# Acceptable Use Policy (AUP)

Vaultas | Vaultas, LLC | Vaultas Alexandria, LLC

**Attachment to Vaultas Master Services Agreement**

Vaultas, Vaultas, LLC, and Vaultas Alexandria, LLC ("Vaultas") Acceptable Use Policy addresses some of the specific requirements that apply to Customer's use of the Internet and Services. Vaultas has no obligation to control, monitor, verify, warrant, approve, edit, censor, review, or take any responsibility for the information that Customers may acquire, transmit or store through the Internet. Accordingly, Vaultas is not responsible for injury that results from inaccurate, unsuitable, offensive or illegal Internet communications. Customers are responsible for compliance with all laws and regulations, as well as the applicable policies of Vaultas Internet and network providers. If, however, Vaultas becomes aware of any violation of law or this Acceptable Use Policy by or through a Customer, Vaultas shall have the right, but not the obligation, without liability to Customer, to take any action to remedy such violation. Such actions may include, without limitation, removal of the information at issue, blocking of offending transmissions, suspension or termination of a Customer's Services with Vaultas, and any other remedy available to Vaultas by contract or law.

1. **Illegal or Improper Use**
   The customer agrees to use the Vaultas' s network for lawful purposes only. Customer shall not use the Vaultas' s Network in connection with any (i) infringement or misappropriation of any copyright, trademark, trade secret or other intellectual property rights; or (ii) defamation, libel, slander, obscenity, or violation of the rights of privacy or publicity; or any other offensive, harassing or illegal conduct.

2. **System and Network Security**
   Vaultas strictly prohibits the use of the Vaultas' s network to violate the security of any system or network, including, without limitation, unauthorized access (often known as "hacking") to, monitoring of, probing, or interference with, computers or networks and distribution of viruses, or interfering with services, such as through denial of service attacks, and other destructive activities. Customer may not through action or inaction permit others to use its network for illegal or inappropriate actions, or to violate the terms of this AUP.

3. **Abuse Email Tactics/Spamming**
   Customers may not engage in abusive email tactics or send unsolicited bulk email, a process commonly known as spamming, which shall include, but not be limited to, the following types of conduct:

   a. Transmitting data in any manner that violates a State or Federal law, rule or regulation against spamming or other prohibited communications, regardless of how such law defines spamming or other such prohibited activity.

   b. Posting a single article or substantially similar articles to an excessive number of newsgroups, or continued posting of articles that are off-topic (e.g., off-topic according to the newsgroup charter, or the article provokes complaints from the regular readers of the newsgroup for being off-topic).

c. Sending unsolicited email messages that provoke complaints from the recipients, which threaten harm to person or property, or which result in harassment of the recipient.

d. Sending unsolicited email messages including, without limitation, commercial advertising, informational announcements, chain letters, or other solicitations.

e. Use of resources not belonging to the customer, without the express permission of the resource owner, to relay email or other internet traffic.

f. Falsifying or forging email or newsgroup header information.

To report a spamming complaint to: TechSupport@vaultas.com

**4. Cooperation with Authorities and Vaultas**

Vaultas will cooperate with law enforcement and other authorities in investigating claims of illegal activity or suspected illegal activity. In addition, Customer shall cooperate with Vaultas in any corrective action that Vaultas deems necessary to correct and prevent impermissible use of Vaultas' s network by any of Customer's end users, including without limitation, providing Vaultas with all information necessary to investigate the suspected violation. In addition, Vaultas may disclose information transmitted over its facilities where necessary to protect Vaultas and its customers from harm, or where such disclosure is necessary to the proper operation of Vaultas' s network.

Vaultas reserves the right to modify this policy at any time, as it deems appropriate in its sole discretion, effective upon posting of the modified Policy at this URL: http://www.vaultas.com/policies