

# FH-Mitteilungen

22. Mai 2015

Nr. 26 / 2015

---

## Netzordnung der Fachhochschule Aachen

vom 22. Mai 2015

# Netzordnung der Fachhochschule Aachen

vom 22. Mai 2015

---

Aufgrund des § 2 Absatz 4 Satz 1 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG) vom 16. September 2014 (GV. NRW. S. 547) hat der Senat der Fachhochschule Aachen die folgende Netzordnung für den Betrieb und die Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur der Hochschule (Hochschul-IT) als Satzung beschlossen:

## Inhaltsübersicht

Präambel	2
§ 1   Geltungsbereich	2
§ 2   Rechtsstellung und Organisation der Datenverarbeitungszentrale	2
§ 3   Aufgaben der DVZ	3
§ 4   Nutzungsberechtigung	3
§ 5   Zulassung zur Nutzung	3
§ 6   Widerruf der Nutzung	4
§ 7   Ausschluss von der Nutzung	4
§ 8   Rechte und Pflichten der Nutzer und Nutzerinnen	4
§ 9   Rechte und Pflichten der DVZ	5
§ 10   Dokumentation und Auswertung	5
§ 11   Einsicht in die Benutzerdateien	6
§ 12   Haftung des Nutzers oder der Nutzerin	6
§ 13   Haftung der Hochschule	6
§ 14   Inkrafttreten, Veröffentlichung	7

## Präambel

Diese Netzordnung soll die möglichst störungsfreie, ungehinderte und sichere Nutzung der Hochschul-IT gewährleisten. Die Netzordnung orientiert sich an den gesetzlich festgelegten Aufgaben der Hochschule sowie an ihrem Mandat zur Wahrung der akademischen Freiheit. Sie stellt Grundregeln für einen ordnungsgemäßen Betrieb der IT-Infrastruktur auf und regelt so das Nutzungsverhältnis zwischen den einzelnen Nutzern und der Hochschule.

## § 1 | Geltungsbereich

Diese Benutzungsordnung gilt für die Nutzung der Informationsverarbeitungsinfrastruktur der Hochschule, bestehend aus den Datenverarbeitungsanlagen, Kommunikationssystemen und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung.

## § 2 | Rechtsstellung und Organisation der Datenverarbeitungszentrale

(1) Die Datenverarbeitungszentrale (DVZ) ist eine zentrale Betriebseinheit der Hochschule gemäß § 29 Absatz 2 Hochschulgesetz NRW. Sie unterstützt die Hochschule bei der Durchführung von Datenverarbeitungsaufgaben und bei der rechnergestützten Informationsverarbeitung.

(2) Die DVZ untersteht als zentrale Betriebseinheit dem Rektor oder der Rektorin. Sie ist als nicht stimmberechtigtes Mitglied im Senat vertreten. Sie leitet die EDV-AG, in der die IT-Administratoren und IT-Administratorinnen (EDV-Ansprechpartner und EDV-Ansprechpartnerinnen) aller Bereiche der Hochschule vertreten sind. Der DVZ-Leiter oder die DVZ-Leiterin ist Mitglied des Sicherheitsmanagementteams (IS-Team).

## § 3 | Aufgaben der DVZ

(1) Der DVZ obliegen insbesondere folgende Aufgaben:

