GLACIER BROADBAND LLC ACCEPTABLE USE POLICY

Effective October 2022

By subscribing to any residential or commercial broadband Internet Service(collectively, the “Services” and individually, a “Service”) provided by Glacier Broadband LLC (“Glacier Broadband”), Customer agrees not to use the Services for any unlawful purpose and to comply with all policies and terms of this Acceptable Use Policy (the “AUP” or “Policy”). This Policy, including its use restrictions, is in addition to the restrictions contained in Glacier Broadband’s Master Services Agreement (“Service Agreement”), which Customer previously entered into with Glacier Broadband. This Policy has been incorporated by reference into the Service Agreement.

Please read this Policy carefully prior to accessing the Services. The term “Customer” refers to the subscriber and any user of the Service. By using the Services, Customer agrees to the terms of this Policy and will require others using the Service through Customer’s account to abide by the terms of this Policy. Glacier Broadband regularly updates and amends this Policy (and may do so without notice at Glacier Broadband’s discretion) and Customer should periodically consult Glacier Broadband’s website to be sure Customer remains in compliance with this Policy. Customer’s continued use of the Service constitutes Customer’s continuing acceptance of and agreement to this Policy and any posted amendments to this Policy.

Glacier Broadband reserves the right to reclassify any Service to a higher grade or to immediately suspend or terminate any Service without prior notice for Customer’s failure to comply with any portion of this Policy or Service Agreement. (Please see the Service Agreement for details on the suspension and termination policy.) In the event of such termination, Customer will be responsible for the full month’s charges to the end of the current term, including, without limitation, unbilled charges, plus a termination fee, if applicable, all of which will become immediately due and payable upon termination of Customer’s Services. Any violation of this Policy and Service Agreement may also lead to prosecution under state and/or federal law. Glacier Broadband will also provide information in response to law enforcement requests, subpoenas, court orders, to protect its rights and property, and in the case where failure to disclose the information may lead to imminent harm to a Customer or others.

Glacier Broadband will access or collect the following customer data (Name, email address, location, user’s phone, contact book data, user’s inventory of installed apps, and user’s screen recording.) Data will not be sold to a third party. Data will be used to help improve the customer service experience. This policy also applies to any Glacier Broadband Mobile Application.

For copyright infringement claims, Customer understands, acknowledges and agrees that Glacier Broadband may remove any content at any time that is alleged to infringe on a third party’s copyrights upon receiving a notice of

infringement under the Digital Millennium Copyright Act ("DMCA"), and to terminate the Customer's Service without prior notice if there is repeat infringement. Please see the Glacier Broadband DMCA Copyright Infringement Notification Process below for details.

1. **PERMITTED USE**. Customer's permitted use of the Services will depend on whether Customer requests the Services for residential or commercial purposes.
    1. "**Residential Service**" includes all Services designated for personal and family use within a single home. The term "single home" means Customer's home and includes any apartment, condominium, flat or other residential unit that may be used as a residence in any multiple dwelling unit. Customer agrees that only Customer and co-residents living in the same home will use the Services. The Services are being provided solely for residential use in Customer's home and any unauthorized access by a third party to e-mail, Internet access, or any other function of the Services is in violation of this Policy and the Service Agreement. Customer is solely responsible for any misuse of the Service that occurs through Customer's account, whether by a member of Customer's household, guests or an authorized or unauthorized third party. Customer shall not use, or allow others to use, the Service to operate any type of business or commercial enterprise, including, but not limited to, IP address translation or similar facilities intended to provide additional access. Customer shall not advertise that the Service is available for use by third parties or unauthorized users. Customer shall not resell or redistribute, or allow others to resell or redistribute, access to the Service in any manner, including, but not limited to, wireless technology.
    2. "**Commercial Service**" includes all Services designed for use by a business entity, or by an individual, in providing goods or services for sale or lease. Customer agrees that Customer will allow only Customer's employees and patrons to utilize the Commercial Service within Customer's office area. Commercial Service is provided solely for Customer's business operations, and any unauthorized access by a third party to e-mail, Internet access, or any other function of the Service is in violation of this Policy and the Service Agreement. Customer is solely responsible for any misuse of the Service that occurs through Customer's account, whether by a member of Customer's employees, patrons, invitees, guests, or an authorized or unauthorized third party.
2. **GENERALLY PROHIBITED ACTIVITIES FOR ALL SERVICES**.
    1. **Misuse of Services** – Customer is responsible for any misuse of the Services, regardless of whether the inappropriate activity was committed by an invitee, licensee, agent, servant, guest, patron,

