Hochschule Niederrhein
University of Applied Sciences

Amtliche Bekanntmachungen

Herausgegeben im Auftrag des Präsidenten der Hochschule Niederrhein

37. Jahrgang Ausgegeben zu Krefeld und Mönchengladbach am 28. September 2012 Nr. 30

Inhalt

Hochschule Niederrhein
University of Applied Sciences

Leitlinie zur IT-Sicherheit

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 IT-Sicherheitsleitlinie der Hochschule Niederrhein beschreibt allgemeinverständlich, was IT-Sicherheit ist und welche Bedeutung sie für die Hochschule Niederrhein hat. Das Dokument zeigt weiterhin auf, wie IT-Sicherheit an der HN gelebt wird, indem das zu erreichende Mindest-IT-Sicherheitsniveau aufgezeigt wird sowie die angestrebten IT-Sicherheitsziele und die verfolgte IT-Sicherheitsstrategie dargestellt werden.

Die IT-Sicherheitsleitlinie 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 wie neue Verfahren oder einen Produktwechsel eingehen zu können, statisch sein und möglichst selten verändert werden.

1.2 Geltungsbereich der IT-Sicherheitsleitlinie

Diese Leitlinie richtet sich an alle Mitglieder und Angehörige der Hochschule Niederrhein. Es werden alle jene Personen angesprochen, die IT-Systeme der HN und die zugrunde liegende Infrastruktur nutzen. 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 IT-Sicherheit orientiert sich die Hochschule Niederrhein an den Empfehlungen des Bundesamtes 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 IT-Sicherheitsleitlinie 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 IT-Sicherheitsleitlinie 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 IT-Sicherheit

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

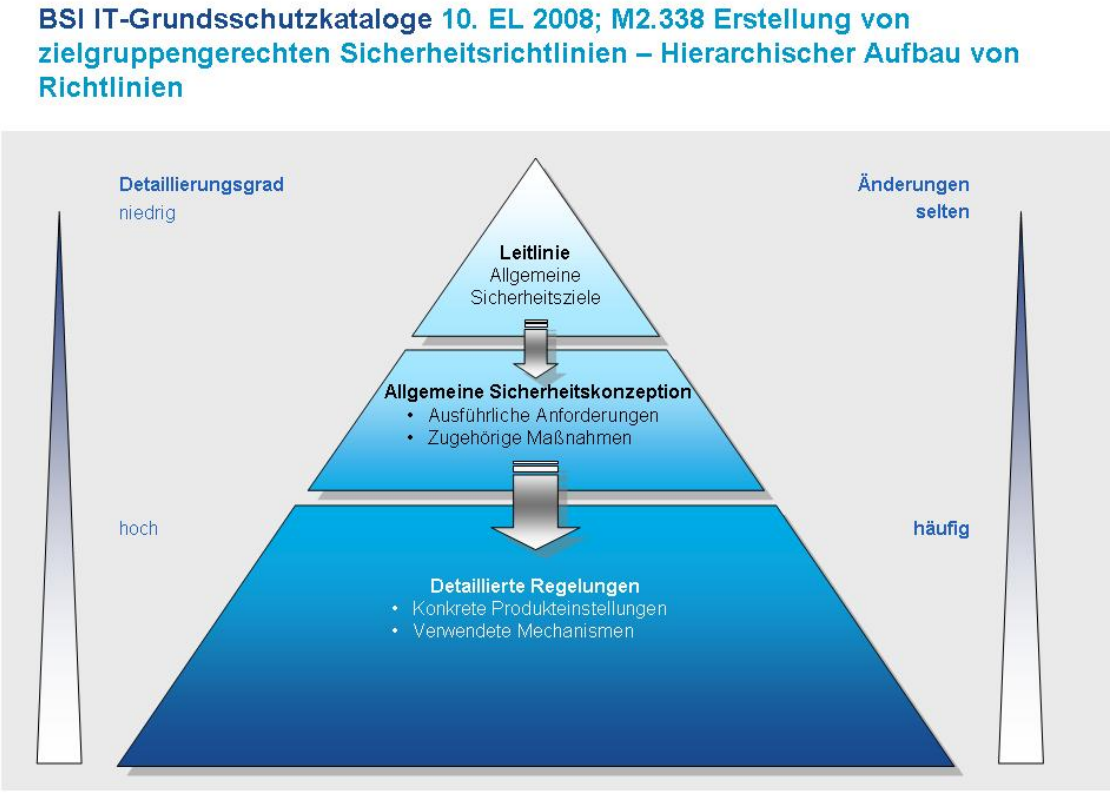

Abb. 1: Beispiel für den hierarchischen Aufbau von IT-Sicherheitsrelevanten Dokumenten

IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie beschreibt allgemeinverständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen IT-Sicherheit innerhalb der Hochschule hergestellt werden soll. Sie beinhaltet die angestrebten IT-Sicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die IT-Sicherheitsleitlinie beschreibt damit auch die IT-Sicherheitsziele und das angestrebte IT-Sicherheitsniveau in der Hochschule.

IT-Sicherheitskonzept

Zum Erreichen der in der IT-Sicherheitsleitlinie festgeschriebenen Ziele wird ein IT-Sicherheitskonzept entworfen und umgesetzt.

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

IT-Sicherheitsrichtlinie

IT-Sicherheitsrichtlinien, häufig auch mit dem engl. Begriff „Policies“ bezeichnet, beschreiben konkrete Maßnahmen zum Umgang mit Anwendungsprogrammen, Netzwerkkomponenten und IT-Systemen, die Informationen verarbeiten[1]. Ebenfalls werden Zugangs- und Zutrittsregeln für Räumlichkeiten und Einrichtungen, die den Zugriff auf IT-Systeme und Informationen gewähren, durch IT-Sicherheitsrichtlinien festgehalten. Die Einhaltung und Umsetzung dieser Richtlinien ist für alle Personen verbindlich. IT-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 IT-Sicherheit

Allgemein anerkannte Oberbegriffe der IT-Sicherheit sind[2]:

- **Authentizität**

  Hiermit wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

- **Integrität**

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

- **Nichtabstreitbarkeit:**

  Hierbei liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen

  - Nichtabstreitbarkeit der Herkunft
  - Nichtabstreitbarkeit des Erhalts

[1] § 3 Abs. (2) DSG NRW: „Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten.“

[2] In Anlehnung an BSI IT Grundschutzkataloge – 11. Ergänzungslieferung: Kap. 4 Glossar und Begriffsdefinitionen

- **Verbindlichkeit**

  Hierunter werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

- **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 dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Die Ziele Vertraulichkeit, Verfügbarkeit und Integrität werden häufig als die *Grundwerte der IT- und Informationssicherheit* bezeichnet.

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 IT-Sicherheitsziele eine Rolle spielen.

2.4 IT-Sicherheitsniveau – allgemeine Aussagen

Die Anforderungen an die IT-Sicherheit 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“ (PC, Anwendung, Raum, Netzwerk usw.).

Im Sinne einer möglichst standardisierten Vorgehensweise wird für die Festlegung des Schutzbedarfs eines Objektes die Zuordnung zu einer der folgenden Kategorien durchgeführt[3]:

- **normal**
  Die Schadensauswirkungen sind begrenzt und überschaubar.

- **hoch**
  Die Schadensauswirkungen können beträchtlich sein oder können mehrere Organisationseinheiten der Hochschule umfassen.

[3] Gemäß BSI Standard 100-2 IT-Grundschutz-Vorgehensweise, Kap. 4.3 Schutzbedarfsfeststellung

- **sehr hoch**
  Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß für die gesamte Hochschule und ihre angeschlossen Institute und Einrichtungen erreichen.

Beispielhafte Kriterien zur Festlegung der Schutzbedarfskategorie *normal* sind gemäß BSI:

- Der Schutz von Informationen, die nur für den internen Gebrauch bestimmt sind, muss gewährleistet sein.
- Kleinere Fehler können toleriert werden. Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkenn- oder vermeidbar sein.
- Längere Ausfallzeiten, die zu Terminüberschreitungen führen, sind nicht zu tolerieren.
- Der Schutz personenbezogener Daten muss gewährleistet sein. Anderenfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Insgesamt gilt: Schäden haben Beeinträchtigungen der Institution zur Folge.

