COMMERCIAL ACCEPTABLE USE POLICY

IN ORDER TO PROVIDE HIGH QUALITY CUSTOMER SERVICE AND TO INSURE THE INTEGRITY, SECURITY, RELIABILITY, AND PRIVACY OF MADISON'S INTERNET PRODUCT NETWORK, MADISON HAS CREATED THIS ACCEPTABLE USE POLICY (AUP). THIS AUP APPLIES ALONG WITH THE TERMS OF SERVICE GOVERNING THE CUSTOMER'S USE OF MADISON'S INTERNET AND RELATED SERVICES (TOS) AND MADISON'S OPEN INTERNET DISCLOSURE, 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 MADISON AND POSTED ON MADISON'S WEBSITE WILL SUPERCEDE ALL PREVIOUS VERSIONS OF THIS DOCUMENT AND THAT CUSTOMER'S CONTINUED USE OF MADISON'S 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 TOS. ANY USER WHO DOES NOT AGREE TO BE BOUND BY THESE TERMS, CUSTOMER MUST IMMEDIATELY CEASE USE OF THE SERVICE.

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.

1. USE

The Service is designed solely for use in Customer's business. Customer is responsible for any misuse of the Service that occurs through Customer's account, whether by an employee of Customer's business or an authorized or unauthorized third-party. 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 to the Service. If the Customer sells or resells advertising or web space to a third party, then the Customer will be responsible for the content of such advertising or on such web space and the actions of such third party. 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. Madison 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:

- 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.

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

- Interference with 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, access points, wireless gateways, security devices and cable modem configuration files.

- Reselling or otherwise redistributing the Service.

- Disrupting any aspect of the Service through any means.

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

- 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 or utilize a Static IP address provided by Madison.

Running any type of server on Madison'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 Madison's Copyright Infringement Policy. Madison reserves the right to suspend or terminate accounts which are in violation of Madison'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, such as the CAN-SPAM Act (See: http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business and http://uscode.house.gov/download/pls/15C103.txt) These communications do not necessarily have to pass through the Service's email infrastructure - it only needs to originate from a Service User.

Madison maintains a zero-tolerance policy on Spam for all of its Internet products and may take immediate action against users violating this AUP. Madison 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 Madison 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 Madison's network or computer equipment owned by Madison or other Madison 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 Madison, 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

Madison reserves the right to use a changing variety of reasonable network management techniques including but not limited to (i) allocation a fixed maximum amount of bandwidth to non-customers seeking to upload peer-to-peer files from customers; (ii) utilizing STM technology to prioritize traffic during times of peak congestion; and (iii) implementing filtering and spam detection techniques to manage reliable email sources and mitigate spam. In limited instances, these techniques may affect the throughput rate at which customers may send and receive data, non-customers' ability to establish session connections within the network (such as peer-to-peer sessions), or result in the delay of certain traffic during times of peak congestion.

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 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.

11. CALLER NAME AND ROBOCALL MANAGEMENT

Madison will investigate when informed of suspicious calling patterns or deceptive caller ID practices; identify the customer(s) or number(s) involved; contact those customers to determine the nature of their calls; and block, suspend or terminate a customer'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 customer 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 customer wishes to modify the caller name associated with the CNAM, customer 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, customer's outgoing calls must use an active, valid telephone number assigned to Customer. Use of invalid or unassigned telephone numbers are prohibited for outgoing calls.

12. ENFORCEMENT

Madison 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 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.

13. 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.

14. 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 to Madison's homepage (www.gomadison.com), by email or by conventional mail, and will be effective immediately upon posting or sending. Customers 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 customer or customer 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 customers can be directed to abuse@gomadison.net.

Version 20210701.v3