N+2 ACCEPTABLE USE POLICY

This Acceptable Use Policy (AUP) is incorporated by reference in Client's Master Services Agreement with n+2 and any applicable SOFs.

Client Services may be suspended or terminated for violation of this AUP by Client or its customers. Capitalized terms used in this AUP shall have the meaning given in the Master Services Agreement with n+2. For purposes of this AUP, "Client" shall mean both Client and its customers utilizing Services provided by n+2.

ABUSE

Client may not use n+2'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 n+2 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 n+2 network or website, or n+2's employees, officers, members, affiliates or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS).

BULK EMAIL

Client may not use a n+2 mail service to send bulk mail. Client may use its dedicated hosted system to send bulk mail, subject to the restrictions in this Acceptable Use Policy.

MAIL REQUIREMENTS

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

- Client's intended recipients have given their consent to receive email from Client via some affirmative means, such as an opt-in procedure;
- Client's 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;
- Client shall retain evidence of each recipient's consent in a form that can be promptly produced on request, and Client honor recipient's and n+2's requests to produce consent evidence within 72 hours of receipt of the request;.
- Client shall 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; Client honor revocations of consent within 48 hours, and Client notify recipients that the revocation of their consent will be implemented in 48 hours;
- Client must post an email address for complaints (such as abuse@Clientdoman.com) in a conspicuous place on any website associated with the email, Client must register that address at abuse.net, and Client must promptly respond to messages sent to that address;
- Client must have a Privacy Policy posted for each domain associated with the mailing;

- Client shall have the means to track anonymous complaints;
- Client may not obscure the source of Client email in any manner, such as omitting, forging, or misrepresenting message headers or return addresses. Client email must include the recipients email address in the body of the message or in the "TO" line of the email;
- The subject line of the email must clearly describe the subject matter contained in the email, and the message must include valid contact information; and
- Client 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 the Services under the CSA, and to messages sent from any network by Client or any person on Client's behalf that directly or indirectly refer the recipient to a site or an email address hosted via a n+2 Service. In addition, Client 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 Client.

N+2 may test and otherwise monitor Client compliance with its requirements. N+2 may block the transmission of email that violates these provisions. N+2 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.

UNSOLICITED COMMUNICATIONS

Client may not use the Services to send email 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 Client will not be in violation of this section if Client comply with the 48 hour removal requirement described above.

VULNERABILITY TESTING

Client may not attempt to probe, scan, penetrate or test the vulnerability of a n+2 system or network, or to breach n+2's security or authentication measures, whether by passive or intrusive techniques, without n+2's express written consent.

NEWSGROUP, CHAT FORUMS, OTHER NETWORKS

Client must comply with the rules and conventions for postings to any bulletin board, chat group or other forum in which Client 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.

Client must comply with the rules of any other network Client access or participate in using Client n+2 services.

OFFENSIVE CONTENT

Client may not publish, transmit or store on or via n+2's network and equipment any content or links to any content that n+2 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 an 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 Client or to n+2; or
- is otherwise malicious, fraudulent, or may result in retaliation against n+2 by offended viewers or recipients, or is intended to harass or threaten.

Content "published or transmitted" via n+2's network or equipment includes Web content, email, bulletin board postings, chat, tweets, and any other type of posting or transmission that relies on the Internet.

LIVE EVENTS

Client may not use Client n+2 Services to stream live sex acts of any kind, even if the content would otherwise comply with the AUP. N+2 may prohibit Client from streaming other live events where there is a special risk, in n+2's reasonable discretion, that the event may violate the Offensive Content section above.

COPYRIGHTED MATERIAL

Client may not use n+2'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:

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

It is n+2's policy to terminate in appropriate circumstances the services of customers who are repeat infringers.

SHARED SYSTEMS

Client may not use any shared system provided by n+2 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 n+2 Mail Services if it has a negative impact on the mail system, or we may require Client to repair coding abnormalities in Client Cloud-hosted code if it unnecessarily conflicts with other Cloud customers' use of the Cloud. Client 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

- Client must have valid and current information on file with Client's domain name registrar for any domain hosted on the n+2 network.
- Client may only use IP addresses assigned to Client by n+2 in connection with Client's n+2 Services or as otherwise agreed in a SOF.
- Client agree that if the n+2 IP numbers assigned to Client account are listed on an abuse database like Spamhaus, Client will be in violation of this AUP, and n+2 may take reasonable action to protect its IP numbers, including suspension and/or termination of Client service, regardless of whether the IP numbers were listed as a result of Client actions.

SLA

No credit will be available under a n+2 service level guaranty or agreement for interruptions of service resulting from AUP violations.