This AUP is incorporated by reference in your hosting services agreement with Data Paradigm.

Your services may be suspended or terminated for violation of this AUP in accordance with the Master Services Agreement or Contract for Services.

Inquiries regarding this policy should be directed to techsupport@dataparadigm.com

Abuse
You may not use Data Paradigm's network or Services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including:

- 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 Data Paradigm 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 email 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); or
- Any conduct that is likely to result in retaliation against the Data Paradigm network or website, or Data Paradigm'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 or Commercial Email
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 have given their consent to receive email 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 email 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 Data Paradigm's requests to produce consent evidence within 72 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 email, or instructions to reply with the word "Remove" in the subject line; you honor revocations of consent within 48 hours, and you notify recipients that the revocation of their consent will be implemented in 48 hours;
- You must post an email address for complaints (such as abuse@yourdoman.com) in a conspicuous place on any website associated with the email, you must register that address at 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 email in any manner. Your email must include the recipients email address in the body of the message or in the "TO" line of the email; and
- You must not attempt to send any message to an email address if 3 consecutive delivery rejections have occurred and the time between the third rejection and the first rejection is longer than fifteen days.

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

Data Paradigm may test and otherwise monitor your compliance with its requirements. **Data Paradigm may block the transmission of email that violates these provisions.** Data Paradigm may, at its discretion, require certain customers to seek advance approval for bulk and commercial email, which approval will not be granted unless the customer can demonstrate that all of the requirements stated above will be met.

Vulnerability Testing
You may not attempt to probe, scan, penetrate or test the vulnerability of a Data Paradigm system or network or to breach Data Paradigm’s security or authentication measures, whether by passive or intrusive techniques, without Data Paradigm's express written consent.

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

- Constitutes, depicts, fosters, promotes or relates in any manner to child pornography, bestiality, or non-consensual sex acts;

- 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 a investigation by law enforcement;
- improperly exposes trade secrets or other confidential or proprietary information of another person;
- 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 trafficking;
- is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to Data Paradigm; or
- is otherwise malicious, fraudulent, or may result in retaliation against Data Paradigm by offended viewers.

Content "published or transmitted" via Data Paradigm's network or equipment includes Web content, email, bulletin board postings, chat, and any other type of posting or transmission that relies on the Internet.

Copyrighted Material
You may not use Data Paradigm'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 Data Paradigm’s policy to terminate in appropriate circumstances the services of customers who are repeat infringers.

Other

- You must have valid and current information on file with your domain name registrar for any domain hosted on the Data Paradigm network.
- You may only use IP addresses assigned to you by Data Paradigm in connection with your Data Paradigm services.
- You agree that if the Data Paradigm IP numbers assigned to your account are listed on an abuse database like Spamhaus, you will be in violation of this AUP, and Data Paradigm may 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 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.

SLA

No credit will be available under your Data Paradigm SLA for interruptions of service resulting from AUP violations.