LUMEN MANAGED PREMISES FIREWALL SERVICES SCHEDULE

1. General. This Service Schedule ("Schedule") is applicable only where Customer orders CenturyLink Managed Premises Firewall Service ("Service") and any of the Service features listed below. "Lumen" or "CenturyLink" is defined for purposes of this Service Schedule as CenturyLink Communications, LLC d/b/a Lumen Technologies Group or its affiliated entities providing Services under this Service Schedule. The Service is subject to and governed by the Master Service Agreement or other service agreement executed between Lumen and Customer, and if none, Lumen's standard Master Service Agreement located at https://www.lumen.com/en-us/about/legal/business-customer-terms-conditions.html which Lumen may update from time to time (the "Agreement"). This Schedule replaces the former Managed Security Services Service Schedule for managed devices on premises (aka MSS-Premise). In the event of any conflict between the terms of the Agreement and this Schedule, this Schedule will control.

2. Definitions. Any capitalized terms used in this Schedule and not otherwise defined will have the meaning set forth in the Agreement.

"Advanced Change" means any change that is not a Basic Change and an additional Order may be required to complete an Advanced Change.

"Basic Changes" are changes that do not directly impact Customer's overall product.

"Customer Provided CPE" means hardware, software, and other tangible equipment and intangible computer code it may contain that is provided, configured, deployed and managed by Customer and/or its designee. Customer is responsible for installing any software, whether Customer or CenturyLink provided, on Customer Provided CPE.

"Event" means any security abnormality detected by the Service and reported by the IDS/IPS feature. An Event does not necessarily constitute an actual security incident and must be investigated further to detect its validity.

"Excused Outage" will also mean, for purposes of this Schedule, the Service Levels will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under the applicable Service Level, for (i) failure of Customer CPE or any other failure or malfunction of equipment, applications, public internet, network or systems not owned, controlled or provided by, or attributable to CenturyLink; (ii) Customers' actions or omissions (including but not limited to not releasing the Service for testing/repair, failure or to provide timely approvals or consents, failure to provide and maintain current contact information and escalation lists; (iii) force majeure events; (iv) Regularly Scheduled Maintenance or emergency maintenance; (v) CenturyLink's lack of access to the Customer premises where reasonably required to restore any equipment, internet, network, or systems owned or controlled by CenturyLink and necessary to provide the Service; or (vi) Customer is in breach of its obligations under the Agreement or this Schedule.

"Incident" means any single Event or collection of Events that have been evaluated and deemed a security threat.

"Portal" means the Service specific web-based portal to which Customer will have access in order to monitor Customer's traffic and view Events.

"Regularly Scheduled Maintenance" means any scheduled maintenance performed to the Service. Regularly Scheduled Maintenance will not normally result in Service interruption. If Regularly Scheduled Maintenance requires an interruption, CenturyLink will: (a) provide Customer seven (7) days' prior written notice, (b) work with Customer to minimize such interruptions, and (c) use commercially reasonable efforts to perform such maintenance between midnight and 6:00 a.m. local time where the Service is located on which such maintenance is performed and. Emergency maintenance may be performed on less or no notice.

"Service Unavailability" is when Service is unable to pass traffic for reasons other than an Excused Outage.

"SOC" means CenturyLink security operations center.

3. Service Description. Premises Firewall Service, referred to as Managed Security Services on an Order, is a security service that manages and monitors traffic, utilizing the Managed Firewall described below, between the Internet and Customer's separately purchased CenturyLink MPLS/IP VPN network, CenturyLink IQ® Networking Private Port, CenturyLink Internet services, or third-party Internet services. CenturyLink continually makes improvements to the Service and reserves the right to make any updates, error corrections, bug fixes, and other feature changes or modifications to any software, equipment or hardware utilized by CenturyLink to provide the Services, at any time. CenturyLink will use reasonable efforts to make changes during Regularly Scheduled Maintenance.

3.1 Service Features. The Service features described below are included with the Service or if noted may be purchased for an additional cost:

(a) Managed Firewall. Managed firewall, which may also appear as "firewall" in an Order, provides monitoring of Customer's web and file transactions using a unified threat management (UTM) device installed, managed, and monitored by CenturyLink on Customer's premises. CenturyLink Managed firewall (i) uses template-based firewall configurations to filter inbound and outbound traffic; and (ii) creates security logs that provide reports of corporate web activity and malicious content blocked. Security logs are only retained for a limited period of time. If the logs are available, Customer may request a copy for an additional charge.

