

Benutzungsrahmenordnung (Satzung) für die Kommunikations- und Datenverarbeitungsinfrastruktur der Fachhochschule Kiel

Aufgrund des § 34 Abs. 3 des Gesetzes über die Hochschulen und das Universitätsklinikum Schleswig-Holstein (Hochschulgesetz - HSG) in der Fassung der Bekanntmachung vom 28. Februar 2007 (GVOBl. Schl.-H. S. 184) zuletzt geändert durch Artikel 1 des Gesetzes vom 4. Februar 2011 (GVOBl. Schl.-H. S. 34, ber. GVOBl. Schl.-H. S. 67), wird mit Beschlussfassung durch den Senat der Fachhochschule Kiel vom 26. Mai 2011 und mit Zustimmung des Hochschulrates vom 17. Mai 2011 die folgende Benutzungsrahmenordnung für die Kommunikations- und Datenverarbeitungsinfrastruktur der Fachhochschule Kiel als Satzung erlassen:

§ 1 Zweck

Die Kommunikations- und Datenverarbeitungsinfrastruktur dient der Gemeinschaft in Bildung und Wissenschaft. Der Missbrauch selbst durch eine kleine Gruppe kann das Ansehen der Hochschule in ihrer Gesamtheit schädigen. Eine sorgfältige Nutzung ist erforderlich, um Nachteile von der Gemeinschaft der Benutzerinnen und Benutzer zu vermeiden.

§ 2 Geltungsbereich

- (1) Diese Satzung ist für alle nutzungsberechtigten Personen (Nutzer) der Kommunikations- und Datenverarbeitungsinfrastruktur verbindlich. Die Kommunikations- und Datenverarbeitungsinfrastruktur der Fachhochschule Kiel besteht aus den Datenverarbeitungsanlagen, Kommunikationssystemen, Netzwerken und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung.
- (2) Diese Satzung regelt die Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur, die Nutzung von elektronischer Post (E-Mail), die Verwendung von Datenspeichern, Internetnutzung und Telefonie, sowie alle an der Kommunikation beteiligten Komponenten.
- (3) Zur Gewährleistung eines ordnungsgemäßen Betriebes der Kommunikations- und Datenverarbeitungsinfrastruktur können weitere Regeln für die Nutzung von DV-Anlagen, wie z.B. Nutzungsbedingungen für die Nutzung von PC-Pools, Seminarräumen, technisch-organisatorische Vorgaben zum Betrieb des Datennetzes oder Betriebsregelungen für Veröffentlichungen auf Servern erlassen werden.

§ 3 Nutzungsberechtigung und Zulassung zur Nutzung

- (1) Zur Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur können zugelassen werden:
 - a) Mitglieder, Angehörige und Einrichtungen der Fachhochschule Kiel einschließlich der Verwaltung der Fachhochschule Kiel;
 - b) Beauftragte der Fachhochschule Kiel zur Erfüllung ihrer Dienstaufgaben;
 - c) Mitglieder anderer Hochschulen des Landes Schleswig-Holstein oder staatlichen Hochschulen außerhalb des Landes Schleswig-Holstein aufgrund besonderer Vereinbarungen;
 - d) staatliche Forschungs- und Bildungseinrichtungen und Behörden des Landes Schleswig-Holstein aufgrund besonderer Vereinbarungen;
 - e) Angehörige des Forschungs- und Entwicklungszentrums Fachhochschule Kiel GmbH soweit der Projektauftrag dieses erfordert;

