Rahmenordnung
zum Datenschutz, zur Datensicherheit sowie zur Vermeidung missbräuchlicher Nutzung der Informations- und Kommunikationsdienste an der Fachhochschule Niederrhein

Aufgrund der §§ 2 Abs. 4 Satz 1, 22 Abs. 1 Satz 1 Nr. 3 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG) vom 14.März 2000 (GV.NRW. S. 190) hat die Fachhochschule Niederrhein zur Wahrung der gesetzlichen Bestimmungen zum Datenschutz, zur Gewährleistung der Datensicherheit sowie zur Vermeidung missbräuchlicher Nutzung von DV-Anlagen, DV-Geräten, Informations- und Kommunikationsdiensten nachstehende „Rahmenordnung zum Datenschutz, zur Datensicherheit sowie zur Vermeidung missbräuchlicher Nutzung der Informations- und Kommunikationsdienste an der Fachhochschule Niederrhein“ erlassen:

Inhaltsverzeichnis[*)]

§ 1 Geltungsbereich

§ 2 Zuständigkeiten, Rechte und Pflichten der einzelnen Organisationseinheiten

§ 3 Allgemeines

§ 4 Übergreifende Regelungen

§ 5 Rechte und Pflichten der Benutzerinnen

§ 6 Netze

§ 7 Nutzungsregelungen für die Beschäftigten der FHN beim PC-Einsatz

§ 8 Regelungen für die Inanspruchnahme von Informations- und Kommunikations-diensten

§ 9 Zugangs- und Zugriffsregelungen

§ 10 Auskünfte und Datenweitergabe

§ 11 Haftung

§ 12 Missbrauch

§ 13 Konsequenzen bei Verstößen

§ 14 Inkrafttreten

[*)] Sämtliche Funktionsbezeichnungen gelten für Männer in der männlichen Form

§ 1
Geltungsbereich

(1) Diese Rahmenordnung dient dem Schutz, der Sicherung und der Verhinderung des Missbrauchs von Daten, unabhängig davon, ob sie personenbezogen sind oder nicht, und unabhängig davon, ob sie automatisiert oder manuell verarbeitet sind; sie dient auch der Vermeidung missbräuchlicher Nutzung der DV-Anlagen, DV-Geräte, Informations- und Kommunikationsdienste, die innerhalb der FHN und auf der Grundlage der Mitgliedschaft der FHN im DFN-Verein im Wissenschaftsnetz (WIN) bereitgestellt werden und dazu dienen, den Anwenderinnen eine leistungsfähige und störungsfreie Infrastruktur bereitzustellen.

(2) Die Bereiche, die personenbezogene Daten verarbeiten, sind aufgrund der Vorschriften zum Datenschutz zu Maßnahmen verpflichtet, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind, Missbrauch zu verhindern. Datenschutz und Datensicherheit obliegen der Eigenverantwortung der Anwenderin und der Aufsichtsverantwortung der Vorgesetzten des datenverarbeitenden Bereiches. Die Bestimmungen des Gesetzes zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen- DSG NRW) bleiben unberührt (s. Anlage).
Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn und soweit dies durch das DSG NRW oder eine andere Rechtsvorschrift erlaubt wird oder die betroffene Person vor der Verarbeitung schriftlich ihre Zustimmung erklärt hat. Personenbezogene Daten sind bei der betroffenen Person mit ihrer Kenntnis zu erheben; bei anderen Stellen oder Personen dürfen sie ohne ihre Kenntnis nur nach Maßgabe der Bestimmungen des DSG NRW erhoben werden. Das Erheben personenbezogener Daten ist nur insoweit zulässig, als ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

(3) Für die Sicherstellung des Datenschutzes und der Datensicherheit in den einzelnen Organisationseinheiten (Fachbereiche, zentrale Betriebseinheiten, Hochschulverwaltung) können diese weitergehende Regelungen treffen.

§ 2
Zuständigkeiten, Rechte und Pflichten der einzelnen Organisationseinheiten

(1) Die einzelnen Organisationseinheiten regeln ihre Rechte und Pflichten in ihren jeweiligen Ordnungen. Wenn und soweit die jeweilige Organisationseinheit keine eigene Ordnung erläßt, gelten die Bestimmungen dieser Rahmenordnung. Die einzelnen Organisationseinheiten stellen durch ihre Ordnungen sicher, dass

(a) alle ihr anvertrauten DV-Einrichtungen unter Berücksichtigung wirtschaftlicher, technischer und organisatorischer Aspekte für die Benutzerinnen bestmöglich betrieben werden und

(b) alle organisatorischen und technischen Maßnahmen ergriffen werden, um eine den Vorschriften und Weisungen entsprechende Verarbeitung von Daten sicherzustellen und Verlust von Daten, unzulässige Verarbeitung von Daten, Nutzung oder Kenntnisnahme von schutzbedürftigen Daten durch Unbefugte zu verhindern.

Das Einsetzen von Sicherheitsmechanismen erfolgt unter Abwägung der Erforderlichkeit für den Datenschutz und die Datensicherheit einerseits und der Verhältnismäßigkeit andererseits.

Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines zu dokumentierenden Sicherheitskonzeptes zu ermitteln. Zum Bestandteil dieses Sicherheitskonzeptes

gehört die Vorabkontrolle hinsichtlich möglicher Gefahren für das geschützte Recht auf informationelle Selbstbestimmung, wobei die Vorabkontrolle vor der Entscheidung über den Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten durchzuführen und das Ergebnis zu dokumentieren ist. Die Vorabkontrolle wird von der zuständigen Datenschutzbeauftragten der FHN durchgeführt.

(2) Bei der Erarbeitung organisationseinheitenbezogener Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten (z.B. Ordnungen, Betriebsregelungen, Dienstanweisungen, etc.) ist die zuständige Datenschutzbeauftragte der FHN frühzeitig zu beteiligen. Personalvertretungsrechtliche Zuständigkeiten bleiben hiervon unberührt.

(3) Die einzelnen Organisationseinheiten benennen für ihren Bereich eine oder mehrere DV-Beauftragte. Der oder den DV-Beauftragten obliegen nachfolgende Aufgaben, wobei je nach Ausbaustand der IuK-Technologien in der jeweiligen Organisationseinheit diese unter Beachtung der Vorgaben der vorliegenden Rahmenordnung durch eine eigene Ordnung die Aufgaben der DV-Beauftragten festlegt:

(a) die Planung, Organisation, Beschaffung und Einführung neuer Informations- und Kommunikationstechnologien sowie des Einsatzes der Datenverarbeitung im Informations- und Kommunikationsnetz und bei PC's auf der Basis des ADV-Konzeptes der FHN einschließlich der Federführung für erforderliche Mitbestimmungs- und Beteiligungsverfahren (Einschaltung des jeweils zuständigen Personalrates),

(b) die Bereitstellung sowie den Betrieb der Datenverarbeitungsanlagen (DV-Anlagen) und Datenverarbeitungsgeräte (DV-Geräte), die Bereitstellung sowie den Betrieb spezialisierter Rechnerleistung in Form von Datei-, Applikations-, Kommunikations- und Informationsservern sowie die Bereitstellung und der Betrieb qualitativ hochwertiger Ressourcen;

(c) die Implementierung und Konfiguration von Anwendersystemen sowie Standard- und Spezialsoftware in Zusammenarbeit mit den jeweils zuständigen Institutionen und Organisationseinheiten;

(d) die System- und Datenbankadministration, soweit nicht ausdrücklich eine andere Zuständigkeit gegeben ist;

(e) die Schaffung der Voraussetzungen für die Gewährleistung von Datenschutz und Datensicherheit, insbesondere Konzeption und Koordination der Datensicherung sowie deren Realisierung, Dokumentation des Sicherheitskonzeptes und Kontrolle; § 1 Absatz 2 Satz 2 gilt entsprechend;

(f) die Beteiligung der zuständigen Datenschutzbeauftragten der FHN zur Wahrung ihrer Verpflichtung der Vorabkontrolle;

(g) die Kooperation mit den DV-Beauftragten der anderen Organisationseinheiten in Sicherheitsfragen.

(4) Soweit ein eigenes Netz betrieben wird, nimmt die DV-Beauftragte zusätzlich zu den in der Ordnung der jeweiligen Organisationseinheit zu regelnden Aufgaben folgende Aufgaben wahr:

(a) die Gewährleistung eines sicheren und möglichst ununterbrochenen Netzbetriebes sowie die Durchführung von Kontrollen zwecks Ermittlung, ob Einbruch bzw. Einbruchsversuche in das Netz unternommen wurden; ggf. sind die Sicherheitsstufen zu erhöhen; bei Bedarf wird dies durch die Mitwirkung der DVZ sichergestellt;

(b) das Netzwerkmanagement sowie die Vergabe von Netzwerkadressen und Passwörtern;

(c) die Erstellung einer Dokumentation der Netze, sämtlicher PC's mit Angabe der jeweiligen Nutzerinnen, des Anschlusses der PC's an das Netz sowie einer Übersicht über alle eingesetzten Programme einschließlich der ständigen Aktualisierung dieser Dokumentation;

(d) die Protokollierung von Zugriffen (Netzüberwachung) im Rahmen der geltenden Gesetze (wie z.B. Datenschutzgesetz NRW; Mediendienste-Staatsvertrag, Informations- und Kommunikationsdienste-gesetz, Telekommunikationsgesetz, Teledienstedatenschutzgesetz, Arbeitnehmerschutzgesetz, etc.) und unter Berücksichtigung dessen, dass Verkehrsflussanalysen nicht zur Erstellung von Kommunikations- und Persönlichkeitsprofilen benutzt werden dürfen.

(5) Die DV-Beauftragte der jeweiligen Organisationseinheit führt über die erteilten Benutzungsberechtigungen eine Nutzerdatei, in der die Benutzer- und Mailkennungen sowie der Name und die Anschrift der zugelassenen Nutzerinnen aufgeführt werden.

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

(7) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass eine Nutzerin auf den Servern einer Organisationseinheit rechtswidrige Inhalte zur Nutzung bereithält, kann die DV-Beauftragte die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.

