Attachment F to Commercial Terms of Service (Enterprise)

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 in conjunction with Spectrum SDFI Service or another provider's internet access service (in the case of Always On Service as explained below), and Spectrum offers the following DDoS Protection Service options with respect thereto.

i. DDoS Protection – Detect and Mitigate. DDoS Protection - Detect and Mitigate Service is for use with Spectrum's SDFI Service, Dedicated Fiber Internet ("DFI") Service, or Enterprise Internet ("EI") Service. It enables detection of DDoS Attacks (defined below) and mitigation countermeasures. Spectrum monitors Customer Internet traffic entering the Spectrum Network to detect anomalies symptomatic of a volumetric DDoS attack, as reasonably determined by Spectrum (a "DDoS Attack"). Once a DDoS Attack is identified, countermeasures (including data scrubbing of "dirty traffic") are initiated automatically, unless Customer directs Spectrum otherwise. Customer has access to a self-service portal to review after-event summary information.

ii. DDoS Protection – Always On. DDoS Protection – Always On Service is for use with Spectrum's SDFI Service, DFI Service or EI Service, or with another provider's internet access service (provided that Customer has at least one DFI or SDFI circuit with Spectrum). DDoS Protection – Always On Service enables continuous detection and

mitigation of DDoS attacks on internet circuits to which it applies. All inbound traffic to Customer's designated IP address block is routed through a DDoS scrubbing center to detect and deploy counter measures against volumetric or application-based DDoS attacks, as reasonably determined by Spectrum

b) General; Customer Requirements. DDoS Protection Service and countermeasures are designed to reduce disruption of Customer's legitimate traffic. However, Customer may experience slower Internet traffic speed during a DDoS attack. Spectrum will remove countermeasures and restore normal traffic flow after determination that the DDoS attack has ended. DDoS Protection Services are not available in all locations. DDoS Protection Service is provided on an connection by connection basis. In the event Customer has more than one connection advertising the same IP address(es), Customer is required to purchase DDoS Protection Service for each connection. Spectrum's ability to provide DDoS Protection Service 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.

c) Disclaimers. Customer acknowledges and agrees that:

i. 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.

ii. 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.

d) Termination. If Customer terminates an SDFI Service for which Customer has also subscribed to a 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.