



h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

IT-Dienste und Anwendungen

h-da.local Hochschulnetz - Benutzerrichtlinien für Studierende

Version 1.0

Beschluss des Präsidiums der h_da am 12.08.08

Inhalt

§ 1.....	Motivation.....	3
§ 2.....	Geltungsbereich	3
§ 3.....	Benutzungsrichtlinien	3
§ 4.....	Benutzungsberechtigung	3
§ 5.....	Systembetreiber.....	4
§ 6.....	Verpflichtungen des Benutzers	4
§ 7.....	Datenschutz.....	5
§ 8.....	Aufgaben, Rechte und Pflichten des Systembetreibers	5
§ 9.....	Haftung des Systembetreibers/Haftungsausschluss	6
§ 10.	Folgen einer missbräuchlichen oder gesetzeswidrigen Benutzung	6
§ 11.....	Sonstige Regelungen.....	6
§ 12.	Schlussbestimmungen und salvatorische Klausel	7

§ 1 Motivation

Zum Wintersemester 2008/2009 plant die Abteilung IT-Dienste und Anwendungen (IT-DuA), den Studierenden zentrale Accounts sowie eine E-Mail-Adresse zur Verfügung zu stellen. Im Zuge der Bereitstellung dieses Service sollen die folgenden Benutzerrichtlinien verbindlich werden.

Die Benutzerrichtlinien sollen für die Studierenden auf unseren h_da-Webseiten publiziert werden, mit denen die Accounts von den Studierenden freigeschaltet werden.

Diese Benutzerrichtlinie soll nicht die geplante IT-Security Policy ersetzen. In diesem Dokument werden ausschließlich maskuline Wortformen verwendet, es sind jedoch sowohl weibliche als auch männliche Personen gemeint.

§ 2 Geltungsbereich

Die vorliegenden Benutzungsrichtlinien regeln die Bedingungen für alle Studierenden der Hochschule Darmstadt, unter denen das Leistungsangebot des IT-Netzwerks und der IT-Dienste der Hochschule (zentrale Domäne h-da.local mit allen angeschlossenen Systemen und Servern – im Folgenden h-da.local genannt) zur Verfügung gestellt wird und genutzt werden kann.

Diese Benutzungsrichtlinien gelten für alle durch die h-da.local zur Verfügung gestellten IT-Systeme sowie alle per Datenaustausch mit dem Netzwerk verbundenen Systeme, sofern sie keine eigenen Benutzungsrichtlinien definieren.

§ 3 Benutzungsrichtlinien

Die Benutzungsrichtlinien

- stellen Grundregeln für einen ordnungsgemäßen Betrieb der IT-Infrastruktur der Hochschule Darmstadt auf,
- weisen hin auf die zu wahren Rechte Dritter (z.B. bei Softwarelizenzen, Auflagen der Netzbetreiber, Datenschutzaspekte),
- verpflichten den Benutzer zu korrektem Verhalten und zum ökonomischen Gebrauch der angebotenen Ressourcen,
- klären auf über eventuelle Maßnahmen des Betreibers (der Abteilung IT-Dienste und -Anwendungen) bei Verstößen gegen die Benutzungsrichtlinien.

§ 4 Benutzungsberechtigung

Die Berechtigung zur Nutzung des h-da.local-Hochschulnetzes wird durch die Vergabe einer Startkennung, die sogenannte h_da Benutzer-ID und eines Startpasswortes erteilt. Die Ausgabe der Zugangsdaten erfolgt in einem geschlossenen Umschlag durch die Fachbereiche.

Die Berechtigung zur Nutzung der Studentenservices erlischt mit der Exmatrikulation des Studierenden.

Eine weitere Nutzung von eingeschränkten Diensten ist nach der Exmatrikulation als „Alumnus“ mit der dort zugeteilten Kennung möglich.

