ACCEPTABLE USE POLICY

Effective Date: as posted at this URL. Applicable to all services provided by Fiberlink MDU, LLC.

1. PURPOSE AND SCOPE

Fiberlink MDU, LLC ("Fiberlink," "we," "us," or "our") provides facilities-based broadband and communications services, including bulk fiber Wi-Fi to multiple dwelling unit ("MDU") properties, managed in-unit internet, common-area Wi-Fi, small-business and commercial connections, dedicated internet access, voice services, and related infrastructure (collectively, the "Services"). This Acceptable Use Policy (the "AUP") governs the use of the Services and is incorporated by reference into Fiberlink's Standard Terms and Conditions (the "T&Cs") and every executed Service Order or Statement of Work.

This AUP is designed to address the realities of an MDU broadband deployment, in which different categories of users access the same network for different purposes. The AUP therefore distinguishes among four categories of persons subject to it, defined in Section 4 below. By using the Services in any capacity, each such person agrees to comply with this AUP.

2. UPDATES TO THIS AUP

Fiberlink may update this AUP from time to time. The procedure for, and effect of, an update depends on the nature of the change. This Section 2 controls all amendments, revisions, and updates to the AUP, and is intended to coordinate with Section 1.5 of the T&Cs.

2.1 Non-Material Updates. Fiberlink may at any time, and without prior notice, post non-material updates to this AUP. Non-material updates include (without limitation): typographical and grammatical corrections; updates to contact information, designated agents, email addresses, or mailing addresses; renumbering of sections; addition of clarifying examples; updates to statutory or regulatory citations; addition of a new specifically prohibited activity that is illegal or is generally recognized as abusive (for example, a newly identified malware family, a newly enacted statute, or a newly recognized abuse vector); and similar housekeeping or compliance changes that do not materially diminish a right of the Customer or a User, do not materially increase a burden of the Customer or a User, and do not impose a new fee. Non-material updates take effect upon posting at the AUP URL, and continued use of the Services constitutes acceptance.

2.2 Material Updates Affecting the Customer. A "Material Update" is any amendment to this AUP that (i) materially diminishes a right of the Customer under an executed Service Order; (ii) materially increases a burden of the Customer; (iii) imposes a new fee on the Customer; or (iv) materially restricts the scope of permitted use in a manner that affects the Customer's operations at the Service Site. A Material Update shall not take effect with respect to a Customer under an executed Service Order during the then-current Initial Service Term or Renewal Term unless: (a) the Customer consents in writing to the Material Update; or (b) Fiberlink delivers written notice of the Material Update to the Customer at least sixty (60) days

before its effective date, in which case the Material Update takes effect on the stated date and the Customer's sole remedy if it does not wish to accept the Material Update is to deliver a written notice of non-renewal in accordance with the auto-renewal provisions of the T&Cs, OR, if the Material Update is scheduled to take effect prior to the next renewal date, to terminate the affected Service Order without payment of the Termination Charge effective on the Material Update's effective date by delivering written notice to Fiberlink not later than thirty (30) days after receipt of Fiberlink's notice. This Section 2.2 implements and coordinates with Section 1.5 of the T&Cs.

2.3 Updates Affecting Residential Tenants and Common-Area Users. For an update to this AUP that materially changes the rules applicable to Residential Tenants (Section 5), Common-Area Users (Section 6), or both, Fiberlink shall: (i) post the updated AUP at the AUP URL; (ii) deliver written notice to the Customer not less than thirty (30) days before the update takes effect; and (iii) refresh the captive portal and any splash-page terms presented to Common-Area Users to reflect the update. Customer shall use commercially reasonable efforts to redistribute the updated AUP through the communication channels described in Section 5.1, including updated lease addenda for new leases entered into after the effective date, refreshed common-area postings, and refreshed move-in materials. Existing Residential Tenants and Common-Area Users are deemed to have accepted the updated AUP by continued use of the Services thirty (30) days after the update is posted and notice is given to the Customer.

