IT-Sicherheitsrichtlinie der Hochschule Fulda

Die IT-Sicherheitsrichtlinie wurde am 23. Oktober 2008 vom Präsidium der Hochschule Fulda verabschiedet und ist seitdem in Kraft.

1. Überblick

Die Hochschule Fulda erwartet von den Benutzern und Benutzerinnen der Computer und der Netze der Hochschule einen verantwortungsbewussten Umgang bei deren Gebrauch. Als Reaktion auf Verstöße gegen die Sicherheitsrichtlinie oder gegen gesetzliche Bestimmungen sind die Hochschule Fulda und ihre Organisationseinheiten berechtigt, Benutzern und Benutzerinnen Zugangsberechtigungen zeitweise oder auf Dauer zu entziehen, bei Bedarf Daten von Computern der Hochschule Fulda zu löschen und Computer aus dem Netz zu entfernen. Bei Unklarheiten oder in Streitfällen entscheidet der oder die IT-Sicherheitsbeauftragte der Hochschule Fulda und in zweiter Instanz der Leiter oder die Leiterin des Rechenzentrums der Hochschule über solche Maßnahmen.

Basierend auf der Benutzungsordnung für die Rechner und Netze an der Hochschule Fulda stellt diese Richtlinie eine Detaillierung der allgemeinen Regeln für Benutzung und Betrieb der Rechner und Netze in Bezug auf die IT-Sicherheit dar. Falls Sie ein sicherheitsrelevantes Ereignis bemerken, melden Sie es bitte. Hinweise finden Sie im Dokument "IT-Sicherheitsvorfall melden".

1.A Begründung

Die Hochschule Fulda möchte allen Nutzern und Nutzerinnen ein effizientes und ungestörtes Arbeiten ermöglichen. Daher enthält die IT-Sicherheitsrichtlinie eine Liste von nicht zulässigen Verhaltensweisen (regelwidrige Benutzung), **deren Unterlassung jeder Benutzer und jede Benutzerin einfordern kann**, um sich vor Belästigungen und Bedrohungen zu schützen und die Hochschule Fulda und ihre Organisationseinheiten vor Schäden und rechtlichen Konsequenzen zu bewahren. Um den einwandfreien Betrieb zu gewährleisten, werden in der IT-Sicherheitsrichtlinie Standards für die Sicherheit von Computern, Netzen und Daten festgelegt. Es handelt sich dabei um Mindestanforderungen. Die Organisationseinheiten der Hochschule Fulda können für ihren Verantwortungsbereich schriftlich strengere Regeln festlegen.

1.B Gültigkeitsbereich

Die IT-Sicherheitsrichtlinie ist verbindlich für alle Angehörigen der Hochschule Fulda sowie Personen, denen durch Vereinbarungen die Benutzung von Computern und Netzen der Hochschule Fulda möglich ist.

Darüber hinaus bildet sie die Grundlage für Reaktionen auf alle sicherheitsrelevanten Vorfälle von außerhalb.

1.C Version

Version 1.0 vom 23. September 2008

An dieser Stelle werden Überarbeitungen des Dokuments mit einer kurzen Zusammenfassung der Änderungen vermerkt. Die Richtlinie sollte regelmäßig (z. B. alle zwei Jahre) auf Aktualität überprüft werden. Schwerwiegende Veränderungen der verwendeten Technologien oder organisatorischer Art können kurzfristigere Überarbeitungen zur Folge haben.

Seitenanfang

2. Einleitung

Der Gebrauch von Computern und Netzen ist für die Angehörigen der Hochschule Fulda zur alltäglichen Routine geworden. Bei ordnungsgemäßer Benutzung erleichtert er viele Tätigkeiten und manche Arbeiten wären ohne den Einsatz von Computern gar nicht denkbar. Fahrlässige oder gar gesetzwidrige Verwendung hingegen kann die Rechte anderer Benutzer oder Benutzerinnen verletzen. Die Hochschule Fulda verlangt daher von allen Benutzern und Benutzerinnen sorgfältigen und verantwortungsvollen Umgang beim Gebrauch von Computern und Netzen.

