studierendenwerk bodensee
seezeit

NETZWERKREGELN UND BENUTZERPFLICHTEN

Gültig in allen Seezeit-Wohnanlagen an allen Standorten

Seezeit Studierendenwerk Bodensee AöR stellt als Betreiber des Datennetzwerks dieses den Bewohnern seiner studentischen Wohnanlagen zum Zweck ihrer Hochschulausbildung zur Verfügung. Grundsätzlich ist jeder Nutzer des Datennetzwerks verpflichtet, auf die Sicherheit des Datennetzwerks und auf die Sicherheit anderer Nutzer zu achten, siehe hierzu auch die Ausführungen in den Allgemeinen Netzwerkregeln.
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!**

Ihr Anschluss – Ihre Verantwortung

NETWORK RULES AND USER'S OBLIGATIONS

Valid in all Seezeit-Dormitories at all sites

Seezeit Studierendenwerk Bodensee AöR as the operator of the network provides the residents of its dormitories with it for the purpose of their education. As a matter of principle, every user of the network is obliged to mind the security of the network as well as the security of other users, see also the explanations in the „Allgemeinen Netzwerkregeln".
Given below - only as a help - are the 10 most important rules and obligations in short form. Please keep in mind, that principally all rules and obligations mentioned in the "Allgemeinen Netzwerkregeln" are thoroughly valid and thus to be observed all the time.

1. **Assembly and use of private networks is strictly forbidden!**
2. **Installation and use of devices and programs which automatically assign IP-addresses or function as a DNS is strictly forbidden!**
3. **Visiting websites which contain potential dangers is strictly forbidden!**
4. **Illegally copying data and other materials is strictly forbidden!**
5. **Antivirus-Software has to be installed and to be regularly updated!**
6. **A firewall has to be activated as a protection against attacks over the network!**
7. **The operating system has to be regularly updated!**
8. **Data or attachments send by unknown persons are not to be opened!**
9. **Illegal or insecure sources and information shall not be used!**
10. **Passwords and personal data are to be kept safe and not to be passed to other persons!**

Your access – your responsibility

Das Datennetzwerk der studentischen Wohnanlagen von Seezeit Studierendenwerk Bodensee AöR wird von diesem betrieben und den Bewohnern in folgenden studentischen Wohnanlagen in Friedrichshafen (Wohnanlage Fallenbrunnen), Konstanz (Wohnanlagen Sonnenbühl West I & West II; Sonnenbühl Ost Gruppenhäuser & Hochhaus; Jan-Hus-Haus; Europahaus; Paradies; Seerhein; Petershauser Bahnhof; Sonnenbühlstraße 38/40), Ravensburg (Wohnanlage Tettnanger Straße) und Weingarten (Lazarettstraße) zur Verfügung gestellt, ohne das hierfür weitere Gebühren erhoben werden. Es hat dabei in erster Linie den Zweck, die Hochschulausbildung der Bewohner der studentischen Wohnanlagen zu fördern, indem ihnen ein komfortabler Zugang zum Internet und seinen Ressourcen zum Durchführen von Recherche- und Forschungsarbeiten ermöglicht wird. Eine Nutzung des Datennetzwerks zu anderen als hochschulausbildungsdienlichen Zwecken ist dabei nicht im Sinne des Betreibers und kann von diesem eingeschränkt als auch verboten werden.

ALLGEMEINE NETZWERKREGELN

Für die Benutzung des Datennetzwerks von Seezeit Studierendenwerk Bodensee AöR gelten die Allgemeinen Netzwerkregeln. Diese sind Bestandteil des mit dem Mieter geschlossenen Mietvertrags. Seezeit Studierendenwerk Bodensee AöR ist berechtigt, die Allgemeinen Netzwerkregeln jederzeit zu ergänzen, zu ändern oder aufzuheben.

Artikel I.
GRUNDSÄTZLICH VERBOTEN

1. Aufbau oder Modifizierung des Datennetzwerks
   - 1.1. Aufbau oder Betrieb eigener privater Netzwerke mittels einem Gerät[1] und unter Ausnutzung des Datennetzwerks
   - 1.2. Installation oder 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. 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
   - 1.4. Installation und Nutzung von verschiedenen Arten von Gameservern
   - 1.5. Installation und Nutzung von Geräten wie Router oder Firewalls, die auf allen Arten von Linux, Mac OSX, Unix, Sun OS, BSD, xBSD, Windows basieren und den Nutzer eines privaten Netzwerks schützen
   - 1.6. Demontage, Reinstallation, Versetzen oder Ersetzen von Netzwerkkomponenten (bspw. Netzwerk- und Telefondosen), die sich im vom Studenten angemieteten Zimmer befinden
   - 1.7. Änderung der Platzierung von Geräten wie bspw. der Setup-Box ohne Zustimmung des Administratoren oder zuständigen Hausmeisters. Diese gehört zur Ausstattung des angemieteten Zimmers oder Appartements.