2.4 Updates Affecting Commercial Tenants. For an update to this AUP that materially changes the rules applicable to Commercial Tenants (Section 7), Fiberlink shall give the affected Commercial Tenant, through the Customer, not less than sixty (60) days' written notice. A Commercial Tenant that does not wish to accept a Material Update affecting it may terminate its Commercial Service Addendum or applicable Service Order without payment of the Termination Charge by delivering written notice to Fiberlink (through the Customer) not later than thirty (30) days after notice of the Material Update; otherwise, continued use of the Services after the effective date constitutes acceptance.

2.5 Emergency, Legal, and Safety-Driven Updates. Notwithstanding Sections 2.2 through 2.4, Fiberlink may amend this AUP, and the amendment shall take effect immediately upon posting, where the amendment is required to: (i) comply with a new law, regulation, court order, subpoena, or other binding legal requirement; (ii) respond to an active and material threat to the security or integrity of the Services or to the safety of any person; (iii) respond to a directive from a governmental authority with jurisdiction; or (iv) address an active and serious abuse pattern (such as an active malware outbreak, an active DDoS campaign, an active CSAM incident, or a credible threat of imminent harm). Fiberlink shall provide a written explanation of any such emergency amendment to the Customer as soon as reasonably practicable thereafter. An emergency amendment under this Section 2.5 does not waive the Customer's rights under Section 2.2 with respect to subsequent non-emergency Material Updates.

2.6 Versioning and Archive. Each version of this AUP shall identify its effective date. Fiberlink shall maintain an archive of prior posted versions of this AUP available on request. Each Service Order shall reference the AUP by URL, and disputes regarding compliance with the AUP shall be resolved by reference to the version of the AUP in effect at the time the conduct at issue occurred.

2.7 No Right to Diminish Executed Service Order. Nothing in this Section 2 grants Fiberlink the right to unilaterally diminish, modify, or otherwise affect the commercial terms of any executed Service Order, including pricing, term length, escalator, infrastructure ownership, or any provision expressly set forth on the face of the Service Order or in the T&Cs.

3. RELATIONSHIP TO OTHER AGREEMENTS

This AUP supplements but does not replace any executed agreement between Fiberlink and Customer. In the event of a conflict between this AUP and any executed Service Order or the T&Cs, the order of precedence set forth in the T&Cs (Section 1.4) controls. Capitalized terms used but not defined in this AUP have the meanings given in the T&Cs.

4. WHO IS COVERED — DEFINED USER CATEGORIES

This AUP applies to the following four categories of persons, each of which is referred to collectively as a "User" of the Services. Except where a section is expressly limited to one category, every provision of this AUP applies to every category.

CUSTOMER	**RESIDENTIAL TENANT**	**COMMON-AREA USER**	**COMMERCIAL TENANT**
The property owner, manager, HOA, or similar entity that contracts for the Services. Responsible for AUP communication and cooperation with enforcement.	Persons occupying a dwelling unit at the Service Site. Uses the Service inside the unit for personal, household, and remote-work purposes.	Any person accessing the Service in lobbies, clubhouses, pools, gyms, parking areas, or similar shared spaces. Includes residents, guests, and invitees.	Small businesses, professional offices, or retail tenants at the Service Site that receive Service for business purposes under a Commercial Service Addendum or equivalent.

4.1 Customer. The "Customer" is the property owner, property manager, condominium or homeowners association, or other entity that has executed a Service Order with Fiberlink. The Customer is the direct counterparty to Fiberlink and is the entity primarily responsible for compliance with this AUP, including communication of this AUP to Residential Tenants, Common-Area Users, and Commercial Tenants at the Service Site, and cooperation with Fiberlink in enforcement.

4.2 Residential Tenant. A "Residential Tenant" is any person occupying or authorized to occupy a residential dwelling unit at the Service Site, including the leaseholder, the leaseholder's family or household members, and the leaseholder's permitted guests when accessing the Service from within that dwelling unit. Residential Tenants use the Service primarily for personal, family, household, and remote-work purposes.

4.3 Common-Area User. A "Common-Area User" is any person (including a Residential Tenant, a Commercial Tenant, an employee of the Customer, or a guest or invitee) who accesses the Service through a wireless access point located in a common area at the Service Site, including but not limited to the lobby, leasing office, mail room, fitness center, pool deck, clubhouse, lounge, business center, courtyards, garages, parking areas, and similar shared spaces.