Grundsätzlich bleibt es im Rahmen der gesetzlichen Bestimmungen dem Ermessen jedes einzelnen Benutzers bzw. jeder einzelnen Benutzerin bzw. dem Ermessen der Fachbereiche und Einrichtungen der Hochschule Fulda überlassen, in welcher Art und Weise Computer und Netze verwendet werden. Dieser praktizierte Ansatz maximaler Offenheit, hat sich über die Jahre bewährt und soll beibehalten werden. Die Erfahrung der letzten Jahre hat aber deutlich gemacht, dass es einen allgemein anerkannten Konsens geben muss, welche regelwidrige Benutzung nicht akzeptiert wird, welche Mindeststandards für den Betrieb eines Computers bzw. eines Netzes verbindlich sind und welche Konsequenzen bei Nichteinhaltung der Richtlinie gezogen werden.

Der Zweck der IT-Sicherheitsrichtlinie ist es, diese Themenkreise zu formalisieren und allen Benutzern und Benutzerinnen eine einheitliche Grundlage zu bieten, anhand der entschieden werden kann, welche Benutzung konform ist und welche Maßnahmen zu ergreifen sind.

Aufgrund einer maximalen Offenheit kann Missbrauch a priori nicht ausgeschlossen werden. Durch die IT-Sicherheitsrichtlinie soll das Erkennen von Sicherheitsproblemen beschleunigt werden, um den Schaden für jede(n) Einzelne(n) und die Hochschule Fulda gering zu halten. Sie soll als Richtschnur für das eigene Handeln, sowie zur Beurteilung des Handelns der anderen dienen. Damit verringert sich auch die Wahrscheinlichkeit, dass Verstöße ohne Konsequenzen bleiben.

Die Hochschule Fulda ist darauf angewiesen, dass die Nutzer und Nutzerinnen Sicherheits-probleme dem Rechenzentrum und ihren zuständigen IT-Sicherheitsbeauftragten (Ansprech-personen der Organisationseinheiten) melden und die Systemadministratoren bzw. System-administratorinnen erkannte Mängel in ihrem Verantwortungsbereich selbst beheben. Die komplette Liste der Kontaktadressen wird regelmäßig aktualisiert.

Seitenanfang

3. Förderung des Sicherheits-Bewusstseins

Die nachfolgenden Maßnahmen sollen die Sicherheit fördern.

3.A Benutzer/Benutzerinnen

- Benutzer und Benutzerinnen sollten sich über Änderungen an der Sicherheitsrichtlinie auf dem Laufenden halten.
- Erforderliche Aktionen auf Grund einer Änderung der Sicherheitsrichtlinie sind umgehend durchzuführen.
- Verstöße oder vermutete Verstöße gegen die Sicherheitsrichtlinie sind umgehend dem oder der zuständigen IT-Sicherheitsbeauftragten mitzuteilen.
- Eine regelmäßige Teilnahme an Schulungen zum Thema IT-Sicherheit wird empfohlen.

3.B Administratoren/Administratorinnen

- Alle obigen Maßnahmen für Benutzer und Benutzerinnen und zusätzlich
- Informieren der Benutzer und Benutzerinnen über sicherheitsrelevante Vorfälle, Bedrohungen usw.
- Schulung der Benutzer und Benutzerinnen, insbesondere über relevante Themen zur Erhaltung und Erhöhung der IT-Sicherheit (auch für neue Benutzer und Benutzerinnen).
- Informieren über Schwachstellen und Bedrohungen in der eingesetzten Software.

Seitenanfang

4. Mindeststandards für den Betrieb eines Computers

Um den ordnungsgemäßen Betrieb eines Computers oder einer aktiven Netzkomponente zu gewährleisten, müssen mindestens die folgenden Anforderungen erfüllt sein. Zusätzlich sind die jeweils gültigen Sicherheitsmaßnahmen des Rechenzentrums zu beachten.