Informationen sowie die zur Verarbeitung genutzten Anwendungen und IT-Systeme haben einen *normalen* Schutzbedarf, wenn durch den Verlust an Vertraulichkeit, Integrität und Verfügbarkeit beispielsweise

- ein Verstoß rechtlich gesehen nur geringfügige Folgen nach sich zieht,
- eine Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen nicht möglich ist oder für diesen tolerabel bleibt,
- eine Beeinträchtigung der persönlichen Unversehrtheit des Einzelnen nicht möglich ist,
- die Aufgabenerfüllung nur geringfügig beeinträchtigt ist,
- nur eine geringe Ansehens- und Vertrauensbeeinträchtigung zu befürchten ist und der finanzielle Schaden tolerabel bleibt.

Der *normale* Schutzbedarf stellt für Informationen mit hohem oder sehr hohem Schutzbedarf sowie die zu ihrer Verarbeitung genutzten Anwendungen und IT-Systeme eine Basis-Sicherung dar, reicht aber möglicherweise nicht alleine zur Sicherung aus. Hier müssen ergänzende Maßnahmen auf Basis einer differenzierten Sicherheitsanalyse ergriffen und die Schutzbedarfskategorien *hoch* oder *sehr hoch* angewendet werden.

3 IT-Sicherheit an der Hochschule Niederrhein

3.1 Stellenwert der IT-Sicherheit an der Hochschule Niederrhein

Die Hochschule Niederrhein ist in der deutschen Hochschullandschaft eine renommierte und attraktive Bildungs- und Forschungseinrichtung. Mit rund 12.000 Studierenden an den Standorten Krefeld und Mönchengladbach gehören wir zu den größten und beliebtesten Hochschulen in Nordrhein-Westfalen.
Fachliche Exzellenz und integrative Kompetenz sind unsere 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 unsere mehr als 600 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 IT-Systeme 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 IT-Sicherheit an der Hochschule Niederrhein.

Durch die Umsetzung von IT-Sicherheitsmaßnahmen soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden (können), um Informationswerte und personenbezogene Daten zu schützen und um die Verfügbarkeit von IKT-Verfahren zu gewährleisten.

3.2 Leitsätze der IT-Sicherheit an der HN

Die IT-Sicherheit an der Hochschule Niederrhein orientiert sich an den folgenden Leitsätzen:

- Die HS Niederrhein 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 Hochschule Niederrhein orientiert sich bei der Ausgestaltung ihres IT-Sicherheitsprozesses an der Methodik des IT-Grundschutz gemäß Bundesamt für Sicherheit in der Informationstechnik BSI.
- Ziel von IT-Sicherheit an der HN ist es, einen Zustand zu erreichen bzw. zu erhalten, in dem die Grundwerte der IT-Sicherheit 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 von Daten und IT-Systemen.
- Der Erfolg von IT-Sicherheit kann nur gewährleistet werden, wenn hochschulweit einheitliche und angemessene IT-Sicherheitsstandards im Sinne eines Mindeststandards definiert und etabliert werden.
- Die Etablierung eines umfassenden IT-Sicherheitsprozesses ist nur durch die Initiierung und aktive Unterstützung des Präsidiums möglich.
- IT-Sicherheit 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 IT-Sicherheitsrichtlinien möglich. Um also hochschulweit einen wirksamen Schutz zu erreichen, ist die aktive Mitwirkung aller Nutzerinnen/Nutzer unverzichtbar.
- Aufwand (finanziell wie personell) und Ziele von Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinander stehen.

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

Hierzu werden seitens der IT-Sicherheits-Verantwortlichen alle erforderlichen Maßnahmen getroffen.

4 IT-Sicherheitsleitlinie der Hochschule Niederrhein

4.1 IT-Sicherheitsziele

Die Aufgaben in Lehre und Forschung sowie Administration und Verwaltung an der Hochschule Niederrhein 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 IT-Sicherheitsziele:

- 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 Informationen, Verwaltungs- oder Forschungsdaten usw.)
- Schutz der IT-Infrastruktur gegen Missbrauch von innen und außen
- Einhaltung gesetzlicher Vorgaben zum Umgang mit Informationen und IT-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 IT-Sicherheitsziele formulieren.

4.2 IT-Sicherheitsniveau an der HN

Ziel von IT-Sicherheit an der Hochschule Niederrhein ist es, hochschulweit mindestens ein IT-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 IT-Sicherheitsstrategie

Die IT-Sicherheitsstrategie wird durch die Leitung der Hochschule festgelegt und niedergeschrieben. Dabei wird ihr von der IT-Sicherheitsbeauftragten sowie dem Arbeitskreis IT-Sicherheit zugearbeitet.

