

Weisung zur Nutzung von IT-Mitteln durch Studierende der Pädagogischen Hochschule Zürich

(vom 15. Februar 2010) ⁶

Gestützt auf § 24 Abs. 2 Fachhochschulgesetz vom 2. April 2007

beschliesst die Hochschulleitung:

1. Abschnitt: Allgemeine Bestimmungen

§ 1 Zweck

Diese Weisung dient dem sicheren, gesetzmässigen, wirtschaftlichen, störungsfreien sowie benutzerfreundlichen Gebrauch der Informatik und Multimedia-Infrastruktur (IT-Mittel) an der Pädagogischen Hochschule Zürich (PHZH).

§ 2 Geltungsbereich

¹ Dieser Weisung unterstehen die Studierenden sowie Teilnehmerinnen und Teilnehmer von Weiterbildungsveranstaltungen der PHZH (Nutzende). Auf weitere Personen, die Leistungen der PHZH beziehen, ist sie analog anwendbar, sofern diese Zugang zu den IT-Mitteln der PHZH haben.⁵

² Die Weisung gilt für die Nutzung sämtlicher IT-Mittel, unabhängig davon, ob sie von der PHZH zur Verfügung gestellt werden oder im Eigentum der Nutzenden stehen, namentlich:⁵

- a) Computer und mobile Geräte wie Laptops, Tablets, Smartphones;⁶
- b) Peripherie-Geräte wie Drucker;⁵
- c) Telefone, Voicemail und mobile Kommunikationsgeräte;
- d) Cloud Computing;³
- e) Software;
- f) Netzwerke und Netzwerkgeräte;
- g) Internetzugang;
- h) Dateiablagen, Datenbanken, web-basierte Plattformen;⁵
- i) IT-Dienste (E-Mail und andere Kommunikationskanäle);⁵
- j) Audio-, Video- und andere Multimediageräte.

³ Aufgehoben.

§ 3 Missbrauch

¹ Missbräuchlich ist jede Nutzung von IT-Mitteln, die gegen diese Weisung oder gegen andere Bestimmungen der geltenden Rechtsordnung verstösst oder Rechte Dritter verletzt.

² Missbräuchlich sind insbesondere folgende Handlungen:

- a) unzulässige Internet- oder E-Mail-Nutzungen gemäss § 14 bis § 16b sowie²
- b) unbefugtes Kopieren, Verändern und Löschen von Daten;

- c) Bearbeitung von Daten mit rassistischem, sexistischem, pornographischem oder gewaltverherrlichendem Inhalt (vorbehalten bleibt eine Bearbeitung solcher Daten zu Lehr- und Forschungszwecken);
- d) unbefugter Zugang zu den IT-Mitteln sowie unbefugte Manipulation (insbesondere Erstellen oder Verbreiten von schädlichen Programmcodes, wie z.B. Viren, Trojaner, Würmer);⁶
- e) Inbetriebnahme eigener WLAN-Access-Points oder eigener Netzwerke (Hubs, Switches, Router usw.) mit Verbindung zum Netz der PHZH ohne Zustimmung der Informatikdienste;
- f) Belästigung oder Irreführung anderer Personen mit IT-Mitteln;
- g) Verwendung der IT-Mittel in einer Weise, welche den Datenschutz oder Urheber- und Lizenzrechte verletzt.⁶

³ Bei einem Missbrauch oder einem begründeten Verdacht eines Missbrauchs ordnet die Rektorin oder der Rektor alle zur Aufrechterhaltung oder Wiederherstellung des rechtmässigen Zustandes erforderlichen Massnahmen an. Namentlich kann sie oder er die Nutzung der IT-Mittel untersagen oder einschränken und Daten blockieren oder löschen lassen. Zudem kann sie oder er Zugänge sperren und Beweissicherungen vornehmen lassen. Das Verfahren richtet sich gegebenenfalls nach der Verordnung zum Fachhochschulgesetz (Disziplinarordnung). § 22a bleibt vorbehalten.⁶

⁴ Ein Missbrauch kann sodann disziplinar- sowie straf-, zivil- und haftungsrechtliche Konsequenzen haben.⁶

§ 4 Erklärung

¹ Alle Nutzenden geben eine Erklärung ab, wonach sie den Inhalt dieser Weisung und die möglichen Konsequenzen eines Missbrauchs zur Kenntnis genommen haben.

