Introduction

The Acceptable Use Policy ("AUP") of Concergent, LLC ("Concergent"), as such policy may be subsequently amended, modified or supplemented from time to time is designed to (i) protect (a) Concergent's customers, (b) users of Concergent's website, products, service, and data center, including its networks and physical infrastructure, (c) the interests of Concergent and its affiliates, and (d) the legitimate interests of third parties; (ii) further comply with all relevant laws and regulations; (iii) promote the security and availability of Concergent's website, network and physical infrastructure; and (iv) regulate and restrict the use of all networks, physical infrastructure, products and services utilized, offered or provided by Concergent or its affiliates or housed at any Concergent data center (collectively, "Concergent IT Environment").

This AUP applies to each user who subscribes for Internet, IP or technology services or use of the Concergent IT Environment offered by Concergent ("Concergent Services"), all users of Concergent Services ("Customer" or "Customers") and all users who access or utilize Concergent Services or Concergent IT Environment, whether or not such users are Customers, including the customers of Customers ("Third Party Users"), and every server or network device that is under each User's control or is attached to, resides within, utilizes or communicates with or through Concergent's network or physical infrastructure as a part of Concergent IT Environment; including specifically any server physically hosted at any Concergent data center . The term "User" as used in this AUP means both Customers and Third Party Users.

This AUP is incorporated by this reference into each of Customer's Terms and Conditions, Master Services Agreement, Purchase Order, Rental Form or other contract that specifically references this AUP ("Customer Documents"). Capitalized terms used herein without being expressly defined herein shall have the meaning ascribed to such capitalized term in the Customer Documents. Customer's use of the Concergent IT Environment is subject to Customer's acceptance and compliance with this AUP. **CUSTOMER HEREBY REPRESENTS AND WARRANTS THAT IT HAS READ, UNDERSTANDS AND ACCEPTS THE TERMS OF THIS AUP AND THAT CUSTOMER'S USE OF THE CONCERGENT IT ENVIRONMENT CONCLUSIVELY EVIDENCES CUSTOMER'S ACCEPTANCE OF THIS AUP.** Concergent reserves the right to amend or modify this AUP from time to time, and modify the scope and nature of any User's permitted use of the Concergent IT Environment, including the physical infrastructure, effective immediately upon changes to the AUP being posted on Concergent's website (www.concergent.com) and subsequent use of any portion of the Concergent IT Environment will constitute the User's acceptance of any such amendments or modifications.

Customers are responsible for complying with this AUP. Customers shall take all reasonable steps to ensure that their customers and users comply with this AUP. Customer shall be liable for all damages arising from violations attributable to their customers and users, whether authorized or not by a Customer.

This AUP does not (a) obligate Concergent to monitor, review, or police the data or content residing on Concergent IT Environment or (b) create any obligation or duty of Concergent to any Third Party User. Unless and until notified, Concergent is not likely to be aware of violations of this AUP or any violations of law. Concergent expects all Users to notify Concergent of any violations of law or violations of this AUP of which a User becomes aware. **If Users believe that a violation of this AUP has occurred, please review the information under "Reporting Violations" that contains important information concerning the reporting of potential violations.**

CONCERGENT EXPRESSLY DISCLAIMS ANY LIABILITY FOR THE DATA AND CONTENT TRANSMITTED THROUGH OR INTERMEDIATELY, OR TEMPORARILY OR PERMANENTLY STORED ON THE CONCERGENT VIRTUAL ENVIRONMENT 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 the Concergent IT Environment that, in Concergent's sole determination, constitutes a violation of any federal, state, local or international law, regulation, ordinance, court order or other legal process ("Applicable Laws"). Users shall be responsible for determining which Applicable Laws are applicable to their use. Prohibited content includes, without

limitation, (a) content or code that facilitate any violation of, or describe ways to violate, this AUP, (b) "harvested" addresses or information, (c) "phishing" websites, and (d) "spamvertising" sites.

Offensive Content

Users may not publish, transmit or store on or via the Concergent IT Environment any content or links to any content that the Concergent 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 Users or to Concergent; or
- is otherwise malicious, fraudulent or may result in retaliation against Concergent by offended viewers.

In addition to any other actions it may take under this AUP, Concergent 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 Laws.

