MANAGED SECURITY GATEWAY SERVICE ATTACHMENT

1. APPLICABILITY OF SERVICE ATTACHMENT AND SERVICE OPTIONS.

1.1 Applicability. This Managed Security Gateway Service Attachment sets forth the terms and conditions of Lightpath's Managed Security Gateway ("**MSG**") service (the "**Service Attachment**"). MSG is designed, configured, and installed on a designated port(s) on the Service Equipment which will be the point of demarcation for providing the Service to Customer (the "**Demarcation Point**"). Unless otherwise defined herein, all capitalized terms in this Service Attachment will have the same meaning as defined in the Standard Service Agreement. By signing the Service Order, Customer agrees to the terms of this Service Attachment.

1.2 Service offering: MSG provides security features and is offered in two (2) options, Managed Security Gateway Service (basic) or Managed Security Gateway Service with Unified Threat Management ("**UTM**").

1.2.1 Managed Security Gateway Service (basic).

a. Basic firewall (aka stateful firewall) with Network Address Translation
   i. Allows traffic initiated from LAN (outbound traffic).
   ii. Lightpath will configure Customer's firewall to allow outbound traffic.
   iii. Lightpath will carry out configuration changes to Customer's Layer 3 firewall on request, where necessary.
   iv. If Lightpath accepts a request from Customer to alter its firewall policy, Customer accepts responsibility for these changes.
   v. Lightpath will provide a standard security configuration template for MSG, however, Customer will own and will be responsible for this configuration, including any changes or additions that Customer requests Lightpath to make to its configurations and policies.

1.2.2 Managed Security Gateway Service with UTM.

a. Next generation firewall (aka stateful firewall)
   i. Layer 3 firewall as indicated above and Layer 7 firewall with the ability to specify IP addresses (L3) or applications (L7) that should be blocked or allowed.
   ii. Layer 7 firewall with application control - Layer 7 firewall allows the ability to set rules to block specific web-based services, websites, or types of websites without having to specify IP addresses or port ranges. Note that Lightpath automatically blocks certain categories by default to ensure the security of the Lightpath Network. Customer may request a list of blocked categories, however, note that any list is subject to change.
   iii. Geo-based firewalls offering the ability to block or allow traffic to or from different countries (e.g. traffic from North Korea).

   Lightpath is not responsible for how the applications are categorized, the regularity of updates or for evaluating which applications fall under each category.
b. Site-to-site VPN
   i. Interconnecting devices using IPSec or other tunnelling protocols (single WAN link).
c. Application control
   i. The ability to view the different traffic transported by the network (i.e., Salesforce, O365, YouTube, etc.) and being able to prioritize applications (e.g., give business applications priority over YouTube).
   ii. Traffic shaping offering the ability to limit the amount of bandwidth available for a type of traffic (e.g., limit the amount of bandwidth that YouTube can consume).
d. Client VPN
   i. The ability for mobile devices (PC, tablets, phones) to connect to the MSG device via the Internet using IPsec or other tunnelling protocols (remote access for mobile employees). Mobile device configurations are not supported.
e. Content Filtering
   i. The ability to block access to different categories of website or individual websites (e.g., adult content, non-education content). Note that Lightpath automatically blocks certain categories by default to ensure the security of the Lightpath Network. Customer may request a list of blocked categories, however, note that the list is subject to change.
      - Lightpath will provide Content Filtering in two modes: the full list mode or the top sites only mode. Lightpath will set Customer's default configuration to the full list mode for better coverage.
      - Customer may choose to switch settings to the top sites only setting after the initial installation.
   ii. To block access to sites that employ https rather than http Customer must change to the full list mode. Customer understands that it is not possible to return an explanatory page to a user where the URL filtering element has blocked an https based website.
   iii. Lightpath is not responsible for how the applications are categorized, the regularity of updates or for evaluating which applications fall under each category.
f. Advanced Malware Protection Service ("AMP")
   i. AMP scans software transported in the data stream that enters the MSG device to check if they are malicious. Malicious software can be either reported, or blocked and reported.