² Die Erklärung wird im Studierendendossier abgelegt.⁶

§ 5 Ausleihe

¹ Der Bereich Digital Learning betreibt für die Nutzenden eine Ausleihe mit Multimediageräten.⁶

² Er setzt Ausleihbedingungen fest.⁶

§ 6 Betrieb Informatik und Multimedia-Infrastruktur⁶

¹ Für den Betrieb der Informatik und Multimedia-Infrastruktur der PHZH und alle damit verbundenen Prozesse und Supportleistungen sind die Informatikdienste (ID) verantwortlich. Der Betrieb von privaten IT-Mitteln wird grundsätzlich nicht unterstützt.

² Die ID erlassen Merkblätter oder informieren elektronisch über Verhaltensregeln zum sicheren und zweckmässigen Gebrauch der IT-Mittel. Bei akuten Sicherheitsproblemen informieren sie die Nutzenden und geben Instruktionen.

³ Die ID können IT-Mittel, Teile oder bestimmte Funktionen davon jederzeit für Wartungsarbeiten und zur Entwicklung des Angebots ändern oder ausser Kraft setzen. Entsprechend können sie die Nutzung und den Zugang beschränken. Sie sind bestrebt, die IT-Mittel möglichst unterbrechungsfrei zur Verfügung zu stellen und Ausfallzeiten kurz zu halten.¹

2. Abschnitt: Allgemeine Nutzungsvorschriften

§ 7 Nutzungsgrundsätze

¹ Die von der PHZH zur Verfügung gestellten IT-Mittel sind mit der gebotenen Sorgfalt zu behandeln.⁵

² Sie sind wirtschaftlich einzusetzen.

³ Die Nutzenden sind persönlich dafür verantwortlich, dass sie mit dem Gebrauch der IT-Mittel nicht gegen die vorliegende Weisung und nicht gegen andere Bestimmungen der geltenden Rechtsord-

nung (Strafrecht, Datenschutzgesetzgebung, geistiges Eigentum, Persönlichkeitsrechte usw.) verstossen.

§ 8 Nutzungsberechtigte

¹ Die Weitergabe von zur persönlichen Nutzung zur Verfügung gestellten IT-Mitteln der PHZH an Dritte ist nicht gestattet. Eine ausdrückliche Erlaubnis aufgrund der anwendbaren Lizenzbestimmungen durch die ID bleibt vorbehalten.⁵

² Ein Verkauf gemäss Weisung zum Verkauf von ausgemustertem Material ist zulässig.⁶

§ 9 Nutzungsumfang

¹ Die von der PHZH zur Verfügung gestellten IT-Mittel sind für den Einsatz im Studium oder in der Weiterbildung bestimmt.

² Die private Nutzung von IT-Mitteln der PHZH ist erlaubt, sofern sie für den persönlichen Gebrauch, d.h. weder für eine kommerzielle oder andere öffentliche Verwendung, bestimmt ist und nicht gegen Rechte Dritter verstösst. Sie ist auf ein Minimum zu beschränken und umgehend einzustellen, sobald die IT-Mittel zu Studienzwecken oder von Mitarbeitenden für die Aufgabenerfüllung an der PHZH benötigt werden oder wenn sie zu einer Beeinträchtigung des Betriebs führt.⁵

³ Eine ausdrückliche Erlaubnis aufgrund der anwendbaren Lizenzbestimmungen durch die ID bleibt vorbehalten.³

§ 10 Sicherheit

Die Nutzenden haben geeignete Massnahmen zu treffen, damit die IT-Mittel nicht durch andere Personen oder Systeme genutzt werden können. Insbesondere sind folgende Verhaltensregeln zu beachten:

- a) Die persönlichen Benutzeraccounts und Passwörter sowie andere Zugangsberechtigungen und Identifikationsmethoden dürfen unter keinen Umständen anderen Personen weitergegeben oder zugänglich gemacht werden.
- b) Unbeaufsichtigte Computer sind hinunterzufahren, mittels manuellem Ausloggen oder Sperren oder mit passwortgeschütztem Bildschirmschoner zu schützen.
- c) Mobile Geräte sind mit einem ausreichenden Zugriffsschutz (z.B. Log-In oder Verschlüsselung) zu versehen und bei Nichtbetrieb von allen Datennetzen zu trennen, auszuschalten und sicher aufzubewahren.⁵
- d) Von den ID vorgegebene oder implementierte Schutzmassnahmen (wie Firewall und Virenschutz) dürfen weder ausgeschaltet noch umgangen oder unwirksam gemacht werden.⁵

