

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.

Citizens Mutual Telephone Cooperative

ACCEPTABLE USE POLICY

Page 3 of 5

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		
	50 Mg (Bundled)	50 Mg	54.95
	50 Mg (Stand Alone)	50 Mg	69.95
	100 Mg	100 Mg	79.95
	500 Mg	100 Mg	99.95
	1 Gig	1 Gig	129.95

Business Plans:	<u>Upload</u>	<u>Download</u>	<u>Price</u>
	6 Mg	6 Mg	44.95
	*No Longer Available To New Customers		
	50 Mg (Bundled)	50 Mg	54.95
	50 Mg (Stand Alone)	50 Mg	69.95
	100 Mg	100 Mg	79.95
	500 Mg	100 Mg	99.95
	1 Gig	1 Gig	129.95

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.

Citizens Mutual Telephone Cooperative

PRIVACY POLICY

Effective Date: This Privacy Policy (“**Policy**”) was last updated on 11/20/2020, and such updates are effective immediately. If you have any questions concerning this Privacy Policy, please contact using the contact information at the end of this Policy.

Important Notice: This Policy applies to voice, video and data communications services provided by Citizens Mutual Telephone Cooperative (together with any subsidiaries or affiliates providing your communications services, “**we**,” “**us**,” or the “**Company**”). This Policy explains how the Company collects, uses, and discloses information about our subscribers when they subscribe to, access, or use our communications services. Some of the information we may collect is “personally identifiable information” and/or “customer proprietary network information,” each as defined by applicable Federal law. Our use or sharing of such information is governed by applicable Federal law (as described herein) and this Policy. **Your use of any Company services constitutes your acceptance of this Policy.**

This Policy does not apply to the areas of the Company’s websites that are accessible to the general public, which are governed by the Company’s website privacy policy (available via the applicable website). The Company is not responsible for information, content, applications or services provided by others. Before you access, use, link to or download a service or application on your computer or wireless device, you should review the associated terms of service and privacy policy. Personal information you submit in those contexts may be read, collected or used by the service or application provider and others associated with these forums in a manner different from that described here.

This Policy applies across our family of companies and, except as otherwise specified herein, applies to all of the communications services we provide. This Policy explains our practices in the following areas:

1. Our Responsibilities and Your Rights under Federal Law
2. Information We Collect and How We Collect and Use It
3. How We Share Your Information
4. How to Limit the Sharing and Use of Your Information
5. How Long We Keep Your Information
6. How We Protect Your Information
7. How You May Access and Correct Your Information
8. Changes to This Policy
9. Violations of This Policy or Your Rights
10. Availability of This Policy
11. How You May Contact Us

1. Our Responsibilities and Your Rights Under Federal Law

When you communicate with us, we collect information from you that we use to deliver, provide, confirm, change, bill, monitor, maintain and repair your services and service-related devices. Some of this information may be “personally identifiable information” or “customer proprietary network information” (“**CPNI**”) as defined by Federal law.

Section 631 of the federal Cable Communications Policy Act of 1984, as amended (the “**Cable Act**”) provides special privacy protections for personally identifiable information we may collect about our

cable and multichannel video service subscribers. For these purposes, personally identifiable information is information that identifies a particular person or persons, it does not include aggregate data that does not identify a particular person or persons.

If you subscribe to our multichannel video programming services, you have a right to know:

- the nature of any personally identifiable information we may collect and the ways we may use this information;
- under what circumstances and to what parties we may disclose personally identifiable information;
- how long we will maintain personally identifiable information;
- the times and places where you may access your personally identifiable information; and
- your rights under the Cable Act concerning personally identifiable information.

Section 702 of the federal Telecommunications Act of 1996, as amended (the “**Telecommunications Act**”) provides special privacy protections for CPNI we may collect about our telecommunications and Voice over Internet Protocol (VoIP) service subscribers. CPNI generally includes information about the quantity, technical configuration, type destination, location and amount of your use of voice services and information contained on your bill concerning the type of voice services and features you subscribe to or receive. If you subscribe to our voice services, you have the right, and the Company has a duty, to protect the confidentiality of CPNI.

As required by the Cable Act and the Telecommunications Act, this Policy describes: what personally identifiable information or CPNI we collect and how we collect it; how we use or share that personally identifiable information or CPNI; how long we keep your personally identifiable information and/or CPNI; how we protect such information in our possession; and your rights and remedies if we violate this Policy or applicable Federal or State law.

In the event we determine there are any conflicts between this Policy and applicable Federal law (for example, the Cable Act or Telecommunications Act), we will comply with the applicable Federal law. In addition to Federal law, we will also comply with any applicable State law.

2. Information We Collect and How We Collect and Use It

Information Collected When You Communicate with Us

When you communicate with us, we collect information from you that we use to deliver, provide, confirm, change, bill, monitor, maintain and repair your services and service-related devices. This information is also used to resolve issues with your order, with our products and services, or with your account. The information we collect may include your name, addresses, and other contact information; the reason for the contact; and your Social Security Number and payment information. We use this information to establish and maintain your customer account and billing records (including establishing credit), provide services to you, authenticate you (i.e., confirming your identify in connection with service or before sharing sensitive personal or account information), and contact you about services that we offer.