2. Illegale Handlungen
   - 2.1. 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
   - 2.2. Speicherung, Verbreitung und Weitergabe von Materialien, die gegen das nationale und internationale Recht, gegen Traditionen und 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

[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

2.3. Spam-Versand (massiver Versand nicht gewünschter Informationen mit kommerziellem und unkommerziellem Inhalt)
2.4. Ausspionieren und Scannen des Netzwerkverkehrs (Traffic)
2.5. Angriffe auf Passwörter innerhalb des Datennetzwerks und Internets, mit dem Ziel, diese zu knacken oder herauszufinden (bruteforce)
2.6. Eindringen in die Privatsphäre anderer Benutzer des Netzwerks und Verletzung dieser unter Verwendung von illegal erworbenen Sicherheitscodes, Passwörtern oder anderen vertraulichen Daten
2.7. Eindringen in fremde E-Mail Konten oder www/ FTP/ E-Mail-Server, sowie in fremde Computer, die sich im lokalen Netzwerk und im Internet befinden als auch Modifizierung der Inhalte
2.8. Angriffe gegen Computer anderer Benutzer im lokalen Netzwerk, gegen Server und gegen das Internet unter Anwendung von DOS, DDOS und ähnlichem
2.9. Handlungen unter Verwendung von falschen oder vorgetäuschten Identitäten (identity hijacking), die anderen Benutzern des Netzwerks Schaden zufügen
2.10. Verbreitung von Viren und Programmen vom Typ Malware als auch trojanische Pferde, Backdoor-Viren, Spyware, Addware, Scareware, Grayware etc. im lokalen Netz und Internet

3. Besuchen von Webseiten, die potentielle Gefahren beinhalten, z.B.: pornografische Webseiten, unsichere Webseiten und spezielle Crack-Seiten

4. Verhindern oder Erschweren der Netznutzung mit all seinen Ressourcen für andere Nutzer

5. Nutzung von Programmen, die zu einer Überlastung des Netzes führen

6. Kommerzielle Nutzung des Datennetzwerks mit dem Ziel, Geld zu verdienen

7. Manuelle Konfiguration der automatisch zugewiesenen Einstellungen oder Änderungen des IP-Bereichs ohne Zustimmung der Administratoren
   Die IP-Adressen im Datennetzwerk liegen im Bereich von 10.80.82.1 – 10.80.95.254 und werden automatisch zugewiesen.
   7.1. Wird bei einem IP-Adressen Konflikt ein Nutzer aufgespürt, 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.
   7.2. Wird ein Nutzer aufgespürt, 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.

8. Jede Art von Handlung, die dem Ruf von "Seezeit Studierendenwerk Bodensee AöR" schadet oder schaden kann.

Artikel II.
REGELN UND BENUTZERPFLICHTEN

1. Jeder Nutzer des Datennetzwerks ist jederzeit verpflichtet, auf die Sicherheit des Datennetzwerks und auf die Sicherheit anderer Nutzer des Datennetzwerks zu achten. Ein Nichtbefolgen dieser Regel führt absichtlich als auch unabsichtlich zu einer Verminderung der Netzsicherheit und stellt unmittelbar eine Gefahr für das Datennetzwerk und seine Benutzer dar und kann im Zweifelsfall mit geeigneten Maßnahmen geahndet werden.

2. 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.

3. Vorgaben des Administrators im Zusammenhang mit der Nutzung des Datennetzwerks sind stets zu befolgen.

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

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

6. Die automatischen Updates des Betriebssystems müssen aktiviert sein, um das Betriebssystem regelmäßig mit wichtigen Aktualisierungen versorgen zu können. Wird das Betriebssystem nicht automatisch mit Updates versorgt, muss grundsätzlich dafür Sorge getragen werden, dass es anderweitig regelmäßig auf den aktuellsten Stand gebracht wird.

7. Zur eigenen Sicherheit als auch zur Sicherheit des Netzwerks sollte nur Software installiert werden, die aus sicheren Quellen stammt.

8. Der Computer sollte durch Verwendung von geeigneten Passwörtern vor einem Zugriff durch andere geschützt werden. Diese sollten in regelmäßigen Abständen verändert werden.