1. Die Planung, Realisierung und der Betrieb der Datenverarbeitungsanlagen der DVZ für Aufgaben in Lehre, Forschung, Studium und Verwaltung.
2. Die Betreuung der für die Hochschule verfügbaren Datenverarbeitungsressourcen und die betriebsfachliche Aufsicht über alle Datenverarbeitungsanlagen in der Hochschule.
3. Die Abstimmung und Genehmigung des Betriebs von Datenverarbeitungsanlagen/Ressourcen durch andere Organisationseinheiten.
4. Die Koordinierung der Beschaffung von Datenverarbeitungsanlagen in der Hochschule, insbesondere Stellungnahme zu Investitionsmaßnahmen in Datenverarbeitungssysteme, Nutzungsanalysen vorhandener Systemkomponenten und Bedarfsplanung.
5. Die Auswahl, der Erwerb, die Verwaltung, Dokumentation, Pflege und Weiterentwicklung der Softwaregrundversorgung (Betriebssystem und Bürosoftware), insbesondere Hochschul- und Campuslizenzen.
6. Die Unterweisung, Beratung und Unterstützung der EDV-Ansprechpartner und EDV-Ansprechpartnerinnen, welche für die Anwenderbetreuung zuständig sind.
7. Die Unterstützung der EDV-Ansprechpartner und EDV-Ansprechpartnerinnen bei der Durchführung von Schulungs- und Fortbildungsmaßnahmen sowie IT-gestützten Lehrveranstaltungen für Angehörige der Hochschule.

(2) Die DVZ ist überdies für die Planung, Installation und den Betrieb rechnergestützter Informations- und Kommunikationsnetze einschließlich der erforderlichen zentralen Server sowie der Datenkommunikationssysteme zuständig. Diesbezüglich obliegen ihr insbesondere folgende Aufgaben:

1. Bereitstellung und Aufrechterhaltung eines störungsfreien und möglichst ununterbrochenen Betriebes des Kommunikationsnetzes;
2. Koordination des Ausbaus und der Wartung des Kommunikationsnetzes;
3. Verwaltung der Adress- und Namensräume;
4. Bereitstellung von Netzwerkdiensten und zentralen Netzwerk-Servern;
5. Unterstützung der EDV-Ansprechpartner und EDV-Ansprechpartnerinnen bei der Nutzerbetreuung.

(3) Zur Gewährleistung eines ordnungsgemäßen Betriebes des Informations- und Kommunikationsnetzes kann der Leiter oder die Leiterin der DVZ weitere Regeln für die Nutzung der DV-Anlagen erlassen.

## § 4 | Nutzungsberechtigung

(1) Zur Nutzung der Dienste der Hochschul-IT sind berechtigt:

1. Mitglieder, Angehörige und Einrichtungen einschließlich der Verwaltung der Hochschule
2. Beauftragte der Hochschule zur Erfüllung ihrer Dienstaufgaben
3. Mitglieder und Angehörige anderer Hochschulen des Landes NRW oder staatlichen Hochschulen außerhalb des Landes NRW aufgrund besonderer Vereinbarungen
4. Sonstige staatliche Forschungs- und Bildungseinrichtungen und Behörden des Landes NRW aufgrund besonderer Vereinbarungen
5. Studentenwerk Aachen
6. Kooperationspartner und Kooperationspartnerinnen im Rahmen vertraglicher Vereinbarungen.

(2) Die Hochschule behält es sich vor, den Nutzerkreis einzuschränken.

## § 5 | Zulassung zur Nutzung

(1) Die Zulassung erfolgt vorrangig zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, zu Zwecken der Bibliothek und der Hochschulverwaltung, zur Aus- und Weiterbildung sowie zur Erfüllung sonstiger rechtlich zugewiesener Aufgaben der Hochschule. Für Mitarbeiter und Mitarbeiterinnen der Hochschule erfolgt die Nutzung im Rahmen der Dienstvereinbarung über die Nutzung von IT-Ressourcen an der Fachhochschule Aachen.

(2) Die Zulassung zur Nutzung der Einrichtungen und Dienste der Hochschul-IT erfolgt durch Erteilung einer Nutzungserlaubnis durch den DVZ-Leiter oder die DVZ-Leiterin.

(3) Eine Nutzungserlaubnis für Dritte kann von weiteren Erklärungen abhängig gemacht werden.

(4) Die Nutzungserlaubnis ist auf das beantragte Vorhaben beschränkt und kann zeitlich befristet werden. Zur Gewährleistung eines ordnungsgemäßen und störungsfreien Betriebs kann die Nutzungserlaubnis überdies mit einer Begrenzung der Rechen- und Onlinezeit sowie mit anderen nutzungsbezogenen Bedingungen und Auflagen verbunden werden.

