Evangelische Hochschule Darmstadt
University of Applied Sciences
eh-darmstadt.de

Nutzung der Informationstechnologie der Evangelischen Hochschule Darmstadt (EHD)

Inhalt

I Allgemeine Nutzungsordnung für die Informationstechnologie (IT) der Evangelischen Hochschule Darmstadt (EHD)

1. Geltungsbereich und Begriffsbestimmung

Diese Nutzungsordnung gilt für die von der EHD betriebene Informationstechnologie (IT) und der darauf basierenden Dienste. Diese umfasst Computer, Drucker, Scanner, Netzwerk- und Internetverbindungen sowie die von der EHD bereitgestellte Software.

2. Nutzungsberechtigung

Die IT der Evangelischen Hochschule Darmstadt steht ausschließlich für Arbeiten im Zusammenhang mit der dienstlichen Tätigkeit zur Verfügung.

3. Gesetzliche Einbindung

Die IT der EHD darf nur in rechtlich korrekter Weise genutzt werden. Es wird ausdrücklich darauf hingewiesen, dass nach dem Strafgesetzbuch unter Strafe gestellt sind:

a) Ausspähen von Daten (§ 202a STGB)

b) Unbefugtes Verändern, Löschen, Unterdrücken oder Unbrauchbarmachen von Daten (§ 303a StGB)

c) Computersabotage (§ 303b StGB) und Computerbetrug (§ 263a StGB)

d) Die Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) oder rassistischem Gedankengut (§ 130 StGB);

e) Die Verbreitung gewisser Formen von Pornografie im Netz (§ 184 Ziffer 3 StGB)

f) Abruf oder Besitz von Dokumenten mit Kinder- und/oder Jugendpornografie (§§ 184b / 184c StGB)

g) Ehrdelikte wie Beleidigung oder Verleumdung (§185ff. StGB), Beschimpfungen von Bekenntnissen, Religionen oder Weltanschauungen (§ 166 StGB)

h) Urheberrechtsverletzungen, z.B. durch urheberrechtswidrige Vervielfältigung von Software oder die Eingabe geschützter Werke in eine DV-Anlage (§ 106 ff. UrhG).

In einigen Fällen ist bereits der Versuch strafbar.

Die Be- und Verarbeitung personenbezogener Daten ist durch das Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) definiert.

4. Pflichten der Nutzer/innen

4.1 Der/Die Nutzer/in ist verpflichtet, darauf zu achten, dass er/sie die vorhandenen Betriebsmittel (z. B. Arbeitsplätze, CPU-Kapazität, Plattenspeicherplatz, Leitungskapazitäten, Peripheriegeräte und Verbrauchsmaterialien) verantwortungsvoll und ökonomisch sinnvoll nutzt. Der/die Nutzer/in ist verpflichtet, Beeinträchtigungen des Betriebs, soweit sie vorhersehbar sind, zu unterlassen und nach bestem Wissen alles zu vermeiden, was Schaden an der IT der EHD oder bei anderen Nutzern/innen verursachen kann. Zuwiderhandlungen können Schadenersatzansprüche begründen und zum Nutzungsausschluss führen.

4.2 Der/Die Nutzer/in hat jegliche Art der missbräuchlichen Benutzung der Infrastruktur der EHD zu unterlassen. Er/Sie ist insbesondere dazu verpflichtet

a) ausschließlich mit Nutzungsberechtigungen zu arbeiten, deren Nutzung ihm/ihr gestattet wurde; die Weitergabe von Nutzerkennungen (Nutzername, Passwort) ist grundsätzlich nicht gestattet;

b) den Zugang zu den Ressourcen soweit wie möglich zu schützen, z.B. durch ein geheim zu haltendes Passwort oder ein gleichwertiges Verfahren; Vorkehrungen zu treffen, damit unberechtigten Dritten der Zugang zu den EHD-Ressourcen verwehrt wird; dazu gehört es insbesondere, naheliegende Passwörter zu meiden, die **Passwörter öfter zu ändern** und die Systemabmeldung (Logout) nicht zu vergessen;

c) fremde Nutzerkennungen und Passwörter weder zu ermitteln noch zu nutzen sowie keinen unberechtigten Zugriff auf Informationen anderer Nutzer/innen zu nehmen und bekannt gewordene Informationen anderer Nutzer/innen nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern.