9. Passwörter und persönliche Daten sollten an einem sicheren Ort aufbewahrt und nicht an andere weitergegeben werden.

10. Andere Personen sollten nicht unbeaufsichtigt mit Ihrem Computer das Seezeit-Datennetzwerk nutzen. Dies vor dem Hintergrund, dass es Ihr Anschluss ist und somit auch Ihre Verantwortung.

JEDE ZUWIDERHANDLUNG GEGEN DIESE REGELUNGEN WIRD VERFOLGT UND KANN MIT SPERRUNG DES NUTZERS GEAHNDET WERDEN.

Artikel III.
HAFTUNG
Jeder Nutzer des Datennetzwerks haftet für alle Nachteile, die durch missbräuchliche oder rechtswidrige Verwendung der Nutzungsberechtigung entstehen als auch in Fällen, in denen der Nutzer schuldhaft seine Pflichten aus dieser Ordnung verletzt.

Artikel IV.
GEWÄHRLEISTUNG
Es können keine Rechtsansprüche auf ein funktionierendes Datennetzwerk gestellt werden. Der Betreiber und das durch ihn mit der Betreuung des Datennetzwerks beauftragte Unternehmen sind bemüht, einen dauerhaften Betrieb aufrecht zu erhalten und ggfls. auftretende Fehler so schnell wie möglich zu beheben.

Artikel V.
SALVATORISCHE KLAUSEL
Sollten einzelne Bestimmungen aus den Allgemeinen Netzwerkregeln ungültig sein, werden oder von einem zuständigen Gericht für nichtig oder gesetzwidrig erklärt werden, behalten die anderen ihre Gültigkeit. Anstelle der unwirksamen Bestimmung tritt eine gültige Bestimmung, die der ungültigen Bestimmung in Wortlaut und Inhalt am nächsten kommt.

Artikel VI.
BELWUE
Neben den vorgenannten Verboten und Regelungen gelten zusätzlich die Regelungen durch den Provider BelWü, in der jüngsten Fassung.

studierendenwerk bodensee
seezeit

RICHTIGES VERHALTEN UND ANDERE INFORMATIONEN

Inhaltsverzeichnis

1. Netzwerksicherheit und eigene Sicherheit – was sollte man beachten?

Für alle Nutzer des Datennetzwerks ist es wichtig, dass die eigene Sicherheit als auch die Sicherheit des Netzwerks bei der Nutzung aufrechterhalten bleibt, denn nur so sind alle vor möglichen Risiken aus dem Netzwerk geschützt. Um die Sicherheit aufrechterhalten zu können, sollten daher Regeln oder Vorgaben, wie bspw. Artikel I, Punkt 3, unbedingt beachtet werden, da ein Benutzer durch eine Nutzung von unsicheren oder gefährlichen Quellen, wissentlich oder unwissentlich, die Sicherheit im Netzwerk bedrohen kann.

- **Gefahrenquellen, die die Netzwerksicherheit bedrohen können**
  Einige Webseiten oder Informationsquellen beinhalten Gefahrenquellen, die auf den ersten Blick nicht immer erkennbar sind. In der Regel handelt es sich hierbei um spezielle, vom Anbieter zur Verfügung gestellte, Programme wie Video- oder Media-Player Programme, die für die Nutzung der Webseite oder für die Nutzung ihrer Inhalte erforderlich sind und deshalb zunächst heruntergeladen werden müssen. In 99 % aller Fälle sind diese Dateien und Programme mit verschieden Viren, Spionageprogrammen oder anderen Malware- Programmen ausgestattet. Webseiten mit derartigen Gefahrenquellen sind beispielsweise:
  - Webseiten, mit pornografischem Inhalt und Webseiten, die Bilder und Filme mit pornografischem Inhalt anbieten
  - Webseiten mit unbekanntem Ursprung, die freie Musikdateien anbieten
  - Webseiten, die freie und illegale Programme, Spiele und Filme anbieten, wie z.B.: Rapidshare, BitTorrent, Warez und FTP-Server.
  - p2p-Netzwerke, denn die meisten in diesem Netzwerk angebotenen Programme, Spiele, Film- und Musikdateien als auch Bilder können Viren, Spionageprogramme als auch Trojaner und Sperrprogramme enthalten

