AMTLICHE MITTEILUNGEN

Hochschule Düsseldorf
University of Applied Sciences

Verkündungsblatt
der Hochschule Düsseldorf

HSD NR. 866

Das Verkündungsblatt der Hochschule
Herausgeberin: Die Präsidentin

24.11.2022
Nummer 866

IT-Ordnung der Hochschule Düsseldorf

Vom 24.11.2022

Aufgrund des § 2 Abs. 4 S. 1 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG) vom 16.09.2014 (GV. NRW. S. 547) in der aktuell gültigen Fassung hat die Hochschule Düsseldorf die folgende Ordnung als Satzung erlassen.

Inhaltsverzeichnis

§ 1 – GEGENSTAND UND GELTUNGSBEREICH

Diese IT-Ordnung regelt den Einsatz und die Nutzung von Informations-, Kommunikations- und vernetzter Medientechnik an der Hochschule Düsseldorf, soweit dazu ein allgemeiner Regelungsbedarf besteht. Sie regelt weiterhin die dabei erforderliche Zusammenarbeit der Organisationseinheiten und Gremien. Von der Ordnung erfasst werden

- der von der Campus IT oder anderen zentralen Einrichtungen verantwortete zentrale IT-Betrieb
- der von Fachbereichen, Instituten und anderen Einrichtungen verantwortete dezentrale IT-Betrieb und
- der Einsatz von Informations-, Kommunikations- und vernetzter Medientechnik in Forschung und Lehre, entweder als deren Gegenstand oder als Werkzeug zu ihrer (fachbezogenen) Unterstützung.

§ 2 – BEGRIFFSBESTIMMUNGEN

(1) Ein IT-System dient der digitalen Verarbeitung von Daten und Informationen. 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.

(2) Ein IT-Dienst wird auf der Basis eines IT-Systems oder mehrerer IT-Systeme realisiert und Nutzungsberechtigten gemäß § 9 zur Verfügung gestellt.

(3) Die IT-Infrastruktur der HSD besteht aus technischen, organisatorischen, finanziellen und personellen IT-Ressourcen. Zu den technischen Ressourcen gehören Rechnernetze, Computerhardware, Computersoftware und sonstige IT-Systeme – als Komponenten der IT-Infrastruktur – die an der HSD 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.

(4) Arbeitsprozesse, die eine arbeitsorganisatorisch abgeschlossene Einheit bilden und ein gemeinsames Ziel haben, bilden ein Verfahren. Ein durch IT unterstütztes Verfahren, das automatisiert Daten verarbeitet, wird im Sinne dieser Ordnung als IT-Verfahren bezeichnet.

§ 3 – AUFGABENPROFILE

(1) Verfahrensverantwortliche sind für die Einführung und den ordnungsgemäßen Einsatz der jeweiligen IT-Verfahren und den Betrieb der zugehörigen IT-Systeme sowie deren informationstechnische Belange verantwortlich.

a) Verfahrensverantwortliche stellen die Umsetzung und Dokumentation geeigneter technischer und organisatorischer Maßnahmen zur Informationssicherheit, die entsprechend dem Schutzbedarf der verarbeiteten Daten und Informationen ausgewählt werden, sicher. Dazu stimmen sie sich in der Regel mit dem oder der Chief Information Security Officer ab. Sie überprüfen die Einhaltung aller informationsrechtlichen Regelungen für das Verfahren.

b) Sie setzen ebenfalls geeignete technische und organisatorische Maßnahmen zum Datenschutz um, falls personenbezogene Daten verarbeitet werden. Dabei beachten sie die Risiken für die Rechte und Freiheiten der betroffenen Personen. Sie sind verantwortlich für die Aufnahme in die datenschutzrechtlich vorgesehenen Dokumentationen und stimmen sich nötigenfalls mit dem oder der Datenschutzbeauftragten ab.

c) Sie unterstützen die Information und Beteiligung der Personalräte durch die dafür zuständigen Stellen innerhalb der Hochschule.

d) Sie erteilen den technischen Administratorinnen und Administratoren sowie den Fachadministratorinnen und -administratoren die erforderlichen Weisungen.

(2) Fachadministratorinnen und -administratoren sind für die fachliche Betreuung eines IT-Verfahrens zuständig.

