LUMEN NETWORK FIREWALL SERVICE SCHEDULE

1. General. This Service Schedule is applicable only where Customer orders Network Firewall Service ("Network Firewall Service") which may be designated as "Enterprise Security Gateway" (ESG), "Adaptive Network Security" (ANS), or "Network Based Security" (NBS), and related features as further described below in the Order, Order acceptance, service delivery, billing and related documents (collectively, the "Services"). "Lumen" is defined for purposes of this Service Schedule as CenturyLink Communications, LLC d/b/a Lumen Technologies Group and 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"). Terms used but not defined in this Service Schedule will have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this Service Schedule, this Service Schedule will control.

1.1 Additional General Terms. 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 Lumen affiliate that provides the local Service(s). Such Lumen affiliate will invoice Customer or its local affiliate for the respective local Service(s).

2. Services. Network Firewall Service is a security service that manages and monitors traffic between the Internet and Customer's separately purchased Lumen MPLS/IP VPN network, Lumen IQ® Networking Private Port, Lumen Internet services, or third-party Internet services. Lumen 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 Lumen to provide the Services, at any time. Lumen will use reasonable efforts to make changes during Regularly Scheduled Maintenance. Customer must purchase at least one (1) Lumen provided MPLS/IP VPN port to utilize ANS Site with Secure Access Cellular Service. MPLS/IP VPN is sold under separate terms and conditions.

2.1 Service Features. The following additional service features may be purchased by Customer:

(a) Firewall. Firewall provides monitoring of Customer's web and file transactions using a unified threat management (UTM) device installed by Lumen within a Gateway. Firewall uses template-based firewall configurations to filter inbound and outbound traffic. The Firewall feature also 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) Intrusion Detection and Prevention ("IDS/IPS"). The IDS/IPS feature 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 firewall 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 firewall policy consists of a set of signatures, each of which has a severity and has a defined action to "pass," "alert" or "block."

(c) Content Filtering. 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.

(d) Application Awareness and Control with ANS Premium. Application Awareness and Control is a feature that (1) enables visibility to traffic passing through the firewall using advanced application identification, (2) provides controls by enforcing selected firewall policies based on application identification.

(e) Data Loss Prevention ("DLP"). The DLP feature scans or filters outbound traffic to detect potential data ex-filtration transmissions. DLP is designed to monitor, detect, block information designated as sensitive by the Customer, and alert Customer to take action.

(f) Anti-Malware Sandboxing. Anti-Malware Sandboxing analyzes files by looking for malicious indicators, including host changes, outbound traffic, and attempts to bypass anti-virus analysis. If detected, a signature to address the threat is created and implemented.

(g) Adaptive Network Security Mobility. Adaptive Network Security Mobility may be delivered by Secure Sockets Layer Virtual Private Network ("SSL VPN") or by IPSEC. Delivery by SSL VPN requires an Internet connection and a standard SSL enabled web browser. If delivered by SSL VPN, Adaptive Network Security Mobility securely provides access to Customer's internal network for remote users and allows Customer's end users to remotely connect to Customer's network. At the external port, the URL directs the traffic to Customer's appropriate network access point. If delivered by IPSEC, Customer's or the applicable end user is required to license and install Endpoint Client Software on the end user's work station. Lumen is not responsible for issues caused by the installation or use of the Endpoint Client Software on Customer devices. Export restrictions must be followed for encryption technology. Adaptive Network Security Mobility provides an encrypted layer 3 connection into Customer's network.

(h) Log Streaming. Log Streaming is an optional feature available with certain Service package types as determined by Lumen that allows Customers to receive logs and security event data at Customer's designated infrastructure destination for third party event monitoring and in-house analytics.