1. Das System muss fachgerecht installiert werden.
2. Die notwendigen *Security Patches* oder *Upgrades* müssen zeitnah installiert werden.
3. Falls ein System nicht über geeignete Schutz-Mechanismen verfügt, muss es netzwerkseitig geschützt werden, z. B. durch eine *Firewall*.
4. Nicht mehr verwendete Benutzerzugänge müssen entfernt werden.
5. Passwörter müssen sofort geändert werden, wenn sie in fremde Hände geraten sind oder der Verdacht besteht, dass sie unautorisierten Personen bekannt geworden sind und es müssen sichere Passwörter oder stärkere Authentifizierungsmethoden (z. B. *Public Key*) benutzt werden.
6. Passwörter dürfen nicht im Klartext über die Grenzen des Hochschulnetzes versendet werden und sollten auch innerhalb des Hochschulnetzes nach Möglichkeit nicht im Klartext übertragen werden.
7. Passwörter sollten niemals auf der Festplatte gespeichert werden, um deren Eingabe in einem Programm zu umgehen.
8. Wird ein Verfahren eingeführt oder wesentlich geändert, in dem personenbezogene Daten verarbeitet werden, ist zuvor ein Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 DS-GVO zu erstellen. Das Ergebnis ist dem bzw. der Datenschutzbeauftragten der Hochschule Fulda zuzusenden.

Falls einem Benutzer bzw. einer Benutzerin eines Computers Sicherheitsmängel auffallen, ist er bzw. sie **verpflichtet**, die Mängel der Person mitzuteilen, die für die Systemadministration zuständig ist oder, falls er bzw. sie die Person nicht kennt, dem oder der IT-Sicherheitsbeauftragten der Organisationseinheit. Der oder die IT-Sicherheitsbeauftragte ist verpflichtet, ihm oder ihr bekannte bzw. bekannt gemachte Informationen über Sicherheitsmängel eines Rechners an die Person weiterzuleiten, die für die Systemadministration zuständig ist. Diese wiederum ist verpflichtet, geeignete Gegenmaßnahmen zu ergreifen.

Seitenanfang

5. Mindeststandards für den Betrieb eines Netzes

Ein Netzbetrieb im Sinne dieser Richtlinie liegt dann vor, wenn dedizierte Netzwerk-Hardware (z. B. *Router*) betrieben wird oder auf logischer Ebene Netzwerkdienste angeboten werden, wie z. B. *NAT-Gateways*, *DNS*- oder *DHCP-Server*.

1. Zu jedem Bereich (Subnetz, IP-Bereich, DNS-Domäne) ist mindestens eine verantwortliche Person zu benennen (besser mehrere Personen, sodass im Falle von Fehlern oder Sicherheitsvorfällen immer eine verantwortliche Person erreicht werden kann), die auch technisch in der Lage ist, Notmaßnahmen durchzuführen.
2. Der Zugang zum Netz darf nicht unkontrolliert erfolgen. Der Netzzugang muss entweder physikalisch (geschlossener Raum) oder administrativ durch Zugriffslisten, VPN-Zugang o. ä. geregelt sein.
3. Werden IP-Adressen vergeben, so muss nachvollziehbar sein, wer bzw. welches Gerät eine IP-Adresse zu einer bestimmten Zeit hatte.
4. Die Standorte aller im Netz befindlichen Komponenten, auch die der angeschlossenen Rechner, müssen den verantwortlichen Personen bekannt sein.

5. Die Namen und / oder Adressen der Netzwerkkomponenten (einschließlich der Rechner) sollten außen am Gerät sichtbar sein.

Seitenanfang

6. Regelwidrige Benutzung

Die in der Sicherheitsrichtlinie festgelegten Regelverstöße sind thematisch in die folgenden vier Bereiche gegliedert. Strafrechtlich sanktioniertes Verhalten ist immer regelwidrig.

