Nfina Technologies, Inc. Acceptable Use Policy

General Statement

This Acceptable Use Policy (the "Policy" or "AUP") is an integral part of your [Terms of Service Agreement] (policy/terms-of-service/) ("TOS") with NFINA Technologies, Inc., its affiliates and wholly owned subsidiaries ("NFINA") for the provision of services (collectively the "Services") set forth in the TOS agreement. This policy is designed to help protect NFINA's customers from irresponsible and/or illegal activities. 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. NFINA reserves the sole and absolute right to interpret, apply, define and implement this Policy. The Policy is a *non-exclusive* list of the actions prohibited by NFINA and NFINA reserves the right to modify the Policy at any time, effective upon notice to you. Customer's use of the Services after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

IP Addresses

The IP Address Policy (as described in the TOS) which may be changed from time to time at NFINA's sole discretion is incorporated into this AUP by reference. Customer acknowledges and agrees to adhere to the IP Address Policy. All IP Addresses assigned to Customer are owned and managed by NFINA. Such IP Addresses are non-transferable, and Customer retains no ownership or transfer rights to such IP Addresses. All IP Addresses are assigned by NFINA on a per VLAN, per server basis. Attempted use by Customer of any unallocated IP Address or any IP Addresses on VLANs not assigned to Customer is a violation of this AUP.

GENERAL DESCRIPTION OF UNNACEPTABLE CONDUCT

If your use of the Services causes harm to the Services or cause harm to others or if you encourage or assist any third party, or if you yourself do any of the following, you will be in violation of this AUP:
-    engage in activity that harms or disrupts the operation or performance of the Services;
-    misrepresent your identity, impersonate any person or attempt to gain access to or illegally track any account, user, data, device, system, or network related to the Services;
-    use or manipulate the Services in any manner not permitted by us;
-    use the Services in a manner that results in excessive bandwidth usage, as determined by us;
-    use the Services for any illegal purpose, or to publish, post, share, copy, store, backup or distribute any illegal files or data, including infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material that is harmful to children or that violates third party privacy rights;
-    use the Services to publish, post, share, copy, store, backup or distribute material protected by intellectual property rights of a third party unless you own or have necessary rights to such material;
-    use the Services to publish, post, share, copy, store, backup or distribute material that contains viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or any other similar software that may damage the operation of the Services or another person's device or property;
-    engage in online activities that would encourage other parties to cause damage to the Services;
-    directly or indirectly reverse engineer, decompile, disassemble, modify, reproduce or create derivative works of the Services;
-    alter or modify any disabling mechanism, which may be included in Services, including tampering with the security of the Services or tamper with other customer accounts of NFINA;
-    assign, sublicense, rent, timeshare, loan, lease or otherwise transfer the Services;
-    remove or alter any proprietary notices (e.g., copyright, trademark notices, legends, etc.) from the Services or copy any ideas, features, functions, or graphics of the Services;

-       build or assist someone else to build a competitive solution using similar ideas, features, functions, or graphics of the Service, or allow any person or entity that offers or provides services that are competitive to or with NFINA's products and/or services to use or access the Services, or encourage any Customer to patronize a service that competes with the Services;

-       use the Services to send unsolicited advertising and/or promotional materials, including, without limitation, 'spam' or bulk e-mail; or

-       attempt to probe, scan or test the vulnerability of the Services or to breach the security or authentication measures without proper authorization.

Unlawful Activities

The Services shall not be used in violation of any criminal, civil or administrative law, rule or regulation of any local, state, provincial, federal, national governmental entity which has or may have jurisdiction over NFINA, the Services or the Customer or in violation of any international law, treaty, court order, ordinance, regulation or administrative rule. This includes, but is not limited to:

1.   Unlawful gambling activities;
2.   Threats, harassment and abuse of any individual, organization or business;
3.   Fraudulent activities;
4.   Terrorist websites or other sites advocating human violence and hate crimes based upon religion, ethnicity or country of origin; or
5.   High Yield Investment Plans or Ponzi schemes with the intent to defraud end users are illegal and not allowed on the network. This includes hosting, linking and/or advertising via email websites or schemes designed to defraud.

Export Regulations

You represent and warrant that you are not on the United States Department of Treasury, Office of Foreign Asset Controls list of Specially Designated National and Blocked Persons and are not otherwise a person to whom NFINA is legally prohibited to provide the Services. You may not use the Services for the development, design, manufacture, production, stockpiling, or use of nuclear, chemical or biological weapons, weapons of mass destruction, or missiles in a country listed in Country Groups D: 4 and D: 3, as set forth in Supplement No. 1 to the Part 740 of the United States Export Administration Regulations, or as otherwise prohibited by law, nor may you provide access to the Services to any person (including any natural person or government or private entity) that is located in or is a national of any country that is embargoed or highly restricted under United States export regulations.

