheit verpflichtet und darf wegen der Erfüllung ihrer/seiner Aufgaben nicht benachteiligt werden. Jedes Mitglied der Universität ist berechtigt, sich ohne Einhaltung eines Dienstweges an die/den behDSB zu wenden.

(2) Entsprechend seines gesetzlichen Tätigkeitsrahmens ergeben sich für die/den behDSB im Zusammenhang mit dieser Ordnung v. a. folgende Aufgaben:

- Beratungen und Überprüfungen zu datenschutzrelevanten IT-Systemen und IT-Verfahren an der HU,
- Abstimmungen mit dem/der zentralen IT-Sicherheitsbeauftragten,
- Beratung aller Verantwortungsträger der IT-Ordnung in Datenschutzbelangen,
- Überprüfung von konkreten Maßnahmen und Vorgängen auf Vereinbarkeit mit den Vorgaben des Datenschutzrechts,
- Datenschutzrechtliche Beratung der Benutzerinnen und Benutzer von IT-Dienstleistungen der HU,
- Führen des Verzeichnisses der Dateibeschreibungen gem. § 19 Abs. 2 BlnDSG.

§ 8 Personalvertretungen

(1) Die grundsätzlichen Zuständigkeiten der Personalvertretungen sind im Personalvertretungsgesetz (PersVG) geregelt.

(2) Entsprechend ihres gesetzlichen Tätigkeitsrahmens unterfallen den zuständigen Personalvertretungen innerhalb dieser Ordnung v. a.:

- Beteiligung an allen Angelegenheiten der Einführung und Änderung mitbestimmungspflichtiger IT-Systeme und IT-Verfahren,
- Genehmigung aller IT-Verfahren und IT-Systeme vor Inbetriebnahme (PersVG §85 (2) Abs. 9).

§ 9 Leiterinnen und Leiter der Einrichtungen

(1) Die Leiterinnen und Leiter einer Fakultät, eines Instituts, einer wissenschaftlichen oder sonstigen Einrichtung der HU oder einer Abteilung der Universitätsverwaltung sind für die Planung und den Einsatz der IT und für die Gewährleistung und Weiterentwicklung der

IT-Sicherheit sowie für die Umsetzung und Kontrolle der in dieser Ordnung aufgeführten Maßnahmen in ihren Einrichtungen verantwortlich.

(2) Dazu benennen und beauftragen sie DV-Beauftragte und IT-Sicherheitsbeauftragte für ihre Einrichtungen sowie IT-Verfahrensverantwortliche bzw. IT-Systemverantwortliche für alle in der Einrichtung geplanten oder eingesetzten IT-Verfahren und IT-Systeme. Werden in einem IT-Verfahren oder mit einem IT-System personenbezogene Daten verarbeitet, ist die/der behDSB über die Benennung zu informieren.

(3) Die Verantwortlichkeit für IT-Verfahren und IT-Systeme kann zentralisiert oder auf verschiedene Einrichtungen, Arbeitsgruppen oder Personen aufgeteilt sein.

(4) Abhängig von den eingesetzten Verfahren und Systemen sowie vom zur Verfügung stehenden Personal können Verantwortlichkeiten auch zusammengelegt werden. Das betrifft zum Beispiel DV-Beauftragte und IT-Sicherheitsbeauftragte oder IT-Verfahrensverantwortliche und IT-Systemverantwortliche. Die Benennung kann in Abstimmung mit den beteiligten Leiterinnen und Leitern auch einrichtungsübergreifend erfolgen.

§ 10 Datenverarbeitungs-Beauftragte(r) der Einrichtungen

(1) Datenverarbeitungs-Beauftragte (DV-Beauftragte) sind für das Konzept der Datenverarbeitung und dessen Umsetzung in der Einrichtung verantwortlich.

(2) Sie haben insbesondere folgende Aufgaben:

- Erstellung und Fortentwicklung des DV-Konzepts der Einrichtung in Abstimmung mit den zuständigen Gremien,
- Koordinierung und Beratung bezüglich der Planung, der Beschaffung und des Betriebes von IT-Systemen in Abstimmung mit dem CMS,
- Vertretung der Benutzerinnen und Benutzer der Einrichtung in der Benutzerversammlung und in direktem Kontakt mit dem CMS,
- Ansprechpartner für alle Belange der IT im Verantwortungsbereich,
- Ansprechpartner des CMS zur Abstimmung der IT-Dienste der Einrichtung mit den vom CMS angebotenen Diensten und zur Koordinierung von einrichtungsübergreifenden Aspekten der IT,
- Koordinierung der lokalen Netzanbindung,
- Unterstützung der/des IT-Sicherheitsbeauftragten der Einrichtung und der/des IT-Sicherheitsbeauftragten der HU,
- Information und Beratung der IT-Benutzerinnen und -Benutzer zur ordnungsgemäßen Nutzung von Datennetzen, Hardware und Software der Einrichtung,
- Sicherstellung der korrekten Lizenzierung der im jeweiligen Verantwortungsbereich eingesetzten Software,
- Koordinierung und Anleitung der IT-Systemverantwortlichen der Einrichtung.