4.4 Commercial Tenant. A "Commercial Tenant" is a non-residential tenant — including a small business, professional services office, retail tenant, food service establishment, or co-working operator — that occupies space at the Service Site and receives Services for business purposes under a Commercial Service Addendum, separate Service Order, or other written authorization from the Customer. Commercial Tenants are subject to the special provisions of Section 8.

4.5 Customer's Staff and Contractors. The Customer's on-site staff (leasing agents, maintenance personnel, security personnel, and similar) and the Customer's contractors using the Service in the course of their work for the Customer are treated as Customer for purposes of this AUP, and the Customer is responsible for their compliance.

5. CUSTOMER OBLIGATIONS

5.1 Communication of the AUP. The Customer shall make this AUP available to all Users at the Service Site. Acceptable methods of communication include: (i) including a reference to this AUP and its URL in residential lease agreements, commercial lease agreements, lease addenda, move-in packets, and resident handbooks; (ii) posting a notice referencing this AUP and its URL in common areas where Service is accessible; (iii) including the AUP reference in any captive portal or splash page presented to Common-Area Users; and (iv) such other methods as Fiberlink may reasonably request. Customer's failure to communicate the AUP does not relieve Users from compliance, but does subject Customer to the cooperation and indemnification obligations herein.

5.2 Captive Portal and Common-Area Notice. Where Fiberlink provides a captive portal, splash page, or click-through terms for Common-Area Wi-Fi, Customer agrees that such captive portal may incorporate this AUP by reference and may require Common-Area Users to accept this AUP as a condition of access. Customer shall not disable, bypass, or interfere with such captive portals.

5.3 Cooperation with Enforcement. The Customer shall reasonably cooperate with Fiberlink in investigating and addressing alleged AUP violations at the Service Site, including by: (i) providing Fiberlink with information reasonably necessary to identify the unit, access point, or person associated with an alleged violation; (ii) communicating Fiberlink's notices to the responsible Residential Tenant or Commercial Tenant; (iii) supporting Fiberlink's lawful suspension or termination of Service to an offending unit or User; and (iv) supporting law enforcement requests where required by law.

5.4 Customer's Own Use of the Service. Where the Customer uses the Service for its own purposes (for example, a leasing office network, property management workstations, security camera systems, building automation, smart-building systems, IoT devices, or property Wi-Fi for staff and contractors), such use is subject to all provisions of this AUP. The Customer is responsible for the security of its own networks and devices behind any router or firewall it controls.

5.5 No Resale or Sublicensing. Except as expressly permitted in the Service Order (such as in a bulk-billing arrangement to Residential Tenants or a Commercial Tenant carve-out), the Customer shall not resell, sublicense, rebrand, or otherwise commercialize the Services to third parties, and shall not extend the Service to other properties, adjacent buildings, or off-premises locations not covered by the Service Order. Customer shall not represent itself as the provider of the Service.

5.6 Lease Provisions. Customer shall use commercially reasonable efforts to include in its standard residential and commercial lease forms an acknowledgment that broadband Services are provided pursuant to this AUP and the T&Cs, and that the resident or commercial tenant agrees to abide by the same. Customer's failure to include such provisions does not limit Fiberlink's enforcement rights against the offending User.

6. RESIDENTIAL TENANT — IN-UNIT INTERNET USE

This Section 6 applies to use of the Service by Residential Tenants from within their dwelling units. Common-Area access by Residential Tenants is governed by Section 7.

6.1 Permitted Personal and Household Use. Residential Tenants are encouraged to use the Service for the full range of normal residential and remote-work activities, including: streaming video and music; gaming; video conferencing for work, school, telemedicine, and personal use; remote work and home-office activities (including hosting business video calls, accessing employer VPNs, and similar); educational and research use; connecting smart-home and IoT devices, security cameras, smart appliances, voice assistants, gaming consoles, and personal media servers; cloud backup and file sync; and other lawful personal use.

6.2 Use of VPNs and Encryption. Residential Tenants may use VPNs, end-to-end encrypted messaging, encrypted storage, and other privacy-enhancing technologies for any lawful purpose. Fiberlink does not block, throttle, or otherwise discriminate against lawful encrypted traffic.

