ACCEPTABLE USE POLICY
FOR
QUAIL VALLEY TELECOM, LLC, D/B/A FROG ("FROG")
FIBER INTERNET ACCESS SERVICES - RESIDENTIAL

FROG'S ACCEPTABLE USE POLICY AND HOW IT APPLIES TO USERS

Frog's goal is to operate a secure and reliable fiber-based data network that provides users with a best-in-class high-speed Internet experience. That is why Frog has created this Acceptable Use Policy ("AUP") – to ensure the proper use and integrity of its state-of-the-art network so that all of Frog's customers and service users (collectively, "Users") consistently enjoy the speeds, features and benefits it offers.

To that end, Frog takes this AUP very seriously and reserves the right to restrict, suspend or terminate a User's access to the services and/or account with Frog, without notice, if User uses the services in violation of this AUP or the other customer agreements and terms and conditions to which User is bound (T+Cs), as well as to take any appropriate legal or other action to enforce them (such as takedown of content without notice). Frog reserves the right, in its sole and absolute discretion, to refuse to transmit or post, and to remove or block, any information or materials, in whole or in part, that Frog deems to be in violation this AUP or that otherwise may be harmful to Frog's network or other Users using the Service, regardless of whether such materials or their dissemination is unlawful.

Neither Frog nor any of its affiliates, suppliers or agents have any obligation to monitor transmissions or postings (including e-mail, file transfer, blog, newsgroup, and instant message transmissions, or materials available on the Personal Web Pages and Online Storage features) made available through Frog's services; provided that Frog may monitor these transmissions and postings from time to time for violations of this AUP and disclose, block, or remove them in accordance with this AUP, the T+Cs and/or applicable law.

In no event shall Frog have any liability whatsoever to Users for damages incurred by Users or any third party in connection with Frog's enforcement of this AUP.

By using Frog's services, Users are required to observe and comply with this AUP and the T+Cs. If a User does not wish to be bound by the AUP and/or T+Cs, then User may not use the services and/or immediately must cease using the services and notify Frog of such discontinuance, as commencement or continued use of the services shall be deemed to constitute User's agreement to be bound by the AUP and T+Cs. While User's computers and other devices that are connected to the Internet may be accessed or used by other people, software or devices without User's knowledge or participation, User remains responsible for all such unauthorized access and uses. User is solely responsible to secure User's connected devices to prevent such unauthorized access and uses.

Frog may amend this AUP and/or T+Cs at any time and from time to time. It is User's responsibility to periodically check this AUP and T+Cs to ensure that User is fully informed of the current AUP and T+Cs and is in continued compliance with such policies.

PERMITTED USE OF FROG'S RESIDENTIAL INTERNET SERVICE

Frog's residential Internet access services are provided to User for User's reasonable, personal, non-commercial use only. Frog's services cannot be used for any business or enterprise purpose whatsoever, regardless of whether the business is intended to or actually does generate revenues or make a profit. It if it is User's intention to use any of Frog's services for such a business purpose, please contact Frog regarding a commercial grade service that meets User's needs.

PROHIBITED USES OF FROG'S RESIDENTIAL INTERNET SERVICE

The following is a non-exhaustive list of certain prohibited uses of Frog's services. Users may not use Frog's services:

Regarding Violations of Law
~In violation of any law, rule or regulation.

Regarding Resale and Expanded Use
~For resale or to permit the use of Frog's services, in whole or in part, directly or indirectly, by other persons or entities, regardless of whether for a fee or profit, and regardless of the method (e.g., through Wi-Fi or other methods of networking).

~To use or run programs or dedicated, stand-alone equipment or servers from a User's premises that provide network content or any other services to anyone outside of such premises local area network ("Premises LAN"), also commonly referred to as public services or servers. Examples of prohibited equipment and servers include e-mail, Web hosting, file sharing, and proxy services and servers.

Regarding Network Management
~In any manner that interferes with Frog's ability to effectively manage its network. Frog may use various tools and techniques to protect the security and integrity of its network, which may include tools to detect and quarantine malicious traffic, prevent the distribution or promulgation of viruses and other malicious code, monitor traffic for usage patterns, etc.