(8) Die DV-Beauftragte der jeweiligen Organisationseinheit ist berechtigt, die Sicherheit der System-/Benutzerpasswörter und der Nutzerdaten durch regelmäßige manuelle oder automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen, z.B. 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 die Nutzerin hiervon unverzüglich in Kenntnis zu setzen.

(9) Die DV-Beauftragte der jeweiligen Organisationseinheit ist nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme durch die einzelne Nutzerin zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist:

a) zur Gewährleistung eines ordnungsgemäßen Systembetriebes,

b) zur Ressourcenplanung und Systemadministration,

c) zum Schutz der personenbezogenen Daten anderer Nutzerinnen,

d) zu Abrechnungszwecken,

e) für das Erkennen und Beseitigen von Störungen sowie

f) zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher (vgl. § 12) Nutzung.

Unter den vorgenannten Voraussetzungen der Buchstaben a) bis f) können auch die Verbindungs- 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. Die Verbindungs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Telediensten, die die jeweilige Organisationseinheit zur Nutzung bereithält oder zu denen die jeweilige Organisationseinheit den Zugang

zur Nutzung vermittelt, sind frühestmöglich zu löschen, soweit es sich nicht um Abrechnungs-daten handelt.

(10) Nach Maßgabe der gesetzlichen Bestimmungen ist jede Organisationseinheit zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet.

§ 3
Allgemeines

(1) Beschäftigte, die personenbezogene Daten verarbeiten, haben sich mit den rechtlichen Bestimmungen vertraut zu machen. Die Dienststelle sowie die jeweiligen Organisationseinheiten sorgen für entsprechende Fortbildungs-, Weiterbildungs– und Informationsveranstaltungen.

(2) Die Schlüssel für Geräte und Aktenschränke sind unter Verschluss zu verwahren.

(3) In Bereichen mit Publikumsverkehr darf diesem keine Sichtmöglichkeit auf den Bildschirm oder Datenträger (Listen, Akten, etc.) ermöglicht werden. Dies gilt ebenso beim Verlassen des Raumes oder Nichtgebrauch des Gerätes; Datenträger sind jedwedem unberechtigtem Zugriff zu entziehen.

(4) Unterlagen mit sensiblen personenbezogenen Daten sind nach Dienstschluss unter Verschluss zu nehmen bzw. es ist organisatorisch sicherzustellen, dass die Akten durch die Vorzimmer/Sekretariate unter Verschluss genommen werden.
Unterlagen mit sensiblen personenbezogenen Daten sind solche Unterlagen, die aufgrund von personenbezogenen Angaben der Öffentlichkeit nicht zugänglich gemacht werden dürfen (wie z.B. Personalakten, Prozessakten, Prüfungsakten, Notenlisten, Prüfungsarbeiten, Unterlagen bzgl. Berufungsverfahren, Protokolle über Personalia, Immatrikulations- und Exmatrikulationsunterlagen, etc.). Im Zweifelsfalle entscheidet die Leiterin der jeweiligen Organisationseinheit, welche personenbezogenen Daten als sensibel zu behandeln sind.

(5) Die Aufbewahrungsfristen für gespeicherte Daten richten sich nach den für die einzelnen Belange/Zwecke vorgeschriebenen gesetzlichen bzw. festgelegten Aufbewahrungsfristen.

(6) Mobile Datenträger sind auf jeden Fall unter Verschluss zu halten; Verschlüsselung wird empfohlen.

(7) Auf Datenträgern, die zeitweilig oder auf Dauer Dritten übergeben werden und nicht mehr verwendet werden sollen, sind noch vorhandene Daten dauerhaft zu löschen. Bei der Reparatur durch externe Firmen sind diese auf die datenschutzrechtlichen Bestimmungen im Reparaturauftrag durch die Beschaffungsabteilung des Dezernates IV hinzuweisen/zu verpflichten. Ist ein sicheres Löschen von Daten nicht möglich, sind die Datenträger mechanisch zu zerstören.

(8) Altpapier und Datenträger mit sensiblen personenbezogenen Daten (vgl. § 3 Absatz 4 Satz 2 und Satz 3) sind nach Ablauf der Aufbewahrungsfristen zu vernichten. Eine Vernichtung ist erst dann gewährleistet, wenn es auf keine Weise mehr möglich ist, den Inhalt aus dem vernichteten Schriftgut/Datenträger zu rekonstruieren. Erfolgt die Vernichtung durch eine fachhochschulexterne Institution, hat die jeweilige Organisationseinheit bis zur Abholung dafür Sorge zu tragen, dass Unberechtigte keinen Zugriff nehmen können. Der Vernichtungsvorgang durch die fachhochschulexterne Institution erfolgt im Beisein einer Mitarbeiterin der Organisationseinheit unter Abgabe einer schriftlichen Übernahme- und Vernichtungsbestätigung nach den Bestimmungen des Bundesdatenschutzgesetzes und des DSG NRW.