§ 10a Nutzung von Cloud-Diensten³

¹ Nutzende dürfen im Zusammenhang mit dem Studium oder der Weiterbildungsveranstaltung nur die von der PHZH administrierten und zur Verfügung gestellten Cloud-Dienste verwenden. Andere Cloud-Dienste dürfen nur genutzt werden, wenn eine Genehmigung der HSL vorliegt oder

- a) die Aufzeichnungen keinen Geheimnis- oder Schutzpflichten (wie Persönlichkeitsrecht und Datenschutz) unterliegen;
- b) keine Vorgaben zur Ablage und Archivierung der PHZH verletzt werden und
- c) keine Immaterialgüterrechte der PHZH oder von Dritten betroffen sind.

² Die Nutzenden sind für die Einhaltung der Datenschutzbestimmungen und für die Datensicherung verantwortlich. Sie sind insbesondere dafür verantwortlich, dass die auf mobilen Endgeräten gespeicherten Daten nach den üblichen Standards geschützt sind. Werden Daten in Cloud-Diensten anderen Nutzenden oder Dritten zugänglich gemacht, sind die Personen, welche den Zugang zur Verfügung stellen, für die Einhaltung der Datenschutzbestimmungen verantwortlich.⁵

³ Streng vertrauliche Daten, wie besondere Personendaten gemäss § 3 Gesetz über die Information und den Datenschutz¹ und weitere sensitive Daten mit besonderen Geheimhaltungspflichten dürfen nur verschlüsselt auf einen Cloud-Dienst übermittelt und gespeichert werden.⁵

§ 11 Datentrennung, Virenschutz, Aktualisierung von Software und Betriebssystemen auf privaten Geräten⁵

¹ Private Geräte, die im PHZH-Netzwerk eingesetzt werden, müssen mit einem aktuellen Virenschutz und Betriebssystem ausgerüstet sein. Software und Betriebssysteme sind regelmässig zu aktualisieren.⁵

² Aufgehoben.⁶

³ Daten, die in Zusammenhang mit dem Studium oder der Weiterbildung an der PHZH stehen, sind von privaten Daten klar zu trennen.⁵

§ 12 Meldepflicht

¹ Verluste, Diebstähle oder Schäden von oder an den zur Verfügung gestellten IT-Mitteln oder anderen mobilen Geräten, die im Zusammenhang mit der Aufgabenerfüllung an der PHZH stehende Daten enthalten oder zugänglich machen, müssen unverzüglich den ID gemeldet werden.

² Besteht die Vermutung, dass sich Unbefugte Zugang zu den IT-Mitteln oder Daten der PHZH beschafft haben oder unzulässige Manipulationen vorgenommen wurden, ist dies ebenfalls umgehend mitzuteilen.⁵

§ 12a Haftungsausschluss beim Einsatz privater Geräte

Bei Verlust oder Beschädigung von privaten Geräten oder Daten haftet die PHZH nur, wenn sie den Verlust oder die Beschädigung vorsätzlich oder grobfahrlässig verschuldet hat.

§ 13 Löschung von Benutzeraccount und Daten, Deinstallation von Software⁵

¹ Die ID löschen nach Abschluss des Studiums oder der Weiterbildungsveranstaltung sämtliche persönliche Daten, die persönliche Website und das Postfach mit allen E-Mails, Kalender- und Adressbucheinträgen.³

² Der persönliche Benutzeraccount bleibt bestehen und kann für den späteren Bezug von Leistungen bei der PHZH (z.B. für Kursanmeldungen) benutzt werden.

³ Die Nutzenden sind verpflichtet, nach Abschluss des Studiums oder der Weiterbildungsveranstaltung, über die PHZH lizenzierte Softwareprodukte sowie allfällige Kopie nach Massgabe der anwendbaren Lizenzbestimmungen zu deinstallieren.⁵

3. Abschnitt: Besondere Nutzungsvorschriften

A. Internet, E-Mail und persönliche Website

§ 14 Nutzungseinschränkungen beim Surfen auf dem Internet

Internetseiten mit rechtswidrigem, pornografischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt dürfen aus dem Netz der PHZH weder ausgewählt noch genutzt werden.

