Allgemeine Bedingungen für die Nutzung des Datennetzes in den Wohnheimen des Studierendenwerks Heidelberg

Vorbemerkung

Das Studierendenwerk Heidelberg stellt als Betreiber des Datennetzwerks dieses den Bewohnern seiner studentischen Wohnanlagen zum Zweck ihrer Hochschulausbildung zur Verfügung. Eine Nutzung des Datennetzwerks zu anderen als den oben aufgeführten Zwecken ist dabei nicht im Sinne des Betreibers und kann von diesem sowohl eingeschränkt als auch verboten werden. Grundsätzlich ist jeder Nutzer des Datennetzwerks verpflichtet, auf die Sicherheit des Datennetzwerks und auf die Sicherheit anderer Nutzer zu achten. Nutzungsberechtigt sind ausschließlich Wohnheimbewohner mit gültigem Mietvertrag. Um die Betriebsfähigkeit des Netzes nicht zu gefährden, kann das Transfervolumen eines Anschlusses ggf. limitiert werden.

Das Studierendenwerk übernimmt keinerlei Haftung und keine Gewähr für einen ständigen störungsfreien Betrieb. Betriebsunterbrechungen im Datennetz oder eine Unterbrechung aus anderen Gründen, berechtigen weder zur Erstattung noch zur Minderung der Miete.

Übersicht über die Regelungen in Kurzform

Nachfolgend sind – lediglich als Hilfestellung – die 10 wichtigsten Regeln und Benutzerpflichten in Kurzform aufgeführt. Wir weisen darauf hin, dass grundsätzlich alle Regeln und Pflichten aus den Allgemeinen Netzwerkregeln allzeit Gültigkeit besitzen und als Ganzes zu beachten sind.

1. Aufbau oder Betrieb eigener privater Netzwerke ist verboten!
2. Installation oder Nutzung von Geräten und Programmen, die automatisch IP-Adressen zuweisen oder als DNS fungieren, ist verboten!
3. Besuch von Webseiten, die potentielle Gefahren beinhalten, ist verboten!
4. Illegales Kopieren von Dateien oder Materialien ist verboten!
5. Virenschutz-Software installieren und auf dem aktuellen Stand halten!
6. Rechnereigene Firewall zum Schutz gegen Angriffe aus dem Netzwerk aktivieren!
7. Betriebssystem regelmäßig mit wichtigen Aktualisierungen versorgen!
8. Dateien oder Anhänge, die von unbekannten Personen geschickt wurden, nicht öffnen!
9. Illegale oder unsichere Quellen und Informationen nicht benutzen!
10. Passwörter und persönliche Daten sicher aufbewahren und nicht an andere weitergeben!

ALLGEMEINE NETZWERKREGELN

Für die Benutzung des Datennetzwerks des Studierendenwerks Heidelberg gelten die Allgemeinen Netzwerkregeln. Diese sind Bestandteil des mit dem Mieter geschlossenen Mietvertrags. Das Studierendenwerk Heidelberg ist berechtigt, die Allgemeinen Netzwerkregeln jederzeit zu ergänzen, zu ändern oder aufzuheben.

Absatz I – Untersagt sind:

1. *der Aufbau oder Modifizierung des Datennetzwerks, z.B.*
   - 1.1. *der* Aufbau oder Betrieb eigener privater Netzwerke mittels einem Gerät[1] und unter Ausnutzung des Datennetzwerks
   - 1.2. *die* Nutzung von Geräten und Programmen, die die folgenden Dienste anbieten:
     - 1.2.1. Automatische Zuweisung von IP-Adressen (DHCP - Dynamic Host Configuration Protocol)
     - 1.2.2. DNS (Domain Name Server)
   - 1.3. *die* Installation und Nutzung von verschiedenen Geräten und Programmen, die die folgenden Dienste anbieten:
     - 1.3.1. HTTP / HTTPS (WWW-Server)
     - 1.3.2. HTTP Proxy
     - 1.3.3. P2P (Peer 2 Peer – File Sharing Networks)
     - 1.3.4. FTP
     - 1.3.5. IRC
     - 1.3.6. VPN – mit Ausnahme zu Hochschulen
   - 1.4. *die* Installation und Nutzung von verschiedenen Arten von Gameservern;
   - 1.5. *die* Installation und Nutzung von Routern;
   - 1.6. *die* Demontage, Reinstallation, Versetzen oder Ersetzen von Netzwerkkomponenten (bspw. Netzwerk- und Telefondosen), die sich im vom Studierenden angemieteten Zimmer befinden, Set-Top, WLAN-Access Points oder Telefonen;
   - 1.7. *die* Installation eines W-LANs;
   - 1.8. *die* Installation oder Nutzung von Powerline-fähigen Geräten (Netzwerk über Strom) usw.;
   - 1.9. *die* Installation und Nutzung von File Sharing Clients zur Übertragung urheberrechtlich geschütztem Material (z. B. siehe 2.1).