§ 4
Übergreifende Regelungen

(1) Alle DV-Systeme mit sensitiven Anwendungen bzw. sensiblen personenbezogenen Daten (vgl. § 3 Absatz 4 Satz 2 und Satz 3) sind durch ein Firewall-System oder ein anderes technisches System, welches mindestens den gleichen Schutz gewährleistet, zu schützen. Es verhindert jede unberechtigte Nutzung aller im Hochschulnetz betriebenen Datenverarbeitungsanlagen. Wegen der hohen Sensibilität der personenbezogenen Daten werden die Server, auf denen Datenbanken mit personenbezogenen Daten gespeichert sind, durch ein zusätzliches Firewall-Servermodul geschützt.

(2) Personenbezogene Daten in Texten/Briefen sowie hierfür notwendige Adressdateien sind durch entsprechende Maßnahmen vor missbräuchlicher Nutzung zu schützen.

(3) Jede Organisationseinheit, die für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten verantwortlich ist, ist zur Erstellung eines Verfahrensverzeichnisses gemäß DSG NRW und zur Vorlage dieses Verzeichnisses an die zuständige Datenschutzbeauftragte der FHN verpflichtet.

§ 5
Rechte und Pflichten der Benutzerinnen

(1) Die Benutzerinnen haben das Recht, die für die Bearbeitung ihrer Aufgaben notwendigen DV-Anlagen, DV-Geräte sowie Informations- und Kommunikationsdienste nach Maßgabe der Zulassung im Rahmen der geltenden Ordnungen, Betriebsregelungen und Dienstanweisungen der FHN und ihrer Organisationseinheiten sowie der zur Verfügung stehenden Ressourcen in Anspruch zu nehmen. Sie können sich mit Anregungen und Beschwerden an die Leiterin der jeweiligen Organisationseinheit der FHN wenden.

(2) Die Benutzerinnen sind verpflichtet:

(a) die Vorschriften der geltenden Ordnungen, Betriebsregelungen und Dienstanweisungen der FHN oder ihrer Organisationseinheiten einzuhalten;

(b) regelmäßig an den Fortbildungs-, Weiterbildungs- und Informationsveranstaltungen der Dienststelle sowie der jeweiligen Organisationseinheit teilzunehmen und sich über die jeweils geltenden Bestimmungen bzgl. der Nutzung der DV-Anlagen, DV-Geräte, Informations- und Kommunikationsdienste in den bereitgestellten Informationsdiensten der FHN (z.B. Verkündungsblatt der FHN, die in den Laboratorien und CIP-Räumen bereitgestellten Informationsschriften, Informationsveranstaltungen der einzelnen Organisationseinheiten, etc.) zu informieren;

(c) Geräte, Datenträger, alle Datenverarbeitungsanlagen, Informations- und Kommunikationssysteme sowie sonstige Einrichtungen sorgfältig und schonend zu behandeln;

(d) Störungen, Beschädigungen sowie Fehler an DV-Anlagen, DV-Geräten und Datenträgern nicht selbst zu beheben, sondern unverzüglich der DV-Beauftragten der jeweiligen Organisationseinheit zu melden;

(e) in den Räumen der Datenverarbeitung sowie bei Inanspruchnahme der dortigen Geräte, Anlagen, Datenträgern und sonstiger Einrichtungen den Weisungen des Personals Folge zu leisten sowie Aushänge in den Räumen und an den Geräten zu beachten;

(f) die Benutzungsberechtigung auf Verlangen durch Vorlage eines Studierenden- oder Personalausweises nachzuweisen;

(g) die Benutzung auf das in der Zulassung angegebene Arbeitsthema/Vorhaben zu beschränken;

(h) die Benutzerkennung vor Verwendung durch Dritte zu sichern;

(i) durch ihr eigenes Verhalten dafür Sorge zu tragen, dass unberechtigten Dritten der Zugang zu den DV-Geräten, DV-Anlagen sowie Netzen verwehrt wird (Verpflichtung zum „logout" vor Verlassen des Arbeitsplatzes; regelmäßiges Ändern der Passwörter in nicht zu großen Zeitabständen);

(j) jegliche missbräuchliche Nutzung (§ 12) zu unterlassen;

(k) alles zu unterlassen, was den ordnungsgemäßen Betrieb der DV-Einrichtungen stören könnte;

(l) die DV-Beauftragte der jeweiligen Organisationseinheit unverzüglich über missbräuchliche Nutzung, Missbrauchsversuche sowie Missbrauchsverdacht zu informieren;

(m) die DV-Beauftragte der jeweiligen Organisationseinheit unverzüglich nach Entdecken ggf. bestehender Sicherheitslücken zu benachrichtigen;

(n) evtl. Einschränkungen der Benutzungsberechtigungen (z.B. Kontingente, Beschränkung auf bestimmte Rechner, etc.) auch dann einzuhalten, wenn sie vom System nicht automatisch überprüft werden oder durch Lücken im System umgangen werden können;

(o) der DV-Beauftragten der jeweiligen Organisationseinheit 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;

(p) ihre Daten und Programme so zu sichern, dass Schäden durch Verlust bei der Verarbeitung nicht entstehen können;

(q) vor einer Verarbeitung personenbezogener Daten dies der DV-Beauftragten der jeweiligen Organisationseinheit mitzuteilen und - unbeschadet der eigenen Verpflichtung der Benutzerin zur Beachtung und Einhaltung datenschutzrechtlicher Bestimmungen - die von der DV-Beauftragten vorgeschlagenen Datenschutz- und Datensicherungsvorkehrungen zu beachten und zu nutzen;

(r) bekannt gewordene Informationen über fremde Programme und Daten nicht ohne Genehmigung der befugten Person weiterzugeben oder selbst zu nutzen.