- AMP inspects http file downloads and block or allow file downloads based on their disposition by using a file reputation based protection engine; and
- AMP determines the disposition of a file as "clean," "malicious" or "unknown" using the threat intelligence retrieved from Cisco AMP.

ii. Customer may white list specific URLs and files upon request. Customer may also disable the AMP option entirely upon request.

iii. Customer will be responsible for the configuration and any changes made to the AMP option and any increased risk of being exposed to malicious content.

iv. Use of AMP may result in false positives where a file or URL that Customer deems safe is blocked. Lightpath is not liable when false positives occur and result in legitimate files or URLs being blocked.

g. Intrusion Detection and Protection System

i. IDS/IPS analyses traffic using rules to identify a wide range of traffic patterns that match known threats. Attacks can be just reported or blocked and reported.

ii. IDS/IPS will:

- monitor traffic passing through the MSG Service to identify traffic patterns that match known threats, in accordance with the applicable intrusion signature files currently using Cisco Sourcefire SNORT® Engine;
- implement this monitoring of traffic with a default configuration setting, including a standard signature list which currently works using Cisco Sourcefire SNORT® Engine;
- not be responsible for evaluating the signatures beforehand;
- select the "balanced" ruleset as Customer default detection setting. "Balanced" ruleset contains rules that are from the current year and the previous two (2) years, are for vulnerabilities with a CVSS (Common Vulnerability Scoring System) score of nine (9) or greater. Traffic will be automatically blocked if it is detected as malicious based on the detection ruleset set out here.
- agree to alter the setting from "prevention" to "detection" or "disabled" upon Customer's request. If "detection" mode is selected, the MPV will no longer block traffic patterns which match known threats and only identify them, and if "disabled" mode is selected, no prevention or detection will take place; and
- not pro-actively or reactively investigate or act upon detected or prevented threats or attacks.

iii. Use of Intrusion Prevention may result in false positives where certain applications and traffic flows may cause the feature to block legitimate traffic (e.g. applications not adhering to network communication standards). Lightpath will not be liable if false positives occur and as a result, legitimate traffic is blocked.

iv. If Lightpath agrees to a request from Customer to alter the parameters for applying new signatures to give a greater or lower sensitivity to attacks, Customer will be responsible for the outcome of these changes and accept the potential increased risk of false positives (blocks to legitimate traffic) or the increased risk of threats being missed. This includes whitelisting a specific intrusion detection signature or changing Customers ruleset from 'balanced' to a different mode.

1.3 Security Settings and Configuration.

a. Lightpath will configure Customer's compatible MSG device with a templated set of security policies.
b. Customer will own and will be responsible for this templated configuration, including any changes or additions that Customer asks Lightpath to make to Customer's security configurations and policies.
c. Lightpath will not vet or assess any changes to Customer's security configuration that Customer asks to be made.
d. Lightpath is not responsible for the total security of Customer's network, user devices, connection or Internet traffic.
e. Lightpath will make Customer-desired configuration changes upon Customer's request.
f. Lightpath will implement requested configuration changes during normal business hours with the intent to complete them by the end of next business day.
g. Lightpath may charge Customer for configuration changes if Lightpath considers that the number or frequency of such changes are excessive. Both parties will agree on pricing for any configuration changes before implementation.

1.4 Acceptable Use Policy. Customer will use the Service in compliance with the most current version of Lightpath's Acceptable Use Policy posted at https://lightpathfiber.com/acceptable-use-policy, which is incorporated herein by reference.

1.5 Resale Restrictions. Customer is not permitted to resell, charge, loan, transfer or otherwise dispose of the Service (or any part thereof) to any third party without the prior written consent of Lightpath.

1.6 Utilities. Customer will make available to Lightpath adequate space, power, air conditioning and all other applicable utilities for Service Equipment at the Customer Location at its sole cost.

2. SERVICE DESIGN AND IMPLEMENTATION.

2.1 Installation. MSG solution is cloud based offering simple installation along with remote management via the secure web portal access. Portal provides view only access to visibility with detection and prevention of real time threats and malicious activities while also logging information about ongoing activities to identify repetitive threats. MSG provides automated basic reporting of

security events as long as contact information is provided and configured into the portal and also provides extensive dashboards to review and manage configuration and network activities as well as a "real time view only" of the current configuration and network activities.

2.2 Term. MSG is offered on a minimum three (3) year term.

2.3 Lightpath Responsibilities

a. Conduct Customer assessment with the Customer's technical staff to ascertain security requirements.
b. Ensure site is set up correctly for delivery of MSG. Note that Lightpath is not response for the building or the LAN readiness.
c. Provide 24x7x365 Customer Support.
d. Remotely access MSG device as required to provide change control or troubleshooting.

