

Trioptek Solutions, Inc. Acceptable Use Policy (AUP)

Updated August 2010

This AUP does not (a) obligate TRIOPTTEK to monitor, review, or police the data and content residing on the TRIOPTTEK Network or (b) create any obligation or duty of TRIOPTTEK to any party that is not a Client, including, but not limited to, any Third Party User. Unless and until notified, TRIOPTTEK is not likely to be aware of any violations of this AUP or any violations of law. TRIOPTTEK expects all Users to notify us of any violations of law or violations of this AUP. TRIOPTTEK EXPRESSLY DISCLAIMS ANY LIABILITY FOR THE DATA AND CONTENT TRANSMITTED THROUGH OR INTERMEDIATELY, TEMPORARILY OR PERMANENTLY STORED ON THE TRIOPTTEK NETWORK OR ANY SERVER AND FOR THE ACTIONS OR OMISSION OF USERS.

Prohibited Content

Users shall not allow the posting, transmission, or storage of data or content on or through TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure which, in TRIOPTTEK'S sole determination, constitutes a violation of any federal, state, local or international law, regulation, ordinance, court order or other legal process ("Applicable Law"). Users shall be responsible for determining which Applicable Laws are applicable to their use of TRIOPTTEK Services. Prohibited content includes, without limitation, (a) content or code that facilitate any violation of, or describe ways to violate, this AUP or (b) "harvested" addresses or information, (c) "phishing" websites, or (d) "spamvertising" sites.

A User shall not knowingly host on its Servers, use TRIOPTTEK Services or transmit over the TRIOPTTEK Network, any material believed by TRIOPTTEK to constitute child pornography. In addition to any other actions it may take under this AUP, TRIOPTTEK reserves the right to cooperate fully with any criminal investigation of content located on a Server that constitutes alleged child pornography or an alleged violation of Applicable Law.

Users' Security Obligation

Users must use reasonable care to ensure the security of each Server or Hosted Service, TRIOPTTEK Network and its physical infrastructure. A Client is solely responsible for any intrusions into, or security breaches of, any of its Servers, except as otherwise covered by a specifically designated security administration or firewall security service package ordered by the Client. TRIOPTTEK reserves the right to disconnect without refund or the provision of service credit any Servers which disrupt the TRIOPTTEK Network or any hardware objects on the network as a result of a security compromise.

Network Abuse

Users are prohibited from engaging in any activities that TRIOPTTEK determines, in its sole discretion, to constitute network abuse, including, but not limited to, the following:

1. Introducing or executing malicious programs into any network or server, such as viruses, worms, Trojan Horses, and key loggers.
2. Causing or initiating security breaches or disruptions of network communication and/or connectivity, including port scans, flood pings, email-bombing, packet spoofing, IP spoofing, and forged routing information.
3. Executing any form of network activity that will intercept data not intended for the Client's server or Client related services.

4. Evading or circumventing user authentication or security of any host, network or account, including cracking, brute-force, or dictionary attacks.
5. Interfering with or denying service to any user, host, or network other than the Client's host, such as a denial of service attack or distributed denial of service attack.
6. Conduct designed to avoid restrictions or access limits to specific services, hosts, or networks, including the forging of packet headers or other identification information.
7. Soliciting the performance of any illegal activity, even if the activity is not performed.
8. Using any program, or sending messages of any kind, designed to interfere with or disable a user's terminal session.

For your convenience, you may click on Prohibited Activities to review a list of additional prohibited activities and examples of prohibited activities. All Users are encouraged to review this list to ensure compliance with this AUP. If you believe that a violation of this AUP has occurred please review the information at the Legal section which contains important information concerning the reporting of potential violations.

Intellectual Property Infringement Policy

Users may not transmit, distribute, download, copy, cache, host, or otherwise store on a Server, TRIOPTTEK Network or its physical infrastructure any information, data, material, or work that infringes the intellectual property rights of others or violates any trade secret right of any other person. TRIOPTTEK has the right to disable access to, or remove, infringing content to the extent required under any law or regulation, including the Digital Millennium Copyright Act of 1998. If any Client or any Third Party User, including those that are customers of our Clients, repeatedly violates TRIOPTTEK'S Intellectual Property Infringement Policy, any copyright law or any other intellectual property right, TRIOPTTEK reserves the right to (i) suspend permanently or terminate the TRIOPTTEK Services of such Client and/or (ii) suspend permanently or terminate the access to the TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure by such Third Party User.

