onShore Networks
Acceptable Use Policy

onShore ISP Acceptable Use Policy ("AUP") is provided to give our employees, clients and vendors a clear understanding of what onShore expects of them while using the service. All users of onShore's network and/or internet services, including those who access any of our Services but do not have accounts, must comply with this AUP.

Use of onShore's network and internet service constitutes acceptance and agreement to onShore's AUP.

onShore strives to provide its employees and clients with the highest quality network service available and at the same time respect the business needs of our company and all clients, including sensitive data storage needs. To that end, onShore believes that certain activities and conduct that is inappropriate or abusive will not be tolerated on the onShore network.

onShore supports the uncensored flow of information and ideas over the Internet. Similarly, we do not exercise editorial control over the content of any web site, e-mail transmission, newsgroups, or other material created or accessible over or through the services. onShore employees are authorized to use our network and devices to access the internet exclusively or primarily for their jobs. However, in accordance with this AUP, we may remove any materials that, in our sole discretion, may be considered or thought to be illegal, may subject us to liability, or which may violate this AUP. onShore will cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrongdoing. Your violation of this AUP may result in the suspension of your access, and/or termination of employment or contractor relationship, without prior notice.

Personal Responsibility:

In order to prevent violations of onShore's Acceptable Use Policy, all users must abide by the following requirements.

Any systems that connect to or access data located in onShore Networks' Business network when teleworking, including personally owned devices, must be connected via encrypted connections (for example, VPN or SSL tunneling protocol). All devices that connect to the onShore Networks network, either internal or via encrypted connections, must be protected from intrusion by the use of password or PIN login at start up, as well as requiring a lock screen or password to be entered after a period of inactivity. Users must treat any data stored on or distributed through the device according to it's level of business sensitivity or confidentiality.

Violations of onShore's Acceptable Use Policy

Illegal use: Use of onShore's service to transmit any material (by e-mail, uploading, posting or otherwise) that, intentionally or unintentionally, violates any applicable local, state, national, or international law, or any rules or regulations promulgated thereunder. Examples of such activities includes but is not limited to distributing material that infringes on any copyright, trademark, patent, trade secret or other proprietary rights of any third party; the unauthorized copying of copyrighted material, the digitization and distribution of photographs from magazines, books, or other copyrighted sources; and the unauthorized transmittal of copyrighted software.

Threats and acts of Terrorism: Use of onShore's service to transmit any material (by e-mail, uploading, posting or otherwise) that threatens or encourages bodily harm, encourages destruction of property or promotes senseless hatred toward other groups of people in society is not permitted. This also includes communications or transmissions of any sort to others intended for the purpose of planning unspeakable acts against society. If onShore becomes aware of any such activity it will be reported to the proper authorities without any notice to the user, and disciplinary actions will be taken.

Harassment: Use of onShore's services to transmit any material (by e-mail, uploading, posting or otherwise) that harasses another user or member of society is not permitted.

Harm to minors: Use of onShore's services to harm, or attempt to harm, minors in any way, including, but not limited to child pornography or sexual solicitation is not permitted and may result in criminal charges.

Forgery or impersonation: Adding, removing or modifying identifying network header information in any manner in an effort to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information for non-business intent is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation.

Network Services: to impede another person's use of network services (defined as, but not limited to,: E-mail, web browsing, domain name resolution) for non-business intent will result in the immediate termination of the offending account.

Mail/Message Forging: Forging any message header, in part or whole, of any electronic transmission, originating or passing through onShore's service is in violation of this AUP, unless done for business reasons.

Unsolicited commercial e-mail/Unsolicited bulk e-mail (SPAM): Use of onShore's services to transmit any unsolicited commercial or unsolicited bulk e-mail for non-business intent is expressly prohibited. Violations of this type will result in the immediate suspension and possible termination of the offending account. OPT-IN only lists, such as Listservs, are not exempt from this policy. Such E-mail lists must present the user with a verification of their subscription prior to sending e-mail to the recipient. This verification process must also be able to provide proof of the recipient's approval to prevent account termination.

Unauthorized access: Use of onShore's service to access, or to attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of onShore or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data, is prohibited in all non-business cases, and the offending account is subject to immediate termination.

Network disruptions and unfriendly activity: Use of onShore's service for any activity which affects the ability of other people or systems to use onShore's services or the Internet. This includes, but is not limited to, "denial of service" (DOS) and "distributed denial of service" (DDOS) attacks against another network host or individual user. Interference with or disruption of other network users, services or equipment is prohibited. It is the user's responsibility to ensure that their network is configured in a secure manner. A user may not, through action or inaction, allow others to use their network for illegal or inappropriate actions. A user may not permit their network, through action or inaction, to be configured in such a way that gives a third party the capability to use their network in an illegal or inappropriate manner. Unauthorized entry and/or use of another company and/or individual's computer system will result in immediate account termination and possible disciplinary action.

Distribution of Viruses or Hostile software: Intentional distributions of software that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems are prohibited. Such an offense will result in the immediate termination of the offending account, as well as possible disciplinary action.

Network Performance: onShore accounts operate on shared resources. Excessive use or abuse of these shared network resources by one user may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited by this policy and may result in disciplinary action.

Reporting Violations of onShore's AUP

onShore requests that anyone who believes that there is a violation of this AUP direct the information to the Abuse Department at abuse@onshore.net.

If available, please provide the following information:

- The IP address used to commit the alleged violation
- The date and time of the alleged violation, including the time zone or offset from GMT
- Evidence of the alleged violation

Failure to provide sufficient information, as deemed by onShore, will result in a dismissal of the complaint. onShore regards reports of abuse with the utmost seriousness and requires legitimate information as to avoid falsely accusing users. False accusations will result in reports filed against the reporting party to the appropriate contacts.

E-mail with full header information provides all of the above, as do system log files. Other situations will require different methods of providing the above information.

onShore, at it's sole discretion, may take any one or more of the following actions in response to complaints:

- Issue written or verbal warnings, up to and including employment or contract termination.
- Suspend the user's account
- Bring legal action to enjoin violations and/or to collect damages, if any, caused by violations

Revisions to this Acceptable Use Policy

onShore reserves the right to revise, amend, or modify this AUP, and our other policies and agreements at any time and in any manner.