§ 15 Nutzungseinschränkungen beim E-Mail-Service

¹ Der E-Mail-Service, welcher während des Studiums oder der Weiterbildungsveranstaltung zur Verfügung steht, darf nicht für folgende Handlungen verwendet werden:

¹ LS 170.4

- a) für den Versand von E-Mails mit Inhalten, die in § 14 genannt werden, sowie von E-Mails mit vorgetäuschten oder irreführenden Absenderangaben und Kettenbriefen;
- b) für den Versand von E-Mails mit starker Netzwerkbelastung zu PHZH-fremden Zwecken.

² Der Service „E-Mail an alle Studierende“ darf nur zurückhaltend und nur für Inhalte mit Bezug zur Lehrtätigkeit an der PHZH oder an der Volksschule verwendet werden. Verboten sind der Versand von unverlangten Werbe-E-Mails, Anzeigen jeglicher Art, politisch und religiös motivierten Mails und Mails, die die Integrität von Personen oder Institutionen verletzen. Der Service kann vom Prorektorat Ausbildung oder vom Prorektorat Weiterbildung und Dienstleistungen eingeschränkt oder durch Beschluss der Hochschulleitung gelöscht werden.⁶

³ Bei ausserordentlichen Ereignissen können die ID den Datenverkehr weitergehend einschränken.

§ 16 Persönliche Website

Die persönliche Website, welche die Nutzenden während ihres Studiums oder der Weiterbildungsveranstaltung an der PHZH aufschalten können, darf keine Inhalte, die in § 14 genannt werden, aufweisen und keine Rechte Dritter verletzen.

§ 16a Web-basierte Plattformen³

¹ Die Nutzenden dürfen Materialien und Informationen, die ihnen auf den web-basierten Plattformen (ILIAS, Multimediaportal, Sharepoint usw.) zur Verfügung stehen, zu Lern- und Informationszwecken während des Studiums oder der Weiterbildung an der PHZH nutzen. Eine weitergehende Verwendung ist zulässig, wenn entsprechende Nutzungsrechte und Einverständniserklärungen vorliegen.³

² Studierende der Ausbildung und Teilnehmende von laufenden Weiterbildungsveranstaltungen können eigene Materialien und Informationen zu Lern- und Informationszwecken auf den Plattformen abspeichern, bearbeiten, abrufen und verbreiten. Die Aufzeichnungen dürfen keine Inhalte, die in § 14 genannt werden, aufweisen. Die für die Verbreitung erteilten Nutzungsrechte und Einverständniserklärungen gelten über die Dauer des Studiums oder der Weiterbildung an der PHZH hinaus.³

³ Immaterialgüterrechtlich geschützte Materialien, die immatrikulierte Studierende im Rahmen des Studiums oder der Weiterbildung an der PHZH schaffen und deren ausschliesslichen Verwendungsrechte bei der PHZH liegen, dürfen diese vorbehältlich anderslautender Absprachen mit der zuständigen Abteilungs- bzw. Zentrumsleitung nur für die Verwendung an der PHZH freigeben.⁶

⁴ Die Wahrung des Datenschutzes sowie weiterer Geheimnis- oder Schutzpflichten, die Einhaltung der Vorgaben zur Ablage und Archivierung und der Schutz des geistigen Eigentums sind jederzeit sicherzustellen. Die Nachvollziehbarkeit und Zuordnung der Aufzeichnungen zur oder zum verantwortlichen Nutzenden müssen gewährleistet sein.³

⁵ Für die plattforminterne Kommunikation ist § 15 analog anwendbar.³

§ 16b Social Networks²

¹ Die Versammlung der Studierenden und weitere organisierte Gruppen von Studierenden können nach Absprache mit dem Ressort Kommunikation über die Hauptpräsenz der PHZH auf den Social Network-Plattformen publizieren oder bei Bedarf eigene Konten erstellen. Sie sorgen für eine aktive und rechtskonforme Bewirtschaftung dieser Auftritte.⁶

² Ein Konto, bei welchem keine regelmässige Aktivität erfolgt oder Regelverstösse beobachtet werden, muss gelöscht werden.

B. Software

§ 17 Installation von Software

¹ Die ID sind verantwortlich für das Bereitstellen und die Lizenzierung der an der PHZH eingesetzten Softwareprodukte.⁵

² Die Installation privater Software auf PHZH-Geräten ist nicht zulässig. Ausgenommen von dieser Regelung ist die Verwendung von privater Anwendungssoftware auf Kursraumgeräten für die Dauer einer Lehrveranstaltung. Die ID können bestimmte Software gänzlich verbieten, wenn die Gefahr besteht, dass sie Störungen im Betrieb verursachen. Bei nicht oder nur mit übermässigem Aufwand lösbaren Problemen kann das IT-Mittel von den ID auf die Grundinstallation zurückgesetzt werden.