6.A Verwendung elektronischer Kommunikation für Angriffe gegen Einzelpersonen oder Gruppen von Personen

A1) Verbreitung oder In-Umlauf-Bringen von Informationen, die Personen beleidigen oder herabwürdigen (z. B. aufgrund ihrer Hautfarbe, Nationalität, Religion, ihres Geschlechtes, ihrer politischen Gesinnung oder sexuellen Ausrichtung).

A2) Unbefugte Verarbeitung personenbezogener Daten und Verbreitung von persönlichen oder anderen schützenswerten Informationen über eine Einzelperson oder eine Gruppe von Personen.

A3) Mehrfach unerwünschtes Zusenden von Nachrichten.

6.B Verwendung elektronischer Kommunikation zur Behinderung der Arbeit Dritter

B1) Behinderung der Arbeit anderer (z. B. durch *Mail*-Bomben und ähnliche Techniken).

B2) Aneignung von Ressourcen über das zugestandene Maß (z. B. extremer Datenverkehr).

B3) Versenden von elektronischen Massensendungen (z. B. *SPAM E-Mails*). Ausnahme: Verbreitung von dienstlichen Mitteilungen in Analogie zur Hauspost.

B4) Weitersenden oder In-Umlauf-Bringen von elektronischen Kettenbriefen.

B5) Unberechtigte Manipulation von elektronischen Daten anderer.

B6) Zugriff auf Daten Dritter ohne deren Erlaubnis.

6.C Vergehen gegen Lizenzvereinbarungen oder andere vertragliche Bestimmungen

C1) Die Nutzung, das Kopieren und Verbreiten von urheberrechtlich geschütztem Material im Widerspruch zum Urheberrechtsgesetz, zur Satzung der Hochschule Fulda zur Sicherung guter wissenschaftlicher Praxis, zu Lizenzvereinbarungen oder anderen Vertragsbestimmungen auf Computern der Hochschule Fulda bzw. der Transport dieser Dokumente über Netze der Hochschule Fulda.

C2) Verletzung des Urheberrechts durch Verfälschung elektronischer Dokumente.

C3) Weitergabe von Zugangsberechtigungen an Dritte (z. B. *Accounts*, Passwörter, Chipkarten der Hochschule Fulda)

6.D Verwendung elektronischer Kommunikation für Attacken gegen Computer, das Netz oder *Services*, die darauf erbracht werden

Für die nachfolgenden Verstöße besteht eine Meldepflicht an die jeweiligen IT-Sicherheitsbeauftragten der Organisationseinheit **und** der Hochschule Fulda!

D1) Systematisches Ausforschen von *Servern* und *Services* (z. B. *Port Scans*). Ausnahme: Sicherheitstests nach Absprache mit der Person, die für die Systemadministration zuständig ist.

D2) Unerlaubte Aneignung von Zugangsberechtigungen oder der Versuch einer solchen Aneignung (z. B. *Cracken*). Ausnahme: Sicherheitstests nach Absprache mit der Person, die für die Systemadministration zuständig ist.

D3) Beschädigung oder Störung von elektronischen Diensten (z. B. *Denial-of-Service-Attacks*).

D4) Vorsätzliche Verbreitung oder In-Umlauf-Bringen von schädlichen Programmen (z. B. Viren, Würmer, Trojanische Pferde).

D5) Ausspähen von Passwörtern oder auch der Versuch des Ausspähens (z. B. *Password Sniffer*).

D6) Unberechtigte Manipulation oder Fälschung von Identitätsinformationen (z. B. *E-Mail-Header*, elektronische Verzeichnisse, *IP-Spoofing*, etc.).

D7) Ausnutzen erkannter Sicherheitsmängel bzw. administrativer Mängel.

