



## Dedico AUP (Acceptable Use Policy)

This AUP applies to each user that subscribes for Dedico's Services ("Customers"), all users of Dedico's Services and all users that access or utilize Dedico's website, Dedico's Network or its physical infrastructure, whether or not such users are customers of Dedico, including the customers of our Customers ("Third Party Users"), and every server or network device that is under each User's control and attached to Dedico's Network or physical infrastructure as a part of Dedico's Services (a "Server"). The term "User" as used in this AUP means both Customers and Third Party Users.

**This AUP is incorporated by this reference into each Customer's Terms of Service and Service Level Agreement. This AUP should be read in conjunction with Dedico's Terms of Service, Dedico's Service Level Agreement and Dedico's Privacy Policy. Capitalized terms used herein without being defined herein shall have the meaning ascribed to such capitalized term in the Terms of Service, the SLA or the Privacy Policy, as applicable. Customer's use of Dedico's website, Dedico's Network, the Products and Services is also subject to Customer's acceptance and compliance with the Terms of Service, the SLA and this AUP. Current copies of Dedico's Terms of Service, SLA and Privacy Policy may be reviewed or printed by Customer at the Legal section of Dedico's website. CUSTOMER HEREBY REPRESENTS AND WARRANTS THAT IT HAS READ, UNDERSTOOD AND ACCEPTED THE TERMS OF THE TERMS OF SERVICE, THE SLA AND THIS AUP. Dedico reserves the right to amend or modify this AUP from time to time, and a User's use of Dedico's Services, Dedico's network and physical infrastructure after changes to the AUP are posted on Dedico's website ([www.dedico.com](http://www.dedico.com)) will constitute the User's acceptance of any such amendments or modifications.**

Customers are responsible for complying with this AUP and for violations attributable to their customers and users, whether authorized or not by a Customer or Dedico. Customers must take all reasonable steps to ensure that their customers and users will comply with this AUP.

This AUP does not (a) obligate Dedico to monitor, review, or police the data and content residing on Dedico's Network or (b) create any obligation or duty of Dedico to any party that is not a Customer, including, but not limited to, any Third Party User. Unless and until notified, Dedico is not likely to be aware of any violations of this AUP or any violations of law. Dedico expects all Users to notify us of any violations of law or violations of this AUP. **DEDICO EXPRESSLY DISCLAIMS ANY LIABILITY FOR THE DATA AND CONTENT TRANSMITTED THROUGH OR INTERMEDIATELY, TEMPORARILY OR PERMANENTLY STORED ON DEDICO'S 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 Dedico's Services, Dedico's Network or its physical infrastructure which, in Dedico'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 Dedico's 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 Dedico's Services or transmit over Dedico's Network, any material believed by Dedico to constitute child pornography. In addition to any other actions it may take under this AUP, Dedico 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, Dedico's Network and its physical infrastructure. A Customer 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 Customer. Dedico reserves the right to disconnect without refund or the provision of service credit any Servers which disrupt Dedico's 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 Dedico determines, in its sole discretion, to constitute network abuse, including, but not limited to, the following:

- Introducing or executing malicious programs into any network or server, such as viruses, worms, Trojan Horses, and key loggers.
- 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.
- Executing any form of network activity that will intercept data not intended for the Customer's server.
- Evading or circumventing user authentication or security of any host, network or account, including cracking, brute-force, or dictionary attacks.
- Interfering with or denying service to any user, host, or network other than the Customer's host, such as a denial of service attack or distributed denial of service attack.
- Conduct designed to avoid restrictions or access limits to specific services, hosts, or networks, including the forging of packet headers or other identification information.
- Soliciting the performance of any illegal activity, even if the activity is not performed.
- Using any program, or sending messages of any kind, designed to interfere with or disable a user's terminal session.

### **Intellectual Property Infringement Policy**

Users may not transmit, distribute, download, copy, cache, host, or otherwise store on a Server, Dedico's 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. Dedico 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. For your convenience, information concerning procedures for making claims of copyright infringement for purposes of Title 17, Section 512, of the United States Code is contained at the Legal section of our website. **If any Customer or any Third Party User, including those that are customers of our Customers, repeatedly violates Dedico's Intellectual Property Infringement Policy, any copyright law or any other intellectual property right, Dedico reserves the right to (i) suspend permanently or terminate Dedico's Services of such Customer and/or (ii) suspend permanently or terminate the access to Dedico's Services, Dedico's 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) create 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 (i.e., "splogs") or (iii) 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 or Closed-Loop Opt-In 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 Dedico upon its request. If a User cannot provide positive and verifiable proof of such consents and opt-ins, Dedico 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 or Closed-Loop 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 or Closed-Loop Opt-In elections and provide such records to Dedico upon its request. If a User cannot provide positive and verifiable proof of such consents and Confirmed Opt-In or Closed-Loop Opt-In elections, Dedico 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:

- Use of Dedico's Network for the receipt of replies to unsolicited mass e-mail.
- Forgery of e-mail headers ("spoofing").
- Spamming via third-party proxy, aggregation of proxy lists, or installation of proxy mailing software.
- Configuration of a mail server to accept and process third-party messages for sending without user identification and authentication.
- Hosting web pages advertised within "spam e-mail" sent from another network ("spamvertising").
- Hosting web pages or providing services that support spam.
- 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.
- Instructing others in any activity prohibited by this AUP.

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

**Operating Dedico Service on behalf of, or in connection with, or reselling any service to persons or firms listed in the Spamhaus Register of Known Spam Operations database at [www.spamhaus.org](http://www.spamhaus.org) shall constitute a violation of this AUP.**

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

#### **IP Allocation**

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

#### **IRC Policy**

Customers 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 Customer’s IRC servers are frequently compromised or attract denial of service or distributed denial of service attacks that disrupt or denies service to other Customers or users, Dedico may null-route, filter, suspend, or terminate that Customer’s service.

#### **Usenet Policy**

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

#### **Legal Investigations**

Users will cooperate and comply with any civil or criminal investigation regarding use of Dedico’s Services, Dedico’s Network or its physical infrastructure or content located on its Servers or transmitted using Dedico’s Services, Dedico’s 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”). Dedico may charge a User or any person seeking compliance with an Investigation for the reasonable costs and expenses associated with Dedico’s compliance with any Investigation. **Dedico reserves the right to comply with any Investigation without notice to a User. Customers shall not be entitled to a refund or any service credits, and Dedico shall not be in default under any agreement for Dedico’s 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. Dedico also reserves the right to disclose information relating to Users and their use of Dedico’s Services, Dedico’s 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 Dedico in its sole discretion.**

#### **Violations of AUP**

Dedico 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, Dedico may:

- Disable access to a User’s content that violates this AUP.
- Suspend or Terminate a User’s access to Dedico’s Services, Dedico’s Network or its physical infrastructure.
- Remove DNS records from Servers.
- Block mail or any other network service.
- Effect IP address null routing.

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 Abuse Department at [abuse@dedico.com](mailto:abuse@dedico.com).

If available, please provide the following information:

- The IP address used to commit the alleged violation.
- The date and time of the alleged violation, including the time zone or offset from GMT.
- 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. Dedico may take any one or more of the following actions in response to complaints:

- Issue written or verbal warnings.
- Suspend the User's newsgroup posting privileges.
- Suspend the User's account.
- Terminate the User's account.
- Bill the User for administrative costs and/or reactivation charges.
- Bring legal action to enjoin violations and/or to collect damages, if any, cause by violations.

**If any User uses Dedico's Services, Dedico's Network or its physical infrastructure in a manner that exposes Dedico to potential liability, as reasonably determined by Dedico, Dedico may suspend permanently or terminate the access to Dedico's Services, Dedico's 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 Dedico may take to enforce and ensure compliance with this AUP. Dedico 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.**

Dedico 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, Dedico's Network or its physical infrastructure.

### **Other Prohibited Activities**

- forging, misrepresenting, omitting or deleting message headers, return mailing information, or internet protocol addresses, to conceal or misidentify the origin of a message;
- creating or sending Internet viruses, worms or Trojan horses, flood or mail bombs, or engaging in denial of service attacks;
- hacking, and/or subverting, or assisting others in subverting, the security or integrity of our products or systems;
- soliciting the performance of any illegal activity, even if the activity itself is not performed;
- threatening bodily harm, or encouraging bodily harm or property destruction;
- harassing another, or encouraging harassing behavior;
- engaging in outright fraud, or using services to engage in scams like pyramid schemes;
- collecting personal information about others without their knowledge or consent;
- instructing others in prohibited activities;
- 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
- acting in any manner that might subject Dedico to unfavorable regulatory action, subject us to any liability for any reason, or adversely affect Dedico's public image, reputation or goodwill, as determined by us in our sole and exclusive discretion.
- 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.
- sending spam to weblog sites or automatically posting random comments or promotions for commercial services to weblogs