Acceptable Use Policy

This Acceptable Use Policy (this "**Policy**") describes prohibited uses of the software and related services offered by Zadara Storage Inc. and its subsidiaries and affiliates (the **"Software"** and **"Services**" respectively) and the website located at http://www.zadara.com (the "**Zadara Site**"). The examples described in this Policy are not exhaustive. This Policy applies to yourself and any other entities you or your affiliates enable to utilize the Software (collectively "You"). We may modify this Policy at any time and without notice by posting a revised version on the Zadara Site. By using the Software or accessing the Zadara Site, you agree to the latest version of this Policy. If you violate the Policy or authorize or help others to do so, we may suspend or terminate part or all of your use of the Software and the Services.

1. **No Illegal, Harmful, or Offensive Use or Content**

    You may not use, or encourage, promote, facilitate or instruct others to use, the Software or Zadara Site for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive. Examples of prohibited activities or content include:

    Illegal Activities. Any illegal activities, including advertising, transmitting, or otherwise making available gambling sites or services or disseminating, promoting or facilitating child pornography.

    Harmful or Fraudulent Activities. Activities that may be harmful to others, our operations or reputation, including offering or disseminating fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming), or engaging in other unfair and/or deceptive practices.

    Infringing Content. Content that infringes or misappropriates the intellectual property or proprietary rights of others.

    Offensive Content. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.

    Harmful Content. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.

2. **No Security Violations**

    You may not use the Software to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "**System**"). Prohibited activities include:

Unauthorized Access. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.

Interception. Monitoring of data or traffic on a System without permission.

Falsification of Origin. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

3. **No Network Abuse**

You may not make network connections to any users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include:

Monitoring or Crawling. Unauthorized Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.

Denial of Service (DoS). Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.

Intentional Interference. Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.

Operation of Certain Network Services. Operating network services like open proxies, open mail relays, or open recursive domain name servers.

Avoiding System Restrictions. Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

4. **No E-Mail/Message Abuse**

You will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mailing or other messages, promotions, advertising, or solicitations (e.g., "spam mail"), including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission. You will not collect replies to messages sent from another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

5. **Our Monitoring and Enforcement**

We reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the Software or the Services or Zadara Site. We may, in our sole discretion:

(a) Investigate violations of this Policy or misuse of the Software, the Services or Zadara Site; or

(b) Remove, disable access to, or modify any content or resource that violates this Policy or any other agreement we have with you for use of the Services or the Zadara Site; or

(c) Report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We 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 Policy.

6.   **Reporting of Violations of this Policy**

If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this Policy, please contact us via E-Mail at: support@zadara.com.