(b) For an additional cost, Customer may purchase the following features:

- **Intrusion Detection and Prevention ("IDS/IPS").** The IDS/IPS feature of the Service monitors Customer's network traffic on a 24x7 basis for attack and misuse signatures. IDS detects and monitors web and network transaction activities for suspicious and/or malicious traffic or policy violations and, if detected, provides electronic alerts via the Portal. IPS is a network security/threat prevention tool that examines network traffic flows to help prevent vulnerability exploits. The IPS policy consists of a set of signatures, each of which has a severity and has a defined action to "pass," "alert" or "block."

- **Web Content Filtering.** The Content Filtering feature is designed to classify and block known malicious URLs from affecting Customer's environment. "Good" URLs are categorized to help enable Customer to apply Internet usage policies.

- **Antivirus.** Antivirus feature provides monitoring of the antivirus service elements of a UTM device that are intended to block malicious software over the following protocols: HTTP, FTP, IMAP, POP3, SMTP. CenturyLink will install and manage an antivirus policy for a single virtual domain. Network antivirus does not include quarantine. Application Control is included that enables visibility and user to set controls over numerous applications (e.g. social media, file sharing applications).

- **Antispam.** Antispam feature provides monitoring of the antispam service elements of a UTM device that are intended to tag or block email messages identified as probable unsolicited bulk email or "spam". CenturyLink will install and manage an antispam policy for a single virtual domain.

4. Equipment. Any equipment including any firewalls, intrusion detection devices, servers, and/or modems, and including the UTM devices provided by CenturyLink as part of the Services will be located on a Customer site. Upon expiration or termination of the Service Term, Customer will promptly return any equipment to CenturyLink in good working order (ordinary wear and tear excepted). If Customer fails to do so, Customer agrees to pay CenturyLink the equipment's fair market value (if the same is not returned to CenturyLink within thirty (30) days of the date of termination) or the cost to repair the firewall (if the same is returned to CenturyLink other than in good working order (ordinary wear and tear excepted)).

5. Charges and Customer Delays. Charges for the Service include: (i) non-recurring charges ("NRC") for installation and change requests, (ii) monthly recurring charge(s) ("MRC") for Service features Customer selects, and (iii) any additional charges as may be set forth in the Order. CenturyLink may install and invoice Service features contained in an Order separately.

Customer agrees to pay and/or reimburse CenturyLink for fees, costs and/or expenses related to or resulting from (i) any unreasonable delays or omissions in Customer's performance of its obligations to enable the Service, and/or (ii) additional installation or subsequent work required to be performed, caused by (a) Customer's request for changes (except as set forth in the Change Management section of this Schedule) to the applicable Service unless such change is due to an act or omission of CenturyLink, or (b) any other actions or omissions by Customer which materially affect CenturyLink's ability to perform its obligations hereunder. Charges for certain Services are subject to (a) a property tax surcharge and (b) a cost recovery fee per month to reimburse CenturyLink for various governmental taxes and surcharges. These charges are subject to change by CenturyLink and will be applied regardless of whether Customer has delivered a valid tax exemption certificate. For additional details on taxes and surcharges that are assessed, visit http://www.centurylink.com/taxes.

If CenturyLink partially installs or activates a Service, CenturyLink reserves the right to commence billing on a pro rata basis, and if a Service installation is delayed, incomplete or is not usable by Customer through no fault of CenturyLink or its agents, CenturyLink will commence billing as installed and per the Service Commencement Date.

6. Change Management. Customer may request logical changes to the Service by raising a MACD (Move, Add, Change, Delete) request via a ticket through the Portal. The SOC will review the request and will advise whether the change is a Basic Change or an Advanced Change (with an associated charge).

The Basic/Standard Service package includes five (5) Basic Changes per month per instance without charge. Basic Changes exceeding five (5) may be subject to a charge of $250, or local currency equivalent, per change.

7. Customer Responsibilities and Restrictions.

7.1 Customer Security Contacts. Customer will designate one primary and up to two additional Customer security contacts and provide email and telephone contact details for each contact (the "Customer Security Contacts"). Customer will assure the Customer Security Contacts and all associated details are accurate and current at all times and that at least one Customer Security Contact is available to be contacted by the SOC at any given time (24x7x365). CenturyLink will only accept, discuss or make changes to the Service with the registered Customer Security Contacts or via the Portal. Requests for changes to the list of Customer Security Contacts must be made by an existing Customer Security Contact.