   Der/die Nutzer/in trägt die Verantwortung für alle Aktionen, die unter seiner/ihrer Nutzerkennung vorgenommen werden, und zwar auch dann, wenn diese Aktionen durch Dritte vorgenommen werden, denen er/sie zumindest fahrlässig den Zugang ermöglicht hat.

d) bei Verlassen des Arbeitsplatzes den benutzten Computer zu sperren, dies gilt auch bei Verschließen des Raumes;

e) bewegliche Datenträger die dienstliche, insbesondere personenbezogene Daten enthalten, und somit einen schützenswerten Inhalt darstellen, besonders aufzubewahren (vgl. § 7b DSG-EKD);

f) ein Vorhaben zur Bearbeitung personenbezogener Daten vor Beginn mit der Leitung der Systemadministration sowie ggf. mit dem/der Datenschutzbeauftragten abzustimmen. Dabei sind die von der Systemadministration und dem/der Datenschutzbeauftragten vorgeschlagenen Datensicherungsvorkehrungen zu nutzen;

g) bei der Benutzung von Software (Quellen, Objekte), Dokumentationen und andere Daten die gesetzlichen Regelungen (Urheberrechtsschutz, Copyright etc.) zu beachten;

h) sich über die Bedingungen, unter denen die zum Teil im Rahmen von Lizenzverträgen erworbene Software, Dokumentationen oder Daten zur Verfügung gestellt werden, zu informieren und diese Bedingungen zu beachten;

i) insbesondere Software, Dokumentationen und Daten, soweit nicht ausdrücklich erlaubt, weder zu kopieren noch weiterzugeben noch zu anderen als den erlaubten, insbesondere nicht zu gewerblichen Zwecken zu nutzen;

   Zuwiderhandlungen können Schadenersatzansprüche begründen.

j) dienstliche bewegliche Massenspeicher (z.B. USB-Sticks, iPOD, externe Festplatten) die über keine Verschlüsselungsfunktion verfügen, sind nur innerhalb der EHD zu nutzen – im Übrigen gilt Punkt f).

4.3 Dem/Der Nutzer/in ist es untersagt, ohne Einwilligung der Systemadministration

a) Eingriffe in die Hardware-Installation vorzunehmen;

b) die Konfiguration der Betriebssysteme oder des Netzwerkes zu verändern;

c) Software (z.B. Spiele, Bildschirmschoner), insbesondere aus dem Internet heruntergeladene Software, zu installieren. (vgl. Punkt 4.5).

4.4 Haftung des/der Nutzers/in

a) Der/Die Nutzer/in haftet für alle Nachteile, die der EHD durch missbräuchliche oder rechtswidrige Verwendung der DV-Ressourcen und Nutzungsberechtigung oder dadurch entstehen, dass der/die Nutzer/in schuldhaft seinen/ihren Pflichten aus dieser Benutzungsordnung nicht nachkommt. Die EHD kann verlangen, dass missbräuchlich genutzte Ressourcen und weitere Kosten von dem/der Nutzer/in zu erstatten sind.

b) Der/Die Nutzer/in haftet auch für Schäden, die im Rahmen der ihm/ihr zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er/sie diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe seiner/ihrer Benutzerkennung an Dritte.

c) Der/Die Nutzer/in stellt die EHD von allen Ansprüchen frei sofern etwaige Schäden auf Verstöße gegen diese Nutzungsordnung insbesondere gegen Lizenzbestimmungen Dritter zurückzuführen sind.

5. Rechte und Pflichten der Systemadministration

a) Falls es

- zur Gewährleistung eines ordnungsgemäßen Systembetriebs,
- zur Ressourcenplanung und Systemadministration,
- zum Schutz der personenbezogenen Daten anderer Nutzer,
- zu Abrechnungszwecken,
- für das Erkennen und Beseitigen von Störungen oder
- zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

erforderlich ist, ist die Systemadministration berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme durch einzelne Nutzer/innen zu dokumentieren und auszuwerten.

Der Systemadministration führt eine für jede/n Nutzer/in einsehbare Übersicht über die zu diesen Zwecken gesammelten Daten.

b) Für die unter Absatz a) aufgeführten Zwecke ist die Systemadministration auch berechtigt Einsicht in die Nutzer/innendateien zu nehmen, soweit dies zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Verstößen gegen die Benutzungsordnung erforderlich ist und hierfür tatsächlich Anhaltspunkte vorliegen.

Die Systemadministration dokumentiert in jedem Fall die Einsichtnahme und benachrichtigt unverzüglich den/die betroffene/n Nutzer/in.

c) Für die unter Absatz a) aufgeführten Zwecke ist die IT der EHD ebenfalls berechtigt, Internet- und Netzwerkverbindungen automatisiert auf gefährliche Inhalte zu untersuchen. Über eine Untersuchung von verschlüsselten Verbindungen wird die Systemadministration vorab informieren.

II E-Mail-Richtlinien

1. Versand von E-Mails

Da es z.Z. noch nicht möglich ist, E-Mails effektiv zu verschlüsseln, werden E-Mails als „Postkarte“ betrachtet – d.h. es ist möglich, dass Unbefugte E-Mails mitlesen können. Aus diesem Grund ist es **nicht gestattet, personenbezogene Daten via E-Mail zu übermitteln.**

Die EHD behält sich das Recht vor, **sämtliche** E-Mails vor Erreichen bzw. nach Verlassen des Arbeitsplatzes automatisch mittels Virenscanner und SPAM-Filter auf SPAM und Viren zu überprüfen und diese nötigenfalls abzuweisen, zu markieren oder zu löschen.