Customer acknowledges that Log Streaming service must be setup over an encrypted session. This Log Streaming feature requires Customer to provide Lumen with a digital SSL certificate to be loaded on to Log Streaming platform in order for the traffic to be sent over an encrypted session. Customer is responsible for configuring Customer's SIEM (Security Information and Event management) platform

and network environment to allow, accept and store logs and/or security events transmitted by Lumen. The Log Streaming feature delivers Event notifications for up to 2 Customer provided SIEM or IP addresses. Customer acknowledges that Event notifications sent to the SIEM are delivered over the Internet and such delivery may fail due to Internet connectivity issues outside of Lumen's control. Customer, and not Lumen is responsible for storage of the logs received; however, Lumen has the ability to send/resend buffered logs if needed for up to 14 days. Customer acknowledges and agrees that Log Streaming is provided "as-is" and "as available" and Lumen will have no liability related to or arising from use by Customer of this feature.

(i) Visualization. Threat Visualization provides a fixed single portal view of the near real time threat landscape for Adaptive Network Security Basic and Premium Services. Customers can view interactions with malicious sites, but no automated actions are taken.

(j) Rapid Threat Defense. Rapid Threat Defense is available with the Adaptive Network Security Premium Service package, is an automated threat detection and response capability designed to detect and block threats based on Customer's defined Adaptive Network Security Firewall policies. The Customer selects a security posture based on threat risk score. When threats are discovered that meet or exceed the selected risk score, countermeasures designed to block or prevent access to the malicious entities are automatically deployed and augmented to Adaptive Network Security Firewall policies. Customers must set a security posture threshold for the automated response to take effect, except for Allow and Block IPv4 CIDR lists. These lists are independent of a security posture risk score settings and always take precedence on the ANS Firewall instance policy. Due to the varying nature of malicious activity, Lumen cannot guarantee that all malicious activities or sites intended to be blocked will be identified, detected and blocked. Customer acknowledges that Lumen is implementing actions at Customer's request and in accordance with Customer identified criteria and Lumen is not responsible for the effectiveness of the blocking of all offending sites or malicious activities. Customer's can view automated actions via Threat Visualization.

Customer networks with multiple Adaptive Network Security Gateway Firewall instances must enable Premium Service Level Package across all Gateway firewall instances. Failure to do so may result in the override of Customer owned and managed premises firewall policies with Rapid Threat Defense.

(k) Digital Certificate exchange. The Lumen Certificate Management System (CMS) platform is an automated, systematic and secure way for Customers to generate, store and place and/or change digital certificates on Lumen security devices. The CMS provides auditable security around the handling and storage of all digital key materials of Customer within a private container and security with an independent encryption key. Lumen provides a secure process to move the certificate from that secure storage to the security end device within Lumen's private management network, via a secure Transport Layer Security (TLS) protocol, endpoint connection validation, and role-based access control (RBAC) for the account used to authenticate the actions requested. The CMS feature is made available to Customer as a convenience and is provided "as-is" and "as-available" with no applicable SLA.

(l) ANS – Site. ANS – Site enables Customer to set up a network connection and establish an encrypted IPSEC tunnel across the Public Internet between the Customer remote location via configuration and deployment of a Customer owned or Lumen managed router or premises firewall, with aggregation through ANS to Customer's Lumen provided MPLS/ IP VPN, another ANS-Site with ANS Basic no Features, and/or the Public Internet with ANS Basic or Premium features.

ANS Site Remote Access IPSEC Non-Standard Encryption. ANS offers a remote access IPSEC Virtual Private Network (VPN) capability that enables Customer to build VPNs over the public internet by encrypting traffic between each VPN endpoint using IPSEC. When ordered by Customer, Lumen will configure and support a Lumen non-standard IPSEC VPN with no phase 2 encryption algorithm for the purpose of connecting to the Customer's contracted public cloud security provider. This type of IPSEC configuration does not encrypt the data traversing the VPN and is commonly referred to as an IPSEC NULL Encryption tunnel. As defined within RFC2410, NULL encryption is only suitable where data confidentiality is not a concern. Lumen is not responsible for any Customer security vulnerabilities or sub-standard performance over the encrypted tunnel due to the lack of phase 2 encryption at the ANS Gateway.

