Acceptable Use Policy (AUP)

This Acceptable Use Policy ("**AUP**") is part of the Subscription and Services Agreement between Client and Camtiva (the "**Agreement**").

Client's services may be suspended or terminated for violation of this AUP, as further specified in the Agreement.

Capitalized terms used in this AUP have the meaning given in the Agreement.

1. Use of the Services

Client may not:

- Interfere or attempt to interfere in any manner with the functionality or proper working of the Services;
- Upload to the Camtiva Technology, or use the Services to store or transmit material in violation of third-party privacy rights;
- Upload to the Camtiva Technology, or use the Services to store, transmit, or distribute any malware. Malware means programming (code, scripts, active content, and other software) that is designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, or gain unauthorized access to system resources, or that otherwise exhibits abusive behavior. Malware includes computer viruses, worms, trojan horses, spyware, adware, scareware, crimeware, rootkits, or other malicious or unwanted software or programs;
- Interfere with or disrupt the integrity or performance of the Services or third-party data stored or processed with the Services or attempt to gain unauthorized access to the Services or their related systems or networks;
- Attempt to probe, scan, penetrate or test the vulnerability of a Camtiva system or network, or to circumvent, avoid or breach Camtiva's security or authentication measures, whether by passive or intrusive techniques, or by social engineering, without Camtiva's express prior written consent.

2. Shared Resources

Client may not use Camtiva systems, networks or technology in a way that unnecessarily interferes with their normal operation, or that consumes a disproportionate share of their resources. For example, Camtiva may require Client to repair coding abnormalities in your integration code if it unnecessarily conflicts with other Clients' use of Camtiva resources. Client agrees that Camtiva may quarantine or delete any data stored on Camtiva's systems or networks if the data is infected with any malware, or is otherwise corrupted, and has the potential to infect or corrupt Camtiva systems, networks or technology or other Clients' data that is stored or accessed via Camtiva systems, networks or technology. Client will comply with any written security or network access requirements that Camtiva provides to Client in connection with your use of the Services.

3. Other Networks

Client must comply with the rules of any other network it accesses or participates in when using the Services.

4. Abuse

Client may not use Camtiva'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 Camtiva network or other network through a Denial of Service attack;
- 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, phishing, Internet scamming, password theft, 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 Services to distribute software that covertly gathers information about a user or covertly transmits information about the user; or
- Any conduct that is likely to result in retaliation against the Camtiva network or website, or Camtiva's employees, officers or other agents, including engaging in behavior that results in any Camtiva Service or Service Provider being the target of a denial of service attack (DoS).

5. Offensive Content

Client may not publish, transmit or store on or via Camtiva's network, Services, or Service Providers any content or links to any content that Camtiva reasonably believes:

- Is obscene;
- Contains harassing content or hate speech, or is violent, incites violence, or threatens violence;
- Is unfair or deceptive under the consumer protection laws of any jurisdiction;
- 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, is contrary to applicable law, 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, or violates any privacy right;
- Is illegal or solicits conduct that is illegal under laws applicable to you or to Camtiva; or
- Is otherwise malicious, fraudulent, or may result in retaliation against Camtiva by offended viewers or recipients.

6. Other

Client will not be entitled to any credit or other compensation for any interruptions of service resulting from AUP violations