2.4 Customer Responsibilities

a. Complete pre-installation Questionnaire form including content categories for Customer's ordered service, as applicable.
b. Customer will provide authorized contacts "Admin" identifying responsible persons to work with Lightpath on:
   i. Service Activation/Turn-up/ configuration and ongoing management and maintenance of MSG;
   ii. Billing/Administrative issues;
   iii. Fault / Trouble shooting management to end users.
c. Customer will provide the technical resources necessary to insure implementation and testing of MSG during acceptance testing, at time of turn-up and during the fault management process.
d. Customer must have Internet Service from Lightpath.
e. Customer will appoint a technical single point of contact to manage first line of fault management.
f. In the event of breakage, Customer will be responsible to return, via return label, faulty MSG devices. Replacement MSG devices will be shipped directly to the Customer.
g. Submit change requests, as desired, in the provided format to Customer Support at care@lightpathfiber.com. Lightpath will action the configuration changes during normal business hours and complete it by the end of next business day.
h. Customer retains responsibility for any requested configuration changes.

2.5 Training. Customer will be provided access to web-based training free of charge which provides training on monitoring, analytics, and remote trouble shooting.

3. SERVICES LEVEL AGREEMENT.

3.1 Service Level Agreement. Lightpath provides specific remedies regarding the performance of Service as set forth in the Service Level Agreement attached hereto as Exhibit A. Customer's sole and exclusive remedy for any Service Outage will be the issuance of Service Credits in accordance with Exhibit A. The term **"Service Outage"** means an interruption, delay, or outage in the transmission of the Services between the Demarcation Point and the Service Network.

4. MAINTENANCE AND REPAIR.

4.1 Configuration Changes.

4.1.1 Configuration Changes. Lightpath may charge Customer for configuration changes if Lightpath considers that the number or frequency of such changes are excessive.

4.1.2 Exclusions. Customer is responsible for all end user support (Customer owned devices) and any devices connected to the MSG (i.e. workstations, printers, fax machines, camera's, etc.).

4.2 Service Issues. In the event that Customer experiences any Service-related issues, Customer may contact Lightpath through its Network Maintenance Center ("NMC") at +1 (866) 611 - 3434, which may be amended by Lightpath from time-to-time upon written notice to Customer. Upon receipt of notice of Service problems, Lightpath will initiate diagnostic testing to determine the source and severity of any degradation of Service. If there is a Service Outage, Lightpath and Customer will cooperate to restore Service. If Lightpath dispatches a field technician to Customer Location to perform diagnostic troubleshooting and the problem resides with the Customer's Equipment or facilities or the failure is due to Customer's or end-user's acts or omissions or the acts or omissions of Customer's or end-user's invitees, licensees, customers or contractors, Customer will pay Lightpath for any and all associated time and materials at Lightpath's then-current standard rates.

4.3 Scheduled Maintenance. Lightpath will endeavor to conduct (or cause to be conducted) scheduled maintenance that is reasonably expected to interrupt Service outside of regular business hours during the maintenance window of 12:00 midnight and 6:00 a.m. local time or, upon Customer's reasonable request, at a time mutually agreed to by Customer and Lightpath. Lightpath will use

commercially reasonable efforts to notify Customer of scheduled maintenance that is reasonably expected to interrupt Service via telephone or e-mail, no less than ten (10) business days prior to commencement of such maintenance activities. Customer will provide a list of Customer contacts for maintenance purposes, which will be included on the Service Order, and Customer will provide updated lists to Lightpath, as necessary.

4.4 Emergency Maintenance. Lightpath may perform emergency maintenance in its reasonable discretion, with or without prior notice to Customer, to preserve the overall integrity of the Lightpath Network. Lightpath will notify Customer as soon as reasonably practicable following any such emergency maintenance activity that impacts the Service.

4.5 Other Emergency Actions. If Lightpath determines, in its sole discretion, that an emergency action is necessary to protect the Lightpath Network as a result of Customer's transmissions, Lightpath may block any such Customer transmissions that fail to meet generally accepted telecommunications industry standards. Lightpath will have no obligation or liability to Customer for any claim, judgment or liability resulting from such blockage. Lightpath will notify Customer as soon as practicable of any such blockage. The Parties agree to mutually cooperate to resolve the underlying cause of the blocking, comply with generally accepted telecommunications industry standards and restore the transmission path as soon as reasonably possible, with a completion goal of forty-eight (48) hours.

