Minerva Squad Acceptable Use Policy (AUP) described below defines the actions which HC considers to be abused and strictly prohibited. There are no exclusions in this listing. Please, be aware that the actions listed below are also prohibited from other Internet Presence Providers (IPP's) and their users on behalf of HC to advertise any service hosted by HC or connected via the HC Network. As defined by the Federal Trade Commission Deception Policy Statement, such services are not to be advertised by way of deceptive marketing policies. For abbreviation purposes, Minerva Squad will be referred as HC and companies or individual account owners using our services as CUSTOMERS.

HC Acceptable Use Policy has been formulated with the following goals in mind:

- Ensure security, reliability and privacy of HC systems and network, and the networks and systems of others.
- Avoid situations that may cause HC to incur civil liability.
- Maintain the image and reputation of HC as a responsible organization.
- Preserve the value of Internet resources as a conduit for free expression.
- Encourage the responsible use of net resources, discouraging practices which degrade the usability of network resources and thus the value of Internet services.
- Preserve the privacy and security of individual users.

The Acceptable Use Policy below defines the actions which HC considers to be abusive, and thus, strictly prohibited. The examples named in this list are non-exclusive, and are provided solely for guidance to HC customers. If you are unsure whether any contemplated use or action is permitted, please send mail to abuse@hermescreadia.com and we will assist you. Please note that the actions listed below are also not permitted from other Internet Service Providers on behalf of, or to advertise, any service hosted by HC, or connected via the HC network. Furthermore, such services may not be advertised via deceptive marketing policies, as defined by the Federal Trade Commission Deception Policy Statement.

Acceptable Use Policy ("AUP")

1. General Information. As a provider of websites, web stores, website hosting, and other Internet-related services, MINERVA SQUAD (“the Company”) offers its customers, the means to acquire and disseminate a wealth of public, private, commercial, and non-commercial information. The Company respects that the Internet provides a forum for free and open discussion and dissemination of information, however, when there are competing interests at issue, the Company reserves the right to take certain preventative or corrective actions. In order to protect these competing interests, the Company has developed this Acceptable Use Policy (“AUP”), which supplements and explains certain terms of each customer's respective service agreement and is intended as a guide to the customer's rights and obligations when utilizing the Company’s services. This AUP will be revised from time to time. A customer's use of the Company's services after changes to the AUP are posted on the Company's web site, http://www.hermescreadia.com, will constitute the customer's acceptance of any new or additional terms of the AUP that result from those changes. One important aspect of the Internet is that no one party owns or controls it. This fact accounts for much of the Internet's openness and value, but it also places a high premium on the judgment and responsibility of those who use the Internet, both in the information they acquire and in the information they disseminate to others. When subscribers obtain information through the Internet, they must keep in mind that the Company cannot monitor, verify, warrant, or vouch for the accuracy and quality of the information that users may acquire. For this reason, the user must exercise his or her best judgment in relying on information obtained from the Internet, and also should be aware that some material posted to the Internet is sexually explicit or otherwise offensive. Because the Company cannot monitor or censor the Internet, and will not attempt to do so, the Company cannot accept any responsibility for injury to its users, customers or subscribers that results from inaccurate, unsuitable, offensive, or illegal Internet

communications. When users, customers or disseminate information through the Internet, they also must keep in mind that the Company does not review, edit, censor, or take responsibility for any information its users, customers or subscribers may create. When users place information on the Internet, they have the same liability as other authors for copyright infringement, defamation, and other harmful speech. Also, because the information they create is carried over the Company's network and may reach a large number of people, including both customers and subscribers and non-subscribers of the Company, customers' and subscribers' postings to the Internet may affect other customers and subscribers and may harm the Company's goodwill, business reputation, and operations. For these reasons, customers and subscribers violate the Company policy and the service agreement when they, their customers, affiliates, or subsidiaries engage in activities described herein.

2. Scope. This AUP governs the usage of the Company's products and services (the "Services"). This AUP is incorporated by reference into each contract the Company enters into with a customer (each, a "Customer") for the use of such Services. The Company may modify this AUP at any time without notice. In addition, this AUP is incorporated by reference into the Terms of Service applicable to the Company's Web site so that no person who utilizes the Company's Web site (regardless of whether that person is a Customer) may take any action utilizing the Company's Web site that a Customer would be prohibited to take utilizing the Services.

3. Purpose. The purpose of this AUP is to enhance the quality of the Services and to protect the Company's customers, and the Internet community as a whole, from illegal, irresponsible, or disruptive Internet activities. This AUP applies to each Customer and its employees, agents, contractors or other users of such Customer who obtain Services from the Company (each such person being a "User"). Each User should use common sense and good judgment in connection with the Services. Parents or guardians should always supervise minors in using the Internet. Parents and guardians should remain aware at all times of what is on the Internet and how the minors under their care are using the Services and the Internet.

