



ACCEPTABLE USE POLICY (AUP)

This AUP is incorporated by reference in your hosting services agreement with Dirigo. Terms used in this AUP shall have the meaning given in your hosting services agreement. Your services may be suspended or terminated for violation of this AUP in accordance with your hosting services agreement with Dirigo. Inquiries regarding this policy should be directed to your Dirigo account lead or technician.

Abuse

You may not use Dirigo's network or services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including but not limited to:

- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network;
- Monitoring data or traffic on any network or system without the express authorization of the owner of the system or network;
- Interference with service to any user of the Dirigo or other network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
- Use of an Internet account or computer without the owner's authorization;
- Collecting or using email addresses, screen names, or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting);
- Collecting or using information without the consent of the owner of the information;
- Use of any false, misleading, or deceptive TCP-IP packet header information in an e-mail or a newsgroup posting;
- Use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- Use of the service for distribution of advertisement delivery software unless: (i) the user affirmatively consents to the download and installation of such software based on a clear and conspicuous notice of the nature of the software, and (ii) the software is easily removable by use of standard tools for such purpose included on major operating systems; (such as Microsoft's ad/remove tool);
- Any conduct that is likely to result in retaliation against the Dirigo network or Web site, or Dirigo's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS).

Bulk Email

You may not use a Dirigo Mail Service (such as RS Email, Hosted Microsoft Exchange, or iMail) to send bulk mail without prior consent and authorization by Dirigo. We define bulk e-mail as any email account sending 500 or more of the same or similar type e-mail message in a single day (from 12:00 a.m. to 12:00 p.m. Eastern Time) from a single host. Bulk e-mail presents risks that require special attention. Additional fees are required to manage bulk e-mail.

Mail Requirements

You must comply with the CAN-SPAM Act of 2003 and other laws and regulations applicable to bulk or commercial email. In addition, your bulk and commercial email must meet the following requirements:

- Your intended recipients must have given their consent to receive e-mail from you via some affirmative means, such as an opt-in procedure;
- Your procedures for seeking consent include reasonable means to ensure that the person giving consent is the owner of the e-mail address for which consent is given;

- You retain evidence of each recipient's consent in a form that can be promptly produced on request, and you honor recipient's and Dirigo's requests to produce consent evidence within 72 business hours of receipt of the request;
- You have procedures in place that allow a recipient to revoke their consent, such as a link in the body of the e-mail, or instructions to reply with the word "Remove" in the subject line; you honor revocations of consent within 48 business hours, and you notify recipients that the revocation of their consent will be implemented in 48 business hours;
- You must post an e-mail address for complaints (such as customerservice@yourdomain.com) in a conspicuous place on any Web site associated with the e-mail, you must register that address at www.abuse.net, and you must promptly respond to messages sent to that address;
- You must have a Privacy Policy posted for each domain associated with the mailing;
- You have the means to track anonymous complaints;
- You may not obscure the source of your e-mail in any manner, such as omitting, forging, or misrepresenting message headers or return addresses; your e-mail must include the recipients e-mail address in the body of the message or in the "To" line of the e-mail;
- The subject line of the e-mail must clearly describe the subject matter contained in the e-mail, and the message must include valid contact information; and
- You must not attempt to send any message to an e-mail address if three (3) consecutive delivery rejections have occurred and the time between the third rejection and the first rejection is longer than fifteen days (e.g. management of e-mail bounces and feedback loops).

These policies apply to e-mail messages sent using your Dirigo services, or to messages sent from any network by you or any person on your behalf that directly or indirectly refers the recipient to a site or an e-mail address hosted via your Dirigo service. In addition, you may not use a third-party e-mail service that does not practice similar procedures for all its customers. These requirements apply to distribution lists prepared by third parties as if the list were created by you.

Dirigo may test and otherwise monitor your compliance with its requirements via www.senderbase.org, www.senderscore.com, or other services. Dirigo may block the transmission of e-mail that violates these provisions. Dirigo may, at its sole discretion, require certain customers to seek advance approval for bulk and commercial e-mail, which approval will not be granted unless the customer can demonstrate that all of the requirements stated above will be met.