E-mail and Anti-Spamming Policy

Users may not (i) send unsolicited bulk messages over the Internet (i.e., "spamming"), (ii) send spam to weblog sites or automatically post random comments or promotions for commercial services to weblogs (i.e., "spamming blogs"). Users must comply with all relevant legislation and regulations on bulk and commercial e-mail, including the CAN-SPAM Act of 2003. Mass Mailings – Users may not send mass unsolicited e-mail, which is email that is sent to recipients who have not Confirmed Opt-In to mailings from the User. Users who send mass mailings must maintain complete and accurate records of all consents and opt-ins and provide such records to TRIOPTTEK upon its request. If a User cannot provide positive and verifiable proof of such consents and opt-ins, TRIOPTTEK will consider the mass mailing to be unsolicited.

Mailing Lists – Users are prohibited from operating mailing lists, listservs, or mailing services that do not target an audience that has voluntarily signed up for e-mail information using a Confirmed Opt-In process or that has made their e-mail addresses available to a User for distribution of information. Users who operate mailing lists must maintain complete and accurate records of all consents and Confirmed Opt-In elections and provide such records to TRIOPTTEK upon its request. If a User cannot provide positive and verifiable proof of such consents and Confirmed Opt-In elections, TRIOPTTEK will consider the list mailing to be unsolicited. Any User-maintained mailing list must also allow any party on the list to remove itself automatically and permanently.

Other prohibited activities include, without limitation, the following:

1. Use of the TRIOPTTEK Network for the receipt of replies to unsolicited mass e-mail.
2. Forgery of e-mail headers ("spoofing").
3. Spamming via third-party proxy, aggregation of proxy lists, or installation of proxy mailing software.
4. Configuration of a mail server to accept and process third-party messages for sending without user identification and authentication.
5. Hosting web pages advertised within "spam e-mail" sent from another network ("spamvertising").
6. Hosting web pages or providing services that support spam.
7. Any other unsolicited bulk messages, postings, or transmissions through media such as weblog posts, IRC/chat room messages, guestbook entries, HTTP referrer log entries, usenet posts, pop-up messages, instant messages, or SMS messages.
8. Instructing others in any activity prohibited by this AUP.

If any Client or any Third Party User that is a customer of our Client uses TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure in a manner that causes TRIOPTTEK to be "blacklisted" or blocked, TRIOPTTEK reserves the right to (i) suspend permanently or terminate TRIOPTTEK Services of such Client and/or (ii) suspend permanently or terminate the access to TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure by such Third Party User.

Block Removal – If, as a result of a Client's actions, TRIOPTTEK's mail servers or IP address ranges are placed on black hole lists or other mail filtering software systems, TRIOPTTEK shall charge Client \$100 upfront and \$100 per hour thereafter for any necessary remedial actions.

IP Allocation

TRIOPTTEK owns each IP address that it assigns to a Client. A Client shall not use IP addresses that were not assigned to it by TRIOPTTEK. TRIOPTTEK reserves the right to suspend the network access of any server utilizing IP addresses outside of the assigned range.

IRC Policy

Clients may not operate and maintain IRC servers which connect to global IRC networks such as Undernet, EFnet and DALnet. Use of IRC plug-ins, scripts, add-ons, clones or other software designed to disrupt or deny service to other users is prohibited. Harassing or abusive IRC activity is expressly prohibited under the AUP, including (i) disruption or denial of service or (ii) the use or joining of "botnets" or the use of IRC BNC's or other proxy and re-direction software. If a Client's IRC servers are frequently compromised or attract denial of service or distributed denial of service attacks that disrupt or denies service to other Clients or users, TRIOPTTEK may null-route, filter, suspend, or terminate that Client's service.

Usenet Policy

Usenet posts and content must conform to standards established by the Internet community and the applicable newsgroup charter. TRIOPTTEK reserves the right to determine whether such posts violate the AUP.