When you contact us or we contact you with calls, email, or through a feature on our websites or in our applications, we may monitor or record that communication or keep a record of the transaction to help us train employees and provide high-quality customer service.

Information Collected When You Use Our Products and Services

We collect information about your use of our products, services and sites. Information such as call records, websites visited, wireless location, application and feature usage, network traffic data, product and device-specific information, service options you choose, mobile and device numbers, video streaming and video packages and usage, movie rental and purchase data, and other similar information may be used for billing purposes, to deliver and maintain products and services, or to help you with service-related issues or questions. In addition, subject to any legal restrictions that may apply, this information may be used for other purposes such as providing you with information about service enhancements, determining your eligibility for new services or service packages, and marketing to you based on your use of services. This information may also be used to: (a) manage and protect our networks, services and users from fraudulent, abusive, or unlawful uses; and (b) subject to consent practices described in this policy, help us improve our services, research and develop new services, and offer promotions and other services.

If you subscribe to our high speed data services, we may automatically measure and monitor network performance and the performance of your Internet connection to improve your, or our, service levels and products. If you contact us for service support, we also may access information about your computer, wireless device or other device settings to provide customized technical support or to install specific applications or services that you use or that are necessary to the applications or services you use.

Information Provided to Us by Third Parties

When you apply for or purchase service from us, we may obtain credit information about you from outside credit reporting agencies to help us with customer authentication and credit-related decisions.

Information Collected on Our Websites

When you establish an online account with us, we maintain information about your user identification and password. This information is used to identify you when you sign in to your account.

Information You Provide

When you contact us online or by other means for information about services, we will respond to your request and may use the information you supply us to provide you with additional information about service offerings either at that time or in the future. Information you provide on our websites about your preferred location and other preferences may be used to provide you with more relevant service recommendations, services and special offers.

We may also collect information from you when you agree to participate in surveys or provide other feedback to us regarding our services, when you register to receive newsletters or similar updates, or when you apply for a job with the Company. We use this information only for the purpose for which you provide it.

We may send you emails that communicate information about your account or about services, marketing offers, or promotions that may be of interest to you. When you open an email or click on links within these emails, we may collect and retain information to provide you with future communications that may be more interesting to you. Please note that we will not ask you to send us, via email, sensitive personal or account information.

3. How We Share Your Information

Information Shared Within Our Family of Companies

We share customer information within our family of companies for operational purposes. We also share certain types of customer information within our family of companies for our own marketing purposes unless you advise us not to share. Sharing this information allows us to provide you with the latest information about our products and services and to offer you our latest promotions.

Specific laws govern our sharing and use of CPNI. Our voice customers receive a privacy notice regarding CPNI when they first contract for or order service and every two years thereafter. For more information, please read our applicable CPNI notices. You may choose to opt out of the sharing of your CPNI within our family of companies for certain marketing purposes as described below.

When you are speaking with a customer service representative, we may ask your permission to review your records, including your CPNI, to provide you with information about the full array of services provided by our family of companies.

Information Shared With Third Parties

Except as explained in this Policy, we do not sell, license or share information that individually identifies our customers, people using our networks, or website visitors with others outside our family of companies.

We may use vendors and partners for a variety of business purposes such as to help us offer, provide, repair and bill for services we deliver to you. We share information with those vendors and partners to the extent reasonably necessary for them to perform work on our behalf. For example, we may provide your credit card information and billing address to our payment processing company solely for the purpose of processing payment for a transaction you have requested. We require that these vendors and partners protect the customer information we may provide to them and limit their use of our customer data to the purposes for which it was provided. We do not permit these types of vendors and partners to use this information for their own marketing purposes.

We provide the names, addresses and telephone numbers of wireline telephone subscribers to directory publishers and directory assistance services unless a non-published or non-listed phone number has been requested.

Unless otherwise restricted or prohibited by the Cable Act or Telecommunications Act, we may disclose information that individually identifies our customers or identifies customer devices to third parties in certain circumstances, such as:

- to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law;
- in cases involving danger of death or serious physical injury to any person or other emergencies;
- to protect our rights or property, or the safety of our customers or employees;
- to protect against fraudulent, malicious, abusive, unauthorized or unlawful use of or subscription to our services and to protect our network, services, devices and users from such use;

- to advance or defend against complaints or legal claims in court, administrative proceedings and elsewhere;
- to credit bureaus or collection agencies for reporting purposes or to obtain payment for Company-billed services;
- to a third-party that you have authorized to verify your account information;
- to outside auditors;
- to the FCC, Iowa Utilities Board other federal, state, local or other governmental or quasi-governmental authority with jurisdiction over any Service; or
- with your consent.

If we enter into a merger, acquisition or sale of all or a portion of our assets or business, customer information will also be transferred as part of or in connection with the transaction.