(5) Die DVZ kann die Zulassung zur Nutzung überdies vom Nachweis bestimmter Kenntnisse über die Benutzung der gewünschten Datenverarbeitungssysteme und DV-Dienste abhängig machen.

(6) Wenn die Kapazitäten der DV-Ressourcen nicht ausreichen, um allen Nutzungsberechtigten gerecht zu werden, können die Betriebsmittel für die einzelnen Nutzer

kontingentiert werden, da die Zulassung nur im Rahmen der verfügbaren Kapazitäten erfolgen kann.

## § 6 | Widerruf der Nutzung

Die Nutzungserlaubnis kann ganz oder teilweise versagt, widerrufen oder nachträglich beschränkt werden, insbesondere wenn

1. kein ordnungsgemäßer Antrag vorliegt oder die Angaben im Antrag nicht oder nicht mehr zutreffen;
2. die Voraussetzungen für eine ordnungsgemäße Benutzung der DV-Einrichtungen nicht oder nicht mehr gegeben sind;
3. die nutzungsberechtigte Person nach § 7 von der Benutzung ausgeschlossen worden ist;
4. das geplante Vorhaben des Nutzers oder der Nutzerin nicht mit den Aufgaben der DVZ und den in § 8 Absatz 1 genannten Zwecken vereinbar ist;
5. die vorhandenen DV-Ressourcen für die beantragte Nutzung ungeeignet oder für besondere Zwecke reserviert sind;
6. die Kapazität der Ressourcen, deren Nutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die geplante Nutzung nicht ausreicht;
7. in einem Netzbereich gearbeitet wird, der besonderen Datenschutzerfordernissen genügen muss und kein sachlicher Grund für diese Nutzung ersichtlich ist;
8. zu erwarten ist, dass durch die beantragte Nutzung andere berechnete Vorhaben in unangemessener Weise beeinträchtigt werden.

## § 7 | Ausschluss von der Nutzung

(1) Nutzer und Nutzerinnen können durch den Leiter oder die Leiterin der DVZ vorübergehend oder dauerhaft in der Benutzung der Ressourcen der Hochschul-IT beschränkt oder hiervon ausgeschlossen werden, wenn sie

- a. schuldhaft gegen diese Netzordnung, insbesondere gegen die in § 8 aufgeführten Pflichten, verstoßen (missbräuchliches Verhalten) oder
- b. die Ressourcen der Hochschul-IT für strafbare Handlungen missbrauchen oder der Hochschule durch sonstiges rechtswidriges Nutzerverhalten Nachteile entstehen.

(2) Maßnahmen nach Absatz 1 sollen erst nach vorheriger erfolgloser Abmahnung erfolgen. Dem oder der Betroffenen ist Gelegenheit zur Stellungnahme zu geben. Der betroffene Nutzer oder die betroffene Nutzerin kann das IT-Sicherheitsmanagementteam um Vermittlung bitten. Die DVZ kann zur Aufklärung des Sachverhalts bis zum Abschluss der Ermittlungen eine Sicherungskopie der betroffenen Daten anfertigen. Anschließend ist dem oder

der Betroffenen die Gelegenheit zur Sicherung seiner oder ihrer Daten einzuräumen. Vorübergehende Nutzungseinschränkungen sind aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet erscheint. Eine Nutzungseinschränkung ist dem oder der IT-Sicherheitsbeauftragten zu melden.

(3) Eine dauerhafte Nutzungseinschränkung oder der vollständige Ausschluss eines Nutzers oder einer Nutzerin von der weiteren Nutzung kommt nur bei schwerwiegenden oder wiederholten Verstößen i.S.v. Absatz 1 in Betracht, wenn auch künftig ein ordnungsgemäßes Verhalten nicht mehr zu erwarten ist. Die Entscheidung über einen dauerhaften Ausschluss trifft der Kanzler oder die Kanzlerin auf Antrag des Leiters oder der Leiterin der DVZ und nach Anhörung des IT-Sicherheitsmanagementteams durch Bescheid. Mögliche Ansprüche der Hochschule aus dem Nutzungsverhältnis bleiben unberührt.