employee or any other person who gains access to the Services. Therefore, Customer is responsible to take steps to ensure that others do not gain unauthorized access to the Services, for instance by strictly maintaining the confidentiality of Customer's passwords or by appropriately protecting the use of Customer's computer, network or any wireless devices. Customer is solely responsible for the security of any device Customer choose to connect to the Services, including any data stored on that device.

2. **Objectionable Use and Content** – (i) any use that is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy or other rights, or otherwise objectionable in Glacier Broadband's sole discretion; (ii) any use in connection with surveys, contests, pyramid schemes, chain letters, junk email, spamming, or any duplicative or unsolicited messages not in compliance with the federal CAN-SPAM Act or the Telephone Consumer Protection Act (commercial or otherwise); (iii) publishing, distributing, or disseminating any inappropriate, profane, defamatory, infringing, obscene, indecent, or unlawful material or information; (iv) advertising, soliciting, selling or buying, or attempting to buy and sell any goods for any non-personal purpose under residential Services; (v) harvesting or otherwise collecting information about others, including email addresses or telephone numbers, without their consent; (vi) creating a false identity for the purpose of misleading others as to the identity of the sender or the origin of a message or call; (vii) transmitting or uploading any material that contains viruses, Trojan horses, worms, time bombs, cancel bots, or any other harmful or deleterious programs or software or other material protected by intellectual property laws, rights of privacy or publicity or any other applicable law unless Customer owns or controls the rights thereto or have received all necessary consents; (viii) interfering with or disrupting networks connected to the Services or violate the regulations, policies or procedures of such networks; and (ix) attempting to gain unauthorized access to the Service, other accounts, computer systems, devices, or networks connected to the Service, through password mining or any other means; host any type of publicly accessible file sharing, gaming, or email server including, but not limited to HTTP, FTP, SMTP, POP3, and Peer-to-Peer; interfere with another member's use and enjoyment of the Service or another individual or entity's use and enjoyment of similar Services.

3. **PROHIBITED INTERNET SERVICE ACTIVITIES**. Customer shall use the Internet Service and related Equipment only for lawful purposes. Internet service activities specifically prohibited by Glacier Broadband include but are not limited to the following:

1. **Background and/or server-type applications** – Including but not limited to IRC bots, HTTP servers, MUDs, and any other process which were initiated by the Customer that continues execution on the system upon Customer logout. FCC authorized smart home systems and IoT devices are excluded from this prohibition.
2. **Attempts to compromise system and/or network security** – Programs such as packet sniffers, password crack programs, and similar utilities found to be running from Customer's account are prohibited. This also includes attempts to hack into non-Glacier Broadband systems, networks, servers, websites or applications via the Glacier Broadband Network.
3. **Sharing of accounts** – Sharing Customer's Internet Service with another party for purposes of avoiding payment for a second Service is strictly prohibited. Customer may connect multiple computers/devices within a single location to Customer's modem, router, and/or radio to access the Internet Service, but only through a single Glacier Broadband-issued IP address.
4. **Conducting commercial business through a personal residential account** – The residential single-Customer Internet accounts provided by Glacier Broadband are designed for the home/casual Customer and may not provide the level of service, capacity or speed required for conducting commercial activity. Therefore, running a business with a residential account is not advisable. Please contact Glacier Broadband's sales department to upgrade to a commercial account.
5. **Email abuse** – Email abuse typically comes in one of three forms, the sending or transfer of a message to unsolicited individuals not in compliance with the Federal CAN-SPAM Act, the sending of harassing and/or threatening messages to other users, and the forging of email addresses so as to make the email appear to be from another user.

6. **Pyramid/money-making schemes** – Such activities as the transfer of information or solicitation of persons via the Internet in an attempt to extort money or other valuables or the use of pyramid/chain letters are all prohibited.