Die Hochschule orientiert sich bei der Gestaltung von IT-Sicherheit am Bundesministerium für Sicherheit in der Informationstechnik (BSI) und dessen Methodik des IT-Grundschutz. Eine hochschulweite Zertifizierung wird zurzeit nicht angestrebt. Eine Einzelbetrachtung ausgewählter Bereiche der Hochschule wird in Betracht gezogen.

Für die Erstellung IT-Sicherheitsrelevanter Dokumente ist eine strukturierte Hierarchie in Pyramidenform vorgegeben.

Um das definierte IT-Sicherheitsniveau der Hochschule Niederrhein aufrecht zu erhalten, ist eine fortlaufende Kontrolle und Verbesserung der implementierten Sicherheitsmaßnahmen, Dokumente und des festgelegten IT-Sicherheitsprozesses zwingend erforderlich. Dazu findet regelmäßig eine Erfolgskontrolle und Bewertung durch die Leitungsebene (Präsidium, CIO, IT-Sicherheitsbeauftragte) statt. Dies wird durch die IT-Sicherheitsbeauftragte initiiert. Ebenso wird auch die IT-Sicherheitsleitlinie jeweils im 1. Quartal eines Jahres durch die IT-Sicherheitsbeauftragte überprüft und aktualisiert. Sie wird dabei durch den Arbeitskreis IT-Sicherheit unterstützt.

Der Review-Zyklus erstreckt sich über mehrere Jahre.

4.4 IT-Sicherheitsorganisation

Die Gesamtverantwortung für IT-Sicherheit an der Hochschule Niederrhein fällt in den Bereich des Präsidiums.

Das Präsidium setzt eine IT-Sicherheitsbeauftragte ein, welche zuständig ist für alle Belange der IT-Sicherheit innerhalb der Institution. Sie berät das Präsidium in Fragen der IT-Sicherheit und unterstützt bei der Umsetzung.

Um eine praxis- und zeitnahe Gestaltung von IT-Sicherheit an der Hochschule zu gewährleisten, arbeiten verschiedene Fachkräfte der HN in einem Arbeitskreis (AK) IT-Sicherheit zusammen. Diesem AK IT-Sicherheit gehören zurzeit an:

- die IT-Sicherheitsbeauftragte der HN,
- die Datenschutzbeauftragte der HN,
- der Leiter der zentralen Einrichtung Kommunikations- und Informationssysteme Service KIS,
- Fachkräfte aus den Fachbereichen (FB) und Einrichtungen.

Eine der ersten Aufgaben des Arbeitskreises war die gemeinsame Erarbeitung dieser IT-Sicherheitsleitlinie.

Arbeitsweise sowie Struktur und Arbeitsergebnisse der regelmäßigen quartalsweise angesetzten sowie bei Bedarf durchgeführten Treffen des Arbeitskreises werden separat dokumentiert.

Die IT-Sicherheitsbeauftragte ist organisatorisch in der zentralen Einrichtung Kommunikations- und Informationssysteme Service – kurz KIS – zu finden. Sie berichtet direkt an den CIO sowie den Präsidenten der Hochschule.