6.3 Boundary Between Residential and Commercial Use. The residential bulk Wi-Fi Service is intended for personal, family, household, and remote-work use within a dwelling unit. A Residential Tenant remote-working for an employer, running a side business of typical scale (such as a freelance professional, online seller, content creator, or consultant), or pursuing similar activities is engaging in permitted residential use. However, the following activities constitute commercial use that exceeds the scope of residential service and may require a Commercial Service Addendum or a separate service arrangement: (i) operating publicly-advertised commercial servers, hosting providers, or transit services; (ii) running a brick-and-mortar business from the unit that materially uses the Service for customer-facing purposes; (iii) operating a continuous, commercial-scale workload that consumes a disproportionate share of network resources; or (iv) using the Service in a manner that violates the unit's residential-use covenants under the lease.

6.4 In-Unit Network and Device Responsibility. Residential Tenants are solely responsible for: (i) the security and configuration of their own routers, devices, and personal Wi-Fi networks operating behind the Service's demarcation point; (ii) the conduct of household members, guests, and other persons granted access to the Tenant's in-unit network; (iii) installing and maintaining current security software (anti-virus, anti-malware) on their personal devices; and (iv) applying security updates to their devices.

6.5 Parental Controls. Fiberlink does not, by default, filter or block content delivered to dwelling units. Residential Tenants who wish to restrict content available to children or other household members are responsible for implementing parental controls at the household level (for example, using device-level controls, family-safety features in browsers and operating systems, or third-party filtering services).

6.6 Privacy in the Unit. Subject to Section 10, Fiberlink does not, as an ordinary practice, monitor the content of communications transmitted by Residential Tenants from within their units. The Customer (as building owner) is not entitled to access, monitor, or inspect the content of communications from any Residential Tenant's unit. Fiberlink does not share Residential Tenant traffic content with the Customer except as expressly permitted by law or Tenant consent.

7. COMMON-AREA WI-FI USE

This Section 7 applies to use of the Service through wireless access points located in common areas at the Service Site (the "Common-Area Wi-Fi"). Common-Area Wi-Fi is a public-accessible amenity intended for short-session, lower-throughput, casual use.

7.1 Reduced Privacy Expectation. Common-Area Users have a reduced expectation of privacy compared to use of the Service from within a dwelling unit. Fiberlink and the Customer may, for purposes of network operation, security, abuse investigation, and capacity management, log: (i) MAC addresses or other device identifiers; (ii) session start and end times; (iii) bandwidth consumed; (iv) IP addresses assigned; and (v) other connection metadata. Fiberlink does not, as an ordinary practice, inspect content of Common-Area communications.

7.2 Permitted Use. Common-Area Wi-Fi is intended for casual use by residents, guests, invitees, and the Customer's on-site staff. Permitted use includes general browsing, light streaming, email, messaging, social media, and remote work from common-area spaces. Common-Area Users should treat the Common-Area Wi-Fi as a public network and use a VPN or end-to-end encryption for sensitive activity.

7.3 Session and Bandwidth Management. Fiberlink may impose, and the Customer may direct Fiberlink to impose, reasonable technical limits on Common-Area Wi-Fi sessions, including: (i) session time limits; (ii) per-device bandwidth caps; (iii) restrictions on heavy peer-to-peer or torrent traffic; (iv) limits on the number of simultaneous connections per device; (v) rate limits on data-intensive applications; and (vi) restrictions on certain ports or protocols typically associated with abuse. Such limits are not Service-level commitments and may change without notice.

7.4 Prohibited Use. In addition to the general prohibitions in Section 9, Common-Area Users shall not: (i) attempt to access any non-public network resource through the Common-Area Wi-Fi (including the Customer's management network, in-unit residential networks, or any Commercial Tenant network); (ii) host servers, run services that accept inbound connections from the public internet, or operate commercial workloads on the Common-Area Wi-Fi; (iii) loiter on the Common-Area Wi-Fi for extended periods solely to consume bandwidth; or (iv) use the Common-Area Wi-Fi to record, photograph, or surveil other persons in a manner that violates applicable law.