§ 5 Systembetreiber

Systembetreiber ist die Abteilung IT-Dienste und –Anwendungen der h_da (im Folgenden: IT-DuA). Der Betrieb von fachbereichseigenen Webservern, Mailservern etc. wird in Eigenverantwortung durch die Fachbereiche geregelt. In diesem Falle stellt IT-DuA nur den Zugang (Netzwerk) zu diesen Systemen zur Verfügung.

§ 6 Verpflichtungen des Benutzers

Das h-da.local Netzwerk darf nur für Zwecke genutzt werden, die mit dem Studium an der h_da in Verbindung stehen. Eine Nutzung zu anderen, insbesondere zu gewerblichen Zwecken ist nicht zulässig.

Der Benutzer ist verpflichtet, darauf zu achten, dass er die vorhandenen Betriebsmittel (Speicherplatz, Bandbreite der Leitungen sowie Rechenzeit auf den Servern) verantwortungsvoll nutzt. Der Benutzer ist verpflichtet, Aktionen, die vorhersehbar zu einer Beeinträchtigung des Betriebes führen, zu unterlassen und nach bestem Wissen alles zu vermeiden, was Schaden an der IT-Infrastruktur oder bei anderen Benutzern verursachen kann. Zuwiderhandlungen können Schadensersatzansprüche begründen.

Der Benutzer hat jegliche Art der missbräuchlichen Benutzung der IT-Infrastruktur zu unterlassen. Er ist insbesondere dazu verpflichtet,

- ausschließlich mit Benutzerkennungen zu arbeiten, deren Nutzung ihm gestattet wurde; die Weitergabe von Kennungen und Passwörtern ist grundsätzlich nicht gestattet.
- den Zugang zu seinen Kennungen durch ein geheim zu haltendes (nicht naheliegendes oder primitives) Passwort oder ein gleichwertiges Verfahren zu schützen, die Passwörter häufiger zu ändern, und das Logout nicht zu vergessen.
- seine Kennung nicht für den Versand von unbestellten Massenmails (Spam), sowie zur Verbreitung von anderen rechtswidrigen Inhalten zu nutzen.
- bei der Einbringung von Daten in das System die gesetzlichen Regelungen (Urheberrechtsschutz, Copyright) einzuhalten; sowie Daten aus dem System, soweit nicht ausdrücklich erlaubt, weder zu kopieren noch weiterzugeben, noch zu anderen als den erlaubten, insbesondere nicht zu gewerblichen Zwecken zu nutzen.

Der Benutzer trägt die volle Verantwortung für alle Aktionen, die unter seiner Benutzerkennung vorgenommen werden, und zwar auch dann, wenn diese Aktionen durch Dritte vorgenommen werden, denen er zumindest fahrlässig den Zugang ermöglicht hat. Zuwiderhandlungen können Schadensersatzansprüche begründen.

Die IT-Infrastruktur darf nur in rechtlich korrekter Weise genutzt werden. Es wird ausdrücklich darauf hingewiesen, dass insbesondere folgende Verhaltensweisen nach dem Strafgesetzbuch unter Strafe gestellt sind:

- Ausforschen fremder Passwörter, Ausspähen von Daten (§202 a StGB)
- unbefugtes Verändern, Löschen, Unterdrücken oder Unbrauchbarmachen von Daten (§303 a StGB)
- Computersabotage (§303 b StGB) und Computerbetrug (§263 a StGB)
- Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§86 StGB) oder rassistischem Gedankengut (§131 StGB)
- Verbreitung bestimmter Formen von Pornographie im Netz (§184 Abs. 3 StGB)
- Abruf oder Besitz von Dokumenten mit Kinderpornographie (§184 Abs. 5 StGB)
- Ehrdelikte wie Beleidigung oder Verleumdung (§185 ff StGB)

Die Hochschule behält sich die Verfolgung strafrechtlicher Schritte, zivilrechtliche und andere Ansprüche vor. Die Folgen einer missbräuchlichen oder gesetzeswidrigen Benutzung sind in §10 geregelt.