Users' Security Obligation

Users must use reasonable care to ensure the security of each of its servers operated within the Concergent IT Environment, including its physical infrastructure. A Customer is solely responsible for, and assumes all risks regarding, any intrusions into, or security breaches of, any of its servers, including any server supported by any specifically designated security administration or firewall security service package ordered by the Customer and provided by Concergent. Concergent reserves the right to disconnect or block, without refund or refuse credit for, any computer, mobile device, server or other device which disrupts the Concergent IT Environment as a result of a security compromise.

Vulnerability Testing

Users may not attempt to probe, scan, penetrate or test the vulnerability of the Concergent IT Environment or to breach any of Concergent's security or authentication measures, whether by passive or intrusive techniques, without the prior express written consent of Concergent.

Network Abuse

Users are prohibited from engaging in any activities that Concergent 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;
- 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;
- 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; or
- acting in any manner that might subject Concergent to unfavorable regulatory action, subject us to any liability for any reason, or adversely affect Concergent's public image, reputation or goodwill, as determined by us in our sole and exclusive discretion.

Live Events

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

Intellectual Property Infringement Policy

Users may not transmit, distribute, download, copy, cache, host, or otherwise store on the Concergent IT Environment, including upon any server, network or physical infrastructure included as part of the same, any information, data, material, or work that infringes upon the intellectual property rights of others or violates any trade secret right of any other person.

Specifically, Users may not use the Concergent IT Environment 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:

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

Concergent 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 Users' 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 Customer or any Third Party User, including those who are customers of our Customers, repeatedly violates Concergent's Intellectual Property Infringement Policy, any copyright law or any other intellectual property right, Concergent reserves the right to (i) suspend permanently or terminate Concergent Services to such Customer and/or (ii) suspend or permanently terminate access to the Concergent IT Environment 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 Concergent upon its request. If a User cannot provide positive and verifiable proof of such consents and opt-ins, Concergent will consider the mass mailing to be unsolicited.

Mailing Lists – Users are prohibited from operating mailing lists, listserves, 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 Concergent 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, Concergent 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 Concergent'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; or
- instructing others in any activity prohibited by this AUP.

If any Customer or any Third Party User who is a customer of our Customer uses Concergent Services, the Concergent IT Environment in a manner that causes Concergent to be "blacklisted" or blocked, Concergent reserves the right to (i) suspend or permanently terminate Concergent Services for such Customer and/or (ii) suspend or permanently terminate Concergent Services or access to the Concergent IT Environment by such Third Party User. Utilizing Concergent Services or the Concergent IT Environment 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 shall constitute a violation of this AUP.

Block Removal

If, as a result of a Customer's actions, Concergent's mail servers or IP address ranges are placed on black hole lists or other mail filtering software systems, Concergent shall charge for services rendered at Concergent's then current rates for any necessary remedial actions. The foregoing surcharge shall be in additional to all other remedies and claims that Concergent may lawfully assert against Customer.

IP Allocation

Concergent owns each IP address that it assigns to a Customer. A Customer shall not use IP addresses that are not assigned to it or approved by Concergent. Concergent 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, Concergent 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. Concergent 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 Concergent Services or the Concergent IT Environment, including network, physical infrastructure or content stored or transmitted using Concergent Services or the Concergent IT Environment, 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"). Concergent may charge a User or any person seeking compliance with an Investigation for the reasonable costs and expenses associated with Concergent's compliance with any Investigation. **Concergent reserves the right to comply with any Investigation without providing prior notice to a User.** Customers shall not be entitled to a refund or any service credits, and Concergent shall not be in default under any agreement for Concergent Services, if its compliance with any Investigation causes a User to incur downtime or requires the sequestering of all or a portion of the Concergent IT Environment, including Customer's servers. Concergent also reserves the right to disclose information relating to Users and their use of Concergent Services, the Concergent IT Environment, 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 Concergent in its sole discretion.

Violations of AUP

Concergent 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, Concergent may:

- Disable access to a User's content that violates this AUP.
- Suspend or Terminate a User's access to Concergent Services, the Concergent IT Environment 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@concergent.com or via postal mail to:

Concergent, LLC
Attention: Abuse Department
245 North Waco
Suite T4
Wichita, Kansas 67202

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. Concergent 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, caused by violations.

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

Concergent 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, Concergent's network or its physical infrastructure.