7.2 Access to Managed Devices and Customer Sites. Customer agrees to provide CenturyLink with prompt, reasonable and safe access to any applicable Customer sites necessary for CenturyLink to provide the Service and to comply with any reasonable physical and environmental requirements as may be identified by CenturyLink. Customer is required to provide hands on assistance for the purposes of troubleshooting and/or diagnosing technical difficulties.

7.3 CenturyLink Provided IP Addresses and Domain Names. In the event that CenturyLink assigns to Customer an IP address as part of the provision of the Service, such IP address will (upon CenturyLink's request and to the extent permitted by law) revert to CenturyLink after termination of the applicable Order for any reason whatsoever, and Customer will cease using such address. At any time after termination, CenturyLink may re-assign the IP address to another user. In the event that CenturyLink obtains a domain name for Customer (which may be required in some jurisdictions), Customer will be the sole owner of such domain name. Customer will be

solely responsible for: (i) paying any associated fees (including renewal fees); (ii) complying with any legal, technical, administrative, billing or other requirements imposed by the relevant domain name registration authority; and (iii) modifying the domain name in the event Customer changes service providers. Customer will indemnify, defend and hold CenturyLink (and its employees, affiliates, agents and subcontractors) harmless from any and all third-party claims, losses, liabilities and damages, including reasonable attorney's fees) relating to or arising from Customer's use of domain names as described in this Schedule (including claims for intellectual property infringement).

7.4 Third-Party IP Addresses and Networks. If (i) any of the IP addresses identified by Customer as part of the Service are associated with computer systems owned, managed, and/or hosted by a third-party service provider ("Third-Party Provider") or (ii) any Customer equipment or any other computer systems to be monitored as part of the Service are part of a network owned, managed and/or otherwise controlled by, or collocated on premises owned, managed, and/or otherwise controlled by a Third-Party Provider, Customer warrants that it has and will maintain, the consent and authorization from such Third-Party Provider(s) necessary for CenturyLink (and its affiliates, agents and vendors) to perform all elements of the Service, including but not limited to any vulnerability scanning of the Third-Party Provider networks that may be reasonably necessary as part of the provision of Service. Customer agrees to facilitate any necessary communications and exchanges of information between CenturyLink and the Third-Party Provider(s). Customer will indemnify, defend and hold CenturyLink (and its employees, affiliates, agents and subcontractors) harmless from and against any and all third party claims, losses, liabilities and damages, including reasonable attorney's fees, arising out of Customer's breach of its warranties or obligations in this Section.

7.5 Third Party Software. If any third-party software or agent, including any corresponding documentation, is required in connection with the Service, Customer agrees to use the third party software strictly in accordance with all applicable licensing terms and conditions, including any click to accept terms required as part of the download/install process. Customer acknowledges and agrees that it is solely responsible for selecting and ensuring that Customer provided software and systems, including third party software, is up to date and supportable. Customer's failure to do so may result in CenturyLink's inability to provide the Services and CenturyLink will have no liability therefrom, including for missed Service Levels.

7.6 Customer's Security Policies. Customer acknowledges that CenturyLink implements security policies at Customer's reasonable direction. Customer maintains overall responsibility for maintaining the security of Customer's network and computer systems. Customer acknowledges that notwithstanding anything in this Schedule, the Service is not a warranty against malicious code, deleterious routines, and other techniques and tools employed by computer "hackers" and other third parties to create security exposures.

7.7 Customer Network. Customer acknowledges that Customer network is Customer's sole responsibility. CenturyLink may provide Customer with guidelines for minimum system requirements, compatibility, and other information necessary to use the Service, and Customer is responsible for making any required changes to its network environment in order to utilize the Service.

7.8 Customer Change Notifications. Customer will provide CenturyLink with 5 Business Days' advanced notice by the submission or update of a critical server ticket through the Portal regarding any changes to the network or firewall environment. If advance notice cannot be provided, Customer is required to provide CenturyLink with such notification of changes within 7 Business Days of said network changes.