7.5 No Liability for Common-Area Use. Common-Area Wi-Fi is provided on an "as-is" basis. Neither Fiberlink nor the Customer is liable to Common-Area Users for outages, slowdowns, data loss, security breaches, or any harm arising from use of the Common-Area Wi-Fi. Common-Area Users use the network at their own risk.

7.6 Children and Common-Area Filtering. Where common areas are accessible to minors (community rooms, pool decks, fitness centers, after-school spaces, etc.), the Customer may request, by Service Order amendment, a CIPA-compliant filtered Common-Area SSID. Customer is responsible for posting appropriate signage where filtered service is provided.

8. COMMERCIAL TENANT USE

This Section 8 applies to a Commercial Tenant's use of Service delivered to a non-residential unit or commercial space at the Service Site, whether under a separate Service Order with the Commercial Tenant directly, a Commercial Service Addendum executed by the Customer on the Commercial Tenant's behalf, or other written authorization.

8.1 Commercial-Use Carve-Out. Subject to the prohibitions in Section 9 and the requirements of this Section 8, Commercial Tenants may use the Service for business purposes that would not be permitted on the residential bulk Wi-Fi Service, including (without limitation): (i) operating point-of-sale (POS) systems and payment terminals; (ii) hosting customer-facing guest Wi-Fi for the Commercial Tenant's own customers; (iii) hosting and accessing business servers, applications, and cloud workloads; (iv) running business VoIP, video conferencing, and unified-communications platforms; (v) accepting inbound connections on agreed-upon ports as configured by Fiberlink; and (vi) connecting business-grade equipment (security cameras, alarm systems, access controls, kiosks, digital signage, IoT devices, and the like). A Commercial Tenant requiring static IP addresses, port forwarding, dedicated bandwidth, or similar features shall arrange for the appropriate Service tier via Service Order amendment.

8.2 Commercial Tenant's Guest Wi-Fi. Where a Commercial Tenant offers its own customer-facing or guest Wi-Fi using the Service, the Commercial Tenant is responsible for: (i) configuring its guest Wi-Fi to be logically segregated from its business operational network; (ii) presenting appropriate acceptable-use terms to its own guests; (iii) complying with any applicable consumer protection, privacy, and notice laws (including but not limited to CIPA where children may be present); and (iv) the conduct of its guests using such Wi-Fi. The Commercial Tenant's offering of guest Wi-Fi is not a prohibited resale under Section 5.5 but is also not a sublicense of Fiberlink's Services; the Commercial Tenant remains the responsible party.

8.3 Payment Card and Regulated Data. A Commercial Tenant that transmits, stores, or processes payment card data, personally identifiable information (PII), protected health information (PHI), or other regulated data is solely responsible for compliance with all applicable laws and standards, including PCI-DSS, HIPAA, GLBA, state privacy laws, and analogous foreign laws. Fiberlink provides transport-layer connectivity only and does not provide compliance certifications for any Commercial Tenant's downstream environment unless expressly stated in a Service Order.

8.4 Business Continuity and SLA. Service-level commitments to Commercial Tenants are governed by the SLA in Exhibit A to the T&Cs and any applicable Commercial Service Addendum. Commercial Tenants that require enhanced SLA, redundant connectivity, dedicated bandwidth, or business-continuity-grade Services shall procure the appropriate tier via Service Order. Commercial Tenants should not rely on bulk shared Wi-Fi for mission-critical operations.

8.5 Security Obligations. Commercial Tenants shall maintain commercially reasonable security practices, including: (i) network firewalls between the Commercial Tenant's internal network and any guest or customer-facing network; (ii) up-to-date endpoint security on business devices; (iii) prompt patching of business systems; (iv) reasonable access controls; and (v) incident-response capability. Commercial Tenants shall promptly notify Fiberlink of any security incident that originates from or threatens the Service.

8.6 Servers and Inbound Connections. Operating publicly-accessible servers (web, mail, file, application, game, or otherwise) is permitted for Commercial Tenants on appropriate Service tiers and is not permitted for Residential Tenants or Common-Area Users. The Commercial Tenant remains responsible for the security, lawful operation, and content of any server it operates using the Service.