## § 8 | Rechte und Pflichten der Nutzer und Nutzerinnen

(1) Die Nutzungsberechtigten haben das Recht, die Einrichtungen, Datenverarbeitungsanlagen und Informations- und Kommunikationssysteme der Hochschul-IT im Rahmen der Zulassung und nach Maßgabe dieser Benutzungsordnung sowie der nach § 3 Absatz 3 erlassenen Regeln zu nutzen. Eine hiervon abweichende Nutzung bedarf einer gesonderten Zulassung.

(2) Die Nutzer und Nutzerinnen sind verpflichtet,

1. die Vorgaben der Benutzungsordnung und sonstiger Sicherheitsrichtlinien zu beachten, die Grenzen der Nutzungserlaubnis einzuhalten und insbesondere die Nutzungszwecke nach § 8 Absatz 1 zu beachten;
2. alles zu unterlassen, was den ordnungsgemäßen Betrieb der DV-Einrichtungen der Hochschul-IT stört;
3. alle Datenverarbeitungsanlagen, Informations- und Kommunikationssysteme und sonstigen Einrichtungen der Hochschul-IT sorgfältig und schonend zu behandeln;
4. ausschließlich mit den Benutzungskennungen zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde;
5. dafür Sorge zu tragen, dass keine anderen Personen Kenntnis von den Benutzerpasswörtern erlangen, sowie Vorkehrungen zu treffen, damit unberechtigten Personen der Zugang zu der Hochschul-IT verwehrt wird; dazu gehört auch der Schutz des Zugangs durch ein geheim zu haltendes und geeignetes, d.h. nicht einfach zu erratendes Passwort, das regelmäßig geändert werden sollte;
6. fremde Benutzerkennungen und Passwörter weder zu ermitteln noch zu nutzen;
7. keinen unberechtigten Zugriff auf Informationen anderer Nutzer und Nutzerinnen zu nehmen und bekannt gewordene Informationen anderer Nutzer

und Nutzerinnen nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern;

8. bei der Benutzung von Software, Dokumentationen und anderen Daten die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten der Hochschule zur Verfügung gestellt werden, zu beachten;
9. seitens der Hochschule bereitgestellte Software, 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;
10. in den Räumen der Hochschul-IT den Weisungen des zuständigen Personals Folge zu leisten;
11. die Benutzungsberechtigung auf Verlangen nachzuweisen;
12. Störungen, Beschädigungen und Fehler an DVZ-Einrichtungen und Datenträgern der DVZ nicht selbst zu beheben, sondern unverzüglich den DVZ-Mitarbeitern oder DVZ-Mitarbeiterinnen zu melden;
13. ohne ausdrückliche Einwilligung der DVZ keine Eingriffe in die Hardwareinstallation der Hochschul-IT vorzunehmen
14. der Leitung der DVZ auf Verlangen in begründeten Einzelfällen - insbesondere bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung - zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu erteilen sowie Einsicht in die Programme zu gewähren;
15. eine Verarbeitung personenbezogener Daten mit dem oder der Behördlichen Datenschutzbeauftragten und DVZ-Leiter oder DVZ-Leiterin abzustimmen und - unbeschadet der eigenen datenschutzrechtlichen Verpflichtungen des Nutzers oder der Nutzerin - die von diesen vorgeschlagenen Datenschutz- und Datensicherheitsvorkehrungen zu berücksichtigen.

(3) Auf die folgenden Straftatbestände wird besonders hingewiesen:

1. Ausspähen von Daten (§ 202a StGB),
2. Abfangen von Daten (§ 202b StGB),
3. Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB),
4. Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB),
5. Computerbetrug (§ 263a StGB),
6. Verbreitung pornographischer Darstellungen (§§ 184 ff. StGB), insbesondere Verbreitung, Erwerb und Besitz kinderpornographischer Schriften (§ 184b StGB) und die Verbreitung pornographischer

Darbietungen durch Rundfunk, Medien- oder Teledienste (§ 184c StGB),

7. Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB),
8. Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB),
9. Strafbare Urheberrechtsverletzungen, z. B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG).

