EMERGYS MANAGED INFRASTRUCUTRE AND SERVICES AGREEMENT

ACCEPTABLE USAGE POLICY

This Acceptable Usage Policy ("AUP") is a part of an agreement for certain Emergys Managed Infrastructure and Services Agreement between Emergys and the Client. All capitalized terms not defined in this Policy shall have the same meaning as set forth in the Emergys Managed Infrastructure and Services, General Terms and Conditions (GTC).

1. RESTRICTIONS

Client agrees to use the Managed Infrastructure and Service in accordance with all applicable local, state and federal laws, and shall:

1.1 not conduct any business or activity or solicit the performance of any activity that is prohibited by law, tortuous, or interferes upon the use of Emergys's system by other clients;

1.2 not disseminate, display, send, store, transmit or receive any material that, to a reasonable person may be abusive, obscene, pornographic, defamatory, harassing, grossly offensive, vulgar, threatening, malicious, or violent, regardless of whether the material or its dissemination is unlawful;

1.3 not, directly or indirectly, use the Services and/or Network to engage in any conduct that is likely to result in retaliation against the Network or Emergys's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack,

1.4 not disseminate or transmit unsolicited messages, chain letters or unsolicited commercial email including unintended sending of unsolicited commercial email due to unauthorized access to Client's use of the Managed Infrastructure and Service, whether or not the recipient wishes to receive such mailings;

1.5 not access, send, receive, display, disclose, or store any content in violation of any copyright, right of publicity, patent, trademark, service mark, trade name, trade secret or other intellectual property right or in violation of any applicable agreement, or without authorization;

1.6 not create a false identity or to otherwise attempt to mislead any person as to the identity, source or origin of any communication;

1.7 not directly or indirectly use the Services and/or Network to transmit, distribute or store information or material that is fraudulent or contains false, deceptive, or misleading statements, claims, or representations (such as "phishing"), and/or violates generally accepted standards of Internet usage,

1.8 not export, re-export or permit downloading of any message or content in violation of any export or import law, regulation or restriction of the United States and its agencies or authorities, or without all required approvals, licenses and/or exemptions;

1.9 not interfere, disrupt or attempt to gain unauthorized access to any computer system, server, network or account for which Client does not have authorization to access or at a level exceeding Client's authorization;

1.10 not disseminate or transmit any virus, worms, trojan horse or other malicious, harmful or disabling data, work, code or program;

1.11 not engage in any other activity deemed by Emergys to be in conflict with the spirit or intent of the Agreement or any Emergys policy as examples listed in this Policy are not exhaustive.

1.12 not, directly or indirectly, use the Services and/or Network to monitor data or traffic on any network or system without the authorization of the owner of the system or network

1.13 not, directly or indirectly, use the Services and/or Network to access or use an Internet account or computer without the owner's authorization, including, but not limited to Internet scamming (tricking other people into releasing their passwords), password robbery, security hole scanning, and port scanning

1.14 not, directly or indirectly, use the Services and/or Network to forge any TCP/IP packet header or any part of the header information in an e-mail or a newsgroup posting

1.15 not, directly or indirectly, use the Services and/or Network to violate any charters, policies, rules or agreements promulgated by any search engines, blogs, subscription Web services, chat areas, bulletin boards, Web pages, USENET, or other services accessed via the Services or Network ("Usenet Rules"), including, without limitation, any cross postings to unrelated news groups, continued posting of off-topic messages, and disrupting newsgroups with materials, postings, or activities that are inappropriate (as determined by Emergys in its sole discretion), unless such materials or activities are expressly allowed or encouraged under the Usenet Rules,

1.16 not, directly or indirectly, use the Services and/or Network to provide "shell account" hosting, or the resale of "shell accounts" to third party entities that are not approved clients of Emergys, nor re-sell direct access to hosted server via telnet, ssh or other shell binary,

1.17 not, directly or indirectly, use the Services and/or Network to gain unauthorized access to or use of data, systems or networks, including attempting to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures (including those belonging to Emergys and its clients),