(3) Technische Administratorinnen bzw. -administratoren sind Personen, die für den technischen Betrieb eines IT-Systems zuständig sind.

§ 4 – GRUNDSÄTZE DES IT-BETRIEBES

(1) Zum IT-Betrieb gehört die zur Aufrechterhaltung des Hochschulbetriebs eingesetzte IT-Infrastruktur.

(2) Die Sicherstellung des IT-Betriebs – in der Regel durch zentrale IT-Systeme und -Dienste –, der Informationssicherheit und des Datenschutzes sind grundsätzlich Aufgabe des Präsidiums.

(3) Ein dezentraler IT-Betrieb ist mit Zustimmung der Hochschulleitung möglich, wenn die betreffenden Dienstleistungen, Anwendungen und Infrastrukturen wirtschaftlicher und/oder zweckmäßiger durch dezentrale Einheiten wie Fachbereiche, Institute oder andere Einrichtungen geleistet werden können. Die betreffenden Einrichtungen sind verfahrensverantwortlich gemäß § 3 Abs. 1, sie tragen darüber hinaus die finanzielle Verantwortung für die von ihnen betriebenen IT-Systeme.

(4) Sofern Schnittstellen zwischen zentralen und dezentralen IT-Systemen erforderlich sind, müssen diese vor einer Zustimmung der Hochschulleitung zum dezentralen IT-Betrieb zwischen der für die betroffenen zentralen IT-Systeme verantwortlichen Einrichtung und der für das beantragte dezentrale IT-System verantwortlichen Einrichtung vereinbart werden.

(5) Sollten Systeme des dezentralen IT-Betriebs den zentralen IT-Betrieb beeinträchtigen, so wird die für den zentralen IT-Betrieb verantwortliche Einrichtung angemessen reagieren. Als Ultima Ratio ist die für den zentralen IT-Betrieb verantwortliche Einrichtung zur Sperrung der betreffenden dezentralen Systeme berechtigt.

§ 5 – IT IN FORSCHUNG UND LEHRE

(1) Der Einsatz von IT-, Kommunikations- und vernetzter Medientechnik entweder als Gegenstand von Forschung und Lehre oder als Werkzeug zur (fachbezogenen) Unterstützung von Forschung und Lehre ist nicht genehmigungspflichtig, falls sie in der Verantwortung einzelner Lehrender oder wissenschaftlicher Einrichtungen i.S.d. § 29 Abs. 1 HG NRW betrieben wird. Dieser Einsatz muss aber gegenüber der Hochschulleitung angezeigt werden, sofern eine technische Verbindung zu Systemen des zentralen oder dezentralen IT-Betriebs besteht. Die Campus IT wird von der Hochschulleitung informiert. Die Forschenden bzw. Lehrenden sind für von ihnen eingesetzte IT verfahrensverantwortlich gemäß § 3 Abs. 1.

(2) Sofern Schnittstellen zwischen Systemen des IT-Betriebs und IT-Systemen in Forschung und Lehre erforderlich sind, müssen diese möglichst frühzeitig vor Einsatz zwischen der/dem Verfahrensverantwortlichen im Betrieb und den Forschenden bzw. Lehrenden vereinbart und in die Anzeige gegenüber dem Präsidium gemäß Abs. 1 aufgenommen werden.

(3) Sollten IT-Systeme in Forschung und Lehre den IT-Betrieb beeinträchtigen, so wird die jeweils verfahrensverantwortliche Einrichtung, die das gestörte System betreibt, angemessen reagieren. Als Ultima Ratio ist sie zur Sperrung der betreffenden Systeme berechtigt.

§ 6 – RECHTSSTELLUNG UND AUFGABEN DER CAMPUS IT

(1) Die Campus IT (CIT) ist eine zentrale Betriebseinheit i.S.d. § 29 Abs. 2 HG NRW der Hochschule Düsseldorf. Sie übernimmt für die Hochschule die Durchführung von Datenverarbeitungsaufgaben und die rechnergestützte Informationsverarbeitung. Im Rahmen von Kooperationsvereinbarungen kann die CIT auch Aufgaben für Dritte im Rahmen der gesetzlichen Aufgaben der Hochschule wahrnehmen.