§ 6
Netze

(1) Unter Informations- und Kommunikationsnetzen ist ein technisches System zu verstehen, das aus mehreren Endgeräten (z.B. Personalcomputern, Telefaxgeräten, ISDN-Anlagen, etc.), einem Transportmedium (z.B. Kabelverbindung) und ggf. weiteren Komponenten (z.B. Großrechenanlage) besteht und dazu dient, Informationen von einem Ort an den anderen zu übermitteln.

(2) Die für die Nutzung angebundener Netze (z.B. WIN, Internet, etc.) bestehenden Regelungen (z.B. Verwaltungs- und Benutzungsordnung für die Datenverarbeitungszentrale der Fachhochschule

Niederrhein, die Betriebsregelung für die Nutzung der DV-Geräte und der Kommunikationsdienste der Datenverarbeitungszentrale der Fachhochschule Niederrhein) sind zu befolgen.
Jede Benutzerin hat regelmäßig an den Fortbildungs-, Weiterbildungs- und Informationsveranstaltungen der Dienststelle sowie der jeweiligen Organisationseinheit teilzunehmen und sich über die jeweils geltenden Bestimmungen zu informieren.

(3) Die Netze der Organisationseinheiten bestehen jeweils aus separatem/n Server/n, Datenübertragungseinrichtungen sowie daran angeschlossenen Endgeräten.

Die Server haben sich in einem besonders geschützten Raum der jeweiligen Organisationseinheit zu befinden. Der Zutritt zu diesem Raum ist nur der DV-Beauftragten oder im einzelnen hierzu befugten Mitarbeiterinnen der Organisationseinheit gestattet. Ausgenommen hiervon sind Server in Forschung und Lehre, die keine sensiblen personenbezogenen (vgl. § 3 Absatz 4 Satz 2 und Satz 3) Daten enthalten; diese Server können sich in den jeweiligen Laborräumen befinden, wobei der Zugang von der Laborleiterin geregelt wird.

(4) Der Anschluss von Rechnern oder anderen Endgeräten und deren Änderung darf nur durch die zuständigen Mitarbeiterinnen der jeweiligen Organisationseinheit erfolgen.

(5) Das Netz der jeweiligen Organisationseinheit ist mit den technischen und administrativen Möglichkeiten möglichst optimal vor unberechtigtem Zugriff und vor Computerviren zu schützen.

(6) Netzzugangspunkte, insbesondere Netzanschlussdosen dürfen sich nur in den der Organisationseinheit zugeordneten Räumen befinden. Die Einrichtung und Veränderung von Anschlusspunkten sowie von Identifikationsmerkmalen der Rechner (Netzadressen, Namen, etc.) darf nur von den zuständigen Mitarbeiterinnen der Organisationseinheit durchgeführt bzw. veranlasst werden.

(7) Der Benutzerin ist es untersagt, fremde Daten aus dem Netz „mitzuhören“, auszuspionieren, aufzuzeichnen sowie zu verändern. Fremde Daten sind solche, für die die Benutzerin kein Zugriffsrecht eingeräumt bekommen hat bzw. die nicht für sie bestimmt sind.

(8) Der Benutzerin ist es untersagt, die Kommunikation in den Netzen zu stören (etwa durch den Einsatz besonders netzbelastender Übertragungen) sowie Modifikationen an den Netzen vorzunehmen.

(9) Die Benutzerin darf aus den Netzen nur diejenigen Daten auf ihren Rechner leiten, die für sie bestimmt sind. Die Beschaffung und der Einsatz von Hard- und Software, die einen Missbrauch ermöglichen, sind unzulässig.

(10) Die Benutzerin ist verpflichtet, den zuständigen Mitarbeiterinnen der Organisationseinheit Unregelmäßigkeiten, Störungen oder Missbrauchsversuche unverzüglich anzuzeigen.

(11) Der Betrieb eines Informations- und Kommunikationsnetzes darf nicht für Zwecke der Leistungs- und Verhaltenskontrolle und nicht zur Erschließung von Beurteilungen, Disziplinarmaßnahmen oder des Gesundheitszustandes der Beschäftigten genutzt werden.

§ 7
Nutzungsregelungen für die Beschäftigten der FHN beim PC-Einsatz

(1) Von der FHN beschaffte PC's dürfen von den Beschäftigten der FHN nur zu dienstlichen Zwecken verwendet werden, es sei denn, die Leiterin der jeweiligen Organisationseinheit hat der anderweitigen Nutzung in Ausnahmefällen vorab zugestimmt.

(2) Das Einbringen und Nutzen privater Software ist nur dann erlaubt, wenn dadurch weder Urheberschutz- noch Lizenzrechte verletzt werden. Darüber hinaus ist sicherzustellen, dass der Datenträger keine Viren enthält. Dasselbe gilt für das Herunterladen (download) von Dateien und/oder ausführbaren oder gepackten Dateien aus dem Internet (Email, WWW, FTP, Datenträgern, etc).