7.9 If Customer or CenturyLink detects the Service is being affected by a continuing error, conflict or trouble report, or similar issue (in each case a "Chronic Problem") caused by the Customer, Customer will resolve any Chronic Problem by taking whatever steps are deemed necessary to rectify the same, including, but not limited to: (i) removing or modifying the existing Service configuration (or requesting CenturyLink to remove the same); (ii) making changes to Customer's network in order to adhere to CenturyLink's guidelines in order to utilize the Service; (iii) changing or replacing Customer's equipment or licensing and maintaining third party software required for the Service; (iv) failure of the access medium used by Customer to connect to Customer's Internet or IPVPN, including failing to assure adequate bandwidth to support the Service. If Customer has not remedied the Chronic Problem within 30 days of request by CenturyLink, then CenturyLink may suspend or terminate the Service.

7.10 Unless Customer requests otherwise and CenturyLink agrees, CenturyLink will store the security log files for a rolling 90 days and make the security logs available to Customer in the Portal. In the event any such security log files contain personal data, CenturyLink will not use such personal data except as necessary to provide the Service and provide relevant information to Customer. CenturyLink will not undertake any additional security measures for log files containing personal data.

7.11 Personal Data. Customer and CenturyLink acknowledge that it may be necessary to provide the other party with certain personal data necessary for the performance of each party's obligations under this Schedule, such as business contact information and credentials to access the applicable Portal(s). The parties acknowledge and agree that each is a data controller in its own right with respect to any such personal data exchanged under this Schedule, and any such personal data is provided on a controller-to-controller basis. Any personal data exchanged under this Schedule will be limited solely to the extent necessary for the parties to perform their obligations or exercise their rights under this Agreement. As used in this Schedule, the terms "personal data" and "controller" will have the meanings ascribed to them in applicable data protection laws, including, without limitation, the European Union General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"). Each party will be independently and separately responsible for complying with its obligations as a controller under applciable data protection laws in its capacity as a data controller with respect to the personal data it provides to the other party and/or receives from the other party.

CenturyLink personnel will not access or attempt to access personal data that is processed via the operation of the Service. Processing is typically carried out at machine-level and CenturyLink will not retain any copies of data longer than necessary to perform the applicable Service or perform under the Agreement.

7.12 Acknowledgement. Customer acknowledges that, by virtue of providing the Service, CenturyLink and its third party suppliers may need to process or transfer log data or information in connection with performance of Services wherever CenturyLink and/or its third party suppliers do business, including outside the European Economic Area (EEA), and use processors and permitted subprocessors (including personnel and resources) in locations worldwide. Customer further acknowledges that CenturyLink has no obligation to back up and store any Customer metrics or log related data beyond the 90 day rolling time period detailed in this Schedule and after Agreement expiration or termination at which time CenturyLink will automatically delete all logs. Customer acknowledges and consents that it is solely Customer's responsibility to make copies of or obtain the logs obtained from the firewall services prior to expiration or termination.

7.13 Firewalls and devices, including any software on such devices, will be maintained and serviced only by or at the specific direction of CenturyLink. Customer will not (and will not permit any third party to) use, combine, modify, open, move, service (or attempt to service) or in any way interfere with a firewalls or other equipment or software provided by CenturyLink except as expressly permitted in writing by CenturyLink.

7.14 International Services. For Services provided outside the United States, Customer or its local affiliate may be required to enter into a separate local country addendum/agreement (as approved by local authorities) ("LCA") with the respective CenturyLink affiliate that provides the local Service(s). Such CenturyLink affiliate will invoice Customer or its local affiliate for the respective local Service(s).

8. Modification or Termination of Premises Firewall Services by CenturyLink. CenturyLink reserves the right to modify any features or functionalities of the Service upon 90 days' prior notice to Customer. In the event that such modification materially or detrimentally affects the features or functionality of the Service, then Customer, as its sole remedy, may notify CenturyLink of such impact and if CenturyLink cannot remedy within 30 days, then Customer may cancel the affected Service without termination liability with 60 days' advanced written notice. Additionally, in such case, CenturyLink will notify Customer via e-mail of termination of the affected Service and Customer will not be billed for the terminated Service.

