Leitlinie zur Informationssicherheit

vom 14.02.2019

Inhaltsverzeichnis

Grußwort des Präsidenten

Wir an der Hochschule Niederrhein wollen vor allem eines: gut ausbilden. Fachliche Exzellenz und die Fähigkeit zur Teamarbeit sind uns hier an der Hochschule Niederrhein besonders wichtig – sowohl in der Lehre wie in der Forschung.

Basis für eine hochwertige Lehre und Forschung an unserer Hochschule sowie für einen möglichst reibungslos arbeitenden Verwaltungsbereich bilden Informationen: Lehrinhalte, Forschungsergebnisse, Prüfungsdaten, aber auch Finanz- oder Personaldaten.

Ungewollte Publikation von Informationen, deren unberechtigte Manipulation oder ihr Missbrauch, aber auch eine wesentliche Unterbrechung des Geschäftsbetriebs können der Hochschule hohen Schaden zufügen, sei es finanziell oder mit Blick auf das gute Renommee unseres Hauses.

Unsere Abhängigkeit von modernen Informations- und Kommunikationstechnologien bei der Verarbeitung dieser Informationen nimmt immer weiter zu, genau so wie die fortschreitende Vernetzung sowohl der Hochschule als auch ihrer Angehörigen im beruflichen wie im privaten Bereich mit anderen Hochschulen, Institutionen und Personen durch eine immer intensivere Nutzung sozialer Medien und Netzwerke. Die schnellen Entwicklungen wie auch die immer kürzer werdenden Lebenszyklen von Anwendungen und Systemen erhöhen die Komplexität im Umgang mit der Informations- und Kommunikationstechnologie, vor allem für den normalen Benutzer.

Wollen wir die eigentlichen Werte der Hochschule, also unsere Informationen, schützen, müssen wir unsere IT-Systeme analysieren, Risikopotenziale ausloten, Gefahren erkennen und gewichten und dem Schutzbedarf entsprechend geeignete Sicherheitsmaßnahmen konsequent umsetzen.

Das Präsidium hat daher die folgende Leitlinie zur IT-Sicherheit erlassen.

Damit wir unseren eigenen Ansprüchen genügen können, bedarf es Ihrer aktiven Mitarbeit bei der Umsetzung unserer Sicherheitsmaßnahmen!

Für Ihre Unterstützung dankt

Ihr
Hans-Hennig von Grünberg
Präsident der Hochschule Niederrhein

1 Einleitung

1.1 Intention des Dokuments

Die Leitlinie zur Informationssicherheit der Hochschule Niederrhein (HN) beschreibt allgemeinverständlich, was Informationssicherheit ist und welche Bedeutung sie für die Hochschule Niederrhein hat. Das Dokument zeigt auf, wie Informationssicherheit an der HN gelebt wird, indem das zu erreichende Mindest-Sicherheitsniveau beschrieben wird sowie die angestrebten Informationssicherheitsziele und die verfolgte Informationssicherheitsstrategie dargestellt werden.

Die Leitlinie zur Informationssicherheit ist Bestandteil eines hierarchisch abgestuften Regelwerks. Ganz bewusst wurde diese Leitlinie frei gehalten von konkreten Regelungen oder Handlungsanweisungen, sondern hat eher einen allgemeinen Charakter. Sie soll im Gegensatz zu technischen Feinkonzepten oder organisatorischen Maßnahmen, welche einen dynamischen Charakter haben müssen, um auf aktuelle Gegebenheiten eingehen zu können, statisch sein und möglichst selten verändert werden.

1.2 Geltungsbereich der Leitlinie zur Informationssicherheit

Diese Leitlinie richtet sich an alle Mitglieder und Angehörige der Hochschule Niederrhein. Hierzu zählen auch die Beschäftigten von beauftragten Dienstleistungsunternehmen, Kooperationspartnern, An-Instituten und Nutzerinnen/Nutzer bei allen weiteren Einrichtungen, die an das Hochschulnetz angeschlossen sind oder dessen Netzinfrastruktur, IT-Dienste und/oder den Internetanschluss nutzen.