1.18 comply with the CAN-SPAM Act of 2003, as may be amended from time-to-time and all other laws and regulations applicable to bulk e-mail, and refrain from sending "Unsolicited Bulk Email" which shall also be referred to as SPAM interchangeably within this AUP. For purposes of this section, (a) "Unsolicited" means a message where the Recipient has not granted verifiable permission for the message to be sent, and (b) "Bulk" means that the message is sent as part of a larger collection of messages, all having substantively identical content. A message is considered SPAM, and therefore unacceptable, only if it is both Unsolicited and Bulk. Unsolicited Email may be normal email (examples: first contact enquiries, job enquiries, sales enquiries). Bulk Email can be normal email (examples: subscriber newsletters, client communications, discussion lists). An electronic message is SPAM if: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent. In order for the sending of bulk email to be acceptable, and therefore not considered SPAM, User must comply fully to the processes forth by SPAMHAUS (the "SPAMHAUS Processes") found on the following webpage: http://www.spamhaus.org/whitepapers/permissionpass.html.

Whether the Client is compliant with the SPAMHAUS Processes shall be determined by Emergys in its sole discretion. In addition, the Client and its Users must obtain Emergys's advance approval for any bulk e-mail before using the Service or Network to send such e-mail, which may be withheld for any reason whatsoever.

1.19 not, directly or indirectly, use the Managed Infrastructure and Services to violate the applicable acceptable use policies of other Internet Emergys ("ISPs") when data, content, or other communications are carried across

1.20 not, directly or indirectly, use the Services and/or Network to run any type of IRC software including, but not limited to, IRC client software, IRC server software, IRC bots such as "eggdrop" and "chaos," and/or IRC software that is embedded within a web interface

1.21 not, directly or indirectly, deny server log-in access to Emergys's staff, nor disable or demote the Administrator or Root accounts (sometimes called RedShield01 and RedShield02 accounts) from being Administrator or Root accounts, nor hide any prohibited files on the server(s), and

1.22 not, directly or indirectly, use the Services and/or Network to engage in any other conduct that Emergys believes, in its sole and reasonable discretion, to be illegal, abusive, or irresponsible behavior.

1.23 not use the Services to transmit, distribute or store material in violation of any applicable law, regulation, or judicial order, (b) in a manner that violates the terms of this AUP, the terms of any applicable agreement with Emergys, or any other policy applicable to such Users, (c) in a manner that interferes with or adversely affects the Services or use of the Services including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks, or (d) in a manner that may expose the Emergys to criminal or civil liability

2. FAILURE TO COMPLY

Failure to comply with this Policy in Emergys's reasonable judgment may result in the immediate termination of Managed Infrastructure and Service, responding to law enforcement requests, or any other action deemed necessary by Emergys in order to protect its network, client relationships, and commitment to the highest possible quality of service. Emergys will cooperate with law enforcement in cases where the Managed Infrastructure and Service are being used for any suspected illegal activity.

Except as otherwise expressly provided under the Agreement, the Client shall be solely responsible for the use of the Services and Network in violation of this AUP including, without limitation, (a) use by its users or clients and (b) any unauthorized use. Emergys may charge its hourly rate to correct any violation of this AUP or to repair any security breach (currently USD **$ 200** per hour billed in one-hour minimum increments), plus the cost of equipment and materials, if needed, to: (a) investigate, correct or otherwise respond to any violation or suspected violation of this AUP, (b) remedy any harm caused to Emergys or any of its clients by the use of service in violation of this AUP, (c) respond to complaints, and (d) have the Emergys's Internet Protocol numbers removed from any "blacklist" such as SPEWs or other abuse databases. Emergys retains the right to revise the hourly rate as mentioned in this Section for repair of any security breach, at its sole discretion. If Emergys's administrative accounts are disabled or demoted from Administrator or Root accounts, the Client shall, in addition to any other remedies available to Emergys, be charged the hourly Rate to correct this situation, and no support can be provided to the Client without these accounts being enabled. Emergys retains the right, at its sole discretion, to refuse new service to any individual, group, or business. Emergys also retains the right to discontinue service with notice for repeated violations of this AUP over time.