(3) Das Kopieren von lizenzpflichtigen Programmen ist aus urheberrechtlichen Gründen untersagt.

(4) Bei dem Transport von Datenträgern mit sensiblen personenbezogenen Daten (vgl. § 3 Absatz 4 Satz 2 und Satz 3) ist der Zugriff durch unbefugte Personen jederzeit auszuschließen.

§ 8
Regelungen für die Inanspruchnahme von Informations- und Kommunikationsnetzen

(1) Bei der Nutzung von E-Mail ist aus datenschutzrechtlichen Gründen darauf zu achten, dass keine personenbezogenen sensiblen Daten und/oder Informationen vertraulichen Inhalts (vgl. § 3 Absatz 4 Satz 2 und Satz 3) versendet werden dürfen.

(2) Die Veröffentlichungen auf dem WWW-Server der FHN sollen der internen und externen Verbreitung von Informationen über die Einrichtungen und Dienste der Hochschule dienen und Lehre, Forschung und Verwaltung der FHN unterstützen.

(3) Die Nutzung der WWW-Server der FHN ist nur im Rahmen der festgelegten Bestimmungen zulässig.

§ 9
Zugangs- und Zugriffsregelungen

(1) Die Nutzung der Anwendungssysteme ist nur für eingetragene, berechtigte Nutzerinnen mit Eingabe einer User-Identifizierungs-Kennung (UserID) möglich.

(2) Der Zugang auf die Server ist nur mit einem mindestens 6-stelligen Passwort möglich. Es dürfen keine Namen, Geburtstage oder andere geläufige Begriffe verwendet werden. Das Passwort soll aus einer Kombination von Zahlen, Buchstaben und Sonderzeichen bestehen.
(a) Soweit personenbezogene sensible Daten (vgl. § 3 Absatz 4 Satz 2 und Satz 3) oder sonstige Daten auf PC's verarbeitet werden, ist der Zugriff auf diese Daten durch ein von der Nutzerin

einzugebendes Passwort zu sichern. Die Sicherung über den Bildschirmschonerschutz ist nicht ausreichend. Das Passwort ist spätestens alle drei Monate zu ändern.

(b) Die Nutzerin ist verpflichtet, das Passwort geheimzuhalten.

(3) Eine Einsichtnahme der DV-Beauftragten in von der Benutzerin geschützte Dateien und/oder Verzeichnisse ist grundsätzlich unzulässig.
Abweichend von Satz 1 darf die DV-Beauftragte im Beisein einer von der Hochschulleitung bestellten Person Einsicht in die Dateien und/oder Verzeichnisse der Benutzerin nehmen, wenn

(a) der begründete Verdacht vorliegt, dass die Benutzerin die Infrastruktur der Organisationseinheit für Straftaten benutzt,

(b) konkrete Anhaltspunkte für schwere Verstöße gegen sonstige gesetzliche Vorschriften, Ordnungen der FHN oder Ordnungen, Betriebsregelungen oder Dienstanweisungen der jeweiligen Organisationseinheit gegeben sind oder

(c) es zur Gewährleistung eines ordnungsgemäßen Betriebes der Netze erforderlich ist.

Die Einsichtnahme erfolgt grundsätzlich im Beisein der Benutzerin, es sei denn, sofortiges Handeln ist geboten und die Anwesenheit der Benutzerin ist wegen der Eilbedürftigkeit nicht herstellbar.
Sämtliche Zugriffe sind zu protokollieren und der Benutzerin, bei Mitarbeiterinnen deren Vorgesetzten sowie bei Studierenden und anderen Benutzerinnen der Vorsitzenden der ADV-Kommission unter Angabe des Grundes und des Ergebnisses der Maßnahmen mitzuteilen.

(4) Die elektronische Post (E-mail) der Benutzerin unterliegt besonderen gesetzlichen Schutzbestimmungen (§ 85 TKG; § 206 StGB; §§ 7, 14 TDSV) hinsichtlich der Verpflichtung zur Wahrung der Vertraulichkeit, der Unbeobachtbarkeit sowie der Integrität.
Die Organisationseinheiten sind daher verpflichtet, durch technische und organisatorische Maßnahmen sicherzustellen, dass E-mails grundsätzlich nicht von der DV-Beauftragten mitgelesen werden können und dass die im Klartext übermittelten Nachrichten nicht unzulässigerweise aufgezeichnet (sog. Unzulässiges Mitschneiden) oder ihr Inhalt während des Transportes verändert werden kann.
In die E-mails einer Benutzerin darf bei Vorliegen der Voraussetzungen der unter Absatz 3 genannten Voraussetzungen grundsätzlich nur mit Zustimmung und in Anwesenheit der Benutzerin Einsicht genommen werden.

§ 10
Auskünfte und Datenweitergabe

(1) Schriftliche Datenauskünfte an die betroffene Person sollen durch Kopie erfolgen. Weitergehende Verfahren (z.B. Einsichtnahme in Akten oder elektronisch geführte Unterlagen, etc.) sind durch die Leiterin der Organisationseinheit zu entscheiden. Mündliche Datenauskünfte dürfen im Einzelfall nur nach einwandfreier Identifizierung der betroffenen Person an diese weitergegeben werden.