2. *Illegale Handlungen, wie*
   - 2.1. *die* Illegale Weitergabe, Vervielfältigung, Verbreitung von urheberrechtlich geschütztem Material wie:
     - 2.1.1. Jede Art von Musik, Hörbüchern, eBooks und anderen;
     - 2.1.2. Videofilme, DVD, BlueRay;
     - 2.1.3. Computerprogramme, Spiele;
     - 2.1.4. Bilder, Plakate, Fotografien.
   - 2.2. *die* Speicherung, Verbreitung und Weitergabe von Materialien, die gegen das nationale und internationale Recht, gegen ethische Grundsätze verstoßen, wie bspw.:
     - 2.2.1. Materialien mit pornografischem Inhalt (besonders Kinderpornografie);
     - 2.2.2. Materialien mit rassistischem, faschistischem und terroristischem Inhalt;
     - 2.2.3. Materialien, die gegen die religiöse Würde verstoßen.
   - 2.3. *der* Spam-Versand (massiver Versand nicht gewünschter Informationen mit kommerziellem und unkommerziellem Inhalt);
   - 2.4. *das* Ausspionieren und Scannen des Netzwerkverkehrs (Traffic);
   - 2.5. jeglicher Versuch, Kennwörter innerhalb des Datennetzwerks und Internets zu finden;
   - 2.6. *das* Eindringen in die Privatsphäre anderer Benutzer des Netzwerks und Verletzung dieser unter Verwendung von illegal erworbenen Sicherheitscodes, Passwörtern oder anderen vertraulichen Daten;
   - 2.7. *das* Eindringen in fremde E-Mail-Konten oder www/ FTP/ E-Mail-Server, sowie in fremde Computer, die sich im lokalen Netzwerk oder im Internet befinden als auch Modifizierung der Inhalte;
   - 2.8. Angriffe gegen Geräte anderer Benutzer im lokalen Netzwerk, gegen Server und gegen das Internet unter Anwendung von DOS (Denial of Service), DDOS und ähnlichem;
   - 2.9. Handlungen unter Verwendung von falschen oder vorgetäuschten Identitäten (identity hijacking);

[1] beispielsweise: DSL-Router, Kabel-Router, Ethernet-Router, WLAN-Router oder AccessPoints (AP), Netzwerk-Switch, Netzwerk HUB, Dedizierten Servern sowie alle Arten von Computern, die als Server dienen oder genutzt werden

2.10. *die* Verbreitung von Viren und Programmen vom Typ Malware als auch trojanische Pferde, Spyware, Addware, Scareware, Grayware etc. im lokalen Netz und Internet.

3. *das Besuchen von Webseiten mit den unter 2.2 gelisteten Inhalten und Crack-Seiten;*

4. *das Verhindern oder Erschweren der Netznutzung für andere Nutzer;*

5. *Handlungen, die zu einer Überlastung des Netzes führen;*

6. *die kommerzielle Nutzung des Datennetzwerks;*

7. *die manuelle Konfiguration der automatisch zugewiesenen Einstellungen oder Änderungen des IP-Bereichs.* Die IP-Adressen im Datennetzwerk werden automatisch zugewiesen.

8. *Jede Art von Handlung, die dem Studierendenwerk Heidelberg schadet oder schaden kann.*

Absatz II – Regeln und Benutzerpflichten

1. *Jeder Nutzer des Datennetzwerks ist verpflichtet, die gesetzlichen Bestimmungen zu beachten und einzuhalten. Insbesondere die Vorschriften zum Schutz personenbezogener Daten, die Urheber- und Lizenzrechte, Persönlichkeitsrechte sowie die Strafgesetze.*

2. *Vorgaben des Administrators des Studierendenwerks und seiner beauftragten Dienstleister im Zusammenhang mit der Nutzung des Datennetzwerks sind stets zu befolgen.*