9. Portal. Customer is responsible for maintaining the confidentiality of and protecting access to all usernames and passwords it creates or assigns (collectively, "Credentials") and is solely responsible for all activities that occur under the Credentials, including access to content. Customer agrees to notify CenturyLink promptly of any actual or suspected unauthorized use of any Credentials. CenturyLink reserves the right to terminate upon notice any Credentials that CenturyLink reasonably determines may have been accessed or used by an unauthorized third party. A monthly recurring charge will apply to any Customer users in excess of ten (10). Customer's primary Customer Security Contact will be given access to the Portal in order to facilitate access to reports regarding the Service and to facilitate the placing of change orders. The Service uses two-factor authentication ("2FA") for access to the portal. CenturyLink will provide Customer up to three security two-factor authentication tokens ("2FA Tokens") for access to the Portal. Customer will accept and comply with the End User Rules of Use associated with the 2FA Tokens. The 2FA tokens will be disabled for accounts that have not been active in more than six (6) months requiring such users to request new tokens if they wish to reestablish access. Access to the Portal's security areas is restricted to the authorized Customer Security Contacts. All information received by the Customer from CenturyLink through the Portal's security areas is deemed "Confidential", is solely for Customer's internal use and may not be re-distributed, resold or otherwise transmitted outside of Customer's organization.

10. Intellectual Property. The Service and CenturyLink provided software, and all copyrights, patent rights and all intellectual property rights are the sole and exclusive property of CenturyLink or its third-party provider or licensor(s). Customer is hereby provided a non-exclusive, limited, non-transferrable, personal, revocable (at CenturyLink's sole discretion), non-sublicenseable, non-assignable right to access and/or use the CenturyLink provided software or third party provided software solely in accordance with the Service; *provided, however*, Customer will not reverse engineer, disassemble, decompile, or otherwise attempt to derive the source code of the CenturyLink provided software except to the extent that applicable law prohibits reverse engineering restrictions, nor will Customer remove any disclaimers, copyright attribution statements or the like from the CenturyLink provided software and any breach of this Section will automatically result in termination of the license granted.

11. Disclaimer/Liability.

11.1 Disclaimer. Customer acknowledges the Services endeavor to mitigate security Events, but Events may not always be identified and if identified may not be mitigated entirely or rendered harmless. Customer further acknowledges that it should consider any particular Service as just one tool to be used as part of an overall security strategy and not a warranty of security. The Service provided under this Schedule is a supplement to Customer's existing security and compliance frameworks, network security policies and security response procedures, for which CenturyLink is not, and will not be, responsible. While CenturyLink will use reasonable commercial efforts to provide the Services hereunder in accordance with the SLA, the Services are otherwise provided "as-is". CENTURYLINK MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED, THAT THE PERFORMANCE OF THE SERVICES WILL RENDER CUSTOMER'S SYSTEMS INVULNERABLE TO SECURITY BREACHES, THAT ANY SOFTWARE PROVIDED BY CUSTOMER WILL BE COMPATIBLE WITH THE SERVICE AND/OR THAT CENTURYLINK'S RECOMMENDATIONS, ASSESSMENTS, TESTS, REPORTS OR MONITORING WILL BE ACCURATE, COMPLETE, ERROR-FREE, OR EFFECTIVE IN ACHIEVING CUSTOMER'S SECURITY AND/OR COMPLIANCE RELATED OBJECTIVES. Neither CenturyLink or its vendors will be liable for any damages or liabilities however classified including third party claims which Customer or third parties may incur as a result of: (i) non-compliance with any standards which apply to Customer, and/or (ii) reliance upon (or implementation of recommendations from) results, reports, tests, or recommendations related to the Services; or (iii) loss or corruption of data or information transmitted through the Service. Customer's sole remedies for any non-performance, outages, failures to deliver or defects in Service are contained in the Service Levels and Chronic Problem Sections.

11.2 Direct Damages. Except for the payment and indemnification obligations of Customer, subject to the Damages Limitations provision in the Agreement or similar waiver of consequential damages provision and notwithstanding any cap on direct damages as may be set forth in the underlying Agreement, the total aggregate liability of each party arising from or related to a claim will not exceed in the

aggregate (for all Services provided under this Schedule) the total MRCs, NRCs, and usage charges paid or payable to CenturyLink for the affected Services under this Schedule in the six months immediately preceding the first event giving rise to the cause of action ("Damage Cap").

12. Resale Restriction. Notwithstanding anything to the contrary in the Agreement, Customer is prohibited from reselling any Service provided pursuant to this Schedule without the express written consent of CenturyLink.

13. Service Level Agreement ("Service Levels" or "SLA"). The Service Levels are not available until completion of Service Validation. Whether a Service issue constitutes a Service Level outage or failure for Service credit purposes will be determined by CenturyLink as supported by records, trouble tickets, data and other evidence, including through the use of third party monitoring tools. Credits are only available against the MRC for the affected Service. Service Levels do not apply to Excused Outages, periods of Suspension or to Chronic Problems.