2 Definitionen und Erläuterungen

Bei der Gestaltung von Informationssicherheit orientiert sich die Hochschule Niederrhein an den Empfehlungen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und dessen Vorgehensweise zum IT-Grundschutz. Daher werden die meisten Begriffe analog zum BSI genutzt.

2.1 Begrifflichkeiten

Geltungsbereich

Der Geltungsbereich legt auf oberster Ebene fest, für welche Bereiche die Leitlinie zur Informationssicherheit gültig ist.

IT-Sicherheit

IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Dabei werden vor allem IT-Systeme, Kommunikationswege und Speichermedien sowie der Umgang damit betrachtet.

Informationssicherheit

Informationssicherheit hat den grundsätzlichen Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Der Begriff "Informationssicherheit" statt IT-Sicherheit ist daher umfassender und wird zunehmend verwendet.

Informationstechnik (IT)

Informationstechnik (IT) im Sinne der Leitlinie zur Informationssicherheit umfasst alle Formen der elektronischen Informationsverarbeitung und Telekommunikation.

IKT

Informations- und **K**ommunikations**T**echologie – Erweiterung der IT als reine Datenverarbeitung um Aspekte der Kommunikation (Telefonanlagen, …).

2.2 Dokumente der Informationssicherheit

Die folgenden Erläuterungen lehnen sich an die Definitionen des BSI an.

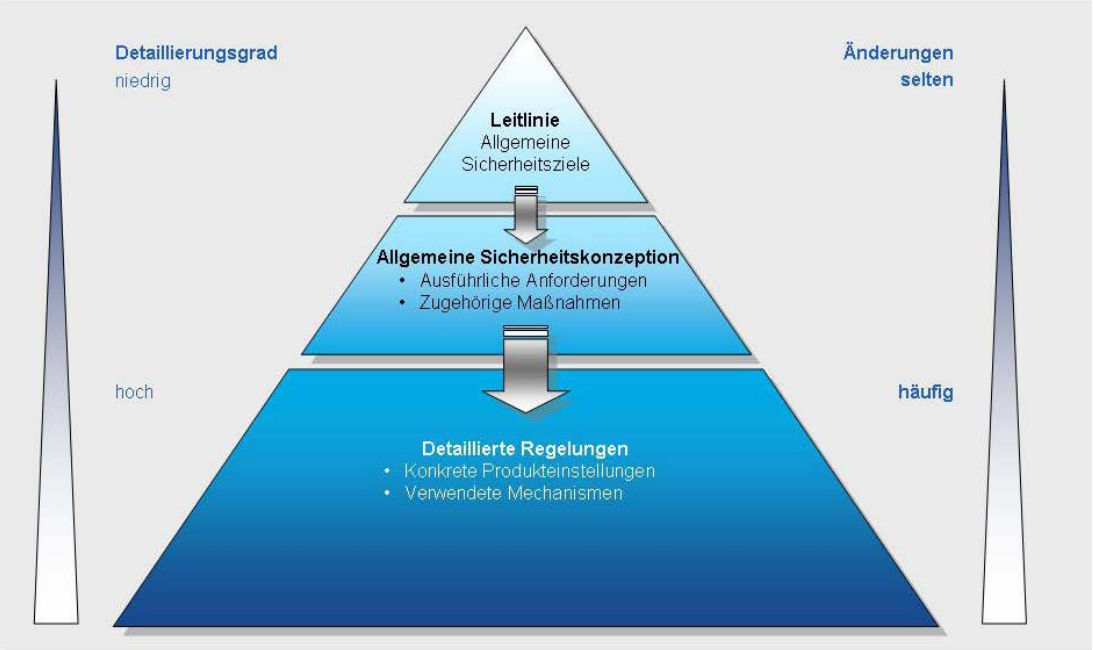

Abb. 1: Beispiel für den hierarchischen Aufbau von sicherheitsrelevanten Dokumenten

Leitlinie zur Informationssicherheit

Die Leitlinie zur Informationssicherheit beschreibt allgemeinverständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Hochschule hergestellt werden soll. Sie beinhaltet die angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Leitlinie zur Informationssicherheit beschreibt damit auch das angestrebte Sicherheitsniveau in der Hochschule.