(3) DV-Beauftragte sind verpflichtet, sich auf dem Gebiet des IT-Einsatzes und der IT-Nutzung weiterzubilden und ihr Wissen auf dem aktuellen Stand zu halten. Sie werden hierbei insbesondere von den Leiterinnen oder Leitern der jeweiligen Einrichtung sowie vom CMS unterstützt.

§ 11 Dezentrale IT-Sicherheitsbeauftragte(r) der Einrichtungen

(1) Dezentrale IT-Sicherheitsbeauftragte sind im ihnen zugeordneten Verantwortungsbereich für die Gewährleistung der IT-Sicherheit verantwortlich.

(2) Sie arbeiten eng mit der oder dem IT-Sicherheitsbeauftragten der HU zusammen und haben insbesondere folgende Aufgaben:

- Konzipierung von Maßnahmen zur Gewährleistung und Weiterentwicklung der IT-Sicherheit der Einrichtung,
- Kontrolle der Umsetzung der Maßnahmen zur IT-Sicherheit,

- Ansprechpartner der oder des DV-Beauftragten, der Leiterin oder des Leiters der Einrichtung, des CMS und der oder des Sicherheitsbeauftragten der HU hinsichtlich der IT-Sicherheit,
- Meldung sicherheitsrelevanter Vorfälle und der Maßnahmen zu ihrer Behebung an die IT-Sicherheitsbeauftragte oder den IT-Sicherheitsbeauftragten der HU, den CMS sowie an die DV-Beauftragte oder den DV-Beauftragten und die Leiterin oder den Leiter der Einrichtung,
- Meldung sicherheitsrelevanter Vorfälle und der Maßnahmen zu ihrer Behebung bei der Verarbeitung personenbezogener Daten an die/den behDSB der HU,
- Beratung der IT-Verfahrensverantwortlichen zu sicherheitsrelevanten Fragen von IT-Verfahren,
- Initiierung und Kontrolle von aktuellen Sicherheitskonzepten für IT-Verfahren und IT-Systeme,
- Koordinierung der Schulung des IT-Personals und der IT-Benutzerinnen und -Benutzer hinsichtlich der IT-Sicherheit.

(3) Die IT-Sicherheitsbeauftragten sind verpflichtet, sich auf dem Gebiet der IT-Sicherheit weiterzubilden und ihr Wissen auf dem aktuellen Stand zu halten. Sie werden hierbei von den Leiterinnen oder Leitern der jeweiligen Einrichtung unterstützt.

(4) IT-Sicherheitsbeauftragte sollen nicht die Leiterin oder der Leiter einer Einrichtung der HU sein.

§ 12 IT-Verfahrensverantwortliche(r)

(1) IT-Verfahrensverantwortliche sind für die Organisation der Einführung und des Einsatzes der jeweiligen Verfahren sowie deren informationstechnische Belange zuständig.

(2) Zu ihren Aufgaben bezüglich der Informationstechnik gehören:

- Erstellung eines Sicherheitskonzeptes für das jeweilige IT-Verfahren (vgl. § 3, Abs. (2)) in dem insbesondere der Schutzbedarf für die Daten und ein Berechtigungskonzeptes für den Datenzugriff festgelegt wird inkl. Abstimmung mit der/dem zuständigen IT-Sicherheitsbeauftragten,
- Einhaltung aller informationsrechtlichen Regelungen für das Verfahren,
- Planung und Kontrolle der Regelungen des Schutzes personenbezogener Daten im IT-Verfahren, Verantwortung zur Erstellung einer Dateibeschreibung nach § 19 Abs. 2 BlnDSG und Meldung an die/den behDSB der HU sowie Abstimmung mit der/dem behDSB,
- Auswahl und Kontrolle der IT-Betreiber der zur Realisierung des Verfahrens einzusetzenden IT-Systeme,
- Abstimmung der zur Realisierung des IT-Verfahrens einzusetzenden IT-Systeme und der in ihren Sicherheitskonzepten festgelegten Sicherheitsparameter mit den IT-Betreibern und Kontrolle der Sicherheitskonzepte der IT-Systeme in Bezug auf die Sicherheitsanforderungen des IT-Verfahrens.

§ 13 IT-Betreiber

(1) Die IT-Systeme im Sinne dieser Ordnung werden einem IT-Betreiber zugeordnet, der für deren ordnungsgemäßen Betrieb verantwortlich ist.