(2) Der CIT obliegen insbesondere folgende Aufgaben:

a) Planung, Realisierung und Betrieb der zentralen Unterstützung für Aufgaben in Lehre und Studium, wissenschaftliche Weiterbildung, Forschung und Transfer sowie Verwaltung durch IT-, Kommunikations- und vernetzte zentrale Medientechnik

b) Betreuung der IT-Infrastruktur und die betriebsfachliche Aufsicht über alle IT-Systeme in der HSD, soweit dies nicht Aufgabe anderer Organisationseinheiten oder Einrichtungen der HSD ist

c) Koordinierung der Beschaffung von zentraler IT in der HSD und optionale Beratung bei der Beschaffung dezentraler IT

d) Erwerb, Verwaltung, Dokumentation, Pflege und Weiterentwicklung von campusweit zur Verfügung gestellter Software sowie Beratung bei Auswahl und Einsatz der in der Hochschulverwaltung eingesetzten Software

e) Beratung und Unterstützung (1st-Level-Support) der Nutzer*innen

f) Fachliche Administration zentraler Anwendungs-Systeme, soweit dies nicht Aufgabe anderer Organisationseinheiten oder Einrichtungen der HSD ist

g) Mitwirkung bei Projekten und Übernahme von Serviceaufgaben für IT-gestützte Lösungen, die den Betrieb der HSD fördern und erleichtern.

(3) Die CIT ist überdies für die Planung, Installation und den Betrieb rechnergestützter Informations- und Kommunikationsnetze zuständig.

(4) Zur Gewährleistung eines ordnungsgemäßen Betriebes des Informations- und Kommunikationsnetzes sowie der Datenverarbeitungssysteme, die der CIT zugeordnet sind, kann die Leitung der CIT ergänzende Regeln zu dieser Ordnung erlassen, wie z. B. technisch-organisatorische Vorgaben zum Betrieb des Datennetzes oder Betriebsregelungen für Veröffentlichungen auf Servern der CIT.

§ 7 – IT-KOMMISSION

(1) Die IT-Kommission der HSD setzt sich zusammen aus

a) dem für den IT-Betrieb zuständigen Mitglied des Präsidiums (Vorsitz),

b) der Leitung der Campus IT bzw. der/dem CIO,

c) je einer Vertreterin oder einem Vertreter jedes Fachbereiches, der/die durch den Fachbereichsrat oder nach einem entsprechenden Beschluss des Fachbereichsrates durch den Dekan oder die Dekanin benannt wird, die Benennung bzw. der Beschluss soll in der konstituierenden Sitzung des Fachbereichsrates erfolgen,

d) einer Vertreterin oder einem Vertreter der Hochschulverwaltung, die oder der vom Präsidium benannt wird,

e) einer Vertreterin oder einem Vertreter der Hochschulbibliothek, die oder der vom Leiter oder von der Leiterin der Hochschulbibliothek benannt wird,

f) einer Vertreterin oder einem Vertreter der Studierenden, die oder der vom AStA benannt wird und

g) dem oder der Chief Information Security Officer (CISO).

(2) Die Personalräte erhalten die Einladungen, Protokolle und Beratungsunterlagen der Kommission und können an den Sitzungen beratend teilnehmen.

(3) Die Mitglieder der IT-Kommission können für einzelne Sitzungen einen Vertreter oder eine Vertreterin benennen.

(4) Die IT-Kommission wählt aus ihrer Mitte eine Stellvertreterin oder einen Stellvertreter der oder des Vorsitzenden. Die Amtszeit beträgt vier Jahre.

(5) Die Aufgaben der IT-Kommission sind in der Grundordnung geregelt.

(6) Die Amtszeit der Mitglieder der IT-Kommission beträgt vier Jahre. Davon abweichend beträgt die Amtszeit der Vertreterin oder des Vertreters der Studierenden zwei Jahre.

(7) Die Hochschulleitung stellt den Mitgliedern der IT-Kommission auf Anfrage alle Informationen zur Verfügung, die für die Erstellung von sachgerechten Empfehlungen erforderlich sind.