(m) Secure Access – Cellular: Secure Access Cellular ("collectively SAC") leverages third party cellular network connectivity and is established utilizing Lumen managed or customer-provided customer premises equipment (CPE) that includes: (1) external enterprise-class cellular to Ethernet bridge device; and (2) router to provide IPSEC connectivity to the Lumen network in a back-up only or failover situation to Lumen MPLS/IP VPN. Lumen provides SAC on a commercially reasonable efforts basis. Lumen does not make any commitment of levels of service, coverage or class of service over third party cellular service. Lumen managed router associated with SAC is subject to the separate terms of the Lumen Service Schedule for Managed Network Services. SAC is an optional configuration with an ANS Site.

2.2 Package Types. The two package types may be designated as "Basic," "Standard," "Premium," or "Unlimited" as applicable in the Order, pricing attachment, Order acceptance, service delivery, billing and related documents.

(a) Basic/Standard. The Basic/Standard package includes Firewall. If Customer orders a Basic ANS package, IDS/IPS is also included.

(b) Premium/Unlimited. The Premium/Unlimited package includes Firewall, IDS/IPS and DLP. If Customer orders an Unlimited NBS package, Content Filtering is also included. If Customer orders a Premium ANS package, Application Awareness Control is included.

2.3 Ala Carte Options. The following can be added as an ala carte option to a Service package where the option is not automatically included in the package:

- Content filtering.
- Anti-Malware Sandboxing (only available with ANS).

- Adaptive Network Security Mobilty (only available with ANS).

2.4 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 per change. If Customer purchases a Premium/Unlimited package, there is no limit on the number of Basic Change requests per instance.

2.5 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 Lumen in its good faith discretion 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 or periods of permitted suspension.

2.5.1 Availability. The Service will be available to pass traffic 99.9% of the total hours in a calendar month (the "Availability SLA"). Service Unavailability is calculated from the timestamp when Lumen opens a trouble ticket following the report of a problem by the Customer until the time the ticket is closed. For Service Unavailability, Customer will be entitled to a service credit off of the MRC for the affected Service based on the cumulative minutes of Service Unavailability in a calendar month.

If the aggregate Service Unavailability during a calendar month meets or exceeds the durations identified below, the following remedies will apply. Service Credits are based on the MRC of the affected Service.

Aggregate Service Unavailability Duration in a Calendar Month (hrs:mins:secs)	Service Level Credit
00:00:01 – 00:43:00 (99.9%)	No credit
00:43:01 – 04:00:00	10% of the MRC
04:00:01 – 08:00:00	15% of the MRC
08:00:01 – 12:00:00	20% of the MRC
12:00:01 – 16:00:00	25% of the MRC
16:00:01 – 24:00:00	30% of the MRC
24:00:01 or greater	35% of the MRC

2.5.2 Security Event Monitoring – Notification and Resolution. 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 Customer Portal.

(a) Incidents. If Lumen'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 determine if an Incident has occurred. If Lumen determines an Incident has occurred, Lumen will submit a trouble ticket on Customer's behalf. Customer may also submit a trouble ticket if it believes an Incident has occurred. Lumen determines how Incidents are classified through the use of signature priorities, algorithms, event correlation, and professional judgment. Lumen reserves the right to modify the categories and classifications of Incidents. Lumen supports a notification Service Level and a resolution Service Level, as set forth below.

(b) Notification. If Lumen submits the trouble ticket on Customer's behalf, Lumen 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 Lumen classifying the Incident as Critical and (ii) within 30 minutes of Lumen classifying the Incident as High. If Customer submits the trouble ticket, there is no notification Service Level.

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

Incident Resolution Table

Priority Level	Target Resolution Time Basic/Standard Packages	Target Resolution Time Premium/Unlimited Packages
Priority 1 – Critical A Network or application attack that has rendered Customer's network inoperable or that poses an imminent threat of compromise.	Within 2 hrs	Within 1 hr
Priority 2 – High A Network or application attack that has caused essential applications or	Within 4hrs	Within 2hrs

functionality to be significantly impaired.		
Priority 3 – Medium An internal, unforeseen Customer network or application security issue or industry vulnerability.	Within 10hrs	Within 6hrs
Priority 4 – Low* 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.	Within 24hrs	Within 12hrs

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

(d) Service Credits. For any day in which Lumen fails to meet the notification and/or resolution Service Levels for reasons other than an Excused Outage, Customer will be entitled to a service credit equal to 1/30th of the MRC of the Service at the applicable Customer site. The service credit cannot exceed 1/30th of such MRC in any day.