~To restrict, inhibit, interfere with, or otherwise disrupt or cause a performance degradation, regardless of intent, purpose or knowledge, to Frog's service or any host, server, backbone network, node or service, or otherwise cause a performance degradation to any facilities used to deliver the services.
~In any manner that interferes with Frog's ability to provide services to other Users, including any actions that result in excessive consumption or utilization of network resources or bandwidth or that may weaken network performance, reliability or security.

~With anything other than a dynamic Internet Protocol ("IP") address that adheres to the dynamic host configuration protocol ("DHCP"). User may not configure services or any related equipment to access or use a static IP address or use any protocol other than DHCP unless User is subject to a Frog service plan that expressly permits User to do so. In addition, User is not permitted to alter, modify, forge or tamper with such IP address, customer ID or any TCP/IP packet header or header information in an email or newsgroup posting.

~To connect Frog-provided equipment or services to any computer or other device outside of User's premises.

Regarding Third Parties and Third Party Networks and Sites
~To restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy Frog's services (except for tools for safety and security functions such as parental controls, for example), including posting or transmitting any information or software that contains a worm, virus, or other harmful feature, or generating levels of traffic sufficient to impede others' ability to use, send, or retrieve information.

~To access or attempt to access any other person's or entity's computer, device, software, data, network or system without their knowledge or consent.

~To breach or attempt to breach the security or protective measures employed by any computer, device, software, network or account of any person or entity, This includes, but is not limited to, accessing data not intended for User, logging into or making use of a server or account that User is not expressly authorized to access, or probing the security of other hosts, networks, or accounts without express permission to do so, including (1) to circumvent or attempt to circumvent the user authentication features or security of any host, network or account; or (2) using or distributing tools designed or used for

determining or compromising security, such as password guessing, decoders, password gathers, keystroke loggers, analyzers, packet sniffers, encryption circumvention devices, Trojan Horse programs and cracking tools. Unauthorized port scanning is strictly prohibited.

~To impersonate any person or entity, engage in sender address falsification, forge any other person or entity's digital or manual signature, or perform any other similar fraudulent activity (such as phishing).

~In violation of the rules, regulations, terms of service, or policies applicable to any network, server, computer database, service, application, system, or Website that User accesses or uses.

~To interfere with computer networking or telecommunications service to any User, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to "crash" a host.

Regarding Content and Transmissions

~To access, upload, post, store, display, transmit or distribute information, data, information, content or material that (1) is illegal, threatening, harassing, hateful, libelous, defamatory or otherwise injurious to any other person or entity; (2) is obscene, pornographic or contains graphic visual depictions of sexual acts or sexually explicit conduct involving children or minors or otherwise may harm a minor; (3) violates, misappropriates, misuses or infringes the intellectual property or proprietary rights of any other person or entity; (4) violates the privacy or dignity of any other person or entity; (5) contains software viruses or other malicious computer code; or (6) that constitutes or encourages conduct that would constitute a criminal offense, or otherwise violate any local, state, federal, or non-U.S. law, order, or regulation.

~To upload, post, publish, transmit, reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the service or otherwise that is protected by copyright or other intellectual property or proprietary right, without obtaining any required permission of the owner.

~To distribute programs that make unauthorized changes to software (cracks).

~To transmit, collect or harvest (1) responses from bulk, commercial or unsolicited messages (spam); (2) non-publicly available personal information about any person without their knowledge or consent; or (3) email addresses, screen names or other identifiers of any person or entity without their prior consent, or deploying or using software or spyware designed to facilitate such activities.

~To send an unreasonable amount of (1) the same or substantially similar message; (2) empty messages or messages that contain no substantive content; or (3) messages or files that disrupt a server, account, blog, newsgroup, chat or other similar service ("mail bombing").

~To engage in deceptive trade practices or consumer fraud, such as illegal gambling, "make money fast" schemes, chain letters, pyramid or other investment schemes, or to make or encourage other persons to accept fraudulent offers for services or products.