IT-SICHERHEITSRICHTLINIE DER FACHHOCHSCHULE WIESBADEN

Inhalt

1. Überblick
    1.A Begründung
    1.B Gültigkeitsbereich
    1.C Version
2. Einleitung
3. Förderung des Sicherheits-Bewusstseins (Awareness)
    3.A BenutzerInnen
    3.B SystemadministratorInnen
4. Mindeststandards für den Betrieb eines Computers
5. Mindeststandards für den Betrieb eines Netzes
6. Regelwidrige Benutzung
    6.A Verwendung elektronischer Kommunikation für Angriffe gegen Einzelpersonen oder Gruppen von Personen
    6.B Verwendung elektronischer Kommunikation zur Behinderung der Arbeit Dritter
    6.C Vergehen gegen Lizenzvereinbarungen oder andere vertragliche Bestimmungen
    6.D Verwendung elektronischer Kommunikation für Attacken gegen Computer, das Netz oder Dienste, die darauf erbracht werden
7. Konsequenzen bei Nichteinhaltung der Richtlinie
8. Maßnahmen durch das IT-Center

1. Überblick

Die Fachhochschule Wiesbaden (FHW) erwartet von den BenutzerInnen der Computer und ihrer Netze verantwortungsbewussten Umgang bei deren Gebrauch. Als Reaktion auf Verstöße gegen die Sicherheitsrichtlinie oder gegen gesetzliche Bestimmungen ist die Fachhochschule Wiesbaden durch ihre Organisationseinheiten berechtigt, BenutzerInnen Zugangsberechtigungen zeitweise oder auf Dauer zu entziehen, bei Bedarf Daten von Computern der Fachhochschule Wiesbaden zu löschen und Computer aus dem Netz zu entfernen. Im Falle von strafrechtlichen Vergehen erfolgt eine Meldung bei den zuständigen Behörden.
Bei Unklarheiten oder Streitfällen hat die Präsidentin / der Präsident nach Vorlage durch den Leiter des ITC bzw. den Beauftragten für IT-Sicherheit zu entscheiden.

Basierend auf der „Allgemeinen IT-Benutzungsordnung der FHW“ (Allgemeine Benutzungsordnung für die Informationsverarbeitungs- und Kommunikations-Infrastruktur) stellt diese Richtlinie eine Detaillierung der allgemeinen Regeln bei Benutzung und Betrieb in Bezug auf die IT-Sicherheit dar.

Als Ergänzung dieser Richtlinie dienen:

- der „Leitfaden zur IT-Sicherheitsrichtlinie“ (Dokument „Ergänzungen zur IT-Sicherheitsrichtlinie“, Abschnitt A)
- das „Musterprotokoll bei Verstößen gegen die IT Sicherheitsrichtlinie“ (Dokument „Ergänzungen zur IT- Sicherheitsrichtlinie“, Abschnitt B)
- das „Glossar zur IT- Sicherheitsrichtlinie“ (Dokument „Ergänzungen zur IT-Sicherheitsrichtlinie“, Abschnitt C)
- die „Maßnahmen zur Erhöhung der IT-Sicherheit an der FHW“

1.A Begründung

Die Fachhochschule Wiesbaden möchte allen NutzerInnen effizientes und ungestörtes Arbeiten ermöglichen. Daher ist in der Sicherheitsrichtlinie eine Liste von nicht zulässigen Verhaltensweisen (regelwidrige Benutzung, Kapitel 6) festgelegt, deren Unterlassung jede Benutzerin / jeder Benutzer einfordern kann, um sich vor Belästigungen und Bedrohungen zu schützen und in Folge die Fachhochschule Wiesbaden vor Schäden und rechtlichen Konsequenzen zu bewahren. Um den einwandfreien Betrieb zu gewährleisten, werden in der Sicherheitsrichtlinie Standards für die Sicherheit von Computern, Netzen und Daten festgelegt. Es handelt sich dabei um Mindestanforderungen. Es bleibt demnach den Organisationseinheiten der Fachhochschule Wiesbaden überlassen, für ihren Verantwortungsbereich schriftlich strengere Regeln festzulegen.

