Attachment F to Spectrum Enterprise Commercial Terms of Service

Secure Dedicated Fiber Internet Service ("SDFI Service")

Secure Dedicated Fiber Internet. If Customer elects to receive the SDFI Service, Spectrum shall provide Customer with a dedicated, scalable internet connection along with routing, security features, and VPN capabilities over a packet-based infrastructure between Customer's Service Location identified on a Service Order and Spectrum's facilities.

SDFI, or features of SDFI, may not be available in all service areas. Spectrum's SDFI is "On-Net" if it is provided by Spectrum to Service Locations through the Spectrum Network. Spectrum may, in its discretion, provide Customer with "Off-Net" services to geographic locations that are outside of Spectrum's service area or are not currently connected to the Spectrum Network through third party service providers. In addition, certain non-facilities-based services provided by third parties may be offered to Customer by Spectrum ("Third Party Services"). Third Party Services and Off-Net Services may be subject to additional terms and conditions.

Customer's use of the SDFI Service is subject to the following additional terms and conditions:

1. SDFI Service Speeds

Spectrum shall use commercially reasonable efforts to achieve the Internet speed attributable to the bandwidth for the SDFI Service selected by Customer on the Service Order, however, actual speed, also known as throughput rate, may vary. Many factors affect speed experienced by Customer as outlined in Spectrum's Network Management Practices.

2. Bandwidth Management

Spectrum shall have the right, but not the obligation, to (a) monitor traffic on its Network; and (b) monitor Customer's bandwidth utilization as Spectrum deems appropriate to efficiently manage the Spectrum Network.

3. Managed Devices

a) Spectrum shall provide Customer with one or more managed device(s) providing various network functions at Customer's Service Location(s) across Customer's network. Customer and End Users are responsible for the provision of power (including any back-up power) at all Service Locations and End User locations (as applicable) in order for Customer and its End Users to utilize the SDFI Service. If power at a Service Location, End User location, or for the Managed Device suffers degradation or is unavailable for any reason, then the Service at such location, or with respect to such managed devices, may be degraded or inoperable.

b) SDFI may include software, firmware, and hardware components supplied by Spectrum or third parties. Spectrum is not the manufacturer or supplier of any software, firmware or hardware components of the SDFI Service. Spectrum may update SDFI Service from time to time based on manufacturer-provided updates.

4. Acceptable Use Policy

Customer shall comply with the terms of Spectrum's Acceptable Use Policy ("AUP") found at https://enterprise.spectrum.com (or the applicable successor URL) and that policy is incorporated by reference into this Service Agreement. Customer represents and warrants that Customer has read the AUP and shall be bound by its terms as they may be amended, revised, replaced, supplemented or otherwise changed from time-to-time by Spectrum with or without notice to Customer. Spectrum may suspend Service immediately for any violation of the Spectrum AUP.

5. DDoS Protection Services

a) This Section only applies if Customer elects to purchase Distributed Denial of Service ("DDoS") Protection Service, which is only available for purchase in conjunction with Spectrum's SDFI Service. The DDoS Protection Service enables detection of DDoS attacks and provides related mitigation services. Spectrum monitors Customer Internet traffic as it traverses the Spectrum Network to detect anomalies that are symptomatic of a volumetric DDoS attack, as reasonably determined by Spectrum (a "DDoS Attack"). Spectrum requires that Customer: (i) provide information regarding Customer's Internet traffic before Spectrum can provision the DDoS Protection Service and (ii) cooperate with Spectrum to conduct mitigation testing in order to activate the DDoS Protection Service. After DDoS Protection Service activation, Spectrum will monitor Customer's Secure SDFI network traffic flow for variations to the baseline traffic patterns. When the DDoS Protection Service detects an anomaly that is symptomatic of a DDoS Attack, Spectrum will notify the Customer. The DDoS Protection Service and associated countermeasures are configured to reduce disruption of Customer's legitimate traffic, but Customer may experience slower Internet traffic speed during a DDoS Attack. Spectrum will remove the countermeasures and redirect Customer's inbound

network traffic to its normal path once Spectrum determines that the DDoS Attack has ended and there is no activity symptomatic of a DDoS Attack for a minimum of 4 hours. Customer may request status updates and reports from Spectrum. Customer may designate whether Spectrum is to provide "Proactive" or "Reactive" mitigation services as further described below. If Customer has designated Proactive mitigation, Customer may switch to Reactive mitigation, and if Customer designated Reactive mitigation, Customer may switch to Proactive mitigation, at any time during the Initial Order Term. Spectrum will use commercially reasonable efforts to implement Customer's change request within five (5) business days of receipt of Customer's request.

b) DDoS Proactive Mitigation Services.
If Customer designates Proactive mitigation services, following service activation, Spectrum will automatically implement countermeasures upon Spectrum's detection of a DDoS Attack.

c) DDoS Reactive Mitigation Services
If Customer designates Reactive mitigation services, Customer understands that Spectrum will not automatically initiate any DDoS countermeasures unless and until a Customer representative calls Spectrum to notify Spectrum that Customer may be experiencing a DDoS Attack. If Spectrum has an existing ticket indicating detection of a DDoS Attack, Spectrum will use commercially reasonable efforts to initiate countermeasures within 15 minutes.

d) Customer Requirements
DDoS Protection Services are only available in connection with Spectrum's On-Net SDFI Service and are not available in all locations. Spectrum's DDoS Protection Service is provided on an SDFI connection by SDFI connection basis. In the event Customer has more than one SDFI connection advertising the same IP address(es), Customer is required to purchase DDoS Protection Service for each SDFI connection. Spectrum's ability to provide the DDoS Protection Services is contingent on (i) Customer providing accurate and timely information to Spectrum, including IP addresses and (ii) Customer-provided equipment and software being compatible with the DDoS Protection Service as determined by Spectrum in its sole discretion.

e) Disclaimers. Customer acknowledges the following additional terms for the DDoS Protection Services:

i. SPECTRUM DOES NOT SUPPORT, AND SHALL HAVE NO OBLIGATION TO PROVIDE, MITIGATION WITH RESPECT TO IPv6.

ii. DDoS mitigation only mitigates the effects of certain types of DDoS attacks and is not designed as a comprehensive security solution. When Customer Internet traffic is traveling over the Spectrum Network, Spectrum makes no guarantees that only DDoS attack traffic will be prevented from reaching the destination or that only legitimate traffic will reach Customer.

iii. Spectrum makes no warranty, express or implied, that: (1) with respect to DDoS Protection Service, all DDoS attacks will be detected; (2) DDoS Protection Service will successfully mitigate the incident, including without limitation if the DDoS attack generates a traffic volume that exceeds the amount of traffic that Spectrum can divert; or (3) the DDoS Protection Services will be uninterrupted or error-free.

f) Termination

If Customer terminates any SDFI Service for which Customer has also subscribed to DDoS Protection Service for any reason other than Spectrum's material, uncured breach, then Customer shall be deemed to have terminated the corresponding DDoS Protection Service and Customer shall pay any applicable Termination Charges in accordance with the Service Agreement.

6. Data Center Cross Connect
A "Cross Connect" shall mean a connection between two networks within a data center. If Spectrum needs to connect its Network to Customer's network within a data center or to a third-party's network within a data center to deliver SDFI Service to Customer, then a Cross Connect will be required where an external network-to-network interface (ENNI) connection is not used/unavailable. In such case, Customer may obtain the Cross Connect from the data center operator to make the connection to Spectrum's Network or Customer can request that Spectrum purchase and coordinate installation of the Cross Connect, and if Spectrum agrees, Customer must execute a Service Order reflecting the applicable MRC and any OTC.