Sicherheitskonzept

Zum Erreichen der in der Leitlinie zur Informationssicherheit festgeschriebenen Ziele wird ein Sicherheitskonzept entworfen und umgesetzt.

Dieses Sicherheitskonzept ist das zentrale Dokument im Informationssicherheitsprozess der Hochschule Niederrhein. Es dient zur Umsetzung der definierten Informationsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele zu erreichen. Das Sicherheitskonzept wird in regelmäßigen Abständen einer Qualitätskontrolle unterzogen und entsprechend aktualisiert.

Sicherheitsrichtlinie

Sicherheitsrichtlinien beschreiben konkrete Maßnahmen zum Umgang mit Anwendungsprogrammen, Netzwerkkomponenten und IT-Systemen, die Informationen verarbeiten. Ebenfalls werden Zutrittsregeln für Räumlichkeiten und Einrichtungen, Zugangsregeln für IT-System/Komponenten und Zugriffsregeln auf Informationen durch Sicherheitsrichtlinien festgehalten. Die Einhaltung und Umsetzung dieser Richtlinien ist für alle Personen verbindlich. Sicherheitsrichtlinien können hochschulweiten Charakter haben. In Abhängigkeit von Umsetzbarkeit und Bedarf können aber auch (fach)bereichs- oder zielgruppenspezifische Vorgaben formuliert werden.

2.3 Grundwerte der Informationssicherheit

Aufgabe der Informationssicherheit ist der angemessene Schutz der drei Grundwerte.

- **Integrität**

  Mit diesem Begriff wird die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen bezeichnet. Bei intakter Integrität sind Daten vollständig und unverändert. Eventuell zugehörige Attribute wurden nicht unerlaubt manipuliert.

- **Verfügbarkeit**

  Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

- **Vertraulichkeit**

  Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen, aber auch der Zutritt zu Räumlichkeiten dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Die Einhaltung weiterer Grundwerte wird für personenbezogene Daten durch den Datenschutz geprüft.

Die hier aufgeführten Definitionen erheben keinen Anspruch auf Vollständigkeit. In Abhängigkeit von den zu schützenden Informationen können sie konkretisiert und ergänzt werden. Auch können je nach Situation, Daten oder Bereich weitere Informationssicherheitsziele eine Rolle spielen.

2.4 Sicherheitsniveau – allgemeine Aussagen

Die Anforderungen an die Informationssicherheit werden davon bestimmt, wie hoch der Schutzbedarf der betrachteten Daten bzw. Informationen ist. Dies beeinflusst im Sinne einer Vererbung die Festlegung des Schutzbedarfs für alle damit verbundenen „Objekte“ (Client, Anwendung, Raum, Netzwerkkomponente usw.).

Im Sinne einer möglichst standardisierten Vorgehensweise wird für die Festlegung des Schutzbedarfs eines Objektes die Definition der Schutzbedarfskategorien in der jeweils gültigen Fassung verwendet.

