RESIDENTIAL INTERNET ACCEPTABLE USE POLICY

In order to provide high quality customer service and to ensure the integrity, security, and reliability of Madison's Internet Product Network, Madison has created this Acceptable Use Policy (AUP). This AUP applies along with the Terms of service (TOS) governing the Subscriber's use of Madison's Internet and related services , Madison's Privacy Policy and Madison's Network Management Practices disclosure statement, to specify use restrictions and requirements applicable to users of the Service. The Subscriber recognizes and agrees that the then current version of the AUP to be maintained by Madison and posted on Madison's website will supersede all previous versions of this document and that Subscriber's continued use of Madison's Internet service will constitute Subscriber's acceptance of this policy as it may be amended.

By using the Service, the Subscriber agrees to abide by, and require each user of the Service to abide by, the terms of this AUP and associated TOS. Any user who does not agree to be bound by these terms must immediately cease use of the Service and notify the Madison Customer Service Department to terminate the account.

1. Use. The Service is designed for personal and family use (residential use only) within a single household. Subscriber agrees that only Subscriber and Subscriber's authorized guests in the same household will use the Service. Subscriber is responsible for any misuse of the Service that occurs through Subscriber's account, whether by a member of Subscriber's household or an authorized or unauthorized third-party. Subscriber will not use, or enable 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. Subscriber will not resell or redistribute, or enable others to resell or redistribute, access to the Service in any manner, including, but not limited to, through the use of wireless technology. Madison 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 or TOS, is objectionable or unlawful, interferes with Madison's systems or network or the Internet or others' use of the Service.

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:

- 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, or to breach security or authentication measures without express authorization of the owner of the system or network.

- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner or network;

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

- Forging the header of any transmitted information packet, email, or Usenet posting;

- Modifying or tampering with any hardware, software, or configuration provided by Madison including but not limited to: routers, switches, and modem configuration files.

- Reselling or otherwise redistributing the Service.

- Disrupting, degrading or otherwise adversely affecting Madison's network or computer equipment owned by Madison or other Madison subscribers.

- Excessive use of bandwidth that in Madison's sole opinion, places an unusually large burden on the network or goes above normal usage. Madison has the right to impose limits on excessive bandwidth consumption via any means available to Madison.

- Transmit unsolicited bulk or commercial messages commonly known as "spam."

- Assuming or assigning a Madison IP address that was not allocated to the user by Madison or its network - all Madison Internet users must use DHCP assigned by the Service to acquire an IP address.

- Either of the following activities by a Subscriber using dedicated machines (also known as "machines" or "dedicated servers") or virtual dedicated servers (also known as "VDS", "VPS", "virtual machines", and/or "virtual servers"): (i) running a tunnel or proxy to a server at another host or (ii) hosting, storing, proxy, or use of a network testing utility or denial of service (DoS/DDoS) tool in any capacity.

Because the Service is for residential use only, any use of the service for non-residential purposes is not permitted and may result in reduction in service, suspension, or termination at the sole discretion of Madison. Non-residential purposes include, without limitation, the following:

- Running any type of server on the system that is not consistent with personal, residential use. This includes but is not limited to FTP, IRC, SMTP, POP, HTTP, SOCS, SQUID, NTP, DNS or any multi-user forums.

- Distributing in any way information, software or other material obtained through the service or otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner

- IP address translation or similar facilities intended to provide additional access.

3. No Illegal or Fraudulent Use. The Service may be used only for lawful purposes. Subscriber 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. Caller Name and Robocall Management. Madison will investigate when informed of suspicious calling patterns or deceptive caller ID practices; identify the subscriber(s) or number(s) involved; contact those subscribers to determine the nature of their calls; and block, suspend or terminate a subscriber's service if it is determined to be engaged in robocalling, deceptive caller ID practices or refuses to cooperate with the Madison investigation.

Madison's voice services will associate the subscriber name on the Madison account to the telephone number to be displayed in association with the caller name lookup services ("CNAM") provided as part of the voice service for all calls made from any of the Madison telephone numbers on the account. In the event that the subscriber wishes to modify the caller name associated with the CNAM, subscriber agrees to the following: caller name submission(s) shall not mislead or impersonate any person or company; caller name submission(s) shall not contain false information and shall accurately represent the name of the person that subscribes to the voice service and that is included in directory listings, if any; caller name submission(s) shall not contain abusive, defamatory, vulgar, obscene, racist or any other language objectionable to any person or entity as determined by Madison, in its sole discretion; and caller name submission(s) shall comply with all relevant laws, rules and regulations. Furthermore, subscriber's outgoing calls must use an active, valid telephone number assigned to Subscriber. Use of invalid or unassigned telephone numbers are prohibited for outgoing calls.

5. Security/Abuse of 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 abuse of resources include without limitation: open news servers, open SMTP servers, unsecure wireless routers, and unsecure proxy

servers. In the instance when the Subscriber is using a wireless router, Madison requires that any wireless network be secure and encrypted. Open, unencrypted wireless networks are strictly prohibited.

Should an issue arise, Subscriber is required to address the problem in a timely fashion. Failure to address an issue after notification will be considered a violation of this AUP.

6. Network Management. Madison uses a variety of reasonable network management tools and practices consistent with industry standards. In the event the periods of congestion necessitate such management, Madison has available the following tools and practices (without limitation and as may be adjusted over time): (i) use of an upper limit of bandwidth allocated for uploading of files during congested periods; (ii) Subscriber Traffic Management (STM) technology to temporarily lower the priority of traffic with the greatest impact on peak congestion; (iii) spam filtering and detection techniques; and (iv) measures to protect the security and integrity of its network, resources and subscribers. In limited instances if employed, these techniques may affect the throughput rate at which subscribers may send and receive data, the ability of users to establish session connections within the network, or result in the delay of certain traffic during times of peak congestion.

For more information about Madison's network management practices and policies, please see the Madison Network Management Practices Statement

7. 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. Madison will take appropriate (as decided by Madison's sole discretion) action against Users infected with computer viruses or worms to prevent further spread.

8. Enforcement. Madison reserves the right to investigate violations of this AUP, including the gathering of information from the Subscriber or other Users involved and the complaining party, if any, and the examination of material on Madison's servers and network. Madison prefers to advise Users of AUP violations and any necessary corrective action but, if Madison, in its sole discretion, determines that a User has violated the AUP, Madison 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. Madison is not liable for any such responsive action and these actions are not exclusive. Madison may take any other legal or technical action it deems appropriate.

9. No Waiver. The failure by Madison or its affiliates 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.

10. Revisions to Policy. Madison 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 on Madison's website at www.gomadison.com, under "Terms of Service/Policies," by email or by conventional mail, and will be effective immediately upon posting or sending. Subscribers should regularly visit Madison'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 subscriber agreement and this Policy, the terms of this Policy will govern. Questions regarding this Policy should be directed to infomtc@gomadison.com. Complaints of violations of it by Madison Subscribers can be directed to abuse@gomadison.com.

Version 20210701.v3