4. How to Limit the Sharing and Use of Your Information

You have choices about how we share and use information.

Customer Proprietary Network Information (CPNI)

Under the Telecommunications Act, you may choose whether to allow us to share your CPNI within our family of companies for certain marketing purposes. You may choose to opt out of the sharing of your CPNI within our family of companies for these marketing purposes by following the instructions on our CPNI notices.

Telemarketing

Federal “Do Not Call” laws allow you to place residential wireline and wireless phone numbers on the National Do Not Call Registry to prevent telemarketing calls to those numbers. If you would like to add your numbers to this list, you may do so by visiting www.donotcall.gov. You should be aware that even if you add your number(s) to the federal or a state Do Not Call list, most telemarketing laws allow companies to contact their own customers. It is the Company’s practice not to engage in telemarketing to our own customers. In order to keep you informed concerning our services and your account, we may use an automatic telephone dialing system, artificial or prerecorded voice, text message, or other form of written or audible communication to your designated contact number(s). For example, these informational contacts may include reminders of payment due dates, maintenance alerts and service cutovers.

Marketing Email, Text Messages, Postal Mail and Door-to-Door Calls

Marketing emails you receive from the Company include an unsubscribe instruction (usually found at the bottom of the email) that you may use to opt out of receiving future marketing-related emails. You may also opt out of receiving marketing related emails from the Company by contacting a customer service representative at Citizens Mutual Telephone Cooperative.

You may opt out of receiving marketing-related postal mailings or prevent text message marketing from the Company by calling a customer service representative at Citizens Mutual Telephone Cooperative. Please note that the Company may use bulk mail service for some marketing mailings. These services deliver offers to all homes in a neighborhood or zip code. This type of mailing will continue even if you opt-out of receiving marketing-related postal mailings from the Company.

5. How Long We Keep Your Information

Under our practices and policies, sensitive records are retained only as long as reasonably necessary for business or legal purposes. We will maintain personally identifiable information about you no longer than necessary for the purpose for which it was collected. This means we may also maintain this information for a period of time after you are no longer a subscriber if it is necessary for business or legal purposes. We will destroy the information if we have no pending requests, orders or court orders for access to this information, after we determine that it is no longer necessary for the purposes for which it was collected and in compliance with any applicable federal, state or local laws or requirements.

6. How Long We Protect Your Information

The Company has technical, administrative and physical safeguards in place to help protect against unauthorized access to, use or disclosure of customer information we collect or store, including Social Security Numbers. Employees are trained on the importance of protecting privacy and on the proper access to, use and disclosure of customer information. Under our practices and policies, access to sensitive personally identifiable information is authorized only for those who have a business need for such access, and sensitive records are retained only as long as reasonably necessary for business or legal purposes. Although we work hard to protect personal information that we collect and store, no program is 100% secure and we cannot guarantee that our safeguards will prevent every unauthorized attempt to access, use or disclose personal information. The Company maintains security and incident response plans to handle incidents involving unauthorized access to private information we collect or store.

7. How You May Access and Correct Your Information

We strive to keep our customer records as accurate as possible. You may correct or update your customer or account information by calling a customer service representative at Citizens Mutual Telephone Cooperative or by accessing your account online and providing the updated information there.

8. Changes to This Policy

We may revise and update this Privacy Policy from time to time in our sole discretion, so please check back periodically for changes. You will be able to see that changes have been made by checking to see if the effective date posted at the beginning the policy. If we elect to use or disclose information that identifies you as an individual in a manner that is materially different from that stated in our policy at the time we collected that information from you, we will give you a choice regarding such use or disclosure by appropriate means, which may include use of an opt-out mechanism.

9. Violations of This Policy or Your Rights.

If you believe that your privacy rights have been violated, please contact us immediately. We will take immediate steps to address your concerns. If you believe that you have been aggrieved as a result of our violation of applicable provisions of the Cable Act or Telecommunications Act, you may enforce the limitations imposed on us through a formal complaint to the FCC and/or a civil lawsuit seeking damages, attorneys' fees and litigation costs. Other rights and remedies may be available to you under federal, state or local laws.

10. Annual Notice and Availability of This Policy

Citizens Mutual Telephone Cooperative
PRIVACY POLICY

It is our practice to provide a copy of this Policy to all customers at the time you first contract for or subscribe to service and to provide a summary of our privacy practices or a copy of this Policy at least annually thereafter. To the extent required by applicable laws or regulations, this policy may be supplemented by service-specific privacy policies or privacy notices (i.e., our cable subscriber privacy notice for video subscribers or our CPNI policies for telephone and broadband subscribers). Subscribers may obtain a copy of this Policy by request (using the contact information and methods described herein) at any time.

11. How You May Contact Us

If you have questions, concerns or suggestions related to our Privacy Policy or our privacy practices you may contact us at:

Citizens Mutual Telephone Cooperative
Email: info@mycmtech.com
Phone: (641) 664-2074
Web: www.mycmtech.com