R.K. Black, Inc. Hosted Network Services Appropriate Use Policy

This Appropriate Use Policy ("AUP") specifies the guidelines for a Client's use of any services ordered from R.K. Black, Inc. (d/b/a R.K. Black, Inc. and referred to herein as "RK Black") and is binding on all Clients that enter into, or subject to, service agreements with RK Black. RK Black reserves the right to modify the AUP at any time, with such modification effective upon posting of the modified AUP to this web site. Clients are responsible for ensuring that their users, representatives, agents, or Clients comply with the provisions of this AUP. This AUP does not create an express or implied obligation of RK Black to any third party, including without limitation any obligation to monitor or review any data or content on RK Black's network or situated in any of its facilities. Any capitalized term not defined herein shall have the same meaning as defined RK Black's standard Master Service Agreement (as amended from time to time).

Please direct all questions regarding this AUP to info@rkblack.com.

Illegal Data and Content

Clients shall not store or transmit data or content that RK Black determines, in its sole discretion, to be in violation of any applicable law, regulation, or order of a court of competent jurisdiction. RK Black reserves the right to cooperate fully with any law enforcement authorities regarding any such data or content. Clients shall be responsible for determining what laws or regulations are applicable to their use of the Services.

Abusive Network Activities

Clients may not engage in, or allow, any activities that RK Black determines to be abusive network activities directed towards any third party or RK Black, which include, without limitation, the following:

- Forging of message headers or sender identity information
- Introduction or propagation of malicious programs (e.g., Trojan Horses, Internet viruses, worms, key loggers)
- Engaging in the unauthorized circumvention of the security or authentication procedures of any host, application, account, or network
- Executing any interference or denial of service to any host, application, user, account, or network
- Intercepting any Internet data not destined for Client's host server
- Disrupting network activity, such as by ping flooding, forged router information, port scanning, email-bombing, packet spoofing, IP address spoofing.

Client Security Responsibilities

Clients are solely responsible for any breaches of the security of any servers or networked hardware under its control or ownership, including safeguarding all authentication and account information. RK Black may immediately, and without prior notice or service credit, disconnect any Client server that it suspects to be involved in any illegal or abusive network activity and initiate an investigation to determine the cause of such activity. Clients are responsible for all costs and expenses incurred by RK

Black and any third party who was damaged by such illegal or abusive network activity. Clients must immediately notify RK Black of any illegal or abusive network activity by contacting RK Black at itservices@rkblack.com and info@rkblack.com.

Intellectual Property Infringement

Clients may not store or transmit any data or content that infringes on a third party's intellectual property rights. RK Black may remove or disable access to any allegedly infringing data or content in order to comply with any court order, regulation or law. RK BLACK MAY PERMANENTLY SUSPEND OR TERMINATE SERVICES TO ANY CLIENT THAT ENGAGES IN REPEATED VIOLATIONS OF THIS INTELLECTUAL PROPERTY INFRINGEMENT POLICY OR ANY APPLICABLE LAW.

Prohibited E-mailing Activities

Clients may not send, or allow to be sent, unsolicited emails ("Spam") over RK Black's network. Client may send e-mail only to parties who have expressly requested to receive such e-mail via a "double opt-in" confirmation process. Clients must maintain complete and updated records of all opt-in consents (including the e-mails and headers from each consenting party) and immediately provide such records and sufficient proof of all consents to RK Black upon request. The aforementioned policy applies to Client-operated listservs, mail lists, or mailing services that do not target an audience that has expressly consented to receiving such e-mail.

Clients may not engage in the following e-mailing practices:

- E-mail header spoofing or forgery
- Use of the Services to receive replies to Spam
- Host web pages that are advertised in Spam sent from another network
- Using third-party proxies in any way to cause the transmission of Spam
- RK Black reserves the right charge Client $300 per hour in consulting fees for any remedial actions that RK Black elects to take in the event that, as a result of Client's activities, RK Black's servers or IP space are placed in any third-party mail filtering software or black hole lists.

Cooperation with Investigations

RK Black may engage in any reasonable action, without prior notice to Client, relating to the Services in order to comply or cooperate with any civil or criminal investigation or cause of action regarding Client data located on RK Black's network or Client-owned equipment located in RK Black's facilities. RK Black shall not be deemed to be in breach of any service agreement, nor will it be obligated to grant any service level credits, for any disruptions to the Services.

AUP Enforcement

RK Black reserves the right at all times to take any necessary actions to enforce this AUP, including suspending, terminating, or limiting the scope of the Services to a Client, and shall not be obligated to issue any service level credits or other compensation for any resulting interruption in Services. Clients

are responsible for any expenses that RK Black incurs for enforcement and remedial measures in connection with AUP violations, including the payment to RK Black of emergency-rate consulting fees.