- **Mögliche Folgen, die bei der Nutzung von unsicheren oder illegalen Quellen auftreten können und die die eigene als auch die Netzwerksicherheit bedrohen können**
  - Infizierung des Computers mit Viren oder Spionage-Programmen wie z.B.: Spyware
  - Infizierung des Computers mit Viren vom Typ „botnet-Wurm“, die zum Aufbau weiterer Botnet-Netze führen, die wiederum für größere Angriffe benutzt werden
  - Zugriffssperre auf die Festplatte und/ oder Datenverlust der Festplatte
  - Unberechtigter Zugriff auf vertrauliche Daten wie Kreditkartennummern, Passwörter etc. als auch auf persönliche Daten wie Vorname, Nachname, Adresse, Geburtsdatum etc.
  - Gefährdung anderer Benutzer durch unabsichtliche Verbreitung von Viren im lokalen Datennetzwerk oder unabsichtliche Verbreitung von Viren über E-Mails

2. Wie kann man sich und seinen Rechner schützen?

Im Folgenden finden Sie einige Tipps und Hinweise, wie sie sich und Ihren Rechner am besten schützen können. Dies auch erklärend zu ihren Pflichten als Benutzer des Datennetzwerks.

- **Benutzen Sie Antiviren-Software und seien sie vorsichtig beim Umgang mit Dateien und Dateiträgern**
  Um die auf einem Computer gespeicherten Daten vor den verschiedenen Computer-Viren zu schützen, ist es wichtig, Antiviren-Software zu installieren, zu benutzen, diese durch Updates auf dem aktuellsten Stand zu halten und den Rechner regelmäßig auf Viren zu überprüfen.
  Viren werden häufig schnell und weit durch Dateianhänge an E-Mails verbreitet oder über USB-Sticks und andere externe Medien. Um eine Infizierung ihres Rechners als auch eine Gefährdung anderer zu vermeiden, öffnen Sie nie Dateianhänge, die von unbekannten Personen geschickt wurden oder verwenden Sie vor dem Öffnen der angehängten Datei als auch vor dem Zugriff auf externe Medien eine Antiviren-Software zur Überprüfung auf mögliche Viren.

- **Verleihen Sie keine Benutzerkonten bzw. Ihren Netzwerkzugang**
  In Ihrem eigenen Interesse sollten Sie Ihren Zugang zum Datennetzwerk nicht anderen Personen unbeaufsichtigt zur Verfügung stellen. Sollten kriminelle oder unethische Handlungen von Ihrem Zugang aus auftreten, werden Sie als Inhaber des Zugangs in die Verantwortung gezogen und müssen für die getätigten Handlungen die Verantwortung mit allen daraus entstehenden Konsequenzen tragen.

- **Verwalten Sie Ihre Passwörter mit Vorsicht**
  Grundsätzlich sollten alle Passwörter, über die Sie Zugang zu Ihrem Rechner als auch zu Anwendungen u.ä. erhalten, mit Vorsicht verwaltet werden. Denn werden Ihre Passwörter gestohlen, können Ihre Konten ohne Ihr Wissen für illegale Zwecke genutzt werden. Stellen Sie daher sicher, dass Ihre Passwörter nicht gestohlen werden können. Beachten Sie dazu die folgenden Schritte:
  - Merken Sie sich ihre Passwörter und speichern Sie sie nicht an öffentlich zugänglichen Plätzen
  - Verwenden Sie für ihre Passwörter keine alphanumerischen Zeichen (z.B. den Namen einer Person, ein Wort, eine Telefonnummer oder ein Geburtsdatum). Diese können leicht von anderen erraten werden.
  - Verwenden Sie nicht das gleiche Passwort über einen längeren Zeitraum. Besonders riskant ist es zudem, das bei einer Registrierung vergebene Passwort weiterhin zu benutzen.

- **Verwalten Sie Ihre persönlichen Daten mit Vorsicht**
  Da in einem Netzwerk viele Menschen Informationen miteinander teilen, ist die Wahrscheinlichkeit hoch, dass persönliche Daten aufgedeckt werden können. Verwalten Sie daher Ihre persönlichen Daten als auch die anderer Personen sorgfältig. Beachten Sie dabei das Folgende:
  - Hinterlegen Sie prinzipiell keine persönlichen Daten auf Rechnern, die an das Netzwerk angeschlossen sind. Erfassen und speichern Sie wichtige Informationen und Daten separat auf externen Speichermedien.
  - Erfassen Sie keine leicht identifizierbaren persönlichen Informationen auf Webseiten oder in Foren. Achten Sie darauf, welche persönlichen Daten Sie für die Öffentlichkeit zugänglich machen.
  - Wenn Sie persönliche Daten und Informationen auf einer Webseite eingeben und von dort übermitteln, achten Sie auf die Sicherheit der Webseite. Kann die Sicherheit nicht bestätigt werden, beantworten Sie keine Fragen, besonders dann, wenn persönliche Informationen wie Kreditkartennummern abgefragt werden.