9. PROHIBITED USES (ALL USERS)

The following uses of the Service are prohibited for all Users, regardless of category. Where a specific category is subject to additional or different rules, those rules are set forth in Sections 6, 7, or 8.

9.1 Illegal Conduct

Any activity that violates federal, state, local, or international law, including (without limitation) fraud, wire fraud, identity theft, securities violations, money laundering, sanctions violations, illegal gambling, illegal drug sales, sex trafficking, or unlawful pornography. All Users shall comply with applicable U.S. export-control laws (EAR) and OFAC sanctions.

9.2 Child Sexual Abuse Material (CSAM)

Any transmission, storage, distribution, possession, or display of child sexual abuse material, or any content that sexually exploits or endangers minors, is strictly prohibited and will result in immediate termination of Service without prior notice. Fiberlink will report such activity to the National Center for Missing & Exploited Children (NCMEC) and to applicable law enforcement as required by 18 U.S.C. § 2258A and other applicable law.

9.3 Intellectual Property Infringement

Any infringement or misappropriation of intellectual property rights, including copyrights, trademarks, service marks, trade secrets, patents, rights of publicity, and rights of privacy. Fiberlink complies with the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512, and may suspend or terminate Service to repeat infringers in accordance with Section 12.

9.4 Network Abuse and Security Violations

Any activity that interferes with, disrupts, degrades, or threatens the security or integrity of Fiberlink's network, the Customer's network, the in-unit network of another Residential Tenant, the network of a Commercial Tenant, or the network of any third party. Prohibited activities include: (i) unauthorized access or attempted unauthorized access to systems, accounts, networks, or devices ("hacking"); (ii) port scanning, vulnerability scanning, packet sniffing, or other reconnaissance directed at systems the User does not own or is not authorized to test; (iii) denial-of-service (DoS or DDoS) attacks; (iv) introducing or

distributing malware, viruses, worms, trojans, ransomware, spyware, or rootkits; (v) credential stuffing or brute-force attacks; (vi) evasion of authentication, rate-limiting, or other technical controls; and (vii) any violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030).

9.5 Lateral Access Between Networks

Users shall not attempt to scan, probe, access, or interact with: (i) any Residential Tenant's in-unit network from outside that unit; (ii) any Commercial Tenant's business network without that tenant's express authorization; (iii) the Customer's property-management network; or (iv) Fiberlink's management, infrastructure, or monitoring networks. The internal segmentation of the network is enforced by Fiberlink for the protection of all Users.

9.6 Spam and Unsolicited Communications

Sending unsolicited bulk email, commercial email, text messages, robocalls, or other electronic communications in violation of CAN-SPAM (15 U.S.C. § 7701 et seq.), TCPA, or other applicable laws. Operating an open SMTP relay, an open proxy, or sending email with forged or falsified headers is prohibited. Harvesting email addresses, phone numbers, or other personal information without consent is prohibited.

9.7 Harmful, Harassing, or Threatening Content

Using the Service to transmit, post, or disseminate content that is defamatory, libelous, threatening, harassing, abusive, hateful, or that incites violence, including content directed at protected groups. Cyberstalking, doxxing, and non-consensual intimate imagery (revenge pornography) are prohibited.

9.8 Excessive or Abusive Bandwidth Use

Bulk fiber Wi-Fi is a shared resource. Activity that consumes a disproportionate share of network resources or that degrades service for other Users at the Service Site is prohibited, including: (i) cryptocurrency mining or other commercial-scale compute workloads on a residential or common-area connection; (ii) operating high-traffic commercial-scale public servers from a residential connection; (iii) sustained 24/7 peer-to-peer seeding at maximum throughput; and (iv) any other activity that materially impairs network performance for other Users. The line between intensive personal use (permitted) and commercial-scale abuse (not permitted) is determined by Fiberlink in its reasonable discretion based on observed network impact.