Unsolicited Communications

You may not use your service to send e-mail or any other communications to a person who has indicated that they do not wish to receive it. If the communication is bulk mail, then you will not be in violation of this section if you comply with the 48 hour removal requirement described above.

Vulnerability Testing

You may not attempt to probe, scan, penetrate, or test the vulnerability of a Dirigo system or network, or to breach Dirigo's security or authentication measures, whether by passive or intrusive techniques, without Dirigo's express written consent. Permission to use services like McAfee Secure will not be unnecessarily withheld if disclosed prior to use.

Newsgroup, Chat Forums, Other Networks

You must comply with the rules and conventions for postings to any bulletin board, chat group or other forum in which you participate, such as IRC and USENET groups including their rules for content and commercial postings. These groups usually prohibit the posting of off-topic commercial messages, or mass postings to multiple forums.

You must comply with the rules of any other network you access or participate in using your Dirigo services.

Offensive Content

You may not publish, transmit or store on or via Dirigo's network and equipment any content or links to any content that Dirigo reasonably believes:

- Constitutes, depicts, fosters, promotes, or relates in any manner to child pornography, bestiality, or non-consensual sex acts or depicts adult pornography;
- is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;
- is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
- is defamatory or violates a person's privacy;
- creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;
- improperly exposes trade secrets or other confidential or proprietary information of another person or organization;
- is intended to assist others in defeating technical copyright protections;
- infringes on another person's copyright, trade or service mark, patent, or other property right;
- promotes illegal drugs, violates export control laws, relates to illegal gambling, or illegal arms or human trafficking;
- is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to Dirigo; or
- is otherwise malicious, fraudulent, or may result in retaliation against Dirigo by offended viewers or recipients, or is intended to harass or threaten.

Content "published or transmitted" via Dirigo's network or equipment includes Web content, e-mail, bulletin board postings, chat, Facebook posts, Tweets, and any other type of posting or transmission that relies on the Internet.

Live Events

You may not use your Dirigo services to stream live sex acts of any kind, even if the content would otherwise comply with the AUP. Dirigo may prohibit you from streaming other live events where there is a special risk, in Dirigo's reasonable discretion, that the event may violate the Offensive Content section above.

Copyrighted Material

You may not use Dirigo's network or services to download, publish, distribute, or otherwise copy or use in any manner any text, music, software, art, image, or other work protected by copyright law unless:

- you have been expressly authorized by the owner of the copyright for the work to copy the work in that manner; or
- you are otherwise permitted by established copyright law to copy the work in that manner.

It is Dirigo's policy to terminate the services of customers who are repeat infringers.

Shared Systems

You may not use any shared system provided by Dirigo in a way that unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of the resources of the system. For example, we may prohibit the automated or scripted use of Dirigo shared e-mail Services if it has a negative impact on the mail system, or we may require you to repair coding abnormalities in your shared-hosted code if it unnecessarily conflicts with other shared customers' use of the server(s). You agree that we may quarantine or delete any data stored on a shared system if the data is infected with a virus, or is otherwise corrupted, and has the potential to infect or corrupt the system or other customers' data that is stored on the same system.

Other

- You must have valid and current information on file with your domain name registrar for any domain hosted on the Dirigo network.
- You may only use IP addresses assigned to you by Dirigo in connection with your Dirigo services.
- You agree that if the Dirigo IP numbers assigned to your account are listed on an abuse database like Spamhaus, you will be in violation of this AUP, and Dirigo will take reasonable action to protect its IP numbers, including suspension and/or termination of your service, regardless of whether the IP numbers were listed as a result of your actions.

- You agree that if you register a DNS record or zone on Dirigo managed or operated DNS servers or services for a domain of which you are not the registrant or administrative contact according to the registrars WHOIS system, that, upon request from the registrant or administrative contact according to the registrars WHOIS system, Dirigo may modify, transfer, or delete such records or zones.

Service Level Agreement

No credit will be available under a Dirigo service level guaranty or agreement for interruptions of service resulting from AUP violations.

October 23, 2010 revision