(2) Der Hauptbetreiber von IT-Systemen der HU ist der Computer- und Medienservice. Er ist für die Versorgung aller Einrichtungen mit IT-Dienstleistungen sowie für die Basis-IT-Systeme der HU zuständig, die allgemein nutzbar sind bzw. einrichtungsübergreifend angeboten werden. Daneben gibt es Arbeitsgruppen oder Einzelpersonen in den Einrichtungen der HU als dezentrale IT-Betreiber sowie ggf. externe IT-Betreiber für die HU.

(3) Der CMS und die dezentralen IT-Betreiber stimmen sich untereinander ab. Der CMS und die dezentralen IT-Betreiber unterstützen die Tätigkeit der DV-Beauftragten, der IT-Sicherheits-beauftragten, der IT-Verfahrensverantwortlichen und der IT-Systemverantwortlichen.

(4) Externe IT-Betreiber, die für die HU IT-Dienstleistungen erbringen, werden vom CMS oder von dezentralen IT-Betreibern im Einvernehmen mit dem CMS beauftragt. Der Auftraggeber ist dafür verantwortlich, dass externe IT-Betreiber auf die Einhaltung der innerhalb der HU geltenden Regelungen verpflichtet wird. Bei der Verarbeitung personenbezogener Daten ist bei der Beauftragung die/der behDSB der HU einzubeziehen.

(5) Die IT-Betreiber sind bei der Erbringung ihrer IT-Dienstleistungen im Auftrag der für die IT-Verfahren zuständigen Einrichtungen oder Personen für die Sicherheit der IT-Systeme und damit für die in den IT-Verfahren behandelten Daten verantwortlich.

(6) Der CMS ist als Betreiber der aktiven Netzkomponenten des Netzes der HU für die Gewährleistung der allgemeinen Netzsicherheit verantwortlich. Wenn für Teilnetze eine erhöhte Netzsicherheit erforderlich ist, sind durch die betroffenen Einrichtungen mit dem CMS Maßnahmen für die zusätzliche Absicherung dieser Teilnetze zu vereinbaren.

(7) Um akute Gefahren für die IT-Sicherheit im Netz der HU abzuwehren, treffen IT-Betreiber im Rahmen ihrer Zuständigkeit erforderliche Maßnahmen zur Gefahrenintervention, wie z. B. die Sperrung von Netzanschlüssen, von kompromittierten Benutzerkonten bzw. IT-Systemen. Die zuständigen Sicherheitsbeauftragten sowie die betroffenen Betreiber und Benutzerinnen und Benutzer sind unverzüglich zu informieren. Sofern personenbezogene Daten betroffen sind, ist die/der behDSB einzubeziehen.

§ 14 IT-Systemverantwortliche(r) und Systemadministrator(in)

(1) IT-Systemverantwortliche sind Personen, die die technische Gesamtverantwortung für ein IT-System haben. Sie sind in der Regel gleichzeitig IT-Systemadministratorin bzw. -administrator.

(2) IT- Systemadministratorinnen bzw. -administratoren sind Personen, die für den technischen Betrieb von IT-Systemen zuständig sind.

(3) Zu den Aufgaben der Systemverantwortlichen gehören:

- Planung, Einrichtung und Administration des IT-Systems (vgl. § 3, Abs. (3)),
- Gewährleistung des stabilen und sicheren Betriebes des IT-Systems,
- Organisation der Servicearbeiten für die Hard- und Software,
- Einhaltung der in dieser Ordnung genannten Maßnahmen zur IT-Sicherheit,
- unverzügliche Information der bzw. des zuständigen IT-Sicherheitsbeauftragen zu Problemen und Vorfällen hinsichtlich der IT-Sicherheit in ihrem Verantwortungsbereich,
- Erstellung eines Sicherheitskonzeptes für das jeweilige IT-System und Abstimmung mit der/dem zuständigen IT-Sicherheitsbeauftragten, Information und Zusammenarbeit mit den Verantwortlichen für IT-Verfahren, die durch die IT-Systeme umgesetzt werden,
- bei der Verarbeitung personenbezogener Daten und datenschutzrechtliche Anforderungen nicht durch anderweitige Verantwortlichkeiten abgedeckt werden: Verantwortung zur Erstellung einer Dateibeschreibung nach § 19 Abs. 2 BlnDSG und Meldung an die/den behDSB der HU sowie Abstimmung mit der/dem behDSB,
- Erstellen einer Schutzbedarfsanalyse; ggf. Konzeptionierung gezielter Schutzmaßnahmen auf Grundlage einer Risikoanalyse, insbesondere bei Verarbeitung personenbezogener Daten,
- je nach Art der zu schützenden Daten die Veranlassung entsprechender Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit,
- Information und Dokumentation der IT-Systeme und ihrer Dienste,
- Einweisung und Beratung von Benutzerinnen und Benutzern des IT-Systems.