§ 8 – Erteilung von Zugriffsberechtigungen auf Datenablagen

In netzbasierten Portalen regeln den Zugang zu Ordnern zur Dateiablage, Webseiten und anderen Inhalten ausschließlich:

a) für persönliche Webseiten, E-Mail-Postfächer und Ordner die jeweilige Person,

b) für Forschungsprojekte, Forschungsstellen und Forschungsschwerpunkte die jeweiligen verantwortlichen Forschenden,

c) für Studiengänge, Lehrbereiche, Lehrprojekte, Labore und Lehrveranstaltungen die jeweiligen verantwortlichen Lehrenden,

d) für Personal- und für weitere Interessenvertretungen die jeweilige Personal- oder Interessenvertretung,

e) für Beratungsstellen für Studierende und Beschäftigte die jeweiligen Beratenden,

f) für den Bereich Datenschutz der oder die Datenschutzbeauftragte,

g) für Institute und zentrale Einrichtungen der oder die jeweilige Leiter oder Leiterin,

h) für übergreifende Webseiten und Ordner einzelner Fachbereiche die jeweiligen Dekanate,

i) für Organe und Gremien der Hochschule und der Studierendenschaft die oder der Vertretungsberechtigte.

Den Zugriff auf zentrale, übergreifende Webseiten und Ordner regelt das Präsidium. Es kann diese Kompetenz an die Leitungen der Dezernate, zentralen Betriebseinheiten und Stabsstellen delegieren.

§ 9 – Nutzungsberechtigte und Zulassung zur Nutzung

(1) Zur Nutzung der IT-Infrastruktur der Hochschule Düsseldorf sind Studierende, Beschäftigte und Lehrbeauftragte der HSD sowie Gäste der Hochschulbibliothek zugelassen. Die Zulassung von weiteren Personen steht im pflichtgemäßen Ermessen der Hochschulleitung.

(2) Die Hochschule behält sich ausdrücklich vor, den Kreis der Nutzerinnen und Nutzer allgemein oder begrenzt auf einzelne Dienste einzuschränken. Dies kann insbesondere aufgrund vertraglicher Verpflichtungen der Hochschule beim Bezug einzelner Dienste erfolgen, die eine Beschränkung erforderlich machen.

(3) Die Zulassung erfolgt ausschließlich zur Erfüllung der gesetzlichen Aufgaben der HSD, insbesondere zur Teilnahme und Durchführung der Lehre, zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, zur Aus- und Weiterbildung sowie zur Erfüllung sonstiger Aufgaben der Hochschule Düsseldorf. Eine hiervon abweichende Nutzung ist zugelassen, wenn die abweichende Nutzung geringfügig ist, sie keinen gesetzlichen oder vertraglichen Verpflichtungen der Hochschule zuwiderläuft und die Zweckbestimmung der Hochschule sowie die Belange der anderen Nutzerinnen und Nutzer nicht beeinträchtigt werden.

(4) Den unter Absatz 1 genannten Personen wird automatisch eine Zulassung erteilt, falls es technische Verfahren gibt, die dies unterstützen. Anderenfalls erfolgt sie durch Antrag an die für die zu nutzenden IT-Dienste verfahrensverantwortlichen Einrichtungen.

(5) Der Antrag soll folgende Angaben enthalten:

a) Name, Anschrift und Unterschrift der Antragstellerin oder des Antragstellers sowie ihren oder seinen Status im Sinne von § 2 Abs. 1;
b) Beschreibung des Nutzungszwecks bzw. des geplanten Vorhabens;
c) Erklärung zur Verarbeitung personenbezogener Daten durch die Nutzerin oder den Nutzer;
d) Anerkennung dieser Ordnung sowie ggf. spezieller Regelungen für einzelne IT-Dienste oder IT-Systeme als Grundlage des Nutzungsverhältnisses;
e) Hinweis auf die Möglichkeiten einer Dokumentation des Nutzungsverhaltens und der Einsichtnahme in die Nutzungsdateien nach Maßgabe dieser Ordnung (vgl. § 11);

(6) Eine Nutzungserlaubnis kann auf bestimmte Dienste beschränkt werden und kann zeitlich befristet werden.

(7) Zur Gewährleistung eines ordnungsgemäßen und störungsfreien Betriebs und bei begrenzter Kapazität der IT-Systeme kann die Nutzungserlaubnis überdies mit einer Begrenzung der Rechen- und Onlinezeit sowie mit anderen nutzungsbezogenen Bedingungen und Auflagen verbunden werden. Eine Priorisierung der Nutzungen erfolgt durch eine Abwägung der jeweiligen Interessen der betroffenen Nutzer und Nutzerinnen und der Hochschule.