1.B Gültigkeitsbereich

Die Sicherheitsrichtlinie ist verbindlich für alle Mitglieder und Angehörigen der Fachhochschule Wiesbaden sowie Personen, denen durch Vereinbarungen die Benutzung von Computern und Netzen der Fachhochschule Wiesbaden möglich ist.

Darüber hinaus gilt sie als Grundlage für Reaktionen bei allen sicherheitsrelevanten Vorfällen von außerhalb.

1.C Version

Die Version 1.0 wurde am xx.yy.2007 vom Präsidium der Fachhochschule Wiesbaden verabschiedet.

An dieser Stelle werden Überarbeitungen des Dokuments mit einer kurzen Zusammenfassung der Änderungen vermerkt. Die Richtlinie ist mindestens alle zwei Jahre von der / dem IT-Sicherheitsbeauftragten der FHW auf Aktualität zu überprüfen. Schwerwiegende Veränderungen der verwendeten Technologien oder organisatorischer Art können Überarbeitungen außerhalb dieses Intervalls bedingen.

2. Einleitung

Die Benutzung von Computern und Kommunikationsnetzen ist für die Mitglieder und Angehörigen der Fachhochschule Wiesbaden zur alltäglichen Routine geworden, und viele Arbeiten wären ohne diese Nutzung nicht möglich.
Fahrlässige oder gar gesetzwidrige Verwendung von Computern und Kommunikationsnetzen hingegen kann die Rechte anderer Benutzer verletzen. Die Fachhochschule Wiesbaden verlangt daher von allen BenutzerInnen sorgfältigen und verantwortungsvollen Umgang beim Gebrauch von Computern und Netzen.

Grundsätzlich bleibt es dem Ermessen der Systembetreiber (Fachbereiche und Einrichtungen) der Fachhochschule Wiesbaden überlassen, in welcher Art und Weise Computer und Netze verwendet werden. Dieser praktizierte Ansatz maximaler Offenheit im Rahmen der geltenden Gesetze, der besagt, dass alles erlaubt ist, was nicht verboten ist, 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 (Kapitel 6) nicht akzeptiert wird, welche Mindeststandards für den Betrieb eines Computers (Kapitel 4) verbindlich sind und welche Konsequenzen bei Nichteinhaltung der Richtlinie (Kapitel 7) gezogen werden.

Zweck der Sicherheitsrichtlinie ist es, diese Themenkreise zu formalisieren und allen BenutzerInnen eine einheitliche Grundlage zu bieten, anhand der entschieden werden kann, welche Benutzung konform ist und welche Maßnahmen zu ergreifen sind, um einen sicheren Betrieb von Computern und Netzen zu gewährleisten.

Durch die Sicherheitsrichtlinie soll das Erkennen von Sicherheitsproblemen beschleunigt werden, um den Schaden für jeden Einzelnen und die Fachhochschule Wiesbaden gering zu halten bzw. auszuschließen. Sie soll als Richtschnur für das eigene Handeln, sowie für die Beurteilung des Handelns der anderen dienen. Damit verringert sich auch die Wahrscheinlichkeit, dass Verstöße ohne Konsequenzen bleiben.

Eine vom IT-Center herausgegebene komplette Liste der Kontaktadressen sowie Erläuterungen und Handlungsanweisungen bei Verstößen zu den in der Sicherheitsrichtlinie behandelten Themen ist im Dokument „Leitfaden zur IT-Sicherheitsrichtlinie“ zu finden. Dieses Dokument wird auf dem aktuellen Stand gehalten. Das IT-Center veröffentlicht Änderungen dieses Leitfadens auf der ITC-Seite im FHW-Web.

Alle Benutzer sind verpflichtet, die dortigen Regelungen einzuhalten und durchzuführen, soweit sie hierzu in der Lage sind. Ansonsten erhalten sie Hilfestellung über die SystemadministratorInnen.

3. Förderung des Sicherheits-Bewusstseins (Awareness)

Nachfolgende Maßnahmen sind gedacht die Sicherheit zu fördern.