9.9 Tampering with Provider Infrastructure

No User shall move, modify, repair, reconfigure, replace, splice into, attach unauthorized equipment to, or otherwise interfere with Provider Infrastructure (as defined in the T&Cs), nor permit any third party to do so. This includes interference with access points in common areas, wiring in risers and conduits, network equipment in telecom closets, and equipment at the demarcation point of any unit. Damage to Provider Infrastructure caused by a User is the financial responsibility of the Customer, who may seek recovery from the responsible User.

9.10 Forging, Spoofing, and Identity Misrepresentation

Forging, spoofing, or misrepresenting message headers, source IP addresses, MAC addresses (other than for legitimate privacy purposes such as MAC randomization), sender identity, or return paths. Impersonating any person or entity, including Fiberlink personnel, Customer staff, or other Users.

9.11 Facilitation of Violations

Advertising, transmitting, distributing, or making available any software, service, or instruction designed to violate this AUP, including spam tools, DDoS-for-hire services, credential-cracking tools, or piracy tools.

9.12 Off-Premises Sharing

Extending, retransmitting, or sharing the Service to locations off the Service Site, to neighboring properties, or to persons not authorized by the Customer is prohibited. This includes high-gain antennas, mesh extensions that reach beyond the Service Site, and similar arrangements.

10. PRIVACY OF COMMUNICATIONS

10.1 General Principle. Fiberlink does not, as an ordinary practice, monitor the content of private communications transmitted over its network. Fiberlink monitors network performance, traffic patterns, security events, and metadata for purposes of operating, maintaining, securing, and improving the Services.

10.2 When Fiberlink May Inspect Content. Fiberlink will inspect the content of a specific User's communications only when: (i) required by law, court order, subpoena, or other valid legal process; (ii) reasonably necessary to investigate a specific complaint of AUP violation; (iii) reasonably necessary to protect the security or integrity of the network or the safety of any person; or (iv) the User has consented.

10.3 Customer Does Not Receive Tenant Content. The Customer is the contracting party for the Service but is NOT entitled to receive the content of Residential Tenant or Commercial Tenant communications. Fiberlink will not provide Customer with access to the contents of Tenants' internet usage. Fiberlink may, on Customer's reasonable request and where consistent with applicable law, provide aggregated or anonymized network statistics, unit-level uptime data, common-area usage statistics, and similar operational information.

10.4 No Inherent Security. No internet communication is fully secure. Users should use TLS, VPNs, end-to-end encryption, and other appropriate security measures for sensitive communications. Fiberlink is not responsible for the security of content transmitted by Users over the Services.

10.5 Common-Area Logging. As noted in Section 7.1, Common-Area Users have a reduced privacy expectation and Fiberlink and the Customer may log connection metadata for the Common-Area Wi-Fi.

11. CHILDREN AND CIPA COMPLIANCE

Fiberlink recognizes that MDU properties typically include households with minor children and that common areas may be accessible to minors. By default, Fiberlink does not filter content for residential units; parental controls are the responsibility of the Residential Tenant (Section 6.5). For common-area spaces accessible to minors, the Customer may request a CIPA-compliant filtered SSID (Section 7.6). For

Commercial Tenants providing services to minors (such as a childcare facility or after-school program), the Commercial Tenant is responsible for any filtering required by law.

12. COPYRIGHT AND DMCA NOTICE PROCEDURE

Fiberlink complies with the Digital Millennium Copyright Act. Copyright owners or their authorized agents may submit notices of alleged infringement to Fiberlink's designated agent:

Fiberlink MDU, LLC — DMCA Designated Agent
Email: dmca@fiberlinkmdu.com

Mail: 1846 Apple Tree Lane, Bethlehem, PA 18015, Attn: DMCA Agent

A proper DMCA notice must include: (i) a physical or electronic signature of the copyright owner or authorized agent; (ii) identification of the copyrighted work claimed to have been infringed; (iii) identification of the material claimed to be infringing and sufficient information to locate it (URL, IP address, etc.); (iv) contact information for the complaining party; (v) a statement that the complaining party has a good-faith belief that the use is not authorized; and (vi) a statement, under penalty of perjury, that the information in the notice is accurate and that the complaining party is authorized to act on behalf of the copyright owner. Misrepresentations may subject the sender to liability under 17 U.S.C. § 512(f). Fiberlink reserves the right to suspend or terminate Service to any User or Customer who is the subject of repeated, valid notices of copyright infringement.