Seitenanfang

7. Konsequenzen bei Nichteinhaltung der Sicherheitsrichtlinie

Die meisten Verstöße resultieren erfahrungsgemäß aus Unkenntnis der Sicherheitsrichtlinie oder technischer Unzulänglichkeit. In solchen Fällen wird es ausreichen, wenn der Verursacher bzw. die Verursacherin über den Verstoß gegen die Sicherheitsrichtlinie der Hochschule Fulda aufgeklärt und die Unterlassung weiterer Verstöße gefordert wird. Bei Verstößen gegen Lizenzvereinbarungen muss gegebenenfalls die Löschung der entsprechenden Daten auf den betroffenen Rechnern verlangt werden. Wenn anzunehmen ist, dass erkannte Verstöße auch andere Fachbereiche, Einrichtungen oder Organisationen (auch außerhalb der Hochschule Fulda) betreffen könnten, sind die betreffenden Verantwortlichen und eventuell auch das Rechenzentrum der Hochschule Fulda zu informieren (z. B. Sperren eines Benutzers bzw. einer Benutzerin, der/die auch über Zugangsberechtigungen auf anderen Computern verfügt).

Falls die direkte Aufforderung ohne Erfolg bleibt oder die Identität des Verursachers bzw. der Verursacherin nicht festgestellt werden kann, ist das Rechenzentrum der Hochschule Fulda in die Lösung des Problems mit einzubeziehen. Der Kontakt mit dem Rechenzentrum sollte am besten über die dafür vorgesehene *E-Mail*-Adresse hergestellt werden.

Neben der Beschreibung des Problems sollte immer explizit angeführt werden, gegen welchen Punkt der Sicherheitsrichtlinie verstoßen wurde. Bei Uneinigkeit über die Richtigkeit der Beschwerde entscheidet der bzw. die IT-Sicherheitsbeauftragte der Hochschule Fulda und in zweiter Instanz der Leiter oder die Leiterin des Rechenzentrums.

7.A Maßnahmen durch das Rechenzentrum

1. Das Rechenzentrum wird den für das Netz oder den Rechner Verantwortlichen auffordern, Regelverstöße zu unterbinden, gegebenenfalls die Zugangsberechtigung des Verursachers bzw. der Verursacherin zu sperren sowie bei Verstößen gegen Lizenzvereinbarungen die betreffenden Informationen von den Rechnern zu löschen.
2. Ist der bzw. die jeweilige Verantwortliche nicht erreichbar oder nicht imstande bzw. nicht bereit, solche Verstöße zu verhindern, so ist das Rechenzentrum verpflichtet, die nächst höhere Instanz (z. B. den Dekan oder die Dekanin) von den Missständen zu informieren und ihn bzw. sie zur Behebung derselben aufzufordern.
3. Bleibt auch die Maßnahme in Punkt 2 ohne Erfolg, so ist das Rechenzentrum berechtigt, den betreffenden Rechner aus dem Netz zu entfernen bzw. die betreffenden *Services* oder ggf. ein ganzes Subnetz zu sperren.
4. Wenn die Umstände es verlangen (Gefahr in Verzug), können Sperren vom Rechenzentrum auch ohne Rücksprache mit dem bzw. der jeweiligen Verantwortlichen vollzogen werden. Das Rechenzentrum ist in solchen Fällen verpflichtet, die Betroffenen (soweit dies möglich ist) und die nächst höhere Instanz unmittelbar danach über die getroffenen Maßnahmen zu informieren.
5. Strafrechtlich relevante Vorfälle sind, z. B. wegen eventueller Schadensersatzforderungen für Schäden, grundsätzlich an die Präsidentin oder den Präsidenten der Hochschule Fulda weiterzuleiten.
6. Zusätzlich kann vom Verursacher bzw. der Verursacherin die schriftliche Kenntnisnahme der IT-Sicherheitsrichtlinie verlangt werden.

7.B Maßnahmen durch die Hochschul-, Landes- und Stadtbibliothek (HLB)

Die Maßnahmen der Hochschul-, Landes- und Stadtbibliothek sind in der "Benutzungsordnung der Hochschule Fulda - University of Applied Sciences für die Hochschul-, Landes- und Stadtbibliothek (HLB) vom 28. März 2019" im "§ 22 Ausschluss von der Benutzung" geregelt.

Seitenanfang

Letzte Änderung: 02. November 2021 | PDF-Version