- f) das Studentenwerk Schleswig-Holstein;
 - g) und sonstige juristische oder natürliche Personen, sofern hierdurch die Belange der unter a) bis f) genannten Nutzer nicht beeinträchtigt werden.
- (2) Die Zulassung erfolgt ausschließlich zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, für Zwecke der Bibliothek und der Hochschulverwaltung, für die Aus- und Weiterbildung sowie zur Erfüllung sonstiger Aufgaben der Fachhochschule Kiel. Eine hiervon abweichende Nutzung kann zugelassen werden, wenn sie geringfügig ist und die Zweckbestimmung der Kommunikations- und Datenverarbeitungsinfrastruktur sowie die Belange der anderen Nutzer nicht beeinträchtigt werden.
- (3) Vor Zulassung zur Nutzung bedarf es der Erteilung einer Nutzungserlaubnis. Diese Erlaubnis wird für Studierende im Zuge der Immatrikulation erteilt. Bei Mitgliedern der Hochschule wird die Nutzungserlaubnis schriftlich auf Antrag des Nutzers erteilt.
- (4) Der Antrag soll unter Verwendung eines vorgegebenen Formblatts der Campus IT folgende Angaben enthalten:
- a) Name, Unterschrift und Informationen zur Anstellung der Antragstellerin/des Antragstellers, sowie die Beschäftigungsdauer;
 - b) Verpflichtungserklärung zur Verarbeitung personenbezogener Daten durch den Nutzer;
 - c) Anerkennung dieser Benutzungsrahmenordnung;
 - d) Einverständniserklärung des Nutzers zur Verarbeitung seiner personenbezogenen Daten;
 - e) Anerkennung der IT-Sicherheitsrichtlinie.
- (5) Die Nutzungserlaubnis ist auf das beantragte Vorhaben beschränkt und kann zeitlich befristet werden.
- (6) 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.
- (7) Wenn die Kapazitäten der IT-Ressourcen nicht ausreichen, um allen Nutzungsberechtigten gerecht zu werden, können die Betriebsmittel für die einzelnen Nutzer entsprechend der Reihenfolge in § 3 Abs. 1 kontingentiert werden, da die Zulassung nur im Rahmen der verfügbaren Kapazitäten erfolgen kann.
- (8) Die Nutzungserlaubnis kann ganz oder teilweise versagt, widerrufen oder nachträglich beschränkt werden, insbesondere wenn
- a) kein ordnungsgemäßer Antrag vorliegt oder die Angaben im Antrag nicht oder nicht mehr zutreffen;
 - b) die Voraussetzungen für eine ordnungsgemäße Benutzung der IT-Einrichtungen nicht oder nicht mehr gegeben sind;
 - c) die nutzungsberechtigte Person nach § 12 von der Benutzung ausgeschlossen worden ist;
 - d) das geplante Vorhaben des Nutzers nicht mit den Aufgaben der Hochschule und den in § 3 Abs. 2 genannten Zwecken vereinbar ist;
 - e) die vorhandenen IT-Ressourcen für die beantragte Nutzung ungeeignet oder für besondere Zwecke reserviert sind;
 - f) die Kapazität der Ressourcen, deren Nutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die geplante Nutzung nicht ausreicht;
 - g) die zu benutzenden IT-Komponenten an ein Netz angeschlossen sind, das besonderen Datenschutzerfordernissen genügen muss und kein sachlicher Grund für die geplante Nutzung ersichtlich ist;
 - h) zu erwarten ist, dass durch die beantragte Nutzung andere berechnete Vorhaben in unangemessener Weise beeinträchtigt werden.