3. Was sind rechtswidrige Handlungen bei der Nutzung des Netzwerks?

Gemäß den Allgemeinen Netzwerkregeln dürfen rechtswidrige Handlungen zu keiner Zeit im Netzwerk ausgeübt werden. Wird ein Verstoß hiervon festgestellt, kann und wird die Strafbarkeit entsprechend des Schadens bemessen. Dies gilt gleichermaßen in Fällen, in denen anderen Personen unwissentlich oder wissentlich Schaden zugefügt wird. Zu Ihrer Information finden Sie einige Beispiele von rechtswidrigen Handlungen unten aufgeführt.

- **Handlungen, die andere verletzen oder ihnen Schaden zufügen**
  Das Begehen von Rufmord, Verleumdung als auch die Verletzung der Privatsphäre von anderen zählen beispielhaft zu den Handlungen, die andere verletzen oder bei denen anderen Schaden zugefügt wird. Solche Handlungen sind sowohl strafrechtlich als auch zivilrechtlich strafbar und können entsprechend verfolgt werden.
  Hierzu zählen beispielhaft:
  - Das Äußern von unvernünftigen Bemerkungen als auch die Verleumdung durch Missbrauch von Anonymität oder Gebrauch eines anderen Namens.
  - Darstellung und Verbreitung von unbegründeten oder falschen Informationen. Hierbei ist zu bedenken, dass sich allgemein jegliche Informationen, die im Netzwerk veröffentlicht werden, schnell und weit verbreiten. Man sollte sich daher immer die Zeit nehmen und zunächst den Inhalt und den Wahrheitsgehalt der übermittelten bzw. zu übermittelnden Informationen prüfen.
  - Darstellung und Verbreitung von diskriminierenden Informationen
  - Versendung von Kettenbriefen und Spam-Mails
  - Registrierung anderer in Mailing-Listen ohne deren Zustimmung

- **Illegale Handlungen, die das Copyright oder andere Besitzrechte verletzen**
  Gemäß den Allgemeinen Netzwerkregeln sind Handlungen wie die illegale Weitergabe, Vervielfältigung und Verbreitung von urheberrechtlich geschütztem Material grundsätzlich verboten (Artikel I, Punkt 2.1). Die unten aufgeführten Handlungen stellen hierbei besondere Beispiele für die Verletzung von Besitzrechten, wie bspw. Copyright, dar.

- Dateien (Musik-, Film-, Bild- und Sprachdateien, Schriftdateien, Programme und anderes), die sich im Besitz von bekannten Personen, Institutionen, Büchern und Zeitschriften befinden, werden häufig im Netzwerk zur Schau gestellt. Werden diese entgegen den Vorgaben des rechtmäßigen Besitzers verwendet oder ohne Erlaubnis des rechtmäßigen Besitzers weiterverbreitet, stellt dies eine Verletzung des Copyrights dar und ist damit eine illegale Handlung, welche entsprechend geahndet werden kann.
- Wird Software, die von kommerziellen Unternehmen oder Netzwerken angeboten wird, kopiert oder verändert und ohne die Zustimmung des rechtmäßigen Besitzers weiterverbreitet oder wird die Software ohne Bezahlung genutzt, stellt dies ebenfalls eine illegale Handlung dar und kann entsprechend geahndet werden.
- Werden Informationen wie Benutzernamen, Passwörter, Seriennummern etc. zur Verwendung von Software, ohne die Zustimmung des rechtmäßigen Besitzers und auf eine Art und Weise, die nicht den Vorgaben des rechtmäßigen Besitzers entspricht, veröffentlicht, stellt dies ebenfalls eine illegale Handlung dar, die entsprechend geahndet werden kann.

➢ **Verbreitung von obszönem Material als auch Material, das gegen das nationale und internationale Recht, gegen Traditionen und ethische Grundsätze verstößt**

Die Verbreitung von obszönem Material oder Material, das als obszön betrachtet werden kann als auch von Material, das gegen das nationale und internationale Recht, gegen Traditionen und ethische Grundsätze verstößt, kann eine rechtswidrige Handlung darstellen und entsprechend verfolgt werden. Hierbei ist es gleich, ob es sich dabei um Texte mit entsprechendem Inhalt oder Bilder und Töne handelt.

➢ **Erschaffung und Verbreitung von Computer-Viren**

Die Erschaffung von Computer-Viren als auch die absichtliche Verbreitung von Computer-Viren mit dem Ziel, anderen Personen, ihren Rechnern oder ihren Daten Schaden zu zufügen, stellt eine rechtswidrige Handlung dar und kann entsprechend verfolgt werden.