3 Informationssicherheit an der Hochschule Niederrhein

3.1 Stellenwert der Informationssicherheit an der Hochschule Niederrhein

Die Hochschule Niederrhein ist in der deutschen Hochschullandschaft eine renommierte und attraktive Bildungs- und Forschungseinrichtung. Mit der Anzahl an Studierenden an den Standorten Krefeld und Mönchengladbach gehört die Hochschule zu den größten und beliebtesten in Nordrhein-Westfalen.
Fachliche Exzellenz und integrative Kompetenz sind die Ausbildungsziele und Basis für Lehre und Forschung. Dieser Bildungsauftrag stützt sich auf ein breites Netzwerk von Unternehmen aus der regionalen Wirtschaft, Partnerhochschulen, Instituten, Studierenden und Mitarbeitern.
Zudem erfordert die Vielzahl eigenständiger Einrichtungen, Organisationseinheiten sowie das oben genannte Netzwerk einen erheblichen Verwaltungsapparat, den die Beschäftigten in Forschung und Verwaltung nur mit Unterstützung der Informationstechnologie bewältigen können.

Moderne Informationstechnologie (IT) wird zunehmend zur Erfüllung dieser Ziele und Aufgaben eingesetzt.

Die Heterogenität, also Verschiedenartigkeit, der Systeme und Komponenten im IT-Umfeld und Nutzerinnen/Nutzer sowie der zu verarbeitenden Informationen, die in der Vielzahl der bereits erwähnten Einrichtungen, Organisationseinheiten und Institute begründet liegt, bietet ein hochinteressantes und breites Angriffsziel für sicherheitskritische Angriffe von innen und außen.

Neben der Abwehr dieser Angriffe auf Daten und Systeme ist die Aufrechterhaltung des Geschäftsbetriebs, also der Lehre und Forschung sowie der Administration und Organisation, ein wesentliches Ziel der Informationssicherheit.

Durch die Umsetzung von Sicherheitsmaßnahmen soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheit geboten wird, um Informationswerte und personenbezogene Daten zu schützen und die Verfügbarkeit zu gewährleisten.

3.2 Leitsätze der Informationssicherheit an der HN

Die Informationssicherheit an der Hochschule Niederrhein orientiert sich an den folgenden Leitsätzen:

- Die HN ist bestrebt, im Rahmen des Geltungsbereiches eine offene IT-Infrastruktur zu betreiben und einen offenen Informationsaustausch zu gewährleisten, sofern keine rechtlichen Belange (z. B. dienst-, urheber- und datenschutzrechtlich) verletzt werden.
- Die HN orientiert sich bei der Ausgestaltung ihres Informationssicherheitsprozesses an der Methodik des IT-Grundschutz gemäß BSI.
- Ziel von Informationssicherheit an der HN ist es, einen Zustand zu erreichen bzw. zu erhalten, in dem die Grundwerte der Informationssicherheit entsprechend der Vorgaben der Hochschulleitung und bestehender rechtlicher Auflagen gewahrt werden und die potentiellen Bedrohungen nur so wirksam werden können, dass die verbleibenden Risiken tragbar sind. Der Fokus liegt dabei auf Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit des jeweiligen Zielobjekts.
- Der Erfolg von Informationssicherheit kann nur gewährleistet werden, wenn hochschulweit einheitliche und angemessene Sicherheitsstandards im Sinne eines Mindeststandards definiert und etabliert werden.
- Die Etablierung eines umfassenden Informationssicherheitsprozesses wird durch das Präsidium initiiert und aktiv unterstützt.
- Informationssicherheit ist eine Gemeinschaftsaufgabe, die von allen Nutzerinnen/Nutzern der IT-Infrastruktur wahrgenommen werden muss. Eine erfolgreiche Umsetzung ist nur durch eine offene Kommunikation und Sensibilisierung der Nutzerinnen/Nutzer sowie durch Einhaltung der Sicherheitsrichtlinien möglich.
- Aufwand (finanziell wie personell) und Ziele von Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinander stehen.

Informationssicherheit ist kein einmaliges Projekt. Informationssicherheit ist ein Prozess, der die Überwachung und Weiterentwicklung der Sicherheitsstandards erfordert. Zur Erfüllung ist die Einführung von Qualitätssicherungsmaßnahmen notwendig.