4. Prohibited Uses. Customers and Users may not:

   a. Utilize the Services to send unsolicited bulk and/or commercial messages over the Internet (known as "spam" or "spamming"). It is not only harmful because of its negative impact on consumer attitudes toward the Company, but also because it can overload the Company's network and disrupt service to its Customers subscribers. Maintaining an open SMTP relay is prohibited. Any direct action, configuration, or setting that causes excessive outbound email traffic is subject to review and possible action. When a complaint is received, the Company has the absolute and sole discretion to determine from all of the evidence whether the email recipients were from an "opt-in" email list, or whether the outbound email traffic generated from an account is suitable for a shared hosting environment.

   b. Utilize the Services in connection with any illegal activity. Without limiting the general application of this rule, Customers and Users may not:

      i. Utilize the Services to copy material from third parties (including text, graphics, music, videos or other copyrightable material) without proper authorization;

      ii. Utilize the Services to misappropriate or infringe the patents, copyrights, trademarks or other intellectual property rights of any third party;

      iii. Utilize the Services to traffic in illegal drugs, illegal gambling, obscene materials or other any products or services that are prohibited under applicable law;

      iv. Utilize the Services to export encryption software to points outside the United States in violation of applicable export control laws;

v. Utilize the Services to Forge or misrepresent message headers, whether in whole or in part, to mask the originator of the message; or

vi. Utilize the Services in any manner that violates applicable law.

c. Utilize the Services in connection with any tortious or actionable activity. Without limiting the general application of this rule, Customers and Users may not:

i. Utilize the Services to publish or disseminate information that (A) constitutes slander, libel or defamation, (B) publicizes the personal information or likeness of a person without that person's consent or (C) otherwise violates the privacy rights of any person. Utilize the Services to threaten persons with bodily harm, to make harassing or abusive statements or messages, or to solicit the performance of acts or services that are illegal under applicable law.

ii. Utilize the Services in connection with any other disruptive or abusive activity. Without limiting the general application of this rule, Customers and Users may not:

a. Utilize the Services to cause denial of service attacks against the Company or other network hosts or Internet users or to otherwise degrade or impair the operation of the Company's servers and facilities or the servers and facilities of other network hosts or Internet users; or

b. Post messages or software programs that consume excessive CPU time, or storage space, or network bandwidth; or

c. Utilize the Services to offer mail services, mail forwarding capabilities, POP accounts or auto responders other than for the User's own account; or

d. Utilize the Services to resell access to CGI scripts installed on the Company's servers; or

e. Utilize the Services to subvert, or assist others in subverting, the security or integrity of any the Company systems, facilities or equipment; or

f. Utilize the Services to gain unauthorized access to the computer networks of the Company or any other person; or

g. Utilize the Services to provide passwords or access codes to persons not authorized to receive such materials by the operator of the system requiring the password or access code; or

h. Utilize the Services to (A) forge the signature or other identifying mark or code of any other person, (B) impersonate or assume the identity or any other person, or (C) engage in any other activity (including "spoofing") to attempt to deceive or mislead other persons regarding the true identity of the User (excluding the use of anonymous re-mailers or Internet nicknames); or

i. Utilize the Services to distribute or post any virus, worm, Trojan horse, or computer code intended to disrupt services, destroy data, destroy or damage equipment, or disrupt the operation of the Services; or

j. Utilize the Services to conduct port scans or other invasive procedures against any server (except any server for which the User is an authorized system administrator); or

k. Utilize the Services to distribute, advertise or promote software or services that have the primary purpose of encouraging or facilitating unsolicited commercial e-mail or Spam; or

l. Utilize the Services to solicit or collect, or distribute, advertise or promote, e-mail address lists for the purpose of

encouraging or facilitating unsolicited commercial e-mail or Spam; or

m. Utilize the Services in any manner that might subject the Company to unfavorable regulatory action, subject the Company to any liability for any reason, or adversely affect the Company's public image, reputation or goodwill, including, without limitation, sending or distributing sexually explicit, hateful, vulgar, racially, ethnically or otherwise objectionable materials as determined by the Company in its sole discretion; or

n. While on a shared hosting platform, utilize, operate, enable, execute, compile, upload or publicly store source code, executable code, programs, or software packages designed to perform tasks not directly associated with website/email hosting, including, without limitation, (A) directly opening any listening port, (B) starting any 'daemon' process, (C) performing local/remote security scans, (D) simulating local shell/OS access by means of a tunneled/encapsulated connection to a remote host, (E) circumventing firewall restrictions, (F) connecting to any IRC/Peer to Peer file sharing server/network, (G) providing 'tracker' services to 'BitTorrent' clients and/or (H) exploiting web browser vulnerabilities, as determined by the Company in its sole discretion; or

o. Attempt to attack, disrupt, or abuse the support- and contact-related mechanisms of the Company, including, but not limited to, telephone lines, email addresses, fax lines, bulletin boards or contact/signup forms; or

p. Utilize the Services in any other manner to interrupt or interfere with the Internet usage of other persons;

5. Violations

a. Disclaimer. The Company expressly disclaims any obligation to monitor its Customers and other Users with respect to violations of this AUP. The Company has no liability or responsibility for the actions of any of its Customers or other Users or any content any User may post on any Web site.

b. Remedies. If the Company learns of a violation of this AUP, the Company will respond to the applicable Customer and may, in the Company's sole discretion, take any of the following actions, in accordance with the severity and duration of the violation:

i. Warning the Customer; and/or

ii. Suspending the offending Customer from the Services; and/or

iii. Terminating the offending Customer from the Services; and/or

iv. Imposing fees or charges on the offending Customer account in accordance with the applicable service contract; and/or

v. Removing the offending content; and/or

vi. Taking other action in accordance with this AUP, the applicable service contract or applicable law.

6. Reservation of Rights. The Company reserves the right to cooperate with appropriate legal authorities in investigations of claims of illegal activity involving the Company's Services, Customers and other Users. The Company reserves all other rights to respond to violations of this AUP to the extent of applicable law and in accordance with any applicable contractual obligations. The Company may utilize technical means to monitor communications into, and out of, its network facilities to prevent the introduction of viruses or other hostile code, to prevent intrusions and otherwise to enforce this AUP and each Customer agrees that the Company is authorized to monitor its communications through the Company's network for such purposes.