Dem Benutzer ist es untersagt, für andere Benutzer bestimmte Nachrichten zur Kenntnis zu nehmen und/oder zu verwerten. Sollte ein Benutzer entdecken, dass das System strafrechtlich verbotene Inhalte enthält, oder dass er auf nicht für ihn bestimmte Daten zugreifen kann, so ist er verpflichtet, dies unverzüglich unter genauer Angabe des Speicherortes/bzw. Verfahrens der Abteilung IT-DuA mitzuteilen.

§ 7 Datenschutz

Personenbezogene Daten außerhalb der von der h_da ins System eingebrachten dürfen auf dem System nicht gespeichert werden, es sei denn die Zustimmung der Abteilung IT-DuA sowie der betroffenen Personen liegt vor. Davon unberührt sind die Verpflichtungen, die sich aus Bestimmungen der Datenschutzgesetze ergeben.

Hat ein Benutzer schreibenden Zugriff auf das System, so werden alle schreibenden Aktionen so aufgezeichnet, dass diese dem Benutzer zuzuordnen sind. Veröffentlicht der Benutzer Beiträge oder Daten z.B. in Diskussionsforen oder Dateiablagen oder ähnlichem, die gegen gesetzliche Regelungen verstoßen, so kann der wirkliche Name des Benutzers (nicht nur seine Benutzerkennung) an die zuständige Strafverfolgungsbehörden übermittelt werden.

§ 8 Aufgaben, Rechte und Pflichten des Systembetreibers

Alle mit h-da.local verbundenen Systeme bedienen sich für die Feststellung der Benutzungsberechtigung der zentralen LDAP-Server, welche als Identifikationssysteme für die Benutzerauthentifizierung verwendet werden. Werden zusätzlich weitere Benutzungsberechtigungen erteilt, so wird eine Dokumentation darüber geführt. Die Unterlagen werden nach Auslaufen der Berechtigung mindestens zwei Jahre aufbewahrt.

Der Systembetreiber (Abteilung IT-DuA) trägt in angemessener Weise, insbesondere in Form regelmäßiger Stichproben, zum Verhindern bzw. Aufdecken von Missbrauch bei.

Hierfür ist er insbesondere dazu berechtigt,

- Aktivitäten des Benutzer zu dokumentieren und auszuwerten, soweit dies Zwecken der Abrechnung, des Verstoßes gegen die Benutzerrichtlinien sowie gesetzlichen Bestimmungen dient. Ebenso können die Benutzeraktivitäten dokumentiert und ausgewertet werden, soweit dies der Fehlerbeseitigung und Überwachung der beteiligten IT-Systeme dient. Diese Daten dienen allein dem Betrieb und der technischen Überwachung des Systems und dürfen ausschließlich für berechtigte Zwecke der Strafverfolgung weiter übermittelt werden,
- bei hinreichendem Verdacht auf Verstöße gegen die Benutzerrichtlinien oder gegen strafrechtliche Bestimmungen unter Beachtung des Vieraugenprinzips und der Aufzeichnungspflicht in Benutzerdateien und Mailboxen Einsicht zu nehmen oder die Netzwerknutzung durch den Benutzer mittels z. B. Netzwerk-Sniffer detailliert zu protokollieren,
- bei Erhärtung des Verdachts auf strafbare Handlungen beweissichernde Maßnahmen, wie z.B. Key-stroke Logging oder Netzwerk-Sniffer, einzusetzen.

Der Systembetreiber ist zur Vertraulichkeit verpflichtet. Der Systembetreiber gibt die Ansprechpartner für die Betreuung seiner Benutzer bekannt. Der Systembetreiber ist verpflichtet, im Verkehr mit Rechnern und Netzen anderer Betreiber deren Benutzungs- und Zugriffsrichtlinien einzuhalten.