§ 4 Rechte und Pflichten der Nutzer

- (1) Die Nutzer haben das Recht, die Einrichtungen, Datenverarbeitungsanlagen und Informations- und Kommunikationssysteme im Rahmen der Zulassung und nach Maßgabe dieser Benutzungsrahmenordnung sowie der nach § 2 erlassenen Regeln zu nutzen. Eine hiervon abweichende Nutzung bedarf einer gesonderten Zulassung.
- (2) Die Nutzer sind verpflichtet,
 - a) die Bestimmungen dieser Benutzungsrahmenordnung zu beachten und die Grenzen der Nutzungserlaubnis einzuhalten, insbesondere die Nutzungszwecke nach § 3 Abs. 2 zu beachten;
 - b) alles zu unterlassen, was den ordnungsgemäßen Betrieb der IT-Einrichtungen der Hochschule stört;
 - c) alle Datenverarbeitungsanlagen, Informations- und Kommunikationssysteme und sonstigen Einrichtungen der Hochschule sorgfältig und schonend zu behandeln;
 - d) ausschließlich mit den Kennungen der Nutzerinnen und Nutzer zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde;
 - e) dafür Sorge zu tragen, dass die Passwörter zugeteilter Kennungen von Benutzerinnen und Benutzern nicht zur Kenntnis anderer Personen gelangen;
 - f) Passwörter zu fremden Kennungen von Nutzerinnen und Nutzern weder zu ermitteln noch zu nutzen;
 - g) nicht unberechtigt auf Informationen anderer Nutzerinnen und Nutzer zuzugreifen und bekannt gewordene Informationen anderer Nutzerinnen und Nutzer nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern;
 - h) bei der Benutzung von Software, Dokumentationen und anderen Daten die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen zu beachten, unter denen Software, Dokumentationen und Daten von der Hochschule zur Verfügung gestellt werden;
 - i) von der Hochschule bereitgestellte Software, Dokumentationen und Daten weder zu kopieren noch an Dritte weiterzugeben, sofern dies nicht ausdrücklich erlaubt ist, noch zu anderen als erlaubten Zwecken zu nutzen;
 - j) in den Räumen und Laboren der Hochschule den Weisungen des zuständigen IT-Personals zu folgen;
 - k) Störungen, Beschädigungen und Fehler an DV-Einrichtungen und Datenträgern der Hochschule nicht selbst zu beheben, sondern unverzüglich dem zuständigen IT-Personal zu melden;
 - l) ohne ausdrückliche Einwilligung des zuständigen IT-Personals keine Eingriffe in Hardwareinstallationen vorzunehmen und die Konfiguration der Betriebssysteme, der Systemdateien, der systemrelevanten Dateien von Nutzerinnen und Nutzern und des Netzwerks nicht zu verändern;
 - m) der IT-Bereichsleitung 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;
 - n) eine Verarbeitung personenbezogener Daten mit der Campus IT abzustimmen und – unbeschadet der eigenen datenschutzrechtlichen Verpflichtungen des Nutzers – die von der Campus IT vorgeschlagenen Datenschutz- und Datensicherheitsvorkehrungen zu berücksichtigen.
- (3) Auf die folgenden Straftatbestände wird besonders hingewiesen:
 - a) Ausspähen von Daten (§ 202a StGB);
 - b) Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB);
 - c) Computerbetrug (§ 263a StGB);

- d) 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);
 - e) Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB);
 - f) Ehrdelikte wie Beleidigungen oder Verleumdung (§§ 185 ff. StGB);
 - g) Strafbare Urheberrechtsverletzung, z.B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG).
- (4) Die geltende IT-Sicherheitsrichtlinie ist zu beachten.
- (5) Mit der Benutzung der IT-Einrichtungen wird anerkannt, dass
- a) betriebsbedingt personenbezogene Daten unter Beachtung der Vorschriften des Datenschutzgesetzes gespeichert werden können;
 - b) betriebsbedingt der Administration alle Nutzerdaten prinzipiell zugänglich sind, wobei den Angehörigen der Administration der Zugriff auf die persönlichen Daten (z.B. E-Mail) der Benutzerinnen und Benutzer untersagt ist;
 - c) trotz des stetigen Bemühens der Netzadministration, einen Missbrauch der Netzeinrichtungen und der Benutzerdaten zu verhindern, dieser technisch bedingt nicht völlig ausgeschlossen werden kann. Die Nutzer können durch Einhalten dieser Benutzungsrahmenordnung einen wesentlichen Beitrag zum Datenschutz leisten.

§ 5 Elektronische Post

(1) Nutzung elektronischer Post (E-Mail):

- a) Elektronische Post in Postfächern der Hochschule soll weitgehend für berufliche Zwecke genutzt werden.
- b) Nicht mehr benötigte Inhalte sind zu löschen.
- c) Das Abonnieren von elektronischer Post über Mailing-Listen soll auf das notwendige Maß beschränkt werden.
- d) E-Mails müssen den Absender eindeutig erkennen lassen.
- e) Das Anlegen von persönlichen Adressbüchern und Verteilerlisten, über die sich eine größere Zahl von Empfängern zeitgleich erreichen lässt, ist zulässig.