(8) Die verfahrensverantwortliche Einrichtung kann die Zulassung zur Nutzung überdies vom Nachweis bestimmter Kenntnisse über die Benutzung der gewünschten Datenverarbeitungssysteme und IT-Systeme abhängig machen.

§ 10 – ALLGEMEINE NUTZUNGSREGELN

(1) Die Nutzerinnen und Nutzer haben das Recht, die IT-Infrastruktur der Hochschule im Rahmen der Zulassung und nach Maßgabe dieser Benutzungsordnung sowie ggf. spezieller Regelungen für einzelne IT-Dienste oder IT-Systeme zu nutzen. Eine hiervon abweichende Nutzung bedarf einer gesonderten Zulassung. Ein Anspruch auf ununterbrochenen und störungsfreien Zugang zu den IT-Diensten der Hochschule sowie auf unveränderte Fortführung des Leistungsangebots erwächst daraus nicht.

(2) Nutzerinnen und Nutzer sind verpflichtet,

(Allgemein)

a) die Vorgaben dieser Ordnung und den weiteren Richtlinien zur Nutzung der IT zu beachten und die Grenzen der Nutzungserlaubnis einzuhalten, insbesondere die Nutzungszwecke nach § 9 Abs. 3 zu beachten;

b) alles zu unterlassen, was den ordnungsgemäßen Betrieb der IT-Systeme der Hochschule Düsseldorf stört;

c) alle IT-Systeme und sonstigen Einrichtungen der Hochschule sorgfältig und schonend zu behandeln;

(Umgang mit Authentifizierungsmedien – Passwörter, Smartcards, u.a.)

d) ausschließlich mit den Authentifizierungsmedien, z.B. Benutzerkennung und Passwörter, zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde;

e) dafür Sorge zu tragen, dass keine anderen Personen Kenntnis von bzw. Zugang zu den Authentifizierungsmedien erlangen, sowie Vorkehrungen zu treffen, damit unberechtigten Personen der Zugang zu den Ressourcen der IT-Systeme der Hochschule verwehrt wird; dazu gehört auch der Schutz des Zugangs durch ein geheim zu haltendes und geeignetes, d.h. nicht einfach zu erratendes Passwort;

f) fremde Authentifizierungsmedien weder zu ermitteln noch zu nutzen;

g) keinen unberechtigten Zugriff auf Daten anderer Nutzerinnen und Nutzer zu nehmen und bekanntgewordene Daten anderer Nutzerinnen und Nutzer nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern;

(Softwarenutzung, Urheberrechte, Datenschutz)

h) bei der Benutzung von Software, Dokumentationen, elektronischen Büchern/Zeitschriften und anderen Daten die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten von der Hochschule zur Verfügung gestellt werden, zu beachten;

i) die nationalen und internationalen Urheber-, Marken-, Patent-, Namens- und Kennzeichenrechte sowie sonstige gewerbliche Schutzrechte und Persönlichkeitsrechte Dritter bei der Nutzung der Dienste zu wahren. Das Abrufen, Anbieten, Hochladen oder Verbreiten von rechtswidrigen Inhalten, insbesondere solchen, die gegen strafrechtliche, datenschutzrechtliche, persönlichkeitsrechtliche, lizenzrechtliche, oder urheberrechtliche Bestimmungen verstoßen, ist unzulässig;

j) von der Hochschule bereitgestellte Software, sowie die Software, die zum Betrieb der Dienste dient, Dokumentationen und Daten weder zu kopieren noch an Dritte weiterzugeben, sofern dies nicht ausdrücklich erlaubt ist, noch zu anderen als den erlaubten Zwecken zu nutzen;

(Nutzung der IT-Dienste der Hochschule)

k) die Benutzungsberechtigung auf Verlangen nachzuweisen;

l) Störungen, Beschädigungen und Fehler an IT-Systemen und Datenträgern der Hochschule nicht selbst zu beheben, sondern unverzüglich dem Personal der Hochschule zu melden;

m) ohne ausdrückliche Einwilligung der Hochschule keine Eingriffe in die Hardwareinstallation der Hochschule vorzunehmen und die Konfiguration der Betriebssysteme, der Systemdateien, der systemrelevanten Nutzerdateien und des Netzwerks nicht zu verändern;

(E-Mail)

n) Studierende sind im Rahmen ihres Studiums zur Nutzung der zentral angebotenen IT-Dienste und im E-Mailverkehr zur Nutzung von E-Mailadressen der Hochschule Düsseldorf verpflichtet. Gleiches gilt für Bedienstete im Rahmen ihrer Dienstaufgaben.

