

POLITIK DER AKZEPTABLEN NUTZUNG (AUP)

Die AUP von RETN sind für alle Nutzer seiner Dienste verbindlich. Alle Kunden sind an diese Bedingungen gebunden und sind ihrerseits dafür verantwortlich, dass ihre Kunden nicht gegen diese Bedingungen verstoßen.

Die inakzeptable Verwendung kann in 4 Hauptkategorien eingeteilt werden:

- - Unerlaubte Verwendung
- - Böswillige Verwendung
- - Verwendung, die die Netzintegrität gefährdet
- - Böswilliges Verhalten gegenüber RETN-Mitarbeitern

RETN behält sich das Recht vor, die AUP jederzeit zu ändern, um neuen Bedrohungen zu begegnen. Änderungen an den AUP sind ab dem Zeitpunkt ihrer Veröffentlichung auf <https://retn.net/> rechtskräftig.

Die Folgen eines Verstoßes gegen die AUP sind in Ihrer MSA ausführlich beschrieben.

Verboten:

Unerlaubte Verwendung

- - Jede Tätigkeit, die in einem der Gebiete, in denen der Kundendienst erbracht wird, als illegal gilt;
 - - Speicherung oder Übertragung von Material, das gegen das Urheberrecht oder das Markenrecht verstößt;
 - - Speicherung oder Weitergabe von Kinderpornografie;
 - - Nutzung der Dienste zur Durchführung oder Unterstützung von Betrug, Identitätsdiebstahl oder anderen schädlichen oder betrügerischen Aktivitäten, einschließlich des Anbietens oder Verbreitens von betrügerischen Waren, Dienstleistungen, Programmen oder Werbeaktionen;
- Nutzung der Dienste zur Verbreitung, Steuerung oder sonstigen Interaktion mit böswilligen Computerprogrammen (Viren, Trojaner, Würmer, Spyware und andere Malware);
- - Software- oder andere Medienpiraterie;
 - - Verstoß gegen örtliche Import-/Exportgesetze.

Böswillige Verwendung

- Belästigung einer Person oder Organisation, sei es durch offene Drohungen, bedrohliche Äußerungen oder die einfache Weigerung, eine Aufforderung zur Unterlassung anzuerkennen;
 - Penetrationstests/Verwundbarkeitstests des RETN-Netzes und der betrieblichen oder administrativen Systeme von RETN oder unbefugter Zugang zu diesen;
- - Unerlaubte Penetrations-/Vulnerabilitätstests von oder Zugang zu den Netzen oder Systemen anderer Unternehmen.
 - - Elektronische Nachahmung einer anderen Person oder Organisation oder andere betrügerische Praktiken;
 - - Spamming; unerwünschte E-Mails, unerwünschte Werbung, Nachrichten, die andere Dienste stören sollen, Nachrichten mit böswilligem Inhalt;
- - Farming von E-Mail-Adressen oder anderen individuellen Online-Kennungen;
 - - Phishing;
 - - Unbefugtes Abfangen von Nachrichten oder anderen Daten;

- - Betrieb von Netzdiensten wie offenen Proxies, offenen Mail-Relays oder offenen rekursiven Domain-Name-Servern.

Nutzung, die die Integrität des Netzes bedroht

Allgemeine Störungen des RETN-Netzes oder seiner Überwachungssysteme.

- - Handlungen, die gegen die AUP des Lieferanten von RETN verstoßen;
- - Handlungen, die dazu führen, dass das RETN-Netz zum Ziel eines DDoS- oder eines anderen gezielten Angriffs wird;
- - Alles, was dazu führt, dass unser IP-Raum von Missbrauchsdatenbanken (Spamhaus usw.) auf eine schwarze Liste gesetzt wird;
- - Handlungen, die zu einer Unterbrechung des RETN-Netzes durch behördliche Anordnung führen;
- - Handlungen, die zu einer Unterbrechung der Dienste für andere RETN-Kunden führen.

Bösartiges Verhalten gegenüber RETN-Mitarbeitern

RETN nimmt den Schutz und das Wohlergehen seiner Mitarbeiter ernst und ist stets bestrebt, ihr Recht auf Arbeit in einem sicheren und freundlichen Umfeld zu schützen. RETN toleriert keine Äußerungen oder Verhaltensweisen gegenüber seinen Mitarbeitern, die:

- beleidigender oder herabwürdigender Natur ist
- Einschließlich jeglicher Form von Gewalt oder körperlicher Bedrohung
- Enthält bedrohliche Sprache
- Enthält negative Kommentare in Bezug auf das (vermeintliche oder andere) Geschlecht, die Religion, das Geschlecht, das Alter, die Ethnie oder homophobe Äußerungen eines Mitarbeiters