(2) Vertretungsregelung

Ziel der Vertretungsregelung ist es, während der Abwesenheit den Zugriff auf Datenbestände und Arbeitsunterlagen zu gewährleisten, um den Betriebsablauf der Hochschule sicherzustellen.

- a) Die Vertretungsregelung gilt für alle Nutzer, mit Ausnahme der Studierenden, soweit sie nicht in einem Beschäftigungsverhältnis mit der Fachhochschule Kiel stehen.
- b) Bei vorhersehbarer Abwesenheit (z.B. Urlaub, Dienstreisen) kann der abwesende Nutzer veranlassen, dass ein automatischer Antworttext an den E-Mail-Absender geschickt wird, in dem auf die Abwesenheit des Empfängers hingewiesen bzw. eine andere E-Mail-Adresse genannt wird.
- c) Der Vertretene kann veranlassen, dass neu eingehende elektronische Post automatisch an den Vertreter weitergeleitet wird.
- d) Bei Nichteinrichtung einer Vertretungsregelung durch den abwesenden Nutzer, auch bei unvorhergesehener Abwesenheit, behält sich die Fachhochschule Kiel vor, veranlasst durch den Vorgesetzten, ohne vorherige Rücksprache mit dem Nutzer eine Vertretungsregelung einzustellen.
- e) Der abwesende Nutzer hat dafür Sorge zu tragen, dass in der Abwesenheitszeit keine privaten E-Mails für ihn eintreffen. Vorgesetzte und Stellvertreter können davon ausgehen, dass ankomm-

mende Emails für den Vertretenen betrieblichen Charakter haben und sind deshalb, soweit nicht aus dem Betreff eindeutig ein privater Charakter der E-Mail erkennbar ist, einsehbar.

(3) **Sicherer E-Mail Betrieb:**

- a) Eingehende E-Mails, deren Absender oder Inhalt zweifelhaft erscheinen, sind ungeöffnet zu löschen.
- b) Die Übermittlung sensibler Daten mittels E-Mail soll unter Einsatz geeigneter Verschlüsselungsverfahren erfolgen, wenn diese verfügbar sind.
- c) Anlagen in Dateiform sind grundsätzlich zulässig.
- d) Greifen Nutzer von außerhalb des Hochschul-Netzwerks auf Postfächer zu, sind diese Zugriffe durch entsprechende Authentisierung und Verschlüsselung des Verbindungskanals abzusichern.
- e) Zur Sicherung des Hochschulnetzwerks werden eingehende E-Mails automatisiert auf das Vorhandensein von Viren oder sonstigen für das System schädlichen Inhalten (auch sog. Bulk-Mails) gescannt. Entsprechende E-Mails können ohne Benachrichtigung des Nutzers oder Absenders gelöscht werden. Eine Einsichtnahme in Postfächer erfolgt dabei - unter Wahrung des Fernmeldegeheimnisses - nur im Ausnahmefall, wenn andere Maßnahmen keinen Erfolg versprechen.
- f) Die Hochschule behält sich vor, Absender- oder Zieladressen von E-Mails zu sperren, ohne Absender oder Empfänger davon zu unterrichten, wenn besondere Rechtfertigungsgründe (z.B. Abwehr von Angriffen auf Anwender oder Infrastruktur) dafür vorliegen.

(4) **Protokollierung:**

- a) Das E-Mail-System führt Protokolldateien über ein- und ausgehende E-Mail.
- b) Die Protokolldateien des E-Mail-Dienstes werden nur in Fehlerfällen zur Klärung der Ursache ausgewertet.
- c) Die Protokolldaten werden nach 90 Tagen gelöscht.