13. REPORTING ABUSE AND SECURITY ISSUES

Reports of AUP violations should be directed to:

- Abuse reports: abuse@fiberlinkmdu.com
- Copyright (DMCA) notices: dmca@fiberlinkmdu.com
- Security vulnerabilities and responsible disclosure: security@fiberlinkmdu.com
- General support: support@fiberlinkmdu.com

Fiberlink welcomes good-faith security research conducted in accordance with reasonable responsible-disclosure practices. Researchers who identify vulnerabilities in Fiberlink-managed systems should report them to security@fiberlinkmdu.com before any public disclosure and should not access data they are not authorized to access. Fiberlink will not pursue legal action against researchers who act in good faith and in accordance with this policy.

14. ENFORCEMENT

14.1 Investigation. Fiberlink may investigate suspected violations of this AUP and may, in the course of investigation, review traffic logs, metadata, and (where permitted under Section 10) communication content. The Customer shall reasonably cooperate with Fiberlink's investigations as required under Section 5.3.

14.2 Tiered Response. Fiberlink's response to AUP violations is generally proportional to the severity, recurrence, and risk of the violation. Available actions include: (i) notice to Customer and, where appropriate, to the responsible User; (ii) blocking specific traffic, ports, or protocols; (iii) rate-limiting or throttling the offending User, unit, or Common-Area device; (iv) suspending Service to a specific dwelling unit, Common-Area access point, Commercial Tenant connection, or User; (v) suspending or terminating the Service Order in accordance with the T&Cs; (vi) reporting to law enforcement; and (vii) preserving evidence in response to legal process.

14.3 Cure Periods. For non-emergency violations, Fiberlink will use commercially reasonable efforts to provide notice and an opportunity to cure before suspending or terminating Service. Cure periods typically are: (i) forty-eight (48) hours for User-specific violations; (ii) the periods set forth in the T&Cs for Customer-level breaches; and (iii) reasonable periods for Commercial Tenant violations as set forth in the applicable Commercial Service Addendum.

14.4 Emergency Suspension. For violations posing imminent risk to the network, the safety of any person, or third-party rights — including CSAM, active DDoS attacks, active malware distribution, credible threats of violence, or ongoing fraud — Fiberlink may immediately suspend the affected unit, access point, or Service without prior notice. Fiberlink will notify the Customer as soon as reasonably practicable thereafter.

14.5 No Obligation to Monitor. Nothing in this AUP obligates Fiberlink to monitor User activity, screen content, or police compliance. Fiberlink's decision not to take action in any particular instance does not waive its right to take action in the future.

15. DISCLAIMERS

No one party owns or controls the internet. Fiberlink cannot verify, warrant, or vouch for the accuracy, quality, legality, or appropriateness of information that Users may obtain through the Services. Some material available on the internet is sexually explicit, violent, false, fraudulent, or otherwise objectionable. Fiberlink does not endorse, recommend, or take responsibility for any content transmitted, received, or accessed through the Services.

THIS AUP IS PROVIDED IN CONJUNCTION WITH THE T&Cs AND DOES NOT EXPAND, MODIFY, OR DIMINISH ANY WARRANTY, DISCLAIMER, LIMITATION OF LIABILITY, OR INDEMNIFICATION PROVISION IN THE T&Cs. NOTHING IN THIS AUP CREATES ANY ADDITIONAL INDEMNIFICATION OBLIGATION OR LIABILITY BEYOND THAT SET FORTH IN THE T&Cs.

16. GOVERNING LAW AND DISPUTES

This AUP is governed by the laws of the Commonwealth of Pennsylvania, without regard to conflict-of-laws principles. Disputes arising from this AUP are subject to the dispute resolution provisions of the T&Cs (Article 12), including binding arbitration in Lehigh County, Pennsylvania.

17. CONTACT

Fiberlink MDU, LLC

1846 Apple Tree Lane, Bethlehem, PA 18015

General: support@fiberlinkmdu.com

Abuse: abuse@fiberlinkmdu.com | DMCA: dmca@fiberlinkmdu.com | Security: security@fiberlinkmdu.com