3. *Eine geeignete Virenschutz-Software muss installiert und genutzt werden und ist durch regelmäßige Updates auf dem aktuellen Stand zu halten.*

4. *Die rechnereigene Firewall oder eine Firewall, die bspw. in einem Antiviren-Programm integriert ist, muss zum Schutz vor Angriffen aus dem Netzwerk und dem Internet eingeschaltet sein.*

5. *Die automatischen Updates des Betriebssystems müssen aktiviert sein, um das Betriebssystem regelmäßig mit wichtigen Aktualisierungen versorgen zu können. Es muss grundsätzlich dafür Sorge getragen werden, dass alle genutzten Geräte auf dem aktuellsten Stand sind.*

6. *Zur eigenen Sicherheit als auch zur Sicherheit des Netzwerks sollte nur Originalsoftware installiert werden, die direkt vom Hersteller bzw. aus vertrauenswürdigen Quellen stammt.*

7. *Andere Personen dürfen nicht unbefugt das Datennetzwerk nutzen. Dies vor dem Hintergrund, dass es Ihr Anschluss ist und somit auch Ihre Verantwortung. Für die Handlungen Dritter haftet der Mieter.*

Absatz III - Sperrung des Anschlusses, Ausschluss und Kündigung

Ein Anschluss kann und wird ohne Vorwarnung gesperrt, falls

- bei einem IP-Adressen Konflikt ein Nutzer aufgespürt wird, dessen IP-Adresse manuell konfiguriert ist, so wird sein Zugang zum Datennetzwerk ohne vorherige Warnung für einen Zeitraum von 3 Tagen bis zu 3 Monaten gesperrt.
- ein Nutzer aufgespürt wird, dessen IP-Adresse sich außerhalb des IP-Bereichs des Datennetzwerks befindet, kann der Zugang zum Datennetzwerk ohne vorherige Warnung für einen Zeitraum von 7 Tagen bis zu 3 Monaten gesperrt werden.

Die Wiederzulassung kann von Auflagen abhängig gemacht werden.

INSBESONDERE BEI VERSTÖSSEN GEGEN DAS STRAFGESETZBUCH WIRD IN JEDEM EINZELFALL STRAFANZEIGE ERSTATTET.

- Nutzer, die wiederholt oder schwerwiegend gegen diese Netzwerkregeln verstoßen oder bei der Benutzung strafbare Handlungen begehen, können zeitweise oder dauernd von der weiteren Benutzung ausgeschlossen werden. Durch den Ausschluss werden die aus dem Benutzungsverhältnis entstandenen Verpflichtungen des Nutzers nicht berührt.

- Das Studierendenwerk Heidelberg ist gem. Ziff. 3 der Richtlinien in diesen Fällen sowohl zur sofortigen unangekündigten Sperrung des Netzanschlusses als auch ggf. zur Kündigung des Mietverhältnisses berechtigt.

Absatz IV – Supportgrenzen

- Leistungsgrenze für die Unterstützung durch das STW oder andere von ihm beauftragte Dienstleister ist der Netzanschluss (LAN-Anschluss oder WLAN), der vom STW zur Verfügung gestellt wird.

- Sollte trotz vorherigen Hinweises ein Support vor Ort gewünscht sein und sich herausstellen, dass der Fehler nach wie vor nicht beim STW liegt, so sind die Kosten vom Mieter zu tragen (Kostenübernahmeerklärung.)

Absatz V – Haftung

- Der Nutzer haftet für alle aus Anlass der Benutzung des Datennetzes durch ihn oder seine befugten Dritten schuldhaft verursachten Schäden. Das gilt insbesondere für Schäden, die durch die Nichtbefolgung der ihm obliegenden Pflichten, durch falsche Angaben über die Nutzungsart und den Verbrauch sowie durch die unbefugte Verwendung fremder Identifikationen, geschützter Daten und geschützter Programme verursacht werden. Der Schadenersatz ist in Geld zu leisten. Der Nutzer ist verpflichtet, das Studierendenwerk von Schadensersatzansprüchen Dritter freizuhalten.

- Das Studierendenwerk haftet nicht für Schäden an Hard- und/oder Software oder Datenverluste durch Störungen im Strom-Leitungsnetz oder im hausinternen Netz. Es übernimmt keine Gewähr dafür, dass der Zugang zum Datennetz ständig störungsfrei besteht.

Studierendenwerk Heidelberg
Heidelberg, Februar 2020