(5) **Zugriffsschutzmechanismen E-Mail:**

Durch technische Maßnahmen ist sicherzustellen, dass der Zugriff auf einzelne Postfächer nur den jeweils Berechtigten möglich ist. Vertretungsregelungen bleiben hiervon unberührt.

§ 6 Internetnutzung

(1) **Nutzung Internet:**

- a) Das Internet darf ausschließlich im Rahmen der Benutzungsrahmenordnung (Satzung) für die Kommunikations- und Datenverarbeitungsinfrastruktur der Fachhochschule Kiel genutzt werden.
- b) Inhalte, die zu beruflichen Zwecken aus dem Internet geladen werden, dürfen nur dann auf einem Server oder dem Arbeitsplatzcomputer gespeichert werden, wenn dies für berufliche Belange erforderlich ist.
- c) Nicht mehr benötigte Inhalte sind zu löschen.
- d) Die Nutzung des Internet und/oder Intranet kann untersagt werden.

(2) **Protokollierung:**

- a) Eine allgemeine, nutzerbezogene Protokollierung von Nutzungsdaten erfolgt nicht.
- b) Zur Sicherung des Hochschulnetzwerkes werden auf den Firewall-Systemen Protokolldateien über folgende Nutzungsdaten erzeugt:
 - die Quell- und Zieladressen,
 - die Kommunikationsports,
 - Datum und Uhrzeit des Zugriffs sowie
 - den Umfang der mit der Kommunikationsverbindung ausgetauschten Daten

- c) Die Firewall-Systeme, Proxy-Systeme, Infrastrukturdienste und Anwendungsdienste können weitere, protokoll- oder anwendungsspezifische Daten erheben.
 - d) Die Protokolldaten können grundsätzlich nicht auf einzelne Nutzer zurückgeführt werden, Zugriff hierauf haben nur die mit der technischen Administration des Systems betrauten Personen; diese sind gem. § 88 TKG auf das Fernmeldegeheimnis bzw. gem. § 5 BDSG auf das Datengeheimnis verpflichtet.
 - e) Die Protokolldaten werden nach 90 Tagen gelöscht.
 - f) Die erhobenen Protokolldaten dürfen zu statistischen Zwecken ausgewertet werden
 - zur Feststellung des Transfervolumens und der Anzahl der aufgerufenen Seiten oder Dienstleistungen, sowie
 - zur Analyse der aufgerufenen Seiten und Dienstleistungen.
 - g) Sofern bei der statistischen Auswertung der begründete Verdacht entsteht, dass auf unzulässige Inhalte gemäß § 4 Abs. 3 zugegriffen wird, kann - solange und soweit es zum Zwecke der Aufklärung des Verdachts erforderlich ist - eine konkrete und personenbeziehbare Protokollierung und Auswertung erfolgen, über die der Datenschutzbeauftragte informiert wird.
 - h) Belegt diese Auswertung den Zugriff auf unzulässige Inhalte gemäß § 4 Abs. 3, können arbeits- bzw. dienstrechtliche Konsequenzen eingeleitet werden.
 - i) Belegt diese Auswertung den Zugriff auf rechtswidrige Inhalte gemäß § 4 Abs. 3, werden Strafverfolgungsbehörden eingeschaltet, der Datenschutzbeauftragte informiert und arbeits- bzw. dienstrechtliche Konsequenzen eingeleitet.
- (3) **Filterung und Sperrung von Inhalten:**
Die Fachhochschule Kiel behält sich vor, den Zugriff auf unzulässige, rechtswidrige oder betriebsgefährdende Inhalte zentral zu sperren.