(2) Die Weitergabe personenbezogener Daten zu anderen Zwecken als für die sie erhoben worden sind, ist an öffentliche Stellen grundsätzlich nur erlaubt, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und die Voraussetzungen des § 13 Absatz 2 Satz 1 DSG NRW (z.B. wenn eine Rechtsvorschrift oder die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen Aufgabe die Verarbeitung dieser Daten zwingend

voraussetzt oder der Betroffene schriftlich eingewilligt hat) vorliegen. Die Datenweitergabe ist zu dokumentieren.

(3) Die Weitergabe von personenbezogenen Daten an Personen oder Stellen ausserhalb des öffentlichen Bereiches ist nur unter den in § 16 DSG NRW genannten Voraussetzungen (z.B. Vorliegen eines öffentlichen oder berechtigten Interesses und kein Widerspruch seitens der betroffenen Person) statthaft.

(4) Auskunftsersuchen von Behörden oder sonstigen öffentlichen Stellen sind nur aufgrund gesetzlicher Regelungen möglich. Die auskunftsersuchende Behörde oder sonstige öffentliche Stelle hat ihr Auskunftsbegehren schriftlich zu begründen. Es ist stets zu prüfen, ob die Behörde oder öffentliche Stelle berechtigt ist, Auskunft zu erhalten. Die Leiterin der jeweiligen Organisationseinheit ist zu beteiligen. Die Auskunft hat schriftlich zu erfolgen; der betroffenen Person ist in der Regel eine Kopie der Auskunft zur Kenntnis zu übersenden.

(5) Sollte in dringendem Einzelfall eine fernmündliche Auskunft an eine Behörde oder sonstige öffentliche Stelle notwendig werden, ist hierfür die Leiterin der entsprechenden Organisationseinheit zuständig. Diese hat die sachlichen und gesetzlichen Voraussetzungen zu prüfen und über die Auskunft zu entscheiden. Die Entscheidungsgründe sind schriftlich festzuhalten und zu den Akten zu nehmen.

§ 11
Haftung

(1) Die Benutzerin haftet für die von ihr schuldhaft verursachten Schäden an DV-Anlagen und -Geräten, Datenträgern und sonstigen Einrichtungen der Organisationseinheiten, für schuldhaft verursachte Verluste und Veränderungen der Daten und Programme der Organisationseinheiten oder Dritter sowie für schuldhaft verursachte Schäden aus Verstößen gegen Rechtsvorschriften sowie die Bestimmungen der Ordnungen, Betriebsregelungen sowie Dienstanweisungen der FHN oder ihrer Organisationseinheiten. Soweit es sich bei der Benutzerin um eine Bedienstete der FHN handelt, gilt die vorstehende Haftungsregelung entsprechend, wobei der arbeitsrechtliche/beamtenrechtliche Haftungsmaßstab (Vorsatz oder grobe Fahrlässigkeit) gilt.

(2) Die FHN haftet für von den Mitarbeiterinnen der jeweiligen Organisationseinheiten vorsätzlich oder grob fahrlässig verursachten Schäden. Die Haftung erstreckt sich jedoch nur auf Ersatzleistungen für unmittelbare Schäden. Die Benutzerin hat durch vorbeugende Maßnahmen einen möglichen Schaden so gering wie möglich zu halten.

(3) Die FHN übernimmt keine Gewähr für die fehlerfreie Funktion ihrer technischen Einrichtungen oder der von ihr zur Verfügung gestellten Programme, die dauernde Verfügbarkeit ihrer DV-Anlagen, DV-Geräte und Informations- und Kommunikationsdienste sowie für die inhaltliche Richtigkeit der Ergebnisse, die auf ihren DV-Anlagen berechnet wurden.

§ 12
Missbrauch

(1) Missbräuchlich ist die Nutzung der DV-Ressourcen sowie der Informations- und Kommunikationsdienste, wenn das Verhalten der Benutzerin gegen einschlägige nationale und internationale Schutzvorschriften (Strafgesetze, Jugendschutzgesetze, Datenschutzgesetze, Wettbewerbsrechtliche Vorschriften, Patent-, Urheber-, Lizenzrechte, etc.), die geltenden Ordnungen der FHN sowie die Ordnungen, die Betriebsregelungen und/oder Dienstanweisungen der Organisationseinheiten der FHN verstößt.

(2) Unbeschadet gesetzlicher Vorschriften ist der bewusste Abruf sowie die Nutzung informationstechnischer Einrichtungen oder der bewusste Abrufs- oder Nutzungsversuch für gewaltverherrlichende, pornographische, rassistische, volksverhetzende, sonstige diskriminierende oder kriminelle Darstellungen in Bild, Ton oder Schrift missbräuchlich. Als Missbrauch gilt auch das Aufdrängen oder das Zur-Verfügung-Stellen von Darstellungen der vorbezeichneten Art an eine sonstige Benutzerin. Es wird ausdrücklich auf die strafrechtlichen Konsequenzen hingewiesen.