2.5.3 Limits. If the Service is used in conjunction with Lumen provided MPLS, Lumen 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 Service Schedule in any month exceed the MRCs for Network Firewall Services provided during the month.

2.5.4 General Terms for all Service Levels. To be eligible for credits, Customer must be current in its obligations, and Customer must contact Lumen 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 Lumen. Duplicative credits will not be awarded for a single failure, incident or outage. The aggregate credits in any calendar month will not exceed 100% of the MRC of the affected Service. The Service Level credits and termination rights stated in this Service Schedule will be Customer's sole and exclusive remedies with respect to any service failure or outage

3. Customer Responsibilities.

3.1 Charges and Customer Delays. Charges on the Order remain in effect during the Service Term and consist of the following: (i) a monthly recurring charge(s) ("MRC") for Service package type/Service element(s) and the bandwidth level Customer selects, (ii) one time, non-recurring charges ("NRC") for installation and change request pricing that may consist of: per ANS gateway firewall instance, shared security bandwidth across multiple use cases based on selected bandwidth, service level package, and optional features; ANS Mobility per set of concurrent users; and (iii) any additional charges as may be set forth in the Order. Adaptive Network Security Mobility requires an additional MRC based on the number of concurrent users. Lumen may install and invoice Service features contained in an Order separately. Adaptive Network Security – Site does not have an MRC nor NRC for remote access. If a Lumen-managed router or Secure Access Cellular is enabled with the remote site, an MRC and NRC will be associated with components.

Customer agrees to pay and/or reimburse Lumen 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 Service Schedule) to the applicable Service, or (b) any other actions or omissions by Customer which materially affect Lumen's ability to perform its obligations under this Service Schedule. Charges for certain Services are subject to (a) a property tax surcharge (or substantially similar local equivalent) and (b) a cost recovery fee per month to reimburse Lumen for various governmental taxes and surcharges. Such charges are subject to change by Lumen 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 www.lumen.com/taxes.

Customer understands and agrees that if Customer fails to take any actions required to enable Lumen to complete delivery of Service, then, 5 days following notice to Customer of Lumen's inability to complete full delivery due to Customer inaction, Lumen will commence billing and Customer will be obligated to pay Lumen for Service.

Customer will pay all applicable termination charges as set forth in the Agreement if termination occurs prior to expiration of the Service Term for the ANS Site with Secure Access Cellular Service. Notwithstanding anything to the contrary in the Agreement, if Customer cancels or terminates Secure Access Cellular Service for convenience or Lumen terminates the Service for cause, Customer will pay Lumen a termination charge equal to the sum of: (A) if prior to delivery of a Connection Notice, (i) any third party termination charges for the cancelled Service; (ii) the non-recurring charges for the cancelled Service; and (iii) Lumen's out of pocket costs (if any) incurred in deploying or constructing facilities necessary for Service delivery or (B) following delivery of a Connection Notice, (i) all unpaid amounts for Service actually provided; (ii) 100% of the remaining monthly recurring charges (if any) for months 1-12 of the Service Term; (iii) 50%

of the remaining monthly recurring charges for month 13 through the end of the Service Term; and (iv) to the extent not recovered by the foregoing, any termination liability payable to third parties by Lumen resulting from the termination.

3.2 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 ensure Customer Security Contacts and all associated details are accurate and current at all times and that at least one Customer Security Contact is reachable 24/7. Lumen 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.