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

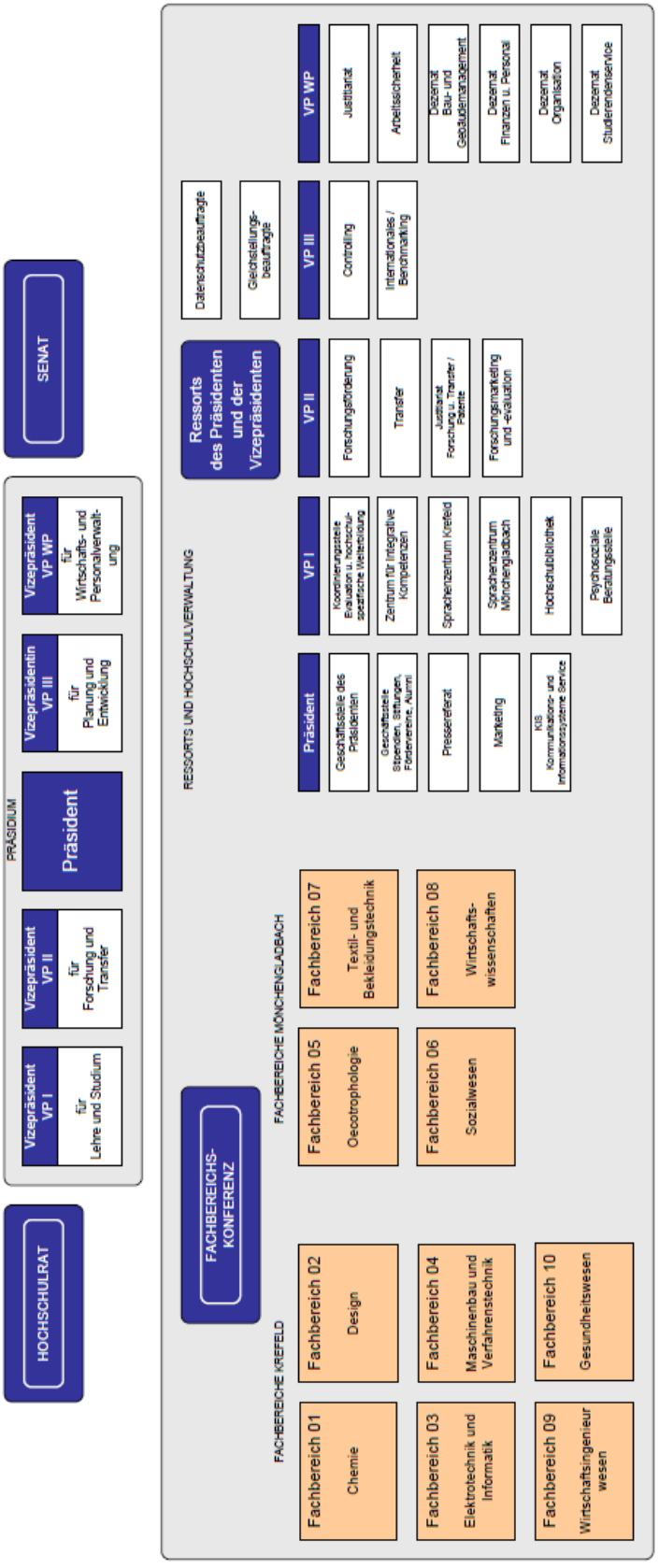

Abb. 2: Organisationsdiagramm der Hochschule Niederrhein (Stand April 2011)