Offensive Content

You may not use any NFINA Service to distribute content or links to content that NFINA reasonably believes:

- Constitutes, depicts, fosters, promotes or relates in any manner to adult content, including, without limitation, child pornography, bestiality, or non-consensual sex acts;
- Is excessively violent, incites violence, threatens violence or contains harassing content or hate speech;
- Is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
- Is defamatory or violates a person's privacy;
- Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security or interferes with an investigation by law enforcement;

- Improperly exposes trade secrets or other confidential or proprietary information of another person;
- Is intended to assist others in defeating technical copyright protections;
- Promotes illegal drugs, violates export control laws, relates to illegal gambling or illegal arms trafficking;
- Is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to NFINA;
- Is otherwise malicious or fraudulent, or may result in retaliation against NFINA by offended recipients; or
- Is intended to be obscene, indecent, racist, libelous, harassing or threatening.

Child Pornography

NFINA has a zero-tolerance policy on child pornography and related sites. 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. The hosting of child pornography or related sites or contact information is in direct violation of federal law and NFINA's AUP.

Denial of Service

You may not use the Services for purposes of any activity to implement or assist in the implementation of any denial of service attack. NFINA 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 use of the Services related to any DoS or DDoS type activity is a direct and material violation of NFINA's AUP.

Server Abuse

Any activity that undermines or causes harm to a NFINA server or subscriber of NFINA is strictly prohibited, including, but not limited to:
- Excessive usage of bandwidth, site visits, disk, memory, or processor of the current standard NFINA Cloud plans, either in repeated bursts or sustained overages;
- Logging into a server or account that you are not authorized to access;
- Accessing data or taking any action to obtain services or information not intended for you or your use without the consent of the owner;
- Tampering, hacking, modifying, or otherwise corrupting or breaching security or authentication measures without proper authorization;
- Transmitting material that contains viruses, Trojan horses, worms, time bombs, cancelbots or other computer programming routines or engines with the intent or effect of damaging, destroying, disrupting or otherwise impairing a computer's functionality or the operation of the NFINA's systems;
- Monitoring data or traffic on any network or system without the express authorization of the owner of the system or network;
- Interfering with, intercepting or expropriating any system, data or information which you do not have the right to access; and
- Interfering with service to any user, host or network including, without limitation, by means of overloading, "flooding," "mail bombing," or "crashing" any computer system.

You agree that we may quarantine or delete any data stored on the NFINA network if the data is infected with a virus, or is otherwise corrupted, and has the potential to infect or corrupt the network or other customers' data that is stored on the network.

IRC

We do not allow IRC, Egg Drops, BNC, or IRC bots to be operated on our servers or network. Files with references to IRC or any likeness thereof are prohibited. Also, any program that acts like an IRC server or that provide chat functions that run as background processes are not allowed.

Proxies

We do not allow proxy servers of any kind, whether for personal or business use. Files with references to any proxy or likeness thereof are prohibited.

Redirect Sites, Ad Networks and Ad Servers

We do not allow ad servers or sites that participate in redirecting between multiple websites for serving ads or link directories on the multi-tenant servers in the NFINA Cloud. If you need this type of application, you must use a NFINA Cloud Private Server.

Game Servers

We do not allow game servers (dedicated game server programs) of any kind.

Fraudulent Activities

NFINA prohibits utilizing dedicated services or network services for fraudulent activities. Participation in fraudulent activities is in direct violation of state and federal law and NFINA's AUP.

Violation of Intellectual Property Rights

Violation of Intellectual Property Rights: The Services and/or Third Party 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 NFINA 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.

Distribution of Malware

NFINA prohibits the storage, distribution, fabrication, or use of malware including virus software, root kits, password crackers, adware, keystroke capture programs and other programs normally used in malicious activity. The use of such programs in the normal ordinary course of business, however, may be requested by Customer and approved by NFINA on a case by case basis. Example: Security company using the Services to analyze the latest root kit for new security analysis/software.

Phishing

NFINA strictly prohibits any activity associated with phishing or systems designed to collect personal information (name, account numbers, user names, passwords, etc.) under false pretense. Splash pages,

phishing forms, email distribution, proxy email or any relation to phishing activities will result in immediate removal or suspension of Customer's account.

Vulnerability Monitoring and Testing

You may not attempt to probe, scan, penetrate or test the vulnerability of a NFINA system, subsystem or network or to attempt to breach security or authentication measures, whether by passive or intrusive techniques, without NFINA's express written consent.

IP Address Usage

You may only use IP addresses assigned to you by NFINA in connection with your NFINA Services. You agree that if the NFINA IP addresses assigned to your account are listed on an abuse database, you will be in violation of this AUP, and NFINA may take reasonable action to protect its IP addresses, including suspension and/or termination of your Service, regardless of whether the IP addresses were listed as a result of your actions.

Bulk Mail

You may not use any NFINA Service to send Bulk Mail. "Bulk Mail" means email messages of similar content that are sent to more than two hundred and fifty (250) recipients. Attempts to circumvent this restriction by breaking up bulk email over time, using multiple accounts, or other means will be a violation of this restriction. A mail message sent to other users within your domain names hosted on the NFINA system is not considered Bulk Mail.

Unsolicited Mail

You may not send unsolicited email by means or use of the Services. Email is unsolicited if you have no pre-existing relationship with the recipient, unless the recipient has published or otherwise provided his or her email address in a manner which implies consent to receive the email. You may not send email of any kind to a person who has indicated that they do not wish to receive it. 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 is prohibited. Any such email shall comply with all laws and regulations, including without limitation, the CAN SPAM Act.