§ 7 Telefonie

- (1) **Nutzung:**
- a) Die Nutzungsregelung Telefonie gilt für alle Nutzer, mit Ausnahme der Studierenden, soweit sie nicht in einem Beschäftigungsverhältnis mit der Fachhochschule Kiel stehen.
 - b) Das Telefonieangebot der Fachhochschule Kiel soll weitgehend für berufliche Zwecke genutzt werden.
 - c) Die Fachhochschule Kiel kann die erreichbaren Ziele anschlussbezogen beschränken.
 - d) Die Fachhochschule Kiel kann Unified Messaging Funktionalität zum Computerzugriff auf Telefonfunktionen (inklusive, aber nicht beschränkt auf Konfiguration, Telefax, Anrufbeantworter/Voicebox, E-Mail Weiterleitung, Wählen vom Computer, SMS) bereitstellen. Die Bereitstellung ist freiwillig und beschränkbar. Der Nutzer ist für die Sicherheit der ihn betreffenden Konfiguration und für die Verhinderung des Zugriffs durch Dritte verantwortlich.
 - e) Inhalte von Anrufbeantworter und Unified Messaging werden nach 60 Tagen automatisiert gelöscht.
 - f) Die Fachhochschule Kiel behält sich vor, die Konfiguration von Telefon, Anrufbeantworter und Unified Messaging bei betrieblichem Bedarf zu ändern. Gespeicherte Inhalte können gelöscht werden.
- (2) **Protokollierung:**
- a) Alle von Telefonen der Fachhochschule Kiel ausgehenden Gespräche werden in einem Einzelbindungsnachweis mit vollständigen Rufnummern protokolliert. Diese Daten werden für Abrechnungszwecke und zur Sicherstellung des bestimmungsgemäßen Gebrauchs genutzt.
 - b) Von Telefonen der Fachhochschule Kiel ausgehende Gespräche können von Abrechnungssystemen zum Zwecke der internen Abrechnung verarbeitet werden.

- c) Eine Aufzeichnung von Gesprächsinhalten durch die Fachhochschule Kiel findet nicht statt. Gesetzliche Vorschriften bleiben unberührt.
- d) Die Protokolldaten werden 180 Tage nach Abschluss der Abrechnung gelöscht.

§ 8 Private Telemedien-Nutzung

- (1) Die private Nutzung der Telemedien ist in geringfügigem Umfang zulässig. Die Nutzung von Telemedien ist auf das Abrufen von Inhalten beschränkt, das Anbieten von Inhalten ist nicht zugelassen. Private Interessen sind grundsätzlich den betrieblichen Belangen der Fachhochschule Kiel unterzuordnen.
- (2) Private Daten sowie privat gesendete und empfangene E-Mails und deren Anhänge dürfen nur in geringfügigem Umfang auf Servern oder Arbeitsplatzcomputern gespeichert werden. Sie unterliegen grundsätzlich dem Fernmeldegeheimnis nach § 88 TKG.
- (3) Private Telefongespräche sind durch den Nutzer als solche kenntlich zu machen. Eine Gebührenumlegung auf den Nutzer kann erfolgen. Die Gebührenregelung wird von der Fachhochschule Kiel festgelegt.
- (4) Die private Nutzung der Ressourcen der Fachhochschule Kiel kann untersagt werden.

§ 9 Ausscheiden eines Nutzers

- (1) Bevor ein Nutzer die Fachhochschule Kiel verlässt, hat er dafür zu sorgen, dass keine privaten Inhalte auf den Datenspeichern und Telefonesystemen der Hochschule hinterlassen werden. Alle verbleibenden Daten werden als betrieblich gewertet.
- (2) Daten der Studierenden werden mit der Exmatrikulation gelöscht. Diese sind vorher durch die Studierenden zu sichern.
- (3) Die auf Geräten der Fachhochschule Kiel verbleibenden Datenbestände werden durch den ausscheidenden Nutzer zum Ablauf seines Beschäftigungsverhältnisses an den Vorgesetzten oder ggf. einen Nachfolger geordnet übergeben.
- (4) Der Vorgesetzte und ggf. ein Nachfolger erhalten vollen Zugriff auf die verbliebenen Datenbestände eines ausgeschiedenen Nutzers.
- (5) Eine Archivierung auf Datenträgern kann vorgenommen werden.