Legal Investigations

Clients will cooperate and comply with any civil or criminal investigation regarding use of TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure or content located on its Servers or transmitted using TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure, including, without limitation, the following: discovery orders, subpoenas, freeze orders, search warrants, information requests, wire taps, electronic intercepts and surveillance, preservation requests, and any other order from a court, government entity or regulatory agency (each an "Investigation"). TRIOPTTEK may charge a User or any person seeking compliance with an Investigation for the reasonable costs and expenses associated with TRIOPTTEK'S compliance with any Investigation. TRIOPTTEK reserves the right to comply with any Investigation without notice to a User. Clients shall not be entitled to a refund or any service credits, and TRIOPTTEK shall not be in default under any agreement for TRIOPTTEK Services, if its compliance with any Investigation causes a User to incur downtime or requires the sequestering of all or a portion of the Servers. TRIOPTTEK also reserves the right to disclose information relating to Users and their use of TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure or information transmitted, owned by or stored by or on behalf of any User, if such information is disclosed in connection with an Investigation or in order to prevent the death of or bodily harm to any individual, as determined by TRIOPTTEK in its sole discretion.

Violations of AUP

TRIOPTTEK may enforce this AUP, with or without notice to a User, by any action it deems reasonable, in its sole discretion. In addition to the remedial provisions provided elsewhere in this AUP, TRIOPTTEK may:

1. Disable access to a User's content that violates this AUP.
2. Suspend or Terminate a User's access to TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure.
3. Remove DNS records from Servers.
4. Block mail or any other network service.
5. Effect IP addresses null routing.
6. Take legal action against a User to enforce compliance with this AUP.

Reporting Violations:

If there is a violation of this AUP direct the information to the TRIOPTTEK Abuse Department at abuse@triopttek.com

If available, please provide the following information:

1. The IP address used to commit the alleged violation.
2. The date and time of the alleged violation.
3. Evidence of the alleged violation.

E-mail with full header information provides all of the above, as do system log files. Other situations will require different methods of providing the above information. TRIOPTTEK may take any one or more of the following actions in response to complaints:

1. Issue written or verbal warnings.
2. Suspend the User's account.
3. Terminate the User's account.
4. Bill the User for administrative costs and/or reactivation charges.
5. Bring legal action to enjoin violations and/or to collect damages, if any, caused by violations.

If any User uses TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure in a manner that exposes TRIOPTTEK to potential liability, as reasonably determined by TRIOPTTEK, TRIOPTTEK may suspend permanently or terminate the access to TRIOPTTEK Services, the TRIOPTTEK Network or its physical infrastructure by such User.

The remedial actions set forth in this AUP shall not be construed in any way to limit the actions or remedies that TRIOPTTEK may take to enforce and ensure compliance with this AUP. TRIOPTTEK reserves the right to recover any and all expenses, and apply any reasonable charges, in connection with a User's violation of this AUP. No refund or service credits will be issued for any interruption in service resulting from violations of this AUP.

TRIOPTTEK reserves the right at all times to investigate any actual, suspected, or alleged violations of this AUP, with such investigation to include accessing of data and records on, or associated with, any Server, the TRIOPTTEK Network or its physical infrastructure.

Prohibited Activities

1. forging, misrepresenting, omitting or deleting message headers, return mailing information, or internet protocol addresses, to conceal or misidentify the origin of a message;
2. creating or sending Internet viruses, worms or Trojan horses, flood or mail bombs, or engaging in denial of service attacks;
3. hacking, and/or subverting, or assisting others in subverting, the security or integrity of our products or systems;
4. soliciting the performance of any illegal activity, even if the activity itself is not performed;
5. threatening bodily harm, or encouraging bodily harm or property destruction;
6. harassing another, or encouraging harassing behavior;
7. engaging in outright fraud, or using services to engage in scams like pyramid schemes;
8. collecting personal information about others without their knowledge or consent;
9. instructing others in prohibited activities;
10. using services to disseminate or display images classified under U.S. law as child pornography, child erotica (regardless of literary or artistic merit) and/or bestiality; and/or
11. acting in any manner that might subject TRIOPTTEK to unfavorable regulatory action, subject us to any liability for any reason, or adversely affect TRIOPTTEK'S public image, reputation or goodwill, as determined by us in our sole and exclusive discretion.
12. creating fake weblog or weblogs which are intended or reasonably likely to promote the author's affiliated websites or to increase the search engine rankings of associated sites.
13. sending spam to weblog sites or automatically posting random comments or promotions for commercial services to weblogs.