ACCEPTABLE USE POLICY

It is prohibited for any user of Vysiion's Network and Services to participate in any of the activities listed below (whether actual or attempted and whether directly or indirectly):

- Other than for legitimate business reasons, posting or sending messages substantially similar in content to 10 or more Usenet or other newsgroups, forums, listservs, or other similar groups or lists (each, a "List");
- Other than for legitimate business reasons, posting or sending messages, articles, or other content to a List which are off-topic according to the charter or other owner-published FAQs or descriptions of the List;
- Sending unsolicited commercial messages or communications in any form ("SPAM");
- Falsifying user or other Service related information, including, but not limited to, intentionally omitting, deleting, forging or misrepresenting transmission information, including headers, return mailing and Internet protocol addresses, provided to Vysiion or to other service users or engaging in any activities or actions intended to withhold or cloak Customer's or a user's identity or contact information;
- Engaging in any other activity that:
  - threatens the integrity and/or security of any network or computer system (including, but not limited to, transmission of worms, viruses and other malicious codes and accessing any device or data without proper authorisation);
  - attempts to use the Service in such a manner so as to avoid incurring charges for or otherwise being required to pay for such usage;
  - violates generally-accepted standards of Internet or other networks conduct and usage, including, but not limited to, denial of service attacks, web page defacement, port and network scanning, and unauthorised system penetrations.
- Using Vysiion's services to guess passwords or access systems or networks without written authorisation;
- Engaging in any of the activities listed above by using another provider's service, but channelling the activity through a Service Provider account, remailer, or otherwise through a Service;
- Configuring customer systems to bypass security controls, including the installation of programs or services that allow the systems to be managed or accessed insecurely or through unauthorized means;
- Conducting online security audits or tests against or through Vysiion systems or networks without coordination with and the explicit, written consent of an authorized officer of Vysiion;
- Gaining, or attempting to gain, unauthorized access to Vysiion networking, security, management, backup, storage or monitoring systems;
- Installing programs or configuring systems to allow the monitoring, or "sniffing," of data traveling over a shared network;
- Accessing, or attempting to access, security-relevant information, such as password files that may, among other things, be used to gain unauthorized access to system accounts;
- Installing or using software for the purpose of cracking encrypted data, including stored passwords;
- Removing or disabling security software or services, including anti-virus software, logging utilities or authentication services;
- Transferring Remote-access accounts from one individual to another or sharing, or permitting the sharing of, the same. Individual remote-access accounts that uniquely and accurately identify the owner of the account shall be maintained as such by the Customer.