³ Die Installation und Deinstallation von Software und Softwareverteilungswerkzeugen auf Geräten, die von der PHZH zur Verfügung gestellt werden, sowie eine Deaktivierung oder Modifikation ist Sache der ID. Sie können Nutzende zu einer solchen Handlung ermächtigen.⁵

⁴ Für die Installation und Deinstallation der von den ID für Studierende bereitgestellten Software auf deren privaten Geräte sind die Nutzenden selbst verantwortlich.⁵

§ 18 Kopieren von Software

Das Kopieren von Software der PHZH ist sowohl für den Eigengebrauch als auch für die Weitergabe an Dritte untersagt. Eine ausdrückliche Erlaubnis aufgrund der anwendbaren Lizenzbestimmungen durch die ID bleibt vorbehalten.

C. CampusCard

§ 19 Abgabe und Leistungsbezug

¹ Sind sämtliche der verlangten Unterlagen eingereicht und die Zulassungsvoraussetzungen erfüllt, wird den Studierenden den Legitimationsausweis (CampusCard) abgegeben.¹

² Die CampusCard berechtigt unter der Voraussetzung einer fristgerechten Bezahlung der Semesterrechnung zum Bezug von Leistungen der PHZH.⁶

³ Sie wird für die gesamte Studiendauer ausgestellt, ist personalisiert und enthält die individuellen Zutrittsberechtigungen für den Campus PH Zürich.⁶

⁴ Der Verlust oder Defekt der CampusCard ist der Kanzlei umgehend zu melden. Die Ausstellung einer neuen CampusCard ist bei selbstverschuldetem Verlust oder Defekt gebührenpflichtig. Die Gebühr richtet sich nach der Weisung zu den Gebühren der Pädagogischen Hochschule Zürich.⁴

⁵ Für Schäden, die aus dem Verlust der CampusCard, insbesondere durch Missbrauch Dritter, entstehen, haften die Studierenden.⁶

⁶ Nach Beendigung des Studiums ist die CampusCard in der Kanzlei abzugeben.

§ 20 Persönliche Daten

¹ Die CampusCard enthält ein Foto des oder der Studierenden und gibt Aufschluss über folgende Daten:

- a) Name;
- b) Vorname;
- c) Geburtsdatum;
- d) Personenkategorie;¹
- e) Matrikel-Nummer;
- f) IDS-Identifikation für die Bibliothek;¹
- g) Evento-Personennummer;¹
- h) Gültigkeitsdauer der Karte;¹
- i) Aktuelles Semester.¹

² Mit dem Empfang der Karte erklären die Studierenden ihr Einverständnis mit der Erhebung und Verwendung dieser Daten für die CampusCard.

³ Die bei der Benutzung der CampusCard generierten Daten werden nach dem Zweck ihrer Erhebung (Zutrittssystem usw.) getrennt in Datenbanken gespeichert. Für die Protokollierung und personenbezogene Auswertungen gelten die §§ 21 und 22 analog.⁶

4. Abschnitt: Protokollierung und Überwachung

§ 21 Protokollierung der Log-Informationen

¹ Die IT-Systeme der PHZH protokollieren Informationen von Benutzeraktivitäten und Applikationen, um einen störungsfreien und gesetzmässigen Betrieb, insbesondere eine frühzeitige Erkennung und Eingrenzung von Systemfehlern und deren rasche Behebung, zu gewährleisten.

² Es werden automatisierte Auswertungen (u.a. zu Statistikzwecken) über die IT-Systeme erstellt. Die einzelnen Log-Informationen können personenbezogene Daten der Nutzenden (Netzwerk-Adresse, Benutzername) enthalten. Eine Unterscheidung hinsichtlich Protokollierung von privaten und im Zusammenhang mit dem Studium oder der Weiterbildung an der PHZH stehenden E-Mails findet aus technischen Gründen nicht statt.⁶

³ Zur Kontrolle der Einhaltung dieser Weisung und anderer Bestimmungen der geltenden Rechtsordnung kann die Rektorin oder der Rektor eine stichprobenweise Überprüfung der Protokollierungen durch die ID anordnen. Insbesondere kann sie oder er Aufschluss über die angewählten Internet-Adressen und soweit möglich über Zeitpunkt, Anzahl der Zugriffe und übertragenen Datenmengen verlangen. Die Berichte weisen auf mögliche Missbräuche hin. Das weitere Verfahren richtet sich nach § 22 Abs. 6 und 7.⁶

§ 22 Personenbezogene Auswertungen

¹ Im Falle eines Missbrauchs oder eines begründeten Verdachts eines Missbrauchs können personenbezogene Auswertungen vorgenommen werden. Nach Möglichkeit werden nur Randdaten (nicht der Inhalt von E-Mails oder Webseiten) ausgewertet.