Hierzu werden seitens der Informationssicherheit-Verantwortlichen alle erforderlichen Maßnahmen getroffen.

4 Informationssicherheitsleitlinie der Hochschule Niederrhein

4.1 Informationssicherheitsziele

Die Aufgaben in Lehre und Forschung sowie Administration und Verwaltung an der HN werden, wie Eingangs beschrieben, zunehmend von der Nutzung der Informationstechnologie als modernes Lehr-, Informations- und Kommunikationsmedium bestimmt.

Daher verfolgt die Hochschule mit Fokus auf Bewahrung der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität die folgenden allgemeingültigen Informationssicherheitsziele:

- Zuverlässige Unterstützung des Hochschulbetriebs und der Geschäftsprozesse durch die IT
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Organisation
- Schutz von Daten und Informationen unter Berücksichtigung ihrer spezifischen Anforderungen (personenbezogene Daten, Verwaltungs- oder Forschungsdaten usw.)
- Schutz der Infrastruktur gegen Missbrauch von innen und außen
- Einhaltung gesetzlicher Vorgaben zum Umgang mit Informationen und Systemen
- Gewährleistung des informationellen Selbstbestimmungsrechts des Betroffenen bei der IT-gestützten Verarbeitung personenbezogener Daten
- Aufrechterhaltung der positiven Außendarstellung

Fachbereiche und Organisationseinheiten können für ihren Bereich weitere, individuelle Informationssicherheitsziele formulieren.

4.2 Sicherheitsniveau

Ziel von Informationssicherheit an der HN ist es, hochschulweit mindestens ein Sicherheitsniveau zu erreichen, das für den normalen Schutzbedarf (gemäß BSI) hochschulrelevanter Informationen angemessen und ausreichend ist (s. 2.4 IT-Sicherheitsniveau – allgemeine Aussagen).

Die hierzu umzusetzenden Maßnahmen liefern einerseits einen soliden Grundschutz für alle Daten und die verbundenen Komponenten, dienen aber andererseits auch als Basis für weitergehende Aktivitäten:

→ Hochschutzbedürftige Informationen, IT-Systeme und Anwendungen usw. werden über diesen Grundschutz hinaus individuell analysiert und abgesichert!

4.3 Informationssicherheitsstrategie

Die Informationssicherheitsstrategie wird durch die Leitung der Hochschule festgelegt und niedergeschrieben. Dabei wird ihr vom Informationssicherheitsbeauftragten (ISB) sowie dem Arbeitskreis Informationssicherheit zugearbeitet.

Die Hochschule orientiert sich bei der Gestaltung von Informationssicherheit am BSI und dessen Methodik des IT-Grundschutz. Eine hochschulweite Zertifizierung wird zurzeit nicht angestrebt.

Für die Erstellung sicherheitsrelevanter Dokumente ist eine strukturierte Hierarchie in Pyramidenform vorgegeben.

Um das definierte Sicherheitsniveau der HN aufrecht zu erhalten, ist eine fortlaufende Kontrolle und Verbesserung der implementierten Sicherheitsmaßnahmen, Dokumente und des festgelegten Informationssicherheitsprozesses zwingend erforderlich. Dazu findet regelmäßig eine Erfolgskontrolle und Bewertung durch die Leitungsebene (Präsidium, CIO, ISB) statt. Hierzu beauftragt der CIO den ISB . Ebenso wird auch die Leitlinie zur Informationssicherheit mindestens alle zwei Jahre, durch den ISB überprüft und aktualisiert. Der ISB wird dabei durch den Arbeitskreis Informationssicherheit unterstützt.

4.4 Informationssicherheitsorganisation

Die Gesamtverantwortung für Informationssicherheit an der HN fällt in den Bereich des Präsidiums.