Message Source

You may not obscure the source of your email in any manner, including by intentionally omitting, forging, or misrepresenting messages headers or return addresses.

Email Abuse Complaints

Complaints from email recipients and third-party abuse agencies (e.g. SpamHaus or Spamcop) shall be deemed proof of the facts stated therein unless you provide compelling evidence to the contrary. NFINA shall have the right to terminate your mail service if we receive excessive or repeated complaints from your email recipients, regardless of whether you are in breach of this AUP or are otherwise at fault.

Blacklisting/Retaliation

NFINA may terminate your Services if your email address or related IP number(s) is/are blacklisted by any third-party, or NFINA is retaliated against as a result of your use of the mail system, regardless of whether you are in breach of this AUP or are otherwise at fault.

UseNet SPAM

The use of dedicated services to send, receive, forward, or post UseNet unsolicited email or posts is a direct violation of NFINA's AUP. This includes UseNet services located within the NFINA network or unrelated third party networks.

Contact Information Filed with Domain Name Registrar

You must have valid and current information on file with your domain name registrar for any domain hosted on the NFINA network. You agree that if you register a DNS record or zone on NFINA managed or operated DNS servers or services for a domain of which you are not the registrant or administrative contact according to the registrar's WHOIS system, that, upon request from the registrant or administrative contact according to the registrar's WHOIS system, NFINA may modify, transfer, or delete such records or zones.

NFINA Administrative Access

You, the customer, acknowledge that in order to facilitate efficient server management, inventory and related activities, the NFINA servers may include a NFINA administrative account and password and/or a NFINA daemon. All reasonable precautions are made by NFINA to maintain the security of these tools and the privacy of client data. You will not tamper, hinder, delete or in any way change the functioning of these tools.

Resellers

If you resell, rent or otherwise allow third parties to use any NFINA Services, you are responsible for use of the Services by such third parties in violation of this AUP to the same extent as if you were using NFINA Services yourself. You are also responsible for all accounting and support for your end customers.

Disclosure to Law Enforcement

Occasionally, NFINA is required by law to submit customer information to law enforcement officials when presented with a valid subpoena or order from a court or governmental entity. Information requested is disclosed as directed pursuant to the subpoena or order. NFINA utilizes great care in keeping customer information safe and private and will only release information described in the subpoena order. NFINA will notify customer of the information request to the extent permitted by the subpoena or order.

Reporting Violation of the Acceptable Use Policy

NFINA accepts reports of alleged violations of this AUP via email sent to support@Nfina.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, NFINA owes no duty to third parties reporting alleged violations. NFINA will review all verified third party reports and will take such actions as it deems appropriate in its sole discretion. NFINA will comply with and respond to valid (as NFINA determines in its sole discretion) subpoenas, warrants, and/or court orders. If permitted by applicable law or regulation,

NFINA will forward such subpoenas, warrants, and/or orders to Customer and Customer may respond; however, NFINA 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.

Methods of Resolution Process for Violations of NFINA's Acceptable Use Policy

The goal of our Methods of Resolution is to mitigate service interruptions while resolving potential violations under this AUP. Our support staff is dedicated to working with the Customer in resolving potential violations, and they are available via phone, ticket, or email. The Methods of Resolution below is provided for informational purposes only and forms the framework and guidance with respect to resolving potential violations, but in the event of any conflicts between the Acceptable Use Policy (in particular its enforcement) and Terms of Services, the Terms of Services shall control. Timing for resolution differs according to the degree of the violation, the nature of the violation, involvement of law enforcement, involvement of third party litigation, or other related factors.

Step 1: First alleged violation of AUP
A ticket will be generated under NFINA to provide the Customer's master user with information regarding the potential violation of NFINA's AUP. This is often a fact-finding email requiring further information or notifying Customer of the potential violation and the required actions to resolve the issue.

Step 2: Acknowledgement of violation of AUP
A ticket is generated under the Customer's master user account with information specific to the violation. This ticket will also include any additional facts about the situation and will notify Customer of the action required to resolve the violation.

Step 3: Violation of AUP disregarded, not properly addressed, or continuing violation if a ticket has been disregarded, not properly addressed, or resolved by the Customer for a specified period of time
NFINA engineers will turn the public network port to the specified dedicated services off. Access to the dedicated services may then be achieved through the secure private service network for Customer resolution. As soon as the violation is addressed, the public access shall be restored and service will continue as normal.

Step 4: Failure to address violation and resolve violation
If Customer fails to address the violation AND fails to resolve the violation, a suspension of services shall occur. This is a last resort for NFINA and only results when the Customer completely fails to participate in NFINA's resolution process. A permanent suspension of services includes reclamation of all dedicated services and the destruction of Customer's data.

Disclaimer: NFINA retains the right, at its sole discretion, to refuse new service to any individual, group, or business. NFINA also retains the right to discontinue service to customers with excessive and/or multiple repeated violations. No credit will be available for interruptions of service resulting from AUP violations.