(4) IT-Systemverantwortliche und IT-Systemadministratorinnen bzw. -administratoren haben besondere Rechte hinsichtlich der Administration und des Datenzugriffs. Daraus resultiert eine hohe Verantwortung bezüglich des Datenschutzes und der Datensicherheit der IT-Systeme und ihrer Vernetzung.

§ 15 Inkrafttreten

(1) Diese IT-Ordnung tritt am Tag ihrer Veröffentlichung im Amtlichen Mitteilungsblatt der Humboldt-Universität zu Berlin in Kraft.

(2) Gleichzeitig tritt die „Computerbetriebsordnung der Humboldt-Universität zu Berlin“ vom 26. Oktober 1996 (Amtliches Mitteilungsblatt Nr. 22/1996) außer Kraft.

Anlage 1 Glossar

Einrichtungen der HU

Einrichtungen der HU sind z. B. Fakultäten, Institute, Zentralinstitute, Graduate Schools, Interdisziplinäre Zentren, Integrative Forschungsinstitute, Zentralinstitute, Zentraleinrichtungen und die Abteilungen der Universitätsverwaltung.

IT-Benutzerinnen und -Benutzer

IT-Benutzerinnen und –Benutzer sind natürliche Personen, welche befugt definierte Anwenderrechte auf IT-Systemen oder in IT-Verfahren eingeräumt erhalten haben, ohne für diese IT-Systeme oder in diesen IT-Verfahren als IT-Personal tätig zu sein.

IT-Betreiber

IT-Betreiber sind Einrichtungen, Arbeitsgruppen oder Personen, die mit ihren Systemverantwortlichen und Systemadministrator/innen für IT-Systeme der HU zuständig sind.

IT-Infrastruktur der HU

Die IT-Infrastruktur der HU besteht aus technischen, organisatorischen, finanziellen und personellen IT-Ressourcen. Zu den technischen Ressourcen gehören Rechnernetze, Computerhardware, Computersoftware und sonstige IT-Systeme, die an der HU zum Einsatz gebracht werden. Bestandteil der technischen Ressourcen sind außerdem die zum Betrieb benötigten infrastrukturellen Einrichtungen wie technische Räume und Anlagen zur Klimatisierung, Stromversorgung, Überwachung und Signalisierung sowie zur Regelung des Zutritts.

IT-Personal

Das IT-Personal der HU umfasst IT-Systemverantwortliche, IT-Systemadministratorinnen und -administratoren, DV-Beauftragte und IT-Sicherheitsbeauftragte.

IT-Systemadministratorinnen bzw. –administratoren

IT-Systemadministratorinnen bzw. –administratoren sind für den technischen Betrieb von IT-Systemen zuständig. Das sind in der Regel die Personen, die Kenntnis vom Administrator-Passwort eines IT-Systems haben.

IT-Systeme

IT-Systeme sind Hardware und/oder Software, die IT-Verfahren informationstechnisch realisieren. Dazu gehören zum Beispiel IT-Anwendungen und ihre Daten, Server, Arbeitsplatzcomputer, mobile Computer, Client-Server-Systeme, Datennetze, Speichersysteme, Voice-over-IP-Systeme, vernetzte Computer in Steuerungs- und Regelungssystemen (embedded systems) sowie virtualisierte Systeme in Einrichtungen der HU.

IT-Verfahren

Eine Vielzahl von Arbeitsprozessen an der HU wird durch IT unterstützt. Arbeitsprozesse, die eine arbeitsorganisatorisch abgeschlossene Einheit bilden und ein gemeinsames Ziel haben bilden ein Verfahren. Ein durch IT unterstütztes Verfahren wird in dieser Ordnung kurz als IT-Verfahren bezeichnet.

Anlage 2 Abkürzungsverzeichnis

behDSB	Behördlicher Datenschutzbeauftragter
BerlHG	Berliner Hochschulgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
DV	Datenverarbeitung(s)
HU	Humboldt-Universität zu Berlin
IT	Informationstechnologie
LGI	Leitungsgruppe Informationsprozesse
PersVG	Personalvertretungsgesetz

Anlage 3 Literaturverzeichnis

[1] BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Version 1.5, BSI 2008
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001.pdf

[2] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Version 2.0, BSI 2008
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002.pdf

[3] BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5, BSI 2008
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003.pdf

[4] BSI-Standard 100-4: Notfallmanagement, Version 1.0, BSI 2008
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004.pdf

[5] IT-Grundschutz-Kataloge, Stand 12. Ergänzungslieferung, BSI 2011
https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf

[6] Leitfaden Informationssicherheit: IT-Grundschutz kompakt, BSI 2009
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf