

Citizens Mutual Telephone Cooperative

ACCEPTABLE USE POLICY

Page 1 of 4

Please read this AUP carefully before you start to use the service. **By using any Service (as defined herein), you accept and agree to be bound and abide by this Acceptable Use Policy and our other applicable terms of Service, all of which have been provided to you and may be accessed at <https://www.mycmtech.com/about-us>.** If you do not agree to this Acceptable Use Policy or our other applicable terms of Service, you should not access or use the service.

1. Services Covered. This Acceptable Use Policy (“AUP”) governs wireline and/or wireless high speed Internet, IP/Ethernet, IP video and/or other data, video, or voice communications service (“**Service(s)**”) provided to you by Citizens Mutual Telephone Cooperative (together with any subsidiaries or affiliates providing your Service, hereafter “**we**” “**us**” or the “**Company**”) and includes the following terms and provisions as the same may be amended or modified from time to time as provided herein. The terms and provisions of this AUP are without limitation of any rights to suspend or terminate Service that the Company otherwise possesses under your service contract, our standard terms and conditions of Service, or applicable law. In delivering Services, the Company may utilize wholesale or other “upstream” providers. This Acceptable Use Policy is specific to the Company’s network and Services, and Services may also be subject to the acceptable use policies and practices of our upstream providers.

2. Applicability. This AUP applies to you as a customer and to any other person using your Service (each such person, a “**User**”). For purposes of this AUP, your use includes, and you are responsible for, the use of all Users who access Service through your account. It is your responsibility to take precautions to limit access to Service to approved Users. If you are a contract customer, this AUP is incorporated into your Service contract. For non-contract customers, by establishing a Service account and using Service, you agree to be bound by this AUP.

3. Compliance Required. Pursuant to your Service contract as a contract customer or by establishing a Service account and using Service as a non-contract customer, all customers have agreed to and must comply with this AUP. The Company reserves the right to terminate or suspend Service immediately or to otherwise disconnect, remove, block, filter or restrict your use of Service if the Company determines, in its sole discretion, that such use is illegal or violates this AUP. The Company will cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong. If the Company believes that you have used Service for an unlawful or abusive purpose, the Company may forward the relevant communication and other information, including your identity, to the appropriate authorities for investigation and prosecution. You hereby consent to the Company’s forwarding of any such communications and information to these authorities. In addition, the Company may provide information in response to law enforcement requests, lawful government 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 you or others. The Company also reserves the right to take action on abuse which is not specifically named in this AUP at the sole discretion of the Company. Use of the Company’s systems and network constitutes understanding and agreement of this policy.

4. Prohibited Uses and Activities. This AUP identifies certain uses and activities that the Company considers to be unlawful or abusive and therefore strictly prohibited. The examples listed herein are non-exclusive and are provided solely for guidance to customers. The Company, at its sole discretion, reserves the right to discontinue Service for any unlawful use. In the event of uncertainty as to whether any contemplated use or activity is permitted, please contact a customer service representative for assistance. In addition to any other illegal or abusive uses or activities, the following constitute violations of this AUP:

a. Resale of Service: Service is available for individual customer internal use only and not for resale. Reselling Service without the Company’s written authorization is strictly prohibited.

b. Unlawful Use: Using Service in any manner that violates local, state or federal law, including without limitation using Service to transmit any material (by email, facsimile, or otherwise) whose transmission is unlawful under any local, state or federal law applicable to such transmission.

c. Copyright or Trademark Infringement: Using Service to transmit any material (by email, file sharing software, direct download, FTP sites or otherwise) that infringes any copyright, trademark, patent, trade secret, or other proprietary rights of the Company or any third party, including, but not limited to, the unauthorized copying of copyrighted material, the digitization and distribution of photographs from magazines, books, or other copyrighted sources, the digitization and distribution of copyrighted video or music, and the unauthorized transmittal of copyrighted software. You may not rebroadcast, transmit, or perform video programming service, charge admission for its viewing, or transmit or distribute running accounts of it.

d. Violation of the Digital Millennium Copyright Act (DMCA): Using Service to circumvent any technological measures used by copyright owners to protect their works or using Service to produce or disseminate technology primarily designed or produced to circumvent DMCA protections, that have only limited commercially significant purpose or use other than to circumvent; or that are marketed for use in circumventing DMCA protections. For additional information concerning your

rights and responsibilities in connection with reporting or responding to claims of copyright infringement, see *Reporting Claims of Copyright Infringement*, below.

e. Harm to Minors: Using Service to harm, or attempt to harm, minors in any way; including but not limited to activities involving child pornography or the sexual exploitation of children.

f. Threats: Using Service to transmit any material (by email or otherwise) that illegally threatens or encourages bodily harm or destruction of property.

g. Harassment and Cyberbullying: Using Service to transmit any material (by email or otherwise) that unlawfully harasses another.

h. Fraudulent Activity: Using Service to make fraudulent offers to sell or buy products, items or Services, or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes", unregistered sales of securities, securities fraud and "chain letters."

i. Forgery or Impersonation: Adding, removing or modifying identifying network, message or article header information in an effort to deceive or mislead is prohibited while using Service. Attempting to impersonate any person by using forged headers or other identifying information is prohibited.

j. Unsolicited Commercial/Unsolicited Bulk Communications Using Service to transmit any unsolicited commercial or bulk email, faxes or other communications in violation of applicable federal or state law. Activities that have the effect of facilitating illegal, unsolicited commercial or bulk email, faxes or other communications are prohibited. Using deliberately misleading headers in emails sent to multiple parties is prohibited.

k. Intentional Network Disruptions and Abusive Activity: Using Service for any activity that adversely affects the ability of other people or systems to use Service. This specifically but without limitation includes excessive consumption of network or system resources whether intentional or unintentional. This also includes "denial of service" (DoS) attacks against another network host or individual user. Interference with or disruption of other network users, network services or network equipment is prohibited. The transmission of viruses, malware, or engaging in "mail bombing," "chat flooding," cybersquatting, and similar unlawful behavior is also prohibited. Attempting to circumvent user authentication or security of any host, network, or account on the Company's systems or the Internet at large ("cracking"). This includes scanning or probing ports without the consent of the owner of the machine being scanned.

l. Unauthorized Access: Using Service to access, or to attempt to access without authority, the accounts of others, or to penetrate, or attempt to penetrate, security measures of the Company's or a third party's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in disruption of Service or the corruption or loss of data.

m. Collection of Personal Data: Using Service to collect, or attempt to collect, personal information about third parties without their knowledge or consent in violation of applicable state or federal law.

5. Network Management Practices. The Company reserves the right to protect its network from harm, which may impact legitimate data flows. The Company reserves the right to limit throughput or amount of data transferred, and to deny or discontinue Service, without notice, to anyone it believes is using an unlimited data plan or feature in any unauthorized or abusive manner or whose usage adversely impacts the Company's network or Service levels. Specific management practices and Service descriptions and disclosure of Service pricing can be obtained by contacting us. You can also find these descriptions and disclosures on our website at: www.mycmtech.com. In addition to this AUP, the Company's broadband Internet access services are subject to the Company's Transparency Statement, the most recent version of which is located at <https://www.mycmtech.com/about-us>.

6. Content. You will be liable for any and all liability that may arise out of the content transmitted by you. You shall assure that your use of Service and content comply at all times with all applicable laws, regulations and written and electronic instructions for use. The Company reserves the right to disconnect or suspend your Service and remove your content from Service if the Company determines, in its sole and absolute discretion, that such use or content does not conform with any applicable law, the requirements set forth in this AUP or interferes with the Company's ability to provide Service to you or others. The Company's action or inaction under this Section will not constitute any review, waiver or approval of your usage or content.

7. Service Monitoring. The Company is under no obligation to monitor a customer's usage, bandwidth, transmissions and/or content of Service. However, the Company may monitor the usage, bandwidth, transmissions and content of Service periodically to (i) comply with any necessary laws, regulations or other governmental requests or (ii) operate Service properly or to protect itself, its network and its customers and subscribers. The Company reserves the right to modify, reject or eliminate any information residing on or transmitted to its server that it, in its sole discretion, believes is unacceptable or in violation of this AUP or any other terms and provisions applicable to Service.

8. Domain Name Service. Keeping registry information updated and accurate is the responsibility of the domain holder and not the Company. Acceptable use of the domain name service does NOT include falsifying or omitting valid domain contact information, including the administrative, technical, zone, and billing contacts. Such usage will result in termination of Service.

9. Web/FTP Sites. Acceptable use of the Company's web/FTP space does NOT include: distribution of illegal pornographic or otherwise indecent or offending materials, distribution of restricted software or materials in violation of copyrights or distribution licenses, or any other illegal activity prohibited under Paragraph 4, above.

10. Theft of Service. You should notify the Company immediately if you become aware at any time that your Service is being stolen, fraudulently used or otherwise being used in an unauthorized manner. When you provide such notification, you must provide your account number and a detailed description of the circumstances of the theft, fraudulent or abusive use of Service. Failure to do so in a timely manner may result in the disconnection of your Service, additional charges to you, and civil or criminal liability. Until such time as the Company receives notice of the theft, fraudulent use or abusive use, you will be liable for all stolen, fraudulent or abusive use of Service. The Company reserves all of its rights at law and otherwise to proceed against anyone who uses Service illegally or improperly.

11. Indemnification. By signing your Service contract (for contract customers) and/or by activating or using Service (for non-contract customers), you agree to use Service only for authorized, lawful purposes in accordance with this AUP. In addition to being subject to other remedies, liabilities and obligations under law or applicable agreements, you shall defend, indemnify, and hold the Company harmless from any claims, damages, losses, or expenses (including without limitation attorneys' fees and legal costs) incurred in connection with all claims, suits, judgments and causes of action for damages arising from the breach by you or your Users of any provision of this AUP.

12. Termination of Service. Access to and use of Service is subject to strict compliance with this AUP and all applicable law and contractual provisions. The Company has the right to terminate access to or use of Service as provided in this this AUP, your Service contract, and our terms of Service, as applicable. If Service is suspended or disconnected for violation of this AUP, you will be responsible for all fees and/or recovery charges associated with termination of Service, as set forth in your service contract or our terms of Service.

13. Modifications. The Company may modify the terms and conditions of this AUP in a commercially reasonable manner from time to time and shall provide you notice of such changes by publication on our website, bill message or other commercially reasonable notice. If you continue to use Service after receiving notice of such changes, your continued use of Service will be in accordance with this AUP, as amended.

14. Survival. The provisions of this AUP that by their sense and context are intended to survive the discontinuance or disconnection of your use of Service shall survive such discontinuance or disconnection.

15. Governing Law. This AUP and the relationship between you and the Company shall be governed by and construed in accordance with the substantive laws of the State of Iowa, without regard to the principles of conflict of law.

16. No Waiver of Rights. The Company's failure to exercise or enforce any right under or provision of this AUP shall not constitute a waiver of such right or provision.

17. Severability. If any part or provision of this AUP is legally declared invalid or unenforceable, that part or provision will be construed consistent with applicable law as nearly as possible, and the remaining parts and provisions will remain in full force and effect. Such invalidity or non-enforceability will not invalidate or render unenforceable any other part or provision of this AUP.

18. Applicability to Attached Sites. Sites directly attached to our Internet backbone are expected to adhere to this AUP. The account owner is responsible for educating site users on acceptable use policies. Violations of the AUP by directly attached sites will be referred to the account owner for resolution. The account owner will be held responsible for any violations of the AUP.

19. Applicability to Wi-Fi Hotspots. If your agreed terms of Service permit establishing one or more Wi-Fi Hotspots, this AUP applies to the use of such Service. Without limiting the preceding, (a) you may not resell Service and (b) you are responsible for compliance with this AUP, including compliance of all Users.

20. Reporting Claims of Copyright Infringement. We take claims of copyright infringement seriously. We will respond to notices of alleged copyright infringement that comply with applicable law. If you believe a User of this service has infringed your copyright, you may report the alleged violation by submitting notification to our Copyright Agent that satisfies the requirements of the DMCA (designated below). In accordance with the Online Copyright Infringement Liability Limitation Act of the Digital Millennium Copyright Act (17 U.S.C. § 512) ("**DMCA**"), the written notice (the "**DMCA Notice**") must include substantially the following:

- Your physical or electronic signature.
- Identification of the copyrighted work you believe to have been infringed or, if the claim involves multiple works on the Website, a representative list of such works.
- Identification of the material you believe to be infringing in a sufficiently precise manner to allow us to locate that material.
- Adequate information by which we can contact you (including your name, postal address, telephone number, and, if available, email address).
- A statement that you have a good faith belief that use of the copyrighted material is not authorized by the copyright owner, its agent, or the law.
- A statement that the information in the written notice is accurate.
- A statement, under penalty of perjury, that you are authorized to act on behalf of the copyright owner.

Our designated copyright agent to receive DMCA Notices is:

Vince Tyson
114 West Jefferson Street,
Bloomfield, IA 52537

If you fail to comply with all of the requirements of Section 512(c)(3) of the DMCA, your DMCA Notice may not be effective.

Copyright owners may use their own notification of claimed infringement form that satisfies the requirements of Section 512(c)(3) of the U.S. Copyright Act. Under the DMCA, anyone who knowingly makes misrepresentations regarding alleged copyright infringement may be liable to Company, the alleged infringer, and the affected copyright owner for any damages (including costs and fees) incurred in connection with the removal, blocking, or replacement of allegedly infringing material under Section 512(f) of the DMCA.

Counter-Notification Procedures

If you believe that material you posted on the Website was removed or access to it was disabled by mistake or misidentification, you may file a counter-notification with us (a "**Counter-Notice**") by submitting written notification to our copyright agent designated above. Pursuant to the DMCA, the Counter-Notice must include substantially the following:

- Your physical or electronic signature.
- An identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access disabled.
- Adequate information by which we can contact you (including your name, postal address, telephone number, and, if available, email address).
- A statement under penalty of perjury by you that you have a good faith belief that the material identified above was removed or disabled as a result of a mistake or misidentification of the material to be removed or disabled.
- A statement that you will consent to the jurisdiction of the Federal District Court for the judicial district in which your address is located (or if you reside outside the United States for any judicial district in which the Website may be found) and that you will accept service from the person (or an agent of that person) who provided the Website with the complaint at issue.

Upon receipt of a Counter Notice, Company shall promptly provide the complaining party with a copy of the Counter-Notice and inform the party we will replace the removed material or cease disabling access to it within 10 business days. The DMCA allows us to restore the removed content no less than 10, but not more than 14 business days after receipt of the Counter-Notice, if the party filing the original DMCA Notice does not file a court action against you.

Please be aware that if you knowingly materially misrepresent that material or activity on the Website was removed or disabled by mistake or misidentification, you may be held liable for damages (including costs and attorneys' fees) under Section 512(f) of the DMCA.

Repeat Infringers

It is our policy in appropriate circumstances to disable and/or terminate the accounts of users who are repeat infringers. For additional information concerning termination of accounts due to DMCA violations, see *DMCA Termination*, below.

21. DMCA Termination. It is the Company's policy to comply with the "safe harbor" provisions for Internet Service Providers set forth in the DMCA. Without limiting any other rights or remedies available to any copyright owner or of the Company under this AUP or applicable law, the Company may terminate Service for repeated and willful violations of the DMCA.

21A. Termination of Service (Residential Accounts). The Company will suspend or disconnect Service if four (4) DMCA offenses are recorded on a residential account in any twelve (12) month period. Service will be suspended or disconnected for a minimum period of 12 months. If Service is suspended or disconnected under this Section, you will be responsible for all fees and/or recovery charges associated with termination of Service, as set forth in our Terms and Conditions of Service.

21B. Termination of Service (Business Accounts). The Company will suspend or disconnect Service if any DMCA offenses are recorded on a business account. Service will be suspended or disconnected for a minimum period of 12 months. If Service is suspended or disconnected under this Section, you will be responsible for all fees and/or recovery charges associated with termination of Service, as set forth in our Terms and Conditions of Service.

22. Redress Options. If you have questions, concerns or inquiries regarding this AUP or customer redress options, please contact the Company via phone at: (641) 664-2074 or email at info@mycmtech.com.

As an Internet service provider (“ISP”) Citizens Mutual Telephone Cooperative (“we,” “us” or the “**Company**”) invests significant resources to bring Internet access to our customers and strives to provide customers an optimum online experience that enables them to access all available and lawful online content and services. The purpose of this document is to disclose information regarding the Company’s network management practices, performance, and commercial terms of its broadband Internet access service, sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device providers to develop, market, and maintain Internet offerings, consistent with applicable federal regulations.

In delivering broadband Internet access services, we may utilize wholesale or other “upstream” providers. This Transparency Statement is specific to the Company’s network and network management practices, and services may also be subject to the network performance and network management policies and practices of our upstream providers.

NETWORK MANAGEMENT PRACTICES

General. High-speed bandwidth and network resources are limited and managing the network is essential to promote the use and enjoyment of the Internet by all of our customers. The Company is committed to providing the best online experience possible for all of its customers and uses reasonable network management practices to ensure that our services are used in ways that are consistent with the specifications of a shared network. The network management practices used by the Company are consistent with industry standards. For example, we use tools and practices to reduce the negative effects of spam, viruses or other harmful code or content, security attacks, network congestion, and other risks and degradations of the service. By engaging in reasonable and responsible network management, the Company can deliver the best possible broadband Internet experience to all of its customers.

The primary features of the Company’s network management practices are:

- **We do not block, throttle, or inhibit any lawful content, specific applications or classes of applications.**
- **We do not restrict the types of devices that can be connected to its network.**
- **We do not engage in paid prioritization or affiliated prioritization.**

Congestion Management. The Company proactively monitors its network on a continual basis to determine if an area of congestion could occur, and if areas of possible congestion are identified, may make network improvements or prior to any congestion occurring. These network improvements may include: the addition of network hardware or network segregation to accommodate additional traffic. If a period of congestion occurs, customers may experience things like: longer times to download or upload files, surfing the Web may seem somewhat slower, or playing games online may seem somewhat sluggish. The Company does not manage congestion based on the online activities, protocols or applications an individual customer uses; it only focuses on the areas with the heaviest usage and works to alleviate any congestion prior to any customer impact. The purpose is to eliminate periods of congestion as quickly as possible.

Application or Content Specific Behavior. The Company does not discriminate against particular types of lawful online content. The Company provides its customers with full access to all the lawful content, services, and applications that the Internet has to offer. However, we are committed to protecting customers from spam, phishing, and other unwanted or harmful online content and activities. In that connection, we use industry standard tools and generally accepted practices and policies to help ensure that our customers are protected from unwanted or harmful content and activities. The Company’s use of these tools, techniques and policies help to identify and restrict certain harmful and unwanted online content, such as spam or phishing Web sites. In other

cases, these tools, techniques and policies may permit customers to identify certain content that is not clearly harmful or unwanted, such as bulk email or Web sites with questionable security ratings and enable those customers to inspect the content further if they want to do so.

Device Attachments. The Company allows for customer owned equipment to be used on the network, so long as such devices do not interfere with the Company's network or our ability to provide the services. In any, case customer-owned devices are not supported or managed by the Company.

Security. The Company (directly or via upstream providers) employs a number of practices to help prevent unwanted communications such as spam as well as protect the security of our customers and network. These practices may include: limiting the number of login, SMTP, DNS, and DHCP transactions per minute (at levels far above "normal" rates) that customers can send to servers in order to protect them against Denial of Service (DoS) attacks and blocking ports that commonly used to send spam, launch malicious attacks, or steal a customer's information, (for example, SQL exploits and Microsoft communication protocol ports). We do not make detailed disclosures concerning these practices in order to better maintain the effectiveness of these defensive measures, which ensure that these critical services are available for all of our customers. In addition, The Company conducts several security initiatives, and offers security tools for our customers, such as DoS monitoring and virus scanning software.

SERVICE PERFORMANCE

Service Technologies. The Company provides broadband Internet access utilizing fiber, coaxial, copper and wireless service technologies. Speed and other performance characteristics may vary based on service technology, and not all service technologies are available in all locations.

Advertised Speeds. The Company provides residential and business customers with a variety of high speed Internet service packages, including the service packages and performance tiers identified in "Commercial Terms" below. The Company advertises its speeds as "up to" a specific level based on the tier of service to which a customer subscribes, and engineers its network to ensure that its customers can enjoy the speeds to which they subscribe. However, the Company does not guarantee that a customer will actually achieve those speeds at all times. In the absence of purchasing an expensive, dedicated Internet connection, no ISP can guarantee a particular speed at all times to a customer.

Actual Speeds and Latency. The "actual" speed that a customer will experience while using the Internet depends upon a variety of conditions, many of which are beyond the control of any ISP. These conditions include:

- Performance of a customer's computer or device, including its age, processing capability, its operating system, the number of applications running simultaneously, and the presence of any adware and viruses. You should make sure you are running the most up-to-date operating system your computer or other Internet connected device can handle (with all available patches installed) to maximize your connection speeds.
- Type of connection between a customer's computer and modem. If there is a wireless router between your modem and your Internet connected device, the connection speed you experience can often be slower than direct connections into a router or modem, and depends on the model and configuration of the router that you use. Certain routers are able to pass data to your Internet connected device more quickly than others. Wireless connections also may be subject to greater fluctuations, interference and

congestion. Wireless modem connections used with higher speed tiers may be particularly impacted, as many wireless connections do not perform at the speeds delivered by these tiers.

- The distance packets travel (round trip time of packets) between a customer's computer and its final destination on the Internet, including the number and quality of the networks of various operators in the transmission path. The Internet is a "network of networks." A customer's connection may traverse the networks of multiple providers before reaching its destination, and the limitations of those networks will most likely affect the overall speed of that Internet connection.
- Congestion or high usage levels at the website or destination. If a large number of visitors are accessing a site or particular destination at the same time, your connection will be affected if the site or destination does not have sufficient capacity to serve all of the visitors efficiently.
- Gating of speeds or access by the website or destination. In order to control traffic or performance, many websites limit the speeds at which a visitor can download from their site. Those limitations will carry through to a customer's connection.
- The performance of modems or other equipment installed at your premises. Modem performance may degrade over time, and certain modems are not capable of handling higher speeds. Our highest speed services may be particularly impacted by computer and communications limitations. We encourage you to promptly contact customer service if you have any concerns about your modem performance or speed capabilities.

Real Time Applications. The Company offers a variety of service packages, with different speeds. For each of these packages, the Company utilizes service technologies with latency characteristics suitable for real-time applications such as voice communication or video streaming services.

Customer Speed Test. The Company offers its customers to the ability to test the speeds that they are receiving on the Company's network from the customer's computer to a test site on the Company's network. Simply go to the speed test site for your service location to test your connection at: <http://aureon.speedtestcustom.com/>. Please note that this and other commercially available speed tests are dependent on several of the factors outlined above, especially the customer's own Wi-Fi network. Therefore, these tests do not necessarily reflect the performance of the Company's network alone.

COMMERCIAL TERMS

Service Packages. The Company offers a variety of service packages, which include pricing for Internet services that vary depending upon the plan and whether the services are bundled with one or more of our other service offerings. Please see below for monthly pricing information for our currently available service packages:

Residential Plans:	<u>Upload</u>	<u>Download</u>	<u>Price</u>
	6 Mg	6 Mg	44.95
	*No Longer Available To New Customers		
	100 Mg	100 Mg	70.00
	500 Mg	100 Mg	80.00
	1 Gig	1 Gig	90.00

Business Plans:	<u>Upload</u>	<u>Download</u>	<u>Price</u>
	6 Mg	6 Mg	44.95
	*No Longer Available To New Customers		
	100 Mg	100 Mg	70.00
	500 Mg	100 Mg	80.00
	1 Gig	1 Gig	90.00

Except as disclosed above, the Company does not limit the amount of usage (by imposing specific data caps) or impose usage-based fees. Except as disclosed above, the Company also does not impose fees for early termination.

Impact of Non-Broadband Internet Access Services. The Company does not currently offer other data services that affect the last-mile capacity or performance of our broadband Internet access services.

Privacy and Other Policies. In addition to this Transparency Statement, the Company’s broadband Internet access services are subject to our Privacy Policy, Acceptable Use Policy and Terms of Service, the most recent version of which are located at <https://www.mycmtech.com/about-us>.

Redress Options. If you have questions, concerns or inquiries regarding this Transparency Statement or customer redress options, please contact us via phone at: (641) 664-2074 or email at info@mycmtech.com.