(3) Unbeschadet der Absätze 1 und 2 liegt Missbrauch insbesondere vor, wenn einer der folgenden Sachverhalte erfüllt ist:

(a) Benutzung von Dienstleistungen der Organisationseinheiten ohne Vorliegen einer gültigen Benutzungsgenehmigung,

(b) Arbeiten mit einer fremden Benutzungsgenehmigung ohne ausdrückliche Zustimmung der Antragstellerin, für den die Benutzungsgenehmigung erteilt wurde, sowie der Organisationseinheit,

(c) Arbeiten mit der eigenen Benutzungsgenehmigung an Problemen, die nicht im Zulassungsantrag angegeben sind,

(d) Nutzung der informationstechnischen Einrichtungen (z.B. durch Benutzung der Mail- oder Newsdienste) unter Vorspiegelung der Identität einer anderen Benutzerin (z.B. mit gefälschten oder anonymisierten Realnamen),

(e) vorsätzliche Verletzung von Zugriffsberechtigungen (z.B. Lesen, Verändern, Löschen und/oder anderweitiges Speichern von Daten und/oder Programmen einer anderen Benutzerin oder der jeweiligen Organisationseinheit ohne deren ausdrückliche Genehmigung, Ausspähen von Benutzerkennungen, etc.),

(f) Ermöglichen des unberechtigten Zugriffs dritter Personen auf die informationstechnischen Einrichtungen ohne ausdrückliche Erlaubnis der Organisationseinheit, insbesondere Weitergabe oder Zugänglichmachen vorgegebener Schutzmechanismen wie Passwörter, Schlüssel oder anderer technischer Hilfsmittel, die den Zugang oder Zugriff einschränken,

(g) Nutzung der Ressourcen in einem solchen Ausmaße, dass eine andere Benutzerin beeinträchtigt wird, wenn dies bei zumutbarem Aufwand vermeidbar gewesen wäre,

(h) Nutzung der informationstechnischen Einrichtungen zur Kontrolle einer anderen Benutzerin.

§ 13
Konsequenzen bei Verstößen

(1) Falls eine Benutzerin schuldhaft gegen nationale und internationale Schutzvorschriften, gegen diese Rahmenordnung der FHN, die Verwaltungs- und Benutzungsordnungen der zentralen Betriebseinheiten oder die hierauf beruhenden Ordnungen, Betriebsregelungen oder Dienstanweisungen der Organisationseinheiten der FHN verstößt oder durch ihr Verhalten der Betrieb der DV-Anlagen, DV-Geräte, Informations- und Kommunikationsdienste der Organisationseinheiten der FHN empfindlich gestört wird, kann die betroffene Organisationseinheit die Zulassung dieser Benutzerin vorübergehend einschränken und in besonders schwerwiegenden Fällen ihre Benutzerkennung sperren. Die Benutzerin muss davon unter Angabe der Gründe schriftlich in Kenntnis gesetzt werden; ihr ist Gelegenheit zur Stellungnahme zu geben. Die Betroffene kann die Vorsitzende der ADV-Kommission um Vermittlung anrufen oder Widerspruch einlegen, über den die Vorsitzende der Hochschulleitung nach Anhörung der ADV-Kommission entscheidet.

(2) Diejenige Benutzerin, die in besonders schwerwiegendem Maße gegen die Ordnungen der FHN, die Ordnungen, Betriebsregelungen oder Dienstanweisungen der Organisationseinheiten verstößt, kann von der weiteren Nutzung der DV-technischen Einrichtungen der Organisationseinheit ausgeschlossen werden.

(3) Werden die DV-Geräte, DV-Anlagen sowie die Informations- und Kommunikationsdienste der Organisationseinheiten für strafbare Handlungen sowie für Handlungen gemäß § 12 Absatz 2 missbraucht, wird die verantwortliche Benutzerin ohne vorherige Abmahnung und Androhung sofort von der weiteren Nutzung ausgeschlossen.

(4) Ein Ausschluss von der Benutzung wird von der Vorsitzenden der Hochschulleitung ausgesprochen. Die aus dem Nutzungsverhältnis entstandenen Verpflichtungen der Benutzerin werden durch Maßnahmen nach Absatz 1 oder einen Ausschluss nach Absatz 2 oder Absatz 3 nicht berührt; insbesondere bleibt der Anspruch der Hochschule auf das vereinbarte Entgelt im Rahmen der erfolgten Benutzung bestehen. Der Benutzerin stehen keine Schadensersatzansprüche aufgrund von Maßnahmen nach Absatz 1, Absatz 2 und/oder Absatz 3 zu.

(5) Unbeschadet der Maßnahmen nach Absatz 1, Absatz 2 und/oder Absatz 3 bleibt die Einleitung von arbeits-, dienstrechtlichen, zivil- oder strafrechtlichen Maßnahmen vorbehalten; auf die Straf- und Bußgeldvorschriften der §§ 33, 34 des DSG NRW wird besonders hingewiesen.
Die Leiterin der jeweiligen Organisationseinheit wird über die entsprechende Maßnahme informiert.

§ 14
Inkrafttreten

Diese Ordnung tritt am Tage nach ihrer Veröffentlichung im Verkündungsblatt der Fachhochschule Niederrhein in Kraft.