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

3.4 Lumen Provided IP Addresses and Domain Names. If Lumen assigns Customer an IP address as part of the provision of Service, the IP address will (to the extent permitted by law) revert to Lumen after termination of the applicable Order for any reason whatsoever, and Customer will cease using the IP address. At any time after termination, Lumen may re-assign the IP address to another user. If Lumen obtains a domain name for Customer (which may be required in some jurisdictions), Customer will be the sole owner. Customer will be solely responsible for: (i) paying any associated fees (including renewal fees); (ii) complying with legal, technical, administrative, billing or other requirements imposed by the relevant domain name registration authority; and (iii) modifying the domain name if Customer changes service providers. Customer will indemnify, defend and hold Lumen (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 (including claims for intellectual property infringement).

3.5 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 necessary for Lumen (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 Lumen and the Third-Party Provider(s). Customer will indemnify, defend and hold Lumen (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.

3.6 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 Lumen's inability to provide the Services and Lumen will have no liability therefrom, including for missed Service Levels.

3.7 Lumen Provided Software. If any third-party software, or agent including any corresponding documentation, is required in connection with the Service, Customer agrees to use 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.

3.8 Customer Provided CPE. Customer may use Customer Provided CPE that is pre-approved by Lumen and supports Lumen's IPSec encryption method standards. All Customer Provided CPE must be up to date and subject to a current maintenance contract supported by the manufacturer. Customer is solely responsible for the installation, operation, maintenance, use and compatibility of Customer Provided CPE. Customer will cooperate with Lumen in setting the initial configuration for the Customer Provided CPE that interfaces with the Services and comply with Lumen's instructions. Customer's failure to comply with its obligations in this section may result in Lumen's inability to provide the Services and Lumen will have no liability therefrom, including for missed Service Levels. Router configuration, deployment and management will be provided by Customer unless Customer separately purchases those services from Lumen.

3.9 Customer's Security Policies. Customer acknowledges that Lumen 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 Service Schedule, the Service is not a guaranty against malicious code, deleterious routines, and other techniques and tools employed by computer "hackers" and other third-parties to create security exposures.

3.10 Customer Network. Customer acknowledges that Customer network is Customer's sole responsibility. LumenLu 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.

3.11 Customer Change Notifications. Customer will provide Lumen 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 Lumen with notification of changes within 7 business days.

3.12 Chronic Problems. Customer will resolve any Chronic Problem by taking whatever steps are deemed necessary to rectify the issue, including, but not limited to: (i) removing or modifying the existing Service configuration; (ii) making network changes in order to adhere to Lumen's guidelines; (iii) changing, maintaining or replacing Customer Provided CPE or other equipment or required for the Service; (iv) Lumen may suspend or terminate the Service if Customer has not remedied the Chronic Problem within 30 days of request by Lumen.

3.13 Vulnerability Testing with ANS. Lumen will permit Customer to perform, or to engage an independent third party to perform, at Customer's expense, vulnerability scanning against Adaptive Network Security service for the sole use of Customer to utilize firewall inspection services, remote access ANS Site and Adaptive Network Security Mobility services.

Customer's right to conduct vulnerability scanning is subject to the following limitations. Customer will: (i) restrict the vulnerability scanning to IP addresses Lumen has issued for Customer's sole use; (ii) restrict the scanning and enumeration of services installed to the sole purpose of identifying applications, open ports, and versions of software code in use; (iii) not under any circumstances exploit, or attempt to exploit in any way, any potential vulnerabilities identified by the vulnerability scan; and (iv) immediately stop scanning activity if instructed to do so by Lumen, and will not perform further scanning activity until notified by Lumen. Customer and Lumen will mutually agree on a vulnerability mitigation process.

3.14 For ANS – Site, Customer is responsible for adhering to Lumen's recommended IPSec encryption standards. If Customer does not adhere to our recommended standards, then Customer information over the encrypted tunnel may be compromised and exposed to more security vulnerabilities and malicious events as it traverses the internet before it is protected by the ANS service. Customer is solely responsible for all equipment and other facilities used in the connection with the ANS-Site which are not provided by Lumen.

