Acceptable Use Policy ("AUP")

General Statement: The purpose of this AUP is to inform all Customers of the acceptable uses of the Services VI is providing. VI is committed to encouraging the use of the Internet through its Services, but such use must be consistent with the laws and regulations governing use of the Internet and must protect the right of its other customers to use its Services. The AUP is designed to achieve these goals. Customer agrees to comply with this AUP and is responsible for the use of the Services by all entities and individuals whom Customer permits to use the Services. In addition to its rights under Section 17.1 of the Terms of Service, VI has the right to change or modify the terms of the AUP at any time, effective when posted at www.vis-intel.com. Customer's use of the Services after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

IP Addresses: The IP Address Policy (as described in the Terms of Services) which may be changed from time to time at VI's sole discretion, is incorporated into this MSA by reference. Customer acknowledges and agrees to adhere to the IP Address Policy. All IP Addresses assigned to Customer are owned and managed by VI. Such IP Addresses are non-transferable, and Customer retains no ownership or transfer rights to such IP Addresses. Attempted use by Customer of any unallocated IP Address is a violation of this AUP.

Prohibited Uses: The following list provides a number of general prohibited uses of the Services that are violations of this AUP. Please note that the following list does not represent a comprehensive or complete list of all prohibited uses.

1. Unlawful Activities. The Services shall not be used in violation of any criminal, civil or administrative violation of any applicable local, state, provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule. This includes, but is not limited to:

a) Child pornography
b) Unlawful gambling activities
c) Threats, harassment and abuse of any individual, organization or business
d) Fraudulent activities
e) Terrorist websites or other sites advocating human violence and hate crimes based upon religion, ethnicity or country of origin
f) Unlawful high yield investment plans, Ponzi schemes or linking to and or advertising such schemes

2. Child Pornography: In particular, the Services shall not be used to publish, submit, receive, upload, download, post, use, copy or otherwise produce, transmit, distribute or store child pornography.

3. Unsolicited Email: The use of the Services to send or receive mass unsolicited email ("SPAM"). This prohibition includes the direct sending and receiving of such messages, support of such messages via web page, splash page or other related sites, or the advertisement of such services. The falsifying of packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin or knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the Customer mails or sends.

4. Email Bombing: The sending, return, bouncing or forwarding of email to specified user(s) in an attempt to interfere with or overflow email services.

5. Proxy Email: The use of the Services as a proxy email server to forward email to unrelated Third Parties.

6. UseNet SPAM: The use of Services to send, receive, forward, or post UseNet unsolicited email or posts. This includes UseNet services located within the VI network or unrelated networks of Third Parties.

7. Hacking: The use of the Services for hacking, attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network.

8. Threatening Material or Content: The Services shall not be used to host, post, transmit, or retransmit any content or material that harasses, or threatens the health or safety of others. In addition, VI reserves the right to decline to provide Services if the content is determined by VI in its sole discretion to be obscene, indecent, hateful, malicious, racist, defamatory, fraudulent, libelous, treasonous, excessively violent or promoting the use of violence or otherwise harmful to others.

9. Violation of Intellectual Property Rights: The Services shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise reproduce, transmit, retransmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of VI or any other party, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

10. Distribution of Malware: The storage, distribution, fabrication, or use of malware, including without limitation, virus software, root kits, password crackers, adware, key stroke capture programs and other programs normally used in malicious activity is prohibited. The use of such programs in the normal ordinary course of business, however, may be requested by Customer and approved by VI on a case by case basis. For example, a security company using the Services to analyze the latest root kit for new security analysis/software.

11. Phishing: Any activity designed to collect personal information (name, account numbers, usernames, passwords, etc.) under false pretense. Splash pages, phishing forms, email distribution, proxy email or any activity related to phishing activities may result in the immediate suspension of Customer's account.

12. Server Abuse. Abuse or excessive use of VI's servers, network and infrastructure is prohibited.

13. Network Abuse. Any activity that involves making network connections to any third party without permission is prohibited. Such activity includes, but is not limited to: intentional network interference, port scanning, monitoring, crawling, denial of service, network penetration, sniffing, spoofing, virus deployment, hack attempts, vulnerability scanning, and avoidance of third party network security, restrictions or limitations.

14. Security Abuse. Any activity that involves violating the security or integrity of any third party network, system, application, device or other technology, account, password protection, or computer is prohibited. Such activity includes, but is not limited to: unauthorized access, internet scamming, password robbery, spidering, harvesting, collection of e-mail addresses or other identifiers, probing, scanning, vulnerability testing, interception, monitoring, network, packet header or e-mail origin falsification (excluding proper use of aliases), and covert user information gathering.

15. Vulnerability Testing. Customer may not perform any kind of vulnerability testing, penetration testing, or network scans, whether by passive or intrusive techniques in order to test the vulnerability of any VI system or VI's Network without VI's express written consent.

Customer Server Security. Customer is responsible for protecting its own server, data, password files, and password. If for any reason VI's network security has been breached because of Customer's failure to maintain such security, Customer will be responsible for the cost incurred by VI to restore the server and / or Network.

VI Network Security. Violation of VI's Network system such as, but not limited to probing, scanning, penetrating, testing, unauthorized access, or trying to breach VI's network security is prohibited.

Data Content and Protection. Customer acknowledges and agrees that VI's network and infrastructure may be exposed to hacker attacks, viruses or other adverse attacks outside of VI's control. VI is not responsible or liable for any loss or damage resulting from said viruses and attacks.

Resellers. Resellers and all of their clients are all bound by this AUP. Any policy or agreement made by a Reseller that contradicts or is not consistent with this AUP is not valid.

Indemnification Customer agrees to indemnify, defend and hold VI harmless against any claims, liabilities, losses, costs, damages, expenses, including attorneys' fees and court costs that arise from any violation of this AUP.

Governing Law. This Policy shall be governed by the laws of the Commonwealth of Pennsylvania, without regard to principles of conflicts of laws. Any litigation, arbitration or other dispute resolution will be filed or initiated in the courts and panels located in Delaware County, Pennsylvania.

Reporting Violations of the Acceptable Use Policy: VI accepts reports of alleged violations of this AUP via email sent to support@vis-intel.com. Reports of alleged violations must be verified and must include the name and contact information of the complaining party, and the IP address or website allegedly in violation, and a description of the alleged violation. Unless otherwise required by law, such as the DMCA, VI owes no duty to Third Parties reporting alleged violations. VI will review all verified Third Party reports and will take such actions as it deems appropriate in its sole discretion. VI will comply with and respond to valid (as VI determines in its sole discretion) subpoenas, warrants, and/or court orders. If permitted by applicable law or regulation, VI will forward such subpoenas, warrants, and/or orders to Customer and Customer may respond; however, VI reserves the right to respond to any such subpoena, warrant and/or order if it is the named party in such subpoena, warrant, and/or order.

Violations and VI's Rights. VI reserves the right, but does not assume the obligation, to investigate any violation of this Policy. VI will act as the sole arbiter as to what constitutes a violation of this Policy. At any time after a violation has occurred, and during the time that any violation is being investigated, VI reserves the right to suspend, restrict or terminate any Services at any time, including without limitation the "blackholing" or "suspension" of suspected IP addresses or hosts, without liability to Customer. No credit will be available under any VI service level agreement or other agreement for interruptions of services resulting from violations of this AUP.