§ 10 Administration

- (1) Das Einrichten von Postfächern und zentralen Datenspeichern sowie die Administration der Telemedien-Dienste erfolgt zentral durch die Systemadministratoren der Fachhochschule Kiel. Dezentralisierung von einzelnen Verwaltungsaufgaben bleibt vorbehalten.
- (2) Es ist nicht zulässig, im Rahmen der Administration (d. h. Einsichtnahme, Veränderung, Löschung) auf Postfächer der Nutzer ohne deren Genehmigung zuzugreifen. § 5 Abs. 3, § 4 Abs. 4, und § 6 Abs. 2 bleiben hiervon unberührt. Die Administratoren sind entsprechend auf das Datengeheimnis verpflichtet worden.
- (3) Personenbezogene Daten, die zur Sicherstellung eines ordnungsgemäßen Betriebes der E-Mail, der Internet- bzw. Intranetdienste und der Telefoniedienste erhoben und gespeichert werden, unterliegen der Zweckbindung des § 31 BDSG.

§ 11 Leistungs- und Verhaltenskontrollen

Eine Leistungs- und Verhaltenskontrolle (z.B. das Erstellen von Kommunikationsprofilen) findet nicht statt.

§ 12 Ausschluss

- (1) Die Nichtbeachtung und/oder Zuwiderhandlung dieser Benutzungsrahmenordnung der Fachhochschule Kiel kann zur sofortigen Aufhebung der Zugangsberechtigung führen.
- (2) Sollte es zur Wahrung der Interessen aller Nutzer und der Fachhochschule Kiel erforderlich sein, ist die Fachhochschule Kiel frei, aufgrund der unzulässigen Nutzung einzelne Personen oder Einrichtungen von der Nutzung der angebotenen Dienste oder Teilen davon auszuschließen. In besonders schwerwiegenden Fällen, bei denen die unzulässige Nutzung eine Verletzung von geltendem Recht darstellt, können zivil- oder strafrechtliche Schritte eingeleitet werden.
- (3) Nutzer können vorübergehend oder dauerhaft in der Benutzung der IT-Ressourcen beschränkt oder hiervon ausgeschlossen werden, wenn sie
 - a) schuldhaft gegen diese Benutzungsrahmenordnung, insbesondere gegen die in § 4 aufgeführten Pflichten, verstoßen (missbräuchliches Verhalten) oder
 - b) die Kommunikations- und Datenverarbeitungsinfrastruktur für strafbare Handlungen missbrauchen oder
 - c) der Hochschule durch sonstiges rechtswidriges Nutzerverhalten Nachteile entstehen.

§ 13 Haftung des Nutzers

- (1) Der Nutzer haftet für alle Nachteile, die der Hochschule durch missbräuchliche oder rechtswidrige Verwendung der Kommunikations- und Datenverarbeitungsinfrastruktur und Nutzungsbeziehung oder dadurch entstehen, dass der Nutzer schuldhaft seinen Pflichten aus dieser Benutzungsordnung nicht nachkommt.
- (2) Der Nutzer haftet auch für Schäden, die im Rahmen der ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe seiner Benutzerkennung an Dritte. In diesem Fall kann die Hochschule Nutzungsentgelt für die Drittnutzung verlangen.
- (3) Der Nutzer hat die Hochschule von allen Ansprüchen freizustellen, wenn Dritte die Hochschule wegen eines missbräuchlichen oder rechtswidrigen Verhaltens des Nutzers auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen. Die Hochschule wird dem Nutzer den Streit erklären, sofern Dritte gegen die Hochschule gerichtlich vorgehen.

§ 14 Haftung der Hochschule

- (1) Die Hochschule übernimmt keine Garantie dafür, dass das System fehlerfrei und jederzeit ohne Unterbrechung läuft.
- (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 oder grober Fahrlässigkeit ihrer Mitarbeiter. Die Haftung der Hochschule ist 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.

§ 15 In-Kraft-Treten

Die Satzung tritt am Tage nach ihrer Bekanntmachung in Kraft.

Kiel, 24. Mai 2011

Fachhochschule Kiel
- Präsident -

Prof. Dr. Udo Beer