3.A 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 der / dem IT-Sicherheitsbeauftragten oder der Leiterin / dem Leiter des IT-Centers mitzuteilen
- Regelmäßige Teilnahme an Schulungen zum Thema IT-Sicherheit wird empfohlen

3.B SystemadministratorInnen

- wie BenutzerInnen (siehe 3.A) sowie:
- Teilnahme an regelmäßigen Treffen mit VertreterInnen des ITC und der / dem IT-Sicherheitsbeauftragten zur Erörterung von Sicherheitsfragen
- Informieren der BenutzerInnen über sicherheitsrelevante Vorfälle, Bedrohungen usw.
- Schulung der BenutzerInnen, insbesondere über relevante Themen zur Erhaltung und Erhöhung der IT-Sicherheit (auch für neue BenutzerInnen)
- Informieren über Schwachstellen und Bedrohungen in der eingesetzten Software

4. Mindeststandards für den Betrieb eines Computers

Um den ordnungsgemäßen Betrieb eines Computers oder einer aktiven Netzkomponente zu gewährleisten, müssen zumindest die folgenden Anforderungen erfüllt sein. Zusätzlich sind die jeweils gültigen Sicherheitsmaßnahmen (siehe „Maßnahmen zur Erhöhung der IT-Sicherheit an der FHW“) des IT-Centers zu beachten.

1. Das System muss fachgerecht installiert werden.
2. Die notwendigen Security Patches oder Upgrades sind zeitnah zu installieren.
3. Falls ein System nicht über geeignete Schutz-Mechanismen verfügt, muss dieses netzwerk-seitig geschützt werden, z.B. durch eine Firewall.
4. Nicht mehr verwendete Benutzer-Zugänge müssen entfernt werden.
5. Regelmäßige Änderung von Passwörtern. Wahl sicherer Passwörter oder stärkerer Authentifizierungsmethoden (z.B. Public Key).
6. Passwörter dürfen nicht im Klartext über die Grenzen des FHW-Netzes versendet werden. Passwörter sollten grundsätzlich nicht im Klartext übertragen werden.

7. Bei der Netzwerk-Anmeldung ist dem ITC eine Verantwortliche / ein Verantwortlicher (SystemadministratorIn) und dessen StellvertreterIn für das System zu benennen. Diese Angabe muss bei einem Wechsel der / des Verantwortlichen aktualisiert werden.

Falls einem Benutzer eines Computers Sicherheitsmängel auffallen, ist dieser verpflichtet, die Systemadministratorin / den Systemadministrator davon zu informieren. Die Systemadministratorin / der Systemadministrator ist verpflichtet, geeignete Gegenmaßnahmen zu ergreifen.

5. Mindeststandards für den Betrieb eines Netzes

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

1. Für jedes System (Subnetz, IP-Bereich, DNS-Domain) ist mindestens eine Verantwortliche / ein Verantwortlicher und eine Vertreterin / ein Vertreter zu benennen, so dass im Falle von Systemfehlern 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 durch abgeschlossene Räume bzw. abgeschlossene Netzwerkschränke gesichert sein oder administrativ durch Access-Listen, authentifizierten Netzzugang 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 ortsfesten Komponenten, auch die der angeschlossenen Rechner, müssen den verantwortlichen Personen bekannt sein.
5. Die Namen und / oder Adressen aller ortsfesten Komponenten (einschließlich der Rechner) sollten außen am Gerät sichtbar sein.

6. Regelwidrige Benutzung

Die in der Sicherheits-Richtlinie festgelegten Regelverstöße sind thematisch in vier Bereiche gegliedert (siehe die ausführliche Beschreibung in tabellarischer Form im Dokument „Leitfaden zur IT-Sicherheitsrichtlinie“). Strafrechtlich sanktioniertes Verhalten ist 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 herab würdigen (z.B. aufgrund ihrer Hautfarbe, Nationalität, Religion, ihres Geschlechtes, ihrer politischen Gesinnung oder sexuellen Ausrichtung).

A2) 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 Mailbomben und ähnliche Techniken).

B2) Aneignung von Ressourcen über das zugestandene Maß (z.B. 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 die 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 zu Lizenzvereinbarungen oder anderen Vertragsbestimmungen auf Computern der FH-Wiesbaden bzw. der Transport über Netze der FH-Wiesbaden.