2. Nutzung

Für dienstliche Zwecke ist die dienstliche Adresse zu benutzen. Die Postfächer sind regelmäßig - mindestens aber einmal arbeitstäglich zu öffnen.

Für die E-Mail-Kommunikation zwischen Hochschule und Studierenden sowie Mitarbeitenden darf nur die von der Hochschule vergebene E-Mail-Adresse verwendet werden.

Die Systemadministration kann in Ausnahmefällen zur Klärung von Zugriffsproblemen, die private E-Mail-Adresse verwenden, um Lösungen mitzuteilen.

3. Vertraulichkeit

Nur die Kommunikation zwischen Mail-Adressen der EHD (vorname.nachname@eh-darmstadt.de zu vorname.nachname@eh-darmstadt.de) ist für vertrauliche Inhalte freigegeben, da das E-Mail-System eine verschlüsselte interne Verbindung verwendet.

Vertrauliche Informationen zu und von "Nicht-EHD-Adressen" sind nicht gestattet.

4. Aufbewahrung

Wichtige E-Mails sind auszudrucken und in die jeweiligen Akten aufzunehmen.

5. E-Mail-Verteiler

Bei dem Versand von E-Mails an mehrere Empfänger ist darauf zu achten, dass die einzelnen Empfänger nicht sichtbar sind. Das bedeutet, bei größeren Verteilern muss das Feld „BCC“ (Blindkopie) genutzt werden. Wird das nicht beachtet, liegt ein Verstoß gegen geltendes Datenschutzrecht vor.

6. Nutzung von E-Mail-Adressen nach Beendigung des Dienstverhältnisses

Der Zugang zu der dienstlichen E-Mail-Adresse wird nach Beendigung des Dienstverhältnisses deaktiviert. Auf Antrag leitet die Systemadministration E-Mails für eine Übergangsfrist auf ein anderes System weiter.

III Regelung über die Nutzung von Skype an IT-Systemen der EHD

Skype als Möglichkeit kostengünstig mit Partnern weltweit zu kommunizieren ist auch für die EHD interessant. Allerdings ist Skype aufgrund seiner Architektur und Proprietät sicherheitstechnisch nicht unbedenklich.

Um die Nutzung von Skype dennoch zu ermöglichen ist als zuerst die Systemadministration über die beabsichtigte Nutzung von Skype zu informieren, denn nicht auf jedem System ist die Nutzung zulässig.

Bei der Nutzung ist folgendes zu beachten:

- Es darf ausschließlich nur mit bekannten Partnern kommuniziert werden.
- Die automatische Annahme von Verbindungen ist nicht gestattet.
- Die Funktion "SuperNode" muss deaktiviert werden.
- Skype ist ausschließlich für die Internet-Telefonie zu nutzen.
- Dateien (insbesondere mit dienstlichem und somit vertraulichen Inhalt) dürfen weder empfangen noch versendet werden.
- Skype ist zu deaktivieren, wenn es nicht mehr benötigt wird.

IV Regelungen zu doodle und anderen Tools dieser Art

Terminvereinbarungen über das Internet sind einfach und beliebt. Doodle als bekanntester Vertreter wird stark genutzt.

Angehörige der EHD sollten jedoch den datenschutzrechtlich unbedenklicheren Terminplaner des DFN nutzen: https://terminplaner.dfn.de.

Falls Angehörige der EHD an einer von außerhalb der EHD gestarteten Umfrage teilnehmen, ist folgendes zu beachten:

- Der Upload von Dateien (z.B. Tagesordnungen, Protokolle) ist nicht gestattet.
- Die Daten sind wenn möglich zu pseudonymisieren.

V Regelungen zu Dropbox und anderen Speicherdiensten

Die Speicherung dienstlicher Daten auf fremden Systemen (wie z. B. gmx.de, web.de, googlemail, Dropbox, Skydrive, iCloud, Google Docs, Microsoft Office 365) ist **nicht** zulässig.

Ausnahmen (z.B. im Rahmen von Forschungsprojekten in verteilten Arbeitsgruppen) müssen bei der Systemadministration individuell beantragt und genehmigt werden. Hierbei wird festgelegt, welche Daten, in welcher Form und mit welcher Sicherungsmaßnahme auf fremden Systemen gespeichert werden dürfen.

Alternativen: Outook Web App zum Zugriff auf dienstlichen E-Mails (https://mail.eh-darmstadt.de/owa)

VPN-Verbindungen der EHD

VI Nutzung privater Geräte (BYOD – Bring your own Device)

Private Endgeräte sind nicht in die Sicherheitsstruktur der EHD eingebunden und stellen somit eine für die Organisation nicht kontrollierbare Umgebung (welche Software ist installiert, ist ein Virenschutz vorhanden und wie ist dieser gepflegt?) dar.

Die Nutzung privater Geräte für dienstliche Zwecke ist daher an der EHD **nicht gestattet**.