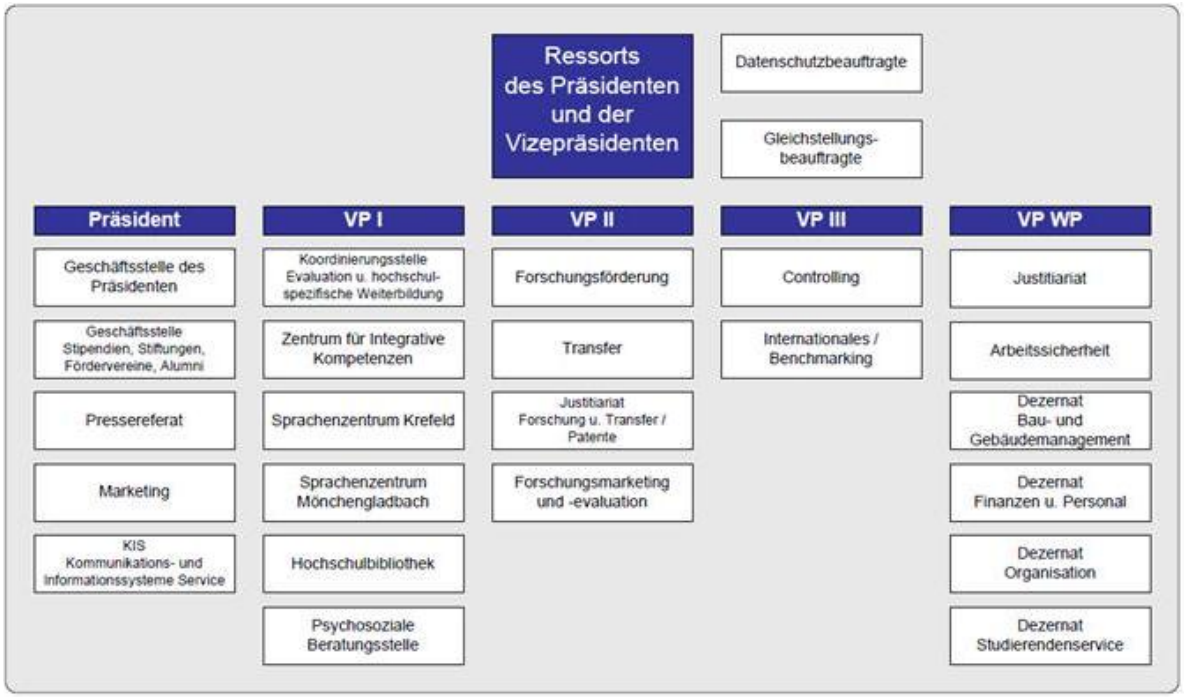

Abb. 3: Organisationsdiagramm der Ressorts der HN (Stand Juli 2011)

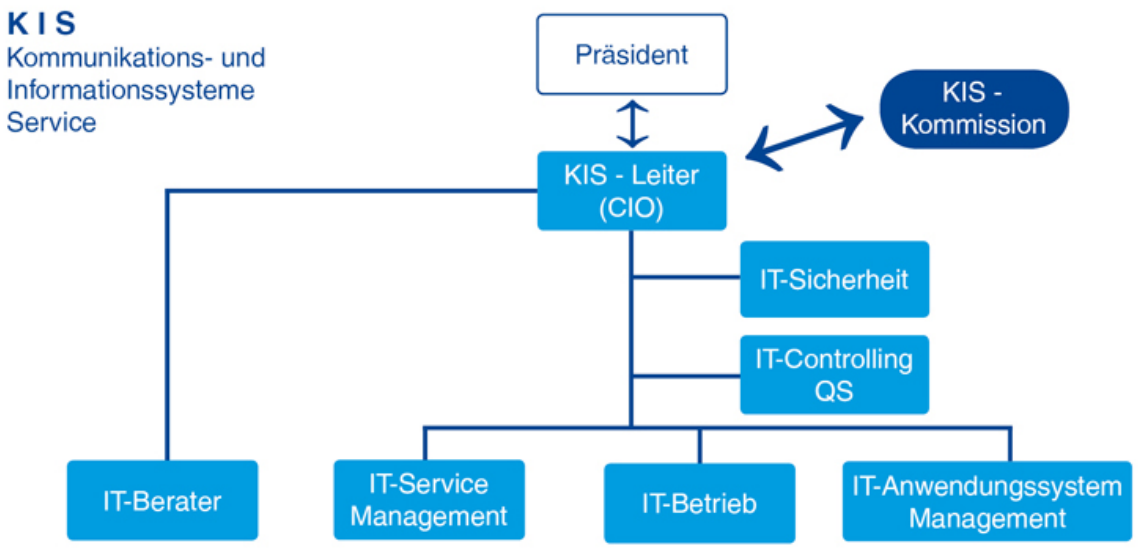

Abb. 4: Organisationsdiagramm der KIS (Stand Juli 2011)

Vertraulichkeit der Kommunikation zwischen Nutzern/Nutzerinnen und der IT-Sicherheitsbeauftragten ist eine Selbstverständlichkeit.

5 Schlusswort

Funktionierende und sichere IT-Prozesse sind eine maßgebliche Voraussetzung für die Leistungsfähigkeit einer Hochschule auf den Gebieten Lehre und Forschung. Wenn wir einige Grundregeln im Umgang mit Informationen und der IT als Werkzeug zu deren Verarbeitung einhalten, sichern wir damit einerseits die gute Qualität des Lehrangebotes unserer Hochschule, aber auch die Arbeitsplätze der vielen hundert Menschen, die an, mit oder für die HN tätig sind.

Die Leitung der Hochschule Niederrhein ist sich ihrer Verantwortung auch für die IT-Sicherheit 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 zu leisten.

IT-Sicherheit schützt IT.

IT-Sicherheit schützt Informationen.

IT-Sicherheit schützt uns.

Abbildungsverzeichnis

Quellenangaben

- Landesdatenschutzgesetz Nordrhein-Westfalen DSG NRW
- Bundesamt für Sicherheit in der Informationstechnik BSI
  - IT-Grundschutz-Kataloge, 11. Ergänzungslieferung,
  - BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise, Version 2.0

Änderungshistorie

Datum	Version	Autor	Beschreibung
05.06.2012	1.0	M. Grofe-Juhlke, IT-Sicherheitsbeauftragte	Erstellung der IT-Sicherheitsleitlinie