Onsharp Hosting Acceptable Use Policy ("AUP")

General Statement: The purpose of this AUP is to inform you ("Customer") of the acceptable uses of Onsharp's Website Essentials and dedicated hosting services ("Services"). These Services must be used consistent with the laws and regulations governing use of the Internet and must protect the right of all Customers to use these Services. The AUP is designed to achieve these goals.

Customer agrees to comply with the AUP and is responsible for the use of the Services by all entities and individuals whom Customer permits to use the Services. Onsharp has the right to change or modify the terms of the AUP at any time. Customer's use of the Services after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

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 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 Onsharp network or unrelated networks of other 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, Onsharp reserves the right to decline to provide Services if the content is determined by Onsharp 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 Onsharp 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 Onsharp on a case by case basis. Example: 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. **Violation of Agreements:** Any activity which violates any third-party agreements.

13. **Denial of Service:** Any activity to implement or assist in the implementation of denial of service attack. Onsharp absolutely prohibits the use of Services for the origination, propagation or control of denial of service attacks ("DoS") or distributed denial of service attacks ("DDoS"). Customers may not utilize the Services to perform DoS or DDoS mitigation activities (such as service proxying or data scrubbing) which may result in attracting inbound denial of service attacks toward the Services. Any relation to DoS or DDoS type activity is a direct violation of this AUP.

Reporting Violation of the Acceptable Use Policy: Onsharp accepts reports of alleged violations of this AUP via email sent to support@onsharp.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, Onsharp owes no duty to third parties reporting alleged violations. Onsharp will review all verified third party reports and will take such actions as it deems appropriate in its sole discretion.

Onsharp will comply with and respond to valid (as Onsharp determines in its sole discretion) subpoenas, warrants, and/or court orders. If permitted by applicable law or regulation, Onsharp will forward such

subpoenas, warrants, and/or orders to Customer and Customer may respond; however, Onsharp 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.

Disclaimer: Onsharp retains the right, at its sole discretion, to refuse new service to any individual, group, or business. Onsharp also retains the right to discontinue service to Customers with excessive and/or multiple repeated violations.