(Sonstiges)

o) dem Leiter oder der Leiterin der verfahrensverantwortlichen Einrichtung unter Beteiligung der oder des Chief Information Security Officer auf Verlangen in begründeten Einzelfällen – insbesondere zur Störungsbeseitigung – zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu erteilen sowie Einsicht in die Programme zu gewähren;

p) eine Verarbeitung personenbezogener Daten mit der zuständigen Stelle in der Hochschule abzustimmen und – unbeschadet der eigenen datenschutzrechtlichen Verpflichtungen der Nutzerin oder des Nutzers – die von der Hochschule vorgeschlagenen Datenschutz- und Datensicherheitsvorkehrungen zu berücksichtigen.

(3) Auf die folgenden Straftatbestände wird besonders hingewiesen:

a) Ausspähen von Daten (§ 202a StGB);

b) Abfangen von Daten (§ 202b StGB);

c) Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB);

d) Datenhehlerei (§ 202d StGB)

e) Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB);

f) Computerbetrug (§ 263a StGB);

g) Verbreitung pornographischer Darstellungen (§§ 184 ff. StGB), insbesondere Verbreitung, Erwerb und Besitz kinderpornographischer Schriften (§ 184b StGB) und die Verbreitung pornographischer Darbietungen durch Rundfunk oder Telemedien (§ 184d StGB);

h) Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB);

i) Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB);

j) Strafbare Urheberrechtsverletzungen, z. B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG).

§ 11 – IT-MONITORING

(1) Die Verfahrensverantwortlichen sind nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der von ihnen betriebenen IT-Systeme durch die einzelnen Nutzerinnen und Nutzer zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist:

a) zur Gewährleistung eines ordnungsgemäßen Systembetriebs,

b) zur Ressourcenplanung und Systemadministration,

c) zum Schutz der personenbezogenen Daten anderer Nutzerinnen und Nutzer,

d) zu Abrechnungszwecken,

e) für das Erkennen und Beseitigen von Störungen,

f) zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

Soweit eine personalisierte Auswertung für den jeweiligen Zweck nicht erforderlich ist und soweit technisch möglich erfolgt diese Auswertung anonymisiert oder pseudonymisiert.

(2) Die Verfahrensverantwortlichen sind berechtigt, Technologien einzusetzen, mit denen die Aktivitäten in von ihnen betriebenen Netzwerken analysiert und visualisiert werden können. Dies erfolgt in pseudonymisierter Form. Die Daten dürfen nur in den folgenden Fällen auf Personen bezogen werden:

a) im Falle rechtmäßiger Anfragen von Ermittlungsbehörden; oder

b) im Falle von Abs. 1 lit. a, e und f.

(3) Unter den Voraussetzungen von Absatz 1 lit. a, e und f sind die Verfahrensverantwortlichen auch berechtigt, unter Beachtung der Datenschutz-Grundverordnung Einsicht in die Nutzungsdaten der von ihnen betriebenen IT-Systeme zu nehmen, soweit dies erforderlich ist zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Missbräuchen, sofern hierfür tatsächliche Anhaltspunkte vorliegen. Eine Einsichtnahme in Nachrichten- und E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung aktueller Störungen im Nachrichtendienst unerlässlich ist. In jedem Fall ist die Einsichtnahme von zwei Beschäftigten zu dokumentieren, und die betroffene Nutzerin oder der betroffene Nutzer ist nach Abschluss der Auswertung unverzüglich zu benachrichtigen.

(4) Unter den Voraussetzungen von Absatz 1 können auch die Verkehrs- und Nutzungsdaten im Nachrichtenverkehr (insbes. E-Mail-Nutzung) dokumentiert werden. Es dürfen jedoch nur die näheren Umstände der Telekommunikation – nicht aber die nichtöffentlichen Kommunikationsinhalte – erhoben, verarbeitet und genutzt werden. Die Verkehrs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Telemediendiensten, die durch Einrichtungen der HSD zur Nutzung bereitgehalten oder zu denen der Zugang durch Einrichtungen der HSD vermittelt wird, sind frühestmöglich, spätestens unmittelbar am Ende der jeweiligen Nutzung, zu löschen, soweit es sich nicht um Abrechnungsdaten handelt.