## § 9 | Rechte und Pflichten der DVZ

(1) Die DVZ führt über die erteilten Benutzungsberechtigungen eine Nutzerdatei, in der die Benutzer- und Mailkennungen sowie der Name und die Anschrift (bei Mitarbeitern und Mitarbeiterinnen Dienstadresse) der zugelassenen Nutzer und Nutzerinnen aufgeführt werden.

(2) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutz der Nutzerdaten erforderlich ist, kann die DVZ die Nutzung ihrer Ressourcen vorübergehend einschränken oder einzelne Nutzerkennungen vorübergehend sperren. Sofern möglich, sind die betroffenen Nutzer und Nutzerinnen hierüber im Voraus zu unterrichten.

(3) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein Nutzer oder eine Nutzerin auf den Servern der Hochschul-IT rechtswidrige Inhalte zur Nutzung bereithält, kann die DVZ die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.

(4) Die DVZ ist berechtigt, die Sicherheit der System-/Benutzerpasswörter und der Nutzerdaten durch regelmäßige manuelle oder automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen, z. B. Deaktivierung unsicherer IT-Systeme, Zugangssperre oder Änderungen leicht zu erratender Passwörter, durchzuführen, um die DV-Ressourcen und Benutzerdaten vor unberechtigten Zugriffen Dritter zu schützen. Bei erforderlichen Änderungen der Benutzerpasswörter, der Zugriffsberechtigungen auf Nutzerdateien und sonstigen nutzungsrelevanten Schutzmaßnahmen ist der Nutzer oder die Nutzerin hiervon unverzüglich in Kenntnis zu setzen.

## § 10 | Dokumentation und Auswertung

(1) Die DVZ und die verantwortlichen Administratoren und Administratorinnen vor Ort sind nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme durch die einzelnen Nutzer und Nutzerinnen zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist:

1. zur Gewährleistung eines ordnungsgemäßen Systembetriebs;
2. zur Ressourcenplanung und Systemadministration;
3. zum Schutz der personenbezogenen Daten anderer Nutzer und Nutzerinnen;
4. zu Abrechnungszwecken;
5. für das Erkennen und Beseitigen von Störungen;

(2) Die Dokumentation kann, auf Anforderung durch die Justiz, zur Aufklärung rechtswidriger oder missbräuchlicher Nutzung herangezogen werden.

## § 11 | Einsicht in die Benutzerdateien

(1) Unter den Voraussetzungen von § 7 Absatz 1 oder § 8 Absatz 2 oder § 8 Absatz 3 sind die DVZ und die verantwortlichen Administratoren und Administratorinnen vor Ort nach Beteiligung des oder der Behördlichen Datenschutzbeauftragten auch berechtigt, unter Beachtung des Datengeheimnisses Einsicht in die Benutzerdateien zu nehmen, soweit dies zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Missbräuchen erforderlich ist, sofern hierfür tatsächliche Anhaltspunkte vorliegen.

(2) Eine Einsichtnahme in die Nachrichten- und E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung akuter Störungen im Nachrichtendienst zwingend erforderlich ist. Hierbei ist der oder die Behördliche Datenschutzbeauftragte zu beteiligen. In jedem Fall ist die Einsichtnahme zu dokumentieren und der betroffene Benutzer oder die betroffene Benutzerin ist nach Zweckerreichung unverzüglich zu benachrichtigen.

(3) Unter den Voraussetzungen von § 7 Absatz 1 oder § 8 Absatz 2 oder § 8 Absatz 3 können auch die Verkehrs- und Nutzungsdaten im Nachrichtenverkehr (insbesondere Mail-Nutzung) dokumentiert werden. Es dürfen jedoch nur die näheren Umstände der Telekommunikation – nicht aber die nicht-öffentlichen Kommunikationsinhalte – erhoben, verarbeitet und genutzt werden.