Das Präsidium hat einen ISB eingesetzt, welcher für alle Belange der Informationssicherheit innerhalb der Institution zuständig ist. Er berät das Präsidium in Fragen der Informationssicherheit und unterstützt bei der Umsetzung.

Um eine praxis- und zeitnahe Gestaltung von Informationssicherheit an der Hochschule zu gewährleisten, sollen zukünftig verschiedene Fachkräfte der HN in einem Arbeitskreis (AK) Informationssicherheit zusammenarbeiten. Diesem AK gehören an:

- Informationssicherheitsbeauftragter
- Datenschutzbeauftragte und Stellvertreter
- Leiter der zentralen Einrichtung Kommunikations- und Informationssysteme Service KIS,
- Fachkräfte aus den Fachbereichen (FB) und Einrichtungen.

Der AK wird durch den CIO oder dem ISB initiiert und trifft sich quartalsweise. Anforderungsorientiert können weitere Treffen anberaumt werden. Arbeitsweise sowie Struktur und Arbeitsergebnisse durchgeführten Treffen des Arbeitskreises werden separat dokumentiert.

Der ISB ist organisatorisch am Präsidium angesiedelt. Er berichtet direkt an den CIO sowie

den an die VPWP der Hochschule.

Die direkte Kommunikation und Abstimmung mit der Datenschutzbeauftragten, welche ebenfalls dem Präsidium zuarbeitet und fachlich weisungsungebunden ist, sichert die hohe Qualität der Ergebnisse.

Die aktuelle Version des Organisationsdiagramms der Ressorts der HN wird auf der Internetseite der HN publiziert und ist unter folgendem Link abrufbar:

https://www.hs-niederrhein.de/organigramm

Organisationsdiagramm der Ressorts der VPWP (Stand Januar 2018):