(5) Nach Maßgabe der gesetzlichen Bestimmungen sind die Verfahrensverantwortlichen zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet.

§ 12 – VERSAGUNG, AUSSCHLUSS UND BESCHRÄNKUNG DER NUTZUNG

(1) Die Nutzungserlaubnis kann ganz oder teilweise versagt bzw. Nutzerinnen und Nutzer können vorübergehend oder dauerhaft in der Benutzung der IT-Dienste bzw. der ihnen zu Grunde liegenden IT-Systeme beschränkt oder hiervon ausgeschlossen werden, wenn

a) kein ordnungsgemäßer Antrag vorliegt oder die Angaben im Antrag nicht oder nicht mehr zutreffen;
b) die Voraussetzungen für eine ordnungsgemäße Benutzung der IT-Dienste nicht oder nicht mehr gegeben sind;
c) das geplante Vorhaben der Nutzerin oder des Nutzers nicht mit den Aufgaben der Hochschule vereinbar ist;
d) die vorhandenen Ressourcen der IT-Dienste für die beantragte Nutzung ungeeignet oder für besondere Zwecke reserviert sind;
e) die Kapazität der Ressourcen der IT-Dienste, deren Nutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die geplante Nutzung nicht ausreicht;
f) die zu benutzenden IT-Dienste in Verbindung mit einem Netz stehen, das besonderen Datenschutzerfordernissen genügen muss, und kein sachlicher Grund für die geplante Nutzung ersichtlich ist;
g) zu erwarten ist, dass durch die beantragte Nutzung andere berechtigte Vorhaben in unangemessener Weise beeinträchtigt werden;
h) sie schuldhaft gegen diese Benutzungsordnung, insbesondere gegen die in § 10 aufgeführten Pflichten, verstoßen (missbräuchliches Verhalten) oder
i) sie die IT-Dienste der Hochschule für strafbare Handlungen missbrauchen oder
j) der Hochschule durch sonstiges rechtswidriges Nutzerverhalten Nachteile entstehen. Hierdurch werden alle sonstigen rechtswidrigen Verhaltensweisen auch außerhalb des Strafrechts erfasst, z.B. Urheberrechts- oder Markenrechtsverletzungen. Ein Nutzungsausschluss wegen eines entsprechenden (rein zivilrechtswidrigen) Verhaltens kommt jedoch nur in Betracht, wenn die Hochschule hiervon selbst betroffen ist, z.B. in Form einer Abmahnung, Unterlassungserklärung oder Schadensersatzforderung.

(2) Maßnahmen nach Abs. 1 sollen erst nach vorheriger erfolgloser Abmahnung erfolgen. Dies gilt nicht für Gefahr im Verzug. Hierüber ist der oder die Betroffene unverzüglich zu informieren. Dem oder der Betroffenen ist Gelegenheit zur Stellungnahme zu geben. In jedem Fall ist ihm oder ihr Gelegenheit zur Sicherung seiner oder ihrer Daten einzuräumen.

(3) Vorübergehende Nutzungsbeschränkungen, über die die Leitung der verfahrensverantwortlichen Einrichtung, die den genutzten IT-Dienst betreibt, entscheidet, sind aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet erscheint.

(4) Eine dauerhafte Nutzungsbeschränkung oder der vollständige Ausschluss einer Nutzerin oder eines Nutzers von der weiteren Nutzung kommt nur bei schwerwiegenden und/oder wiederholten Verstößen i.S.v. Abs. 1 in Betracht, wenn auch künftig ein ordnungsgemäßes Verhalten nicht mehr zu erwarten ist. Die Entscheidung über eine dauerhafte Nutzungseinschränkung trifft das Präsidium auf Antrag der Leitung der verfahrensverantwortlichen Einrichtung durch Verwaltungsakt. Mögliche Ansprüche der Hochschule aus dem Nutzungsverhältnis bleiben unberührt.