3. SUBSCRIPTION SOFTWARE PROVIDED BY EMERGYS

Emergys may provide software on a monthly basis (the "Subscription Software") from Microsoft, RedHat, or VMware, among others (the "Subscription Software Vendors"). By utilizing any Subscription Software provided by Emergys, the Client agrees to utilize such Subscription Software according to such Subscription Software Vendor's licensing terms and conditions. Should a Subscription Software Vendor change its Subscription Software products, business model, licensing terms, or costs to Emergys, the Client agree that (a) Emergys may modify the Subscription Software and (b) Emergys may revise the Subscription Software offerings and fees and costs with 30 days' notice to the Client.

4. REPORTING VIOLATIONS

Violations of this Policy are unethical and may be deemed criminal offenses. Client shall report to Emergys any information Client may have concerning instances in which this Policy has been or is being violated. Emergys may at any time initiate an investigation of any use of the Service for compliance with this Policy and Client agrees to cooperate. Emergys may without notice to the Client (a) report to the appropriate authorities any conduct by the Client that it believes violates applicable criminal law, and (b) provide any information it has about the Client in response to a formal or informal request from a law enforcement or government agency, or in response to a formal request in a civil action that on its face meets the requirements for such a request.

5. CONSEQUENCES OF VIOLATION OF AUP

Emergys may, without limiting its actions or remedies and its sole discretion, suspend the Service and/or remove any content transmitted via the Services and/or Network if it discovers facts that lead it to reasonably believe the Service is being used in violation of this AUP by the Client. Emergys reserves the right to recover any and all expenses, and apply any reasonable charges, in connection with a Client's violation of this AUP. The Client must cooperate with the Emergys's reasonable investigation of any suspected violation of the AUP. The Emergys 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, the Services.

6. SECURITY AND DISCLAIMER

The Client must protect the confidentiality of password(s), and should change the password(s) periodically. A compromised server is potentially disruptive to Emergys's network and other clients. Therefore, Emergys may take the server off line if it is accessed or manipulated by a third party without the Client's consent.

Emergys has no responsibility for any material or information created, stored, maintained, transmitted or accessible on or through the Services or Network and is not obligated to monitor or exercise any editorial control over such material. In the event that Emergys becomes aware that any such material may violate this AUP and/or expose it to civil or criminal liability, Emergys may block access to such material and suspend or terminate any Services without liability. Emergys further reserves the right to cooperate with legal authorities and third parties in investigating any alleged violations of this AUP, including disclosing the identity of any User that it believes is responsible for such violation. Emergys also reserves the right to implement technical mechanisms to prevent AUP violations. Nothing in this AUP shall limit in any way Emergys's rights and remedies at law or in equity that may otherwise be available. Emergys is under no duty, and does not by this AUP undertake a duty, to monitor or police our clients' activities and disclaims any responsibility for any misuse of the network. Emergys disclaims any obligation to any person who has not entered into an agreement with the Emergys for services

7. MALICIOUS ACTIVITY

7.1 Intended: Attempts to exploit other devices or Managed Infrastructure and Service on and off of Emergys's system without the permission or implied permission of that party are not permitted. Violations of system or network security may result in criminal and civil liability. Emergys will cooperate with law enforcement if a criminal violation is suspected. Emergys will limit any traffic from the offending device or network immediately.

7.2 Unintended: Emergys will notify Client of an exploited device being used for potential malicious activity. If the activity is causing severe damage or strain to other devices or networks, Emergys will limit traffic to and from that device immediately. Otherwise Emergys will notify the Client and give a reasonable amount of time to secure the device before limiting traffic to and from that device.

8. CHANGE TO THIS AUP

Emergys may revise this AUP at any time without notice. The Client's continued use of the Services and Network constitutes the Client's agreement to any such revised AUP. The Client may contact Emergys at any time to request the latest version of the AUP.