3.15 For Secure Access – Cellular, Customer will not use SAC other than in support of backup to the Lumen provided MPLS/ IP VPN Services or ANS-Site primary access. Any use of SAC or components of equipment in any capacity other than support backup to Lumen MPLS or ANS-Site primary access will be a violation of this Service Schedule. Without limitation to Lumen's other remedies under the Agreement, Lumen reserves the right to charge, and Customer agrees to pay, for (i) any misuse of SAC or components, and/or (ii) for such usage in excess of Lumen's established data pool for Customer, separately at the rates then charged to Lumen by the third party cellular provider. Additionally, if Lumen provides Customer notice of such use of which Lumen becomes aware, Lumen may terminate SAC within 10 days of such notice if such use does not cease. Any use of SAC in a primary or non-backup manner will give Lumen the right to immediately suspend SAC and Customer will be liable to Lumen for any overage fees that may be charged to Lumen for use of SAC beyond a failover. Lumen is not responsible, however, for monitoring for such usage by the Customer. Customer, at Customer's expense, is responsible for returning the Lumen provided CPE to Lumen at the end of the Service Term.

4. Additional Service Limitations and Disclaimers.

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

4.2 Personal Data. Customer and Lumen acknowledge that it may be necessary to provide the other party with personal data or to access personal data of the other party as necessary for the performance of each party's obligations under the Agreement and/or this Service Schedule, including, but not limited to and where applicable, employees' and authorized representatives' names, business contact information, technical or operational data (such as online identifiers), credentials to access portals and other platforms made available by one party to the other and similar personal data. The parties acknowledge and agree that each is a controller with respect to any such personal data exchanged under the Agreement and/or this Service Schedule, and any such personal data is provided on a controller-to-controller basis. Any personal data exchanged in accordance with this Section will be limited to the extent necessary for the parties to perform their obligations or exercise their rights under the Agreement or this Service Schedule. As used in this Service Schedule, the terms "personal data," "processing," "processor" 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). 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. Unless otherwise set forth in the Agreement, Lumen 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 Lumen will not retain any copies of data longer than necessary to perform the applicable Service or perform under the Agreement. To the extent legally required, Customer and Lumen will enter into separate written agreements required to comply with laws governing the relationship between a controller and processor with respect to the processing of personal data described in this Section, including, without limitation, any agreements required to facilitate necessary cross-border personal data transfers. Customer will be responsible for notifying Lumen whether such written agreements are required based on the nature of the data being processed.

4.3 Customer acknowledges that Lumen 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 expiration or termination of the Service at which time Lumen will automatically delete all logs. Customer acknowledges and agrees that it is solely Customer's responsibility to make copies of or obtain the logs prior to expiration or termination.

4.4 Modification or Termination of Network Firewall Services by Lumen. Lumen reserves the right to modify any features or functionalities of the Service upon 90 days' prior notice to Customer. If the modification materially or detrimentally affects the features or functionality of the Service,Customer will, within 30 days of the change, notify Lumen of the material and detrimental impact and elect to

cancel the affected Service as its sole remedy and without termination liability upon 60 days' advanced written notice if Lumen does not remedy the material and detrimental impact within the notice period.

4.5 Portal. Customer's primary Customer Security Contact will be given access to the Portal in order to view Threat Visualization, Rapid Threat Defense security posture setting, log management, retention, standard reporting, and viewable firewall policy configurations regarding the Service, and also to facilitate the placing of change orders. Lumen 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. If Customer requests more than three 2FA Tokens, Lumen will provide the additional 2FA Tokens for an additional charge. Access to the Portal's security areas is restricted to the authorized Customer Security Contacts. All information received by the Customer from Lumen 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. For the avoidance of doubt, retention of logs and views in the Portal expire with the Service Term.

4.6 Intellectual Property. The Service and Lumen Provided Software, and all copyrights, patent rights and all intellectual property rights are the sole and exclusive property of Lumen or its third-party provider or licensor(s). Lumen grants Customer a non-exclusive, limited, non-transferrable, personal, revocable (at Lumen's sole discretion), non-sublicenseable, non-assignable right to access and/or use the Lumen 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 Lumen Provided Software, nor will Customer remove any disclaimers, copyright attribution statements or the like from the Lumen Provided Software and any breach of this Section will automatically result in termination of the license granted.

