Acceptable Use Policy (Business Services)

Version 2 – July 25, 2024

IN ORDER TO PROVIDE HIGH QUALITY CUSTOMER SERVICE AND TO ENSURE THE INTEGRITY, SECURITY, RELIABILITY, AND PRIVACY OF THE HMP&L FIBER NETWORK, HENDERSON MUNICIPAL POWER & LIGHT ("HMP&L"), HAS CREATED THIS ACCEPTABLE USE POLICY (AUP). THIS AUP APPLIES ALONG WITH THE FIBER SERVICE AGREEMENT GOVERNING THE CUSTOMER'S USE OF HMP&L FIBER INTERNET TO SPECIFY USE RESTRICTIONS APPLICABLE TO USERS OF THE SERVICE. THE CUSTOMER RECOGNIZES AND AGREES THAT THE THEN CURRENT VERSION OF THE AUP TO BE MAINTAINED BY HMP&L AND POSTED ON HMP&L'S WEBSITE WILL SUPERCEDE ALL PREVIOUS VERSIONS OF THIS DOCUMENT AND THAT CUSTOMER'S CONTINUED USE OF HMP&L'S FIBER INTERNET SERVICE WILL CONSTITUTE CUSTOMER'S ACCEPTANCE OF THIS POLICY AS IT MAY BE AMENDED.

BY USING THE SERVICE, THE CUSTOMER AGREES TO ABIDE BY, AND REQUIRE EACH USER OF THE SERVICE TO ABIDE BY, THE TERMS OF THIS AUP AND ASSOCIATED SERVICE AGREEMENT. IF ANY USER DOES NOT AGREE TO BE BOUND BY THESE TERMS, CUSTOMER MUST IMMEDIATELY CEASE USE OF THE SERVICE.

1. **USE.** The Service is designed solely for use in Customer's business. The Customer is responsible for any misuse of the Service that occurs through Customer's account, whether by an employee or authorized or unauthorized visitor. Customer is responsible for any and all e-mail addresses associated with the Customer's account. Customer must take steps to ensure that others do not gain unauthorized access to the Service. Customer is solely responsible for the security of (i) any device Customer chooses to connect to the Service, including any data stored or shared on that device and (ii) any access point of the Service. Customer will not resell or redistribute, or enable others to resell or redistribute, access to the Service in any manner, including, but not limited to, wireless technology, except as expressly provided in any contract for service. HMP&L reserves the right to disconnect or reclassify the Service to a higher grade or to immediately suspend or terminate the Service for failure to comply with any portion of this provision or this Policy, without prior notice.

2. **PROHIBITED ACTIVITIES USING THE SYSTEM, NETWORK, AND SERVICE**. Any activity or use of the Service which violates system or network security or integrity are prohibited and may result in criminal and civil liability. Such violations include, without limitation, the following:

a. Unauthorized access to or use of data, systems, or networks, including any attempt to probe, scan, or test the vulnerability of a system or network, relay communication through a resource, or to breach security or authentication measures without express authorization of the owner of the system or network.

b. Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner or network.

c. Interference with service to any user, host, or network, including but not limited to: mail bombing, flooding, or denial of service attacks.

d. Forging the header of any transmitted information packet, email, or Usenet posting.

e. Modifying or tampering with any hardware, software, or configuration provided by HMP&L including but not limited to: routers, switches, access points, wireless gateways, security devices and cable modem configuration files.

f. Resell the Service or otherwise make available, to anyone outside your premises, the ability to use the Service (for example, though Wi-Fi or other methods of networking), in whole or in part, directly or indirectly. The Service is for business use only and you agree not to use the Service for operation as an internet service provider.

g. Disrupting any aspect of the Service through any means.

h. Excessive use of bandwidth, that in HMP&L's sole opinion, places an unusually large burden on the network or is deemed by HMP&L to be above normal usage. HMP&L has the right to impose limits on excessive bandwidth consumption via any means available to HMP&L.

i. Use or run dedicated, stand-alone equipment or servers from your premises that provide network content or any other services to anyone outside of your premises. Examples of prohibited equipment and servers include, but are not limited to, email, Web hosting, file sharing, and proxy services and servers.

j. Assuming or assigning a HMP&L IP address that was not allocated to the user by HMP&L or its network - all HMP&L internet users must use DHCP assigned by the Service to acquire an IP address or utilize a Static IP address provided by HMP&L.

k. Running any type of server on HMP&L's system that is intentionally used to disrupt other users of the Service or users of the Internet in general.

3. **NO ILLEGAL OR FRAUDULENT USE**. The Service may be used only for lawful purposes. Customer will not use or allow others to use the service in any manner that is in violation of any applicable federal, state, local or international laws or regulations or to promote, engage in, or enable illegal activity or conduct that violates or infringes upon the rights of any person. Transmission or distribution of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization, and material that is obscene illegal, defamatory, constitutes an illegal threat, or violates export control laws. Furthermore, use of the Service to impersonate a person or entity is not permitted.

4. **NO COPYRIGHT OR TRADEMARK INFRINGEMENT**. Use of the Service is also subject to HMP&L's Copyright Infringement Policy. HMP&L reserves the right to suspend or terminate accounts which are in violation of HMP&L's Copyright Infringement Policy.

5. **NO SPAM**. Users may not send any unsolicited bulk email or electronic communication including, but not limited to, instant messenger programs, IRC, Usenet, etc. that promotes or advertises a cause, opinion, money making opportunity, or the like that the recipient did not specifically request from the sender ("Spam"). All commercial email messaging must comply with the Federal, State, and Local law. These communications do not

necessarily have to pass through the Service's email infrastructure - it only needs to originate from a Service User (“User”).

HMP&L maintains a zero-tolerance policy on Spam for its Internet products and may take immediate action against users violating this AUP. HMP&L reserves the right to impose certain limitations on use of the Service's email.

The Services may not be used to collect responses from unsolicited communication regardless of the communication's origination. Moreover, unsolicited communication may not direct the recipient to any web site or other resource that uses the Service and the user may not reference the Service in the header or by listing an IP address that belongs to the Service in any unsolicited communication even if that communication is not sent through the Service or its infrastructure.

Users may not send any type of communication to any individual who has indicated that he/she does not wish to receive messages from them. Continuing to send email messages to anyone that has expressly requested not to receive email from a User is considered to be harassment. Customer is responsible for maintaining confirmed opt-in records and must provide them to HMP&L upon request. The term "opt-in" means that recipient has signed up for mailings voluntarily.

6. **NO SYSTEM DISRUPTION**. Customer will not use, or allow others to use, the Service to disrupt, degrade, and/or otherwise adversely affect HMP&L's network or computer equipment owned by HMP&L or other HMP&L customers.

7. **SECURITY/ABUSABLE RESOURCES**. User is solely responsible for the security of any device connected to the Service, including any data stored on that device. Users shall take all necessary steps to avoid actions that result in the abuse of a resource on their network. Examples of abusable resources include, but are not limited to: open news servers, open SMTP servers, insecure routers, wireless access and insecure proxy servers. Upon notification from HMP&L, Users are required to address the problem in a timely fashion. Failure to address an issue after notification will be considered a violation of this AUP.

8. **NO "HACKING"**. Customer will not use, nor allow others to use, the Service to access the accounts of others or to attempt to penetrate security measures of the Service or other computer systems ("hacking") or to cause a disruption of the Service to other on-line users. Customer will not use, nor allow others to use, tools designed for compromising network security, such as password-guessing programs, cracking tools, packet sniffers or network probing tools.

9. **NETWORK MANAGEMENT**. HMP&L utilizes, as necessary, a variety of reasonable network management practices consistent with industry standards to ensure that all of its Customers have a high quality online experience. These practices are undertaken without regard to the source, destination, content, application, or service, and which are designed to protect Customers from activities that can unreasonably burden our network or compromise security. HMP&L's online network is a bidirectional network, the proper management of which is essential to promote the use and enjoyment of the Internet by all of our Customers. HMP&L monitors its

network and attempts to address projected demand for capacity, taking reasonable steps to expand capacity as necessary.

10. **VIRUSES.** Users must take appropriate action to prevent their systems from becoming infected with and/or distributing computer viruses such as but not limited to worms, "Trojan horses", denial of service attacks, and bots. HMP&L will take appropriate (as decided by HMP&L's sole discretion) action against Users infected with computer viruses or worms to prevent further spread.

11. **ENFORCEMENT.** HMP&L reserves the right to investigate violations of this AUP, including the gathering of information from the Customer or other Users involved and the complaining party, if any, and the examination of material on HMP&L's servers and network. HMP&L prefers to advise Users of AUP violations and any necessary corrective action but, if HMP&L, in its sole discretion, determines that a User has violated the AUP, HMP&L will take any responsive action that is deemed appropriate without prior notification. Such action includes but is not limited to: temporary suspension of service, reduction of service resources, and termination of service. HMP&L is not liable for any such responsive action and these actions are not exclusive. HMP&L may take any other legal or technical action it deems appropriate.

12. **NO WAIVER**. The failure by HMP&L to enforce any provision of this Policy at any given point in time shall not be construed as a waiver of any right to do so at any future time thereafter.

13. **REVISION TO POLICY**. HMP&L reserves the right to update or modify this Policy at any time and from time to time with or without prior notice. Continued use of the Service will be deemed acknowledgment and acceptance of this Policy. Notice of modifications to this Policy may be given by posting such changes to HMP&L's homepage (www.hmpl.com or www.hmplfiber.com), by email or by conventional mail, and will be effective immediately upon posting or sending. Customers should regularly visit HMP&L's website and review this Policy to ensure that their activities conform to the most recent version. In the event of a conflict between any customer or customer agreement and this Policy, the terms of this Policy will govern. Questions regarding this Policy should be directed to support@hmplfiber.com. Complaints of violations of it by HMP&L customers can be directed to support@hmplfiber.com.

HMP&L RESERVES THE RIGHT AT ITS SOLE DISCRETION TO IMMEDIATELY SUSPEND, TERMINATE, OR RESTRICT USE OF THE SERVICE WITHOUT NOTICE IF SUCH USE VIOLATES THE AUP, IS OBJECTIONABLE OR UNLAWFUL, INTERFERES WITH HMP&L'S SYSTEMS OR NETWORK OR THE INTERNET OR OTHERS' USE OF THE SERVICE.