² Der Entscheid zur Durchführung und zum Umfang (einschliesslich Ausdehnung auf Inhalte) einer personenbezogenen Auswertung wird von der Rektorin oder dem Rektor getroffen. Sie oder er kann insbesondere:

- a) eine Auswertung der verdächtigen Protokolle anordnen;
- b) für einen begrenzten Personenkreis eine zeitlich befristete Kontrolle für höchstens drei Monate veranlassen.⁶

³ Die Nutzenden werden auf die bevorstehende personenbezogene Auswertung hingewiesen.⁶

⁴ Die Rektorin oder der Rektor beauftragt die ID mit der Ausführung der Auswertung. Die oder der Data Protection Officer (DPO) ist zu informieren.⁶

⁵ Aufgehoben.⁶

⁶ Die Resultate der Auswertung werden ausschliesslich der Rektorin oder dem Rektor zugestellt. Diese oder dieser entscheidet unter Einbezug des DPO über die Durchführung weiterer Untersuchungen sowie die Anordnung von Disziplinar- und weiteren Massnahmen. Die betroffenen Personen werden über die sie betreffenden Ergebnisse der Auswertung informiert. Entgegenstehende kantonale oder eidgenössische Verfahrensbestimmungen bleiben vorbehalten.⁶

⁷ Verzichtet die Rektorin oder der Rektor auf die Durchführung weiterer Untersuchungen sowie auf die Anordnung von Massnahmen, werden die Auswertungen innert 30 Tagen vernichtet.

§ 22a⁶ Vorsorgliche Massnahmen

¹ Bei Störungen der Systeme oder Verdacht auf Handlungen, welche den Betrieb der PHZH oder deren Interessen erheblich beeinträchtigen und rasches Handeln erfordern, können die ID die betreffenden Nutzenden mittels Netzwerk-Adresse ermitteln, deren Zugangsberechtigung zu PHZH IT-

Mitteln ohne vorgängige Anhörung vorsorglich sperren sowie rechtswidrige und missbräuchliche Daten zu Beweis Zwecken sichern oder aus Sicherheitsgründen löschen. Sie benachrichtigen unverzüglich die Rektorin oder den Rektor sowie die betreffenden Nutzenden.

² Das weitere Verfahren richtet sich nach § 22 Abs. 6 und 7. Die Rektorin oder der Rektor kann die ID anweisen, eine vorsorgliche Sperrung aufzuheben, allenfalls unter Auflagen.

5. Abschnitt: Schlussbestimmungen

§ 23 Übergangsbestimmungen

Die Verwaltungsdirektion (ID und Business Applications) trifft zusammen mit den Prorektoraten Ausbildung sowie Weiterbildung und Forschung bis Ende 2010 die nötigen Vorkehrungen, um die Erklärungen gemäss § 4 von den Nutzenden einzuholen.¹

§ 24 Inkrafttreten

Diese Weisung tritt auf den 1. März 2010 in Kraft und wird im Internet publiziert.

¹ Fassung gemäss Beschluss der Hochschulleitung vom 29. August 2012, in Kraft seit 1. September 2012.

² Fassung gemäss Beschluss der Hochschulleitung vom 30. April 2014, in Kraft seit 1. Mai 2014.

³ Fassung gemäss Beschluss der Hochschulleitung vom 20. August 2014, in Kraft seit 1. September 2014.

⁴ Fassung gemäss Beschluss der Hochschulleitung vom 3. Juni 2015, in Kraft seit 1. Oktober 2015.

⁵ Fassung gemäss Beschluss der Hochschulleitung vom 9. November 2016, in Kraft seit 15. November 2016.

⁶ Fassung gemäss Beschluss der Hochschulleitung vom 27. November 2019, in Kraft seit 1. Januar 2020.