C2) Verletzung des Urheberrechts durch Verfälschung elektronischer Dokumente.

C3) Weitergabe von Zugangsberechtigungen an Dritte (Accounts, Passwörter, Chipkarten)

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

Für die nachfolgenden Verstöße besteht eine Meldepflicht an den Leiter des IT-Center!

D1) Systematisches Ausforschen von Servern und Services (z.B. Port Scans). Ausnahme: Sicherheitstests nach Absprache mit der Systemadministratorin /dem Systemadministrator.

D2) Unerlaubte Aneignung von Ressourcen oder der Versuch einer solchen Aneignung (z. B. Cracken). Ausnahme: Sicherheitstests nach Absprache mit der Systemadministratorin /dem Systemadministrator.

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. „Passwort Sniffer“).

D6) Unberechtigte Manipulation oder Fälschung von Identitätsinformationen (z.B. „Mailheader“, elektronische Verzeichnisse, „IP-Spoofing“, etc.).

D7) Ausnutzen erkannter Sicherheitsmängel bzw. administrativer Mängel.

7. Konsequenzen bei Nichteinhaltung der Richtlinie

Die meisten Verstöße resultieren erfahrungsgemäß aus Unkenntnis der Sicherheits-Richtlinie oder technischer Unzulänglichkeit. In solchen Fällen wird es ausreichen, wenn der Verursacher über den Verstoß gegen die Sicherheitsrichtlinie der FH Wiesbaden aufgeklärt und die Unterlassung weiterer Verstöße gefordert wird. Bei Verstößen gegen Lizenzvereinbarungen muss gegebenenfalls die Löschung von Daten von Computern verlangt werden. Wenn anzunehmen ist, dass erkannte Verstöße auch andere Einrichtungen oder Organisationen (auch außerhalb der FH Wiesbaden) betreffen könnten, sind die betreffenden Verantwortlichen und eventuell auch das ITC zu informieren (z. B. Sperre eines Benutzers, der auch über Zugangsberechtigungen auf anderen Computern verfügt).

Falls die direkte Aufforderung ohne Erfolg bleibt oder die Identität des Verursachers nicht festgestellt werden kann, ist das ITC in die Lösung des Problems mit einzubeziehen. Der Kontakt mit dem ITC sollte am besten über die dafür vorgesehene E-Mail-Adresse hergestellt werden (siehe Dokument „Leitfaden zur IT-Sicherheitsrichtlinie“).

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 (siehe S. 1, Ziffer 1).

Maßnahmen durch das IT-Center (ITC)

1. Das ITC wird den für das Netz oder den Rechner Verantwortlichen auffordern, Regelverstöße zu unterbinden, gegebenenfalls die Zugangsberechtigung des Verursachers zu sperren sowie bei Verstößen gegen Lizenzvereinbarungen die betreffenden Informationen von Rechnern zu löschen.
2. Ist die / der jeweilige Verantwortliche nicht erreichbar oder nicht imstande bzw. nicht bereit, solche Verstöße zu verhindern, so ist das ITC verpflichtet, die nächst höhere Instanz (z. B. die Dekanin / den Dekan) von den Missständen zu informieren und ihn zur Behebung derselben aufzufordern.
3. Bleibt auch die Maßnahme in Punkt 2 ohne Erfolg, so ist das ITC 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 ITC auch ohne Rücksprache mit der / dem jeweiligen Verantwortlichen vollzogen werden. Das ITC ist in solchen Fällen verpflichtet, die Betroffenen (soweit dies möglich ist) und die nächst höhere Instanz dann unmittelbar über die getroffenen Maßnahmen zu informieren.
5. Strafrechtlich relevante Vorfälle sind, z. B. wegen evtl. Schadensersatzforderungen für Schäden, grundsätzlich an die Präsidentin / den Präsidenten der FH Wiesbaden weiterzuleiten.
6. Zusätzlich kann von der / dem Verursacher die schriftliche Kenntnisnahme der Richtlinie verlangt werden. (Ein Musterprotokoll ist im Dokument „Musterprotokoll bei Verstößen gegen die IT Sicherheits-Richtlinie“ enthalten).

Datum, Unterschrift

VP