4.7 Disclaimer/Liability.

4.7.1 Disclaimer. Customer acknowledges that the Services endeavor to mitigate security Events, but Events may not always be identified and if identified may not be mitigated entirely, blocked 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 guarantee of security. The Service provided under this Service Schedule is a supplement to Customer's existing security and compliance frameworks, network security policies and security response procedures, for which Lumen is not, and will not be, responsible. While Lumen will use reasonable commercial efforts to provide the Services in accordance with the SLA, the Services are otherwise provided "as-is". LUMEN MAKES NO WARRANTY, GUARANTEE, 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 OR THAT GEOGRAPHICAL IP ADDRESSES WILL BE 100% ACCURATE, THAT ANY THIRD PARTY SOFTWARE PROVIDED BY CUSTOMER WILL BE COMPATIBLE WITH THE SERVICE AND/OR THAT LUMEN'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 Lumen or its subcontractors 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. Notwithstanding anything to the contrary in any Agreement, Lumen provides no indemnities or warranties on the Services.

4.7.2 Direct Damages. Except for the payment and indemnification obligations of Customer and subject to the Damages Limitations provision in the Agreement or similar waiver of consequential damages provision, the total aggregate liability of each party arising from or related to this Service Schedule will not exceed the total MRCs, NRCs, and usage charges paid or payable to Lumen for the affected Services under this Service Schedule in the six months immediately preceding the first event giving rise to the cause of action ("Damage Cap"). With respect to any Service provided to Customer under this Schedule that is provided for Customer's convenience at no charge, Lumen will not be responsible or liable for any damages whatsoever and Customer's sole liability as it is related to Services provided at no charge is to terminate the affected Service.

4.7.3 Additional Disclaimers. LUMEN DOES NOT REPRESENT OR WARRANT THAT THE SERVICE AND ANY SOFTWARE IS NON-INFRINGING, OR THAT IT WILL BE UNINTERRUPTED, ERROR-FREE OR VIRUS FREE, FREE FROM ERROR, THAT ANY DOCUMENTATION OR MATERIALS ARE COMPLETE OR THAT THE SERVICE OR SOFTWARE WILL MEET OR SUPPORT CUSTOMER'S BUSINESS REQUIREMENTS.

4.7.4 Resale and Premises Restrictions. Notwithstanding anything to the contrary in the Agreement, Customer is prohibited from reselling any Service provided pursuant to this Service Schedule and may only use the Service within Customer owned or controlled enviroments without the express written consent of Lumen.

5. Definitions.

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

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

"Chronic Problem" means a continuing error, conflict, trouble report, or similar issue (individual or collective) caused by the Customer that affects performance of the Service.

“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 Lumen 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 determine 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 Lumen; (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) Chronic Problems(iv) Regularly Scheduled Maintenance or emergency maintenance; (v) Lumen’s lack of access to the Customer premises where reasonably required to restore any equipment, internet, network, or systems owned or controlled by Lumen and necessary to provide the Service; (vi) 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; or (vii) Customer is in breach of its obligations under the Agreement or this Service Schedule.

“Gateway” means the physical location (e.g. gateway, POP) in the network that houses the Lumen equipment utilized to provide each instance of Service.

“Incident” means any single Event or collection of Events 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, Lumen 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.

Secure Access – Site: Secure Access Site enables Customer to set up a network connection and establish a secure tunnel across the Public Internet between the Customer’s remote location and the Customer’s Lumen provided IPVPN network, via configuration and deployment of managed routers. Secure Access Site may be designated as “Secure Internet Access” or “No Firewall “ or “ANS Basic No Features” in Customer Orders, Order acceptance, service delivery, billing and related documents.

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

“SOC” means Lumen security operations center.

Version: March 18, 2026