Exhibit A
Service Level Agreement

This Service Level Agreement ("SLA") covers the local transport area to the Lightpath Demarcation Point including Lightpath equipment associated with the endpoints. The provisions described below shall be Customer's sole and exclusive remedy in the event of a Service Outage.

MEAN TIME TO REPAIR

Lightpath's objective is a four (4) hour mean-time-to-repair ("MTTR").

SERVICE LEVEL GUARANTEE

Service Level Guarantee: If Customer detects a Service Outage, Customer shall open a trouble ticket with Lightpath's Network Management Center by calling 866-611-3434 or via the customer portal at alticebusiness.com. A Service Outage period begins when Customer reports a circuit/service failure, opens a valid trouble ticket and releases it for testing and repair. The controlling record for the purpose of determining the duration of the Service Outage and calculating credits shall be the date/time stamp on the trouble reporting ticket as generated by Lightpath's trouble reporting system. A Service Outage period ends when the circuit/service is operative.

a. If Customer reports a circuit/service to be inoperative but declines to release it for testing and repair, it is considered to be impaired, but not a Service Outage.
b. If a Lightpath technician is dispatched for a reported failure and it is determined that such failure is not within Lightpath's control, Customer will be subject to a truck roll fee for any subsequent dispatch/truck roll(s) requested.
c. Customer may request a credit, in writing, and reference the date of the ticket. Requests for credit must be submitted to Customer Support at care@alticeusa.com or 866-611-3434 within thirty (30) calendar days of the Service Outage.
d. For calculating credit allowances, every month is considered to have thirty (30) days.
e. A credit allowance is applied on a pro rata basis against the Monthly Recurring Charges for the affected circuit/service and is dependent upon the length of the Service Outage.

Lightpath shall credit Customer's Monthly Recurring Charges for the circuit/service experiencing the Interruption as follows:

Outage Duration	**Credit of Monthly Charges**
Less than 30 minutes	none
30 minutes up to but not including 3 hrs	1/10 of a day
3 hrs up to but not including 6 hrs	1/5 of a day
6 hrs up to but not including 9 hrs	2/5 of a day
9 hrs up to but not including 12 hrs	3/5 of a day
12 hrs up to but not including 15 hrs	4/5 of a day
15 hrs up to and including 24 hrs	1 day
Over 24 hours	2 days for each full 24-hour period

Chronic Service Outages: Defined as three (3) separate Service Outages of two (2) hours or more on the same facility, within a consecutive thirty (30) day period and/or a Service Outage that lasts longer than forty-eight (48) hours. In the event Customer experiences Chronic Service Outages in Service, Lightpath will perform a detailed investigation, report the findings to Customer and, if necessary, institute a corrective plan. If Customer experiences any additional Service Outages on the circuit and a plan for corrective action has been implemented for thirty (30) days, Customer may terminate the affected circuit/service without any further liability upon thirty (30) days prior written notice. Customer must exercise its option to terminate within thirty (30) days from the additional Service Outage and Customer waives the right to terminate if Customer does not exercise such termination right within such thirty (30) day period.

Limitations: Total credits in a given month shall not exceed fifty percent (50%) of the Monthly Recurring Charges for the affected circuit/service in that month. If an incident affects the performance of the Service and results in a period or periods of Service Outage, interruption, disruption or degradation in Service, entitling Customer to one or more credits under multiple service level standards, only the single highest credit with respect to that incident will be applied, and Customer will not be entitled to credits under multiple service level standards for the same incident.

No credit allowance will be made for:

a. Customer's (including its Affiliates, agents, contractors and vendors) negligence, intentional act, omission, default and / or failure to cooperate with Lightpath in addressing any reported Service problems, including failing to take any remedial action in relation to a Service as recommended by Lightpath, or otherwise preventing Lightpath from doing so;
b. Failure on the part of Customer Equipment, end-user equipment or Customer's vendor's equipment;
c. Election by Customer, after requested by Lightpath, not to release the Service for testing and repair;
d. Lightpath's inability to obtain access required to remedy a defect in Service;

e. Scheduled maintenance and emergency maintenance periods;
f. Scheduled upgrade of Service at the request of Customer;
g. Force Majeure Event;
h. Disconnection or suspension of the Service by Lightpath pursuant to a right provided under this Service Attachment, the Standard Service Agreement, or Service Order;
i. Lightpath's inability to repair due to utility safety restrictions; and / or
j. No trouble found or where the fault of the trouble is undetermined.