§ 9 Haftung des Systembetreibers/Haftungsausschluss

Der Systembetreiber setzt hochverfügbare Systeme ein und schützt die im System gespeicherten Daten im Rahmen des ihm Möglichen und Zumutbaren. Dessen ungeachtet kann der Systembetreiber keine Garantie dafür übernehmen, dass die Systemfunktionen den speziellen Anforderungen des Nutzers entsprechen oder dass das System fehlerfrei und ohne Unterbrechung läuft. Er kann auch nicht die Unversehrtheit (bzgl. Zerstörung, Manipulation) und Vertraulichkeit der bei ihm gespeicherten Daten garantieren.

Der Systembetreiber haftet nicht für Schäden gleich welcher Art, die dem Benutzer aus der Inanspruchnahme von h-da.local entstehen. Ausgenommen ist vorsätzliches und grob fahrlässiges Verhalten des Systembetreibers oder der Personen, deren er sich zur Erfüllung seiner Aufgaben bedient.

Werden nicht dokumentierte Produkte eingesetzt oder freigegebene Produkte nicht entsprechend der Dokumentation eingesetzt, übernimmt der Betreiber keine Gewährleistung, dass diese Funktionen auch zukünftig verfügbar sind und eingesetzt werden können.

§ 10 Folgen einer missbräuchlichen oder gesetzeswidrigen Benutzung

Bei Verstößen gegen gesetzliche Vorschriften oder gegen die Bestimmungen dieser Benutzungsrichtlinien, insbesondere gegen die Pflichten des Benutzers, kann der Systembetreiber die Benutzungsberechtigung einschränken, ganz oder teilweise entziehen. Es ist dabei unerheblich, ob der Verstoß einen Schaden zur Folge hatte oder nicht.

Bei schwerwiegenden oder wiederholten Verstößen kann ein Benutzer auf Dauer von der Benutzung des Systems h-da.local ausgeschlossen werden.

Verstöße gegen gesetzliche Vorschriften oder gegen die Bestimmungen dieser Benutzungsrichtlinien werden auf ihre strafrechtliche Relevanz sowie auf zivilrechtliche Ansprüche hin überprüft. Bedeutsam erscheinende Sachverhalte werden der Rechtsabteilung der Hochschule übergeben, die die Einleitung geeigneter weiterer Schritte prüft. Der Systembetreiber behält sich die Verfolgung strafrechtlicher Schritte sowie zivilrechtlicher Ansprüche ausdrücklich vor.

Entstehen der h_da durch die Verfolgung von straf- oder zivilgesetzwidrigen Aktionen, oder von Aktionen die dieser Benutzervereinbarung widersprechen, Kosten, so sind diese durch den Verursacher in vollem Umfang zu erstatten.

§ 11 Sonstige Regelungen

Für die Nutzung bestimmter Dienste im Rahmen von h-da.local können Gebühren festgelegt werden.

Für Benutzer mit besonderen Berechtigungen können bei Bedarf ergänzende oder abweichende Nutzungsregelungen festgelegt werden. Diese werden den betroffenen Benutzern eigens bekanntgemacht.

Beschwerden sind an den Support von IT-Dienste und –Anwendungen (E-Mail: it-service@h-da.de oder Telefon +49.6151.16-8888) zu richten.

§ 12 Schlussbestimmungen und salvatorische Klausel

Jegliche Änderungen, Ergänzungen oder die teilweise oder gesamte Aufhebung dieser Benutzervereinbarung bedarf der Schriftform, auch die Abänderung oder Aufhebung des Schriftformerfordernisses.

Sollten Teile dieser Benutzervereinbarung unwirksam sein oder werden, so berührt dies die Wirksamkeit der übrigen Teile nicht.

Gerichtsstand für alle aus dem Benutzungsverhältnis erwachsenden rechtlichen Ansprüche ist Darmstadt.