Acceptable Use Policy

This **ACCEPTABLE USE POLICY** ("AUP") describes acceptable use of and access to the Services offered by KOAMTAC, INC. (hereafter referred to as "KOAMTAC"). By accessing or using the services, you (hereafter referred to as "Customer") agree to the terms of this AUP. If you violate this AUP or authorize or assist others to do so, KOAMTAC may suspend or terminate your use of the Services in accordance with the terms of the KOAMTACON SERVICE PROVIDER AGREEMENT. Unless otherwise defined herein, all terms used within this AUP have the same meaning as ascribed to such terms in the KOAMTACON APPLICATION SERVICE PROVIDER AGREEMENT.

PROHIBITED USE AND CONTENT. Customer may not upload Customer Data, Project and/or Content or otherwise use the Services in a manner that KOAMTAC believes:

1. Undertakes or accomplishes any unlawful purpose. This includes, but is not limited to use and content that KOAMTAC believes violates any local, state, national, foreign, or international statute, regulation, rule, order, treaty, or other law (each of which are hereafter referred to as a "Law" or "Laws"), including, but not limited to, the Digital Millennium Copyright Act (DMCA), or those Laws concerning child pornography and illegal gambling, and/or use and content that KOAMTAC believes to be libelous, obscene, abusive, threatening, defamatory, or otherwise inappropriate;
2. Infringes or misappropriates any intellectual property or proprietary right of another, this includes, but is not limited to the uploading, posting, publishing, transmitting, reproduction, and/or creating of derivative works of, or the distribution of any information, software or other material obtained through the Service or as may otherwise be protected by copyright or other proprietary right, without obtaining any required permission of the owner;
3. Advocates or induces illegal activity;
4. Reverse engineers, disassembles, or decompiles the Services or software included in the Services, except as allowed by local law;
5. Stalks, harasses, or harms anyone, including minors;
6. Impersonates any person or entity or otherwise misrepresents Customer's affiliation with a person or entity;
7. Accesses or uses the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas;
8. Disrupts or otherwise interferes with or the Services or servers or networks connected to the Services;
9. Gains or attempts to gain unauthorized access to any portion of the Services or any System, whether through hacking, password mining, or any other means;
10. Uses any high volume automated means (including robots, spiders, scripts or similar data gathering or extraction methods) to access the Services or any other accounts, computer systems, or networks connected to the Services (each a "System");
11. Violates the security or integrity of a System, including, but not limited to: (i) Accessing or using any System without permission, including attempts to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System; (ii) Hacking, destabilizing, or adapting the Services, or altering another website

to falsely imply it is affiliated with the Services (iii) Monitoring data or traffic on a System without permission; and/or (iv) Uploading Customer Data, Project and/or Content that contains viruses, worms, corrupt files, Trojan horses, or other forms of corruptive code, or any other content that may compromise the Services.

12. Connects to any users, hosts, or networks where Customer does not have permission to communicate with such users, hosts, or networks, including, but not limited to: (i) Conducting denial of service attacks (ii) Monitoring or crawling a System so that such System is impaired or disrupted; (iii) Intentionally interfering with the proper functioning of any System, including any deliberate attempt to overload a system by any means; (iv) Using means (manual or electronic) to avoid any use limitations placed on a System, such as access and storage restrictions; or (v) Operating network services like open proxies, open mail relays, or open recursive domain name servers.
13. Distributes, publishes, sends, or facilitates unsolicited mass e-mailings, promotions, advertising, or solicitations, including commercial advertising and informational announcements, commonly known as “spam”;
14. Falsify, alter, or remove message headers; and/or
15. Impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar fraudulent activity (for example, “phishing”).

MONITORING AND ENFORCEMENT.

KOAMTAC has the sole discretion to determine whether Customer Data, Project and/or Content Customer's use of the Services is prohibited. All Customer Data, Project and/or Content that is provided to KOAMTAC or actions that are performed via Customer's KOAMTACON account, whether provided or performed by Customer's employees, Customer's contractors, or Customer's customers and/or end users, are the sole responsibility of Customer.

While not obligated to perform investigations, in accordance with the terms of the KOAMTACON APPLICATION SERVICE PROVIDER AGREEMENT, KOAMTAC may:

1. Investigate violations of this AUP or misuse of the Services;
2. Investigate and help prevent security threats, fraud, or other illegal, malicious, or inappropriate activity;
3. Remove, disable access to, or modify any Content or resource that KOAMTAC believes violates this AUP or any other agreement KOAMTAC has with Customer for use of the Services; or
4. Suspend or terminate provision of Services to customer for uses that violate this AUP or any other agreement KOAMTAC has with Customer for use of the Services.

KOAMTAC may report any activity that it suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. KOAMTAC reporting may include disclosing appropriate Customer information. KOAMTAC also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

MODIFICATIONS TO THE AUP. KOAMTAC may, in its sole and absolute discretion, modify this AUP from time to time. KOAMTAC will post notice of such changes in the Admin console of KOAMTACON software or as provided in the KOAMTACON APPLICATION SERVICE PROVIDER AGREEMENT. If Customer objects to any such changes, Customer's sole recourse shall be to cease using the Services. Continued use of the Services following notice of any such changes shall indicate Customer's acknowledgement of such changes and agreement to be bound by the terms and conditions of such changes.

REPORT VIOLATIONS/ CONTACT US. Customer can report abuse of this AUP and/or otherwise contact us at info@koamtac.com.