HANKINS INFORMATION TECHNOLOGY
ACCEPTABLE USE POLICY

All Customers must comply with the policies and terms of this Acceptable Use Policy (the "AUP" or "Policy"). This Policy, including its use and behavior restrictions, is in addition to the restrictions contained in the HIT Master Services Agreement ("MSA") and has been incorporated by reference into the MSA. Any capitalized terms used herein shall have the same meaning as defined in the MSA.

Customer understands, acknowledges and agrees that HIT reserves the right to immediately suspend or terminate any Service without prior notice for Customer's failure to comply with any portion of this Policy or the MSA. (Please see the MSA for details on the suspension and termination policy.) Any violation of this Policy and Service Agreement may also lead to prosecution under local, state and/or federal law.

(a) "Acceptable use" is hereby defined as the normal activities associated with the Customer's use of HIT's Services, including without limitation, usage of the HIT Network and any other facilities for accessing the World Wide Web, Internet Relay Chat, USENET Newsgroups, Email, and other Internet-related features. Customer's acceptable use of the Services will depend on whether Customer's Services are designated as residential or commercial.

(i) Residential designation includes all Services designated primarily for personal, family and household use within a single home. Customer shall not use, or allow others to use the Services to operate any type of business or commercial enterprise as a primary purpose or for long-term.

(ii) Commercial designation includes all Services designed for use by a business, governmental, or institutional entity, or by an individual to provide goods or services for sale or lease or operating a commercial enterprise.

(iii) 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.

(b) "<u>General Prohibited Activities for All Services</u>" include without limitation the following, whether any such use or behavior is conducted negligently, recklessly, knowingly, or intentionally:

(i) Misusing the Services, regardless of whether the inappropriate or unlawful use or activity was committed by an invitee, licensee, agent, servant, guest, patron, visitor, 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.

(ii) Using Services to distribute or receive content that is illegal, threatening, abusive, harassing, defamatory, libelous, tortious, malicious, indecent, obscene, deceptive, fraudulent, invasive of another's privacy or other rights, or otherwise objectionable in HIT's sole discretion.

(iii) Using Services in connection with commercial surveys, pyramid schemes, chain letters, junk email, spamming, or any duplicative or unsolicited messages (commercial or otherwise) not in compliance with the federal CAN-SPAM Act or the Telephone Consumer Protection Act ("TCPA") and applicable state laws.

(iv) Advertising, soliciting, selling or buying, or attempting to buy and sell any goods for any non-personal or non-household purposes if using residential Services.

(v) Harvesting or otherwise collecting information about others, including email addresses, telephone numbers, or other Personal Information without consent.

(vi) Creating a false identity for the purpose of, others as to the identity of the sender or the origin of a message or call, website or mobile application ("App").

(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 authorizations.

(viii) Interfering with or disrupting networks connected to the Services or violate the regulations, policies or procedures of such networks.

(ix) Attempting to gain unauthorized access to the Services, other accounts, computer systems, devices, or networks connected to the Services, through password mining or any other means.

(x) Hosting any type of harmful publicly accessible file sharing, gaming, or email server including, but not limited to HTTP, FTP, SMTP, POP3, and Peer-to-Peer that could interfere with the technical operations of the HIT Network, or could interfere with another Customer or user's use and enjoyment of the Services.

(xi) Using the Services or take any action, directly or indirectly, that will result in excessive consumption or utilization of the Services or HIT Network resources, or which may weaken network performance, as determined in HIT's sole discretion, such as (a) using the Service to host a web server site which attracts excessive traffic at Customer's location; (b) continuously uploading or downloading streaming video or audio, USENET hosting, or continuous FTP

uploading or downloading; (c) and continued use of programs or commands which take a large amount of system resources, be that processor time, memory, network bandwidth, and/or drive space on the host system. These activities can hamper the delivery of or disrupt the technical performance of the Services to all Customers.

(c) "Prohibited Internet Service Activities" specifically include without limitation the following, whether any such use or behavior is conducted negligently, recklessly, knowingly, or intentionally:

(i) Using background and/or server-type applications, including without limitation IRC bots, HTTP servers, MUDs, and any other harmful 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.

(ii) Storing files on the HIT Network that are not used regularly for extended periods of time, including without limitation, Customer Material. FCC authorized smart home systems and IoT devices are excluded from this prohibition. Customer should use cloud-based storage programs such as One Drive or iCloud to store any Customer Material.

(iii) Flooding or abusing other Customers or users, including without limitation, ICMP flooding, mail bombing (sending large amounts of email repeatedly to a person for purposes of harassment), phishing, mass mailings to multiple addresses via bulk email not in compliance with the federal CAN-SPAM Act and Telephone Consumer Protection Act, MSG/CTCP flooding on IRC, as well as other, less common methods. "Bulk Email" is defined as the same or similar email messages sent to more than twenty-five (25) recipients.

(iv) Using programs such as packet sniffers, password crack programs, or similar utilities or applications to access HIT Network or systems.

(v) Sharing Services with another person to avoid payment of a second or upgraded Service. 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 HIT -issued IP address.

(vi) Using flood pinging, broadcast pinging, multicast, or IGMP use outside of the private network.

(vii) Using any application, software, or technique to scan any host's ports.

(viii) Abusing email, including without limitation, sending unsolicited messages not in compliance with the CAN-SPAM Act or TCPA, sending harassing and/or threatening messages, and forging of email addresses to make the email appear to be from another person.

(ix) Abusing USENET services or social network platforms, including without limitation, forging of addresses, harassment/threats, posting of the same message to multiple newsgroups (spamming), as well as the posting of information in newsgroups or platforms where it is not relevant and unwanted.

(x) Using or promoting pyramid/money-making schemes, including without limitation, the transfer of information or solicitation of persons to extort money or other valuables.

(xi) Using pirated software to avoid the purchase of any software such as Adobe Photoshop, Microsoft Office, etc. and exporting software or technical information in violation of U.S. export control laws.

(xii) Copying, streaming, broadcasting, posting or any distribution of copyrighted material or software without the authorization of the copyright owner, including without limitation, the digitization and distribution of photographs or other content from magazines, books, or other copyrighted sources.

(d) "Prohibited VoIP Activities" include without limitation the following:

(i) Creating a false Caller ID identity ("ID Spoofing") or false email/SMS address or header, or otherwise attempting to mislead others as to the identity of the sender or the origin of any communication made using the Services.

(ii) Auto-dialing or "predictive" dialing (i.e., non-manual dialing or using a software program or other means to continuously dial or place out-bound calls).

(iii) Sending pre-recorded or artificial voice calls (also known as "Robocalls") for any reason without the prior express consent of the recipient.

(iv) Trunking or forwarding Customer's HIT VoIP number to another phone number(s) capable of handling multiple simultaneous calls, or to a private branch exchange (PBX) or a key system.

(v) Using or hosting bulk call-in lines (e.g., customer support or sales call centers, "hotlines," 900 numbers, sports-line numbers, etc.) for Residential and Commercial Services.

Customer understands, acknowledges and agrees that the unlawful, inappropriate and/or prohibited use and content transmitted through the HIT Services could subject Customer to criminal as well as civil liability, in addition to any actions or penalties as provided in the MSA.

# # #