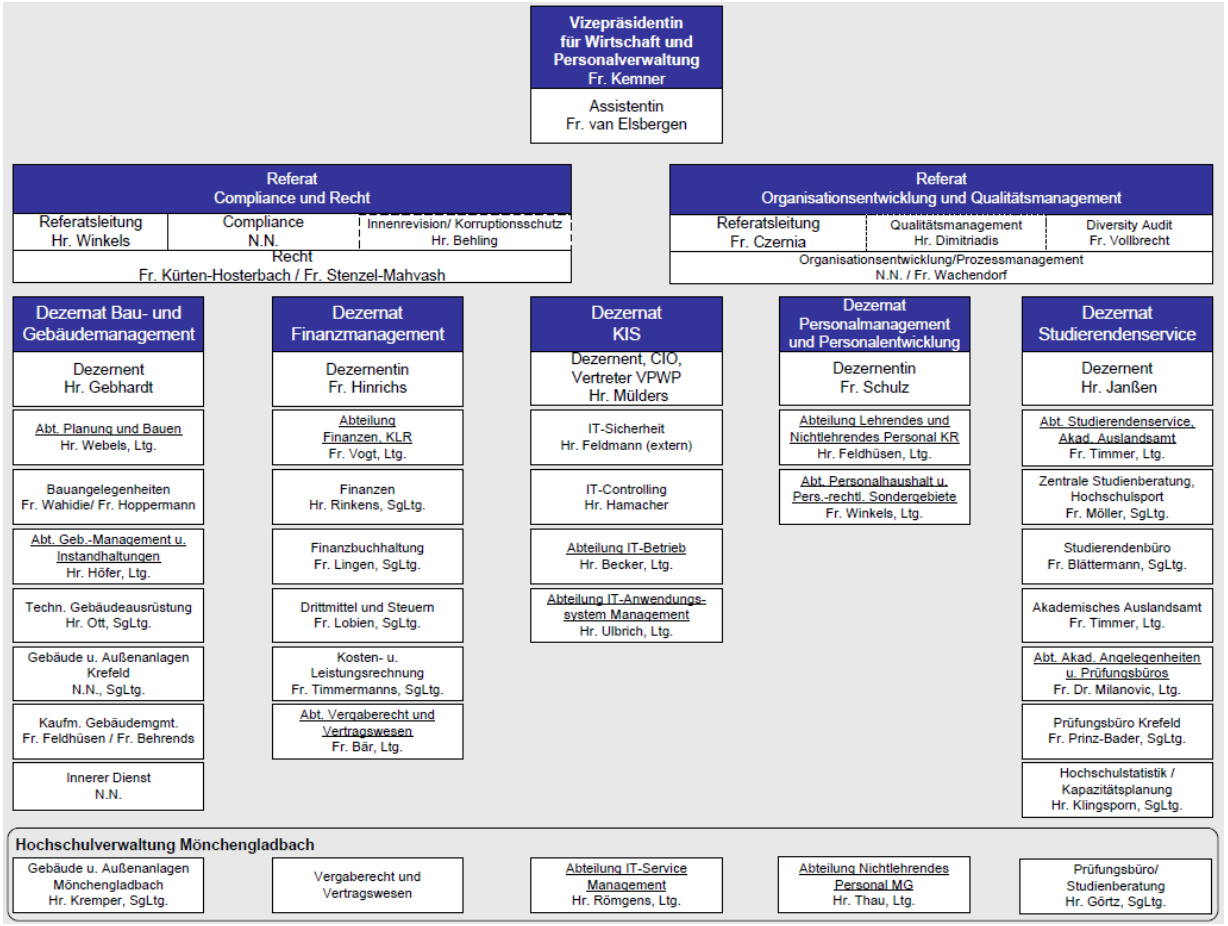

Abb. 2: Organisationsdiagramm der Ressorts der VPWP (Stand Januar 2018)

5 Schlusswort

Funktionierende und sichere Geschäftsprozesse sind eine maßgebliche Voraussetzung für die Leistungsfähigkeit einer Hochschule auf den Gebieten Lehre und Forschung. Wenn die Grundregeln im Umgang mit Informationen und der IT als Werkzeug zu deren Verarbeitung eingehalten werden, werden damit die gute Qualität des Lehrangebotes der Hochschule, aber auch die Arbeitsplätze der vielen hundert Menschen, die an, mit oder für die HN tätig sind, gesichert.

Die Leitung der Hochschule Niederrhein ist sich ihrer Verantwortung für die Informationssicherheit bewusst und unterstützt daher nachdrücklich jegliche Bemühungen.

Das wertvollste Glied in dieser Kette ist jedoch der gesunde Menschenverstand jeder einzelnen Nutzerin, jedes einzelnen Nutzers und Ihre persönliche Bereitschaft, einen Beitrag zur Informationssicherheit leisten.

6 In-Kraft-Treten

Diese Leitlinie tritt mit sofortiger Wirkung in Kraft und ersetzt die Leitlinie vom 05.06.2012

Krefeld, den 14. Februar 2019

Hans-Hennig von Grünberg
(Präsident)

Abbildungsverzeichnis

Quellenangaben

- Datenschutz
- Landesdatenschutzgesetz Nordrhein-Westfalen DSG NRW
- Bundesamt für Sicherheit in der Informationstechnik BSI
    - IT-Grundschutz-Kompendium
    - BSI-Standard 200-2 IT-Grundschutz-Vorgehensweise, Version 1.0

Änderungshistorie

Datum	Version	Autor	Beschreibung
05.06.2012	1.0	M. Grofe-Juhlke, IT-Sicherheitsbeauftragte	Erstellung der IT-Sicherheitsleitlinie
19.12.2018	2.0	Hochschule Niederrhein, Patrick Feldmann, Informationssicherheitsbeauftragter	Aktualisierung der Leitlinie
11.02.2019	2.1	Hochschule Niederrhein, Malte Stock, Informationssicherheitsbeauftragter	Organigramm der Hochschule Niederrhein entfernt und durch Link zur Webseite ersetzt.