13.1 Availability. The Service will be available to pass traffic 99.9% of the total hours during every calendar month. For any day in which CenturyLink fails to meet the availability, response time, and notification and/or resolution Service Levels above, Customer will be entitled to a service credit equal to 1/30th of the MRC of the affected Service at the applicable Customer site. The service credit cannot exceed 1/30th of such MRC in any day.

13.2 Response Time Service Level Objectives ("Response Time SLOs). CenturyLink continuously monitors all firewalls and provides on-site maintenance and repair once CenturyLink has detected a firewall has experienced a failure. The on-site coverage is as follows:

- Next Business Day Response Time SLO with advanced replacement repair coverage and on-site coverage options available at each Customer site varies by country.
- Four Hour Response Time SLO is available for an additional charge, where available, but requires separate contract documents to be executed.

For purposes of this Schedule, "Business Day" means Monday through Friday.

13.3 Security Event Monitoring – Notification and Resolution SLA. If Customer's package does not include IDS/IPS or if the Customer has disabled the IDS/IPS feature, this section does not apply. Customer may view the Event detail (including timestamp, Event name, attack type) on the Portal.

(a) Incidents. If CenturyLink's systems alert the SOC that an Event or series of Events may impact the security of Customer's network, a SOC analyst will analyze the Event(s) to detect if an Incident has occurred. If CenturyLink detects an Incident has occurred, CenturyLink will submit a trouble ticket on Customer's behalf. Customer may also submit a trouble ticket if it believes an Incident has occurred. CenturyLink determines how Incidents are classified through the use of signature priorities, algorithms, event correlation, and professional judgment. CenturyLink reserves the right to modify the categories and classifications of Incidents. CenturyLink supports a notification Service Level and a resolution Service Level, as set forth below.

(b) Notification. If CenturyLink submits the trouble ticket on Customer's behalf, CenturyLink will notify the Customer Security Contacts by phone or email (as agreed upon between the parties) of the occurrence of Incidents (i) within 15 minutes of CenturyLink classifying the Incident as Critical and (ii) within 30 minutes of CenturyLink classifying the Incident as High. If Customer submits the trouble ticket, there is no notification Service Level.

(c) Resolution. CenturyLink will use reasonable efforts to achieve the resolution timeframes for Incidents as identified below. All timeframes start upon CenturyLink's validation and confirmation from Customer that action is necessary.

Event Monitoring and Notification Table

Priority Level	Target Resolution Time
Priority 1 – Critical A Network or application attack that has rendered Customer's network inoperable or that poses an imminent threat of compromise.	Within 15 minutes of classification via telephone or email
Priority 2 – Major A Network or application attack that has caused essential applications or functionality to be significantly impaired.	Within 30 minutes of classification via telephone or email
Priority 3 – Minor An internal, unforeseen Customer network or application security issue or industry vulnerability.	Via weekly report
Priority 4 – Other*	Via weekly report

A non-time sensitive reported security issue. An informational request that may be explained in Portal FAQs, but nonetheless Customer would like to speak about the issue. This includes tuning requests.	

* For Low priority Incidents, these metrics are service objectives only. No service credits or other remedy will apply for failure to achieve these objectives.

13.4 Service Credits. For any day in which CenturyLink fails to meet the availability, response time, and notification and/or resolution Service Levels above, Customer will be entitled to a service credit equal to 1/30th of the MRC of the affected Service at the applicable Customer site. The service credit cannot exceed 1/30th of such MRC in any day.

13.5 Limits. If the Service is used in conjunction with CenturyLink provided MPLS, CenturyLink IQ Networking Private Port, Internet and/or Managed Network Services, Service Levels for those services are subject to separate Service Schedules. Notwithstanding anything to the contrary, in no event will the aggregate service credits available in this Schedule in any month exceed the 100% of the MRCs for Services provided during the month.

13.6 General Terms for all Service Levels. To be eligible for credits, Customer must be current in its obligations, and Customer must contact CenturyLink Billing Inquiries via the contact information provided on their invoice, open a ticket in the Portal or contact their account manager to report any issue for which Customer thinks a Service Level may apply within 30 calendar days after the issue occurs. Credits will only apply against the applicable MRC for the affected Service, and will not apply to any other services provided by CenturyLink. Duplicative credits will not be awarded for a single failure, incident or outage. The Service Level credits and termination rights stated in this Schedule will be Customer's sole and exclusive remedies with respect to any service failure or outage.

Version: March 18, 2026