(4) Die Verkehrs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Telediensten, die die Datenverarbeitungszentrale zur Nutzung bereithält oder zu denen die DVZ den Zugang zur Nutzung vermittelt, sind frühestmöglich, spätestens jedoch unmittelbar zum Ende der jeweiligen Nutzung, zu löschen, soweit es sich nicht um Abrechnungsdaten handelt.

(5) Es wird darauf hingewiesen, dass nach Maßgabe der gesetzlichen Bestimmungen die Mitarbeiter und Mitarbeiterinnen der Hochschul-IT zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet sind.

(6) An jedem Vorgang, an dem der oder die Behördliche Datenschutzbeauftragte beteiligt werden muss, sind auch

die Personalvertretungen zu beteiligen, sofern Mitarbeiterdaten betroffen sein könnten.

## § 12 | Haftung des Nutzers oder der Nutzerin

(1) Der Nutzer oder die Nutzerin haftet für alle Nachteile, die der Hochschule durch missbräuchliche oder rechtswidrige Verwendung der DV-Ressourcen und der Nutzungsberechtigung oder dadurch entstehen, dass der Nutzer oder die Nutzerin schuldhaft seinen oder ihren Pflichten aus dieser Benutzungsordnung nicht nachkommt. Beschäftigte haften im Rahmen der arbeits- bzw. dienstrechtlichen Haftungsregelungen.

(2) Der Nutzer oder die Nutzerin haftet auch für Schäden, die im Rahmen der ihm oder ihr zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er oder sie diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe seiner oder ihrer Benutzerkennung an Dritte.

(3) Der Nutzer oder die Nutzerin hat die Hochschule von allen Ansprüchen freizustellen, wenn Dritte die Hochschule wegen eines missbräuchlichen oder rechtswidrigen Verhaltens des Nutzers oder der Nutzerin auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen. Die Hochschule wird dem Nutzer oder der Nutzerin den Streit verkünden, sofern Dritte auf Grund dieser Ansprüche gegen die Hochschule gerichtlich vorgehen.

## § 13 | Haftung der Hochschule

(1) Die Hochschule übernimmt keine Garantie dafür, dass das System fehlerfrei und jederzeit ohne Unterbrechung läuft. 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) Im Übrigen haftet die Hochschule nur bei Vorsatz und grober Fahrlässigkeit ihrer Mitarbeiter und Mitarbeiterinnen, es sei denn, dass eine schuldhafte Verletzung wesentlicher Pflichten vorliegt, deren Einhaltung für die Erreichung des Vertragszwecks von besonderer Bedeutung ist (Kardinalpflichten). In diesem Fall ist die Haftung der Hochschule auf typische, bei Begründung des Nutzungsverhältnisses vorhersehbare Schäden begrenzt, soweit nicht vorsätzliches oder grob fahrlässiges Handeln vorliegt.

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

## § 14 | Inkrafttreten, Veröffentlichung

(1) Diese Netzordnung tritt am Tag nach ihrer Veröffentlichung im Verkündungsblatt der Fachhochschule Aachen (FH-Mitteilungen) in Kraft. Gleichzeitig tritt die Netzordnung vom 11. Februar 2000 (FH-Mitteilung Nr. 1/2000 vom 17. Februar 2000) außer Kraft.

(2) Ausgefertigt auf Grund des Beschlusses des Senats der Fachhochschule Aachen vom 26. März 2015.

Aachen, den 22. Mai 2015

Der Rektor  
der Fachhochschule Aachen

gez. Marcus Baumann

Prof. Dr. Marcus Baumann

### **Erläuterung:**

Die Netzordnung der Fachhochschule Aachen wurde nach der Musterbenutzungsordnung des DFN-Vereins (aktualisierte Fassung vom 20.01.2011 siehe: <https://www.dfn.de/rechtimdfn/rgwb/rechtsguide/rg-kapitel1/muster>) entwickelt.