§ 13 – HAFTUNG DER NUTZERINNEN UND NUTZER

(1) Die Nutzerinnen und Nutzer haften für alle Nachteile, die der Hochschule durch missbräuchliche oder rechtswidrige Verwendung der IT-Dienste und der Nutzungsberechtigung oder dadurch entstehen, dass die Nutzerin oder der Nutzer schuldhaft ihren oder seinen Pflichten aus dieser Ordnung nicht nachkommt.

(2) Die Nutzerinnen und Nutzer haften auch für Schäden, die im Rahmen der ihr oder ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn sie/er diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe ihrer/seiner Benutzerkennung an Dritte. Die Nutzerin oder der Nutzer stellt die Hochschule im Falle einer Drittnutzung von den dadurch entstehenden Schäden in vollem Umfang frei.

(3) Die Nutzerinnen und Nutzer stellen die Hochschule von allen Ansprüchen frei, wenn Dritte die Hochschule wegen eines missbräuchlichen oder rechtswidrigen schuldhaften Verhaltens der Nutzerin oder des Nutzers auf Schadensersatz in Anspruch nehmen. Die Hochschule wird der Nutzerin oder dem Nutzer den Streit verkünden, sofern Dritte auf Grund dieser Ansprüche gegen die Hochschule gerichtlich vorgehen.

(4) Die beamtenrechtliche Haftung von Beschäftigten bleibt unberührt.

§ 14 – HAFTUNG DER HOCHSCHULE

(1) Die Hochschule übernimmt keine Gewährleistung und Garantie dafür, dass IT-Dienste fehlerfrei und jederzeit ohne Unterbrechung verfügbar sind. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.

(2) Die Hochschule übernimmt keine Verantwortung für die Richtigkeit der zur Verfügung gestellten Programme. Die Hochschule haftet auch nicht für den Inhalt, insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang zur Nutzung vermittelt.

(3) Die Hochschule übernimmt keine Verantwortung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer fahrlässigen Pflichtverletzung der Nutzerin oder des

Nutzers oder einer vorsätzlichen oder fahrlässigen Pflichtverletzung eines gesetzlichen Vertreters oder einer gesetzlichen Vertreterin oder Erfüllungsgehilfen der Nutzerin oder des Nutzers beruhen.

(4) Die Hochschule haftet gegenüber Dritten nur bei Vorsatz und grober Fahrlässigkeit ihrer Mitarbeiter oder ihrer Mitarbeiterinnen.

(5) Mögliche Amtshaftungsansprüche gegen die Hochschule bleiben von den vorstehenden Regelungen unberührt.

§ 15 – WEITERE REGELUNGEN

(1) Datenschutz und Informationssicherheit werden an der HSD gemäß der Leitlinie für Datenschutz und Informationssicherheit (DIS-Leitlinie) und mit dem darin verankerten Datenschutz- und Informationssicherheits-Management-Systems (DISM) gestaltet.

(2) Für alle IT-Verfahren geltende Grundsätze regelt die mit den Personalvertretungen geschlossene IT-Rahmendienstvereinbarung.

§ 16 – IN-KRAFT-TRETEN, AUSSER-KRAFT-TRETEN

Diese IT-Ordnung tritt am Tag nach ihrer Veröffentlichung im Verkündungsblatt der Hochschule Düsseldorf in Kraft. Gleichzeitig tritt die IT-Benutzungsordnung der Fachhochschule Düsseldorf vom 14.02.2012 (Verkündungsblatt der Hochschule Düsseldorf, Amtliche Mitteilung Nr. 288) außer Kraft.

Ausgefertigt aufgrund der Beschlüsse des Präsidiums der Hochschule Düsseldorf vom 17.08.2022 und des Senats der Hochschule Düsseldorf vom 05.07.2022.

Düsseldorf, den 24.11.2022

gez.
Die Präsidentin
der Hochschule Düsseldorf
Prof. Dr. Edeltraud Vomberg

HINWEIS AUF DIE RECHTSFOLGEN NACH § 12 ABS. 5 HG

Nach Ablauf eines Jahres seit der Bekanntgabe dieser Ordnung kann die Verletzung von Verfahrens- oder Formvorschriften des Hochschulgesetzes oder des Ordnungs- oder des sonstigen autonomen Rechts der Hochschule Düsseldorf nur unter den Voraussetzungen des § 12 Abs. 5 Nr. 1 - 4 HG geltend gemacht werden; ansonsten ist eine Rüge ausgeschlossen.