

## SERVICES ADDENDUM\*

This Services Addendum\* (the “**Services Addendum**”) contains additional provisions that apply to specific types of Services offered by Provider. If Customer receives from Provider any one or more of the types of Services described in this Services Addendum, then the pertinent provisions of this Services Addendum shall apply to such Services in addition to the provisions of the Agreement pursuant to which Customer ordered the Services. Capitalized terms used but not defined in this Services Addendum shall have the meanings given them in the applicable Agreement. In the event of conflict or inconsistency between the provisions of this Services Addendum and the provisions of the applicable Agreement, the order of precedence set forth in the Agreement shall apply.

### TABLE OF CONTENTS

|   |           |
|---|-----------|
| <b>ARTICLE 1 – INTERNET ACCESS SERVICE PROVISIONS .....</b>               | <b>2</b>  |
| <b>ARTICLE 2 – BURSTABLE SERVICE PROVISIONS .....</b>                     | <b>4</b>  |
| <b>ARTICLE 3 – ADVANCED SECURITY WITH SD-WAN SERVICES PROVISIONS.....</b> | <b>4</b>  |
| <b>ARTICLE 4 – PHONE SERVICE PROVISIONS .....</b>                         | <b>5</b>  |
| <b>ARTICLE 5 – HOSTED VOICE SERVICE PROVISIONS .....</b>                  | <b>6</b>  |
| <b>ARTICLE 6 – VIDEO CONFERENCING SERVICE PROVISIONS .....</b>            | <b>8</b>  |
| <b>ARTICLE 7 – CLOUD CONTACT CENTER SERVICE PROVISIONS .....</b>          | <b>11</b> |
| <b>ARTICLE 8 – VIDEO SERVICE PROVISIONS.....</b>                          | <b>12</b> |
| <b>ARTICLE 9 – CLOUD HOSTING SERVICE PROVISIONS .....</b>                 | <b>13</b> |
| <b>ARTICLE 10 – DARK FIBER SERVICE PROVISIONS .....</b>                   | <b>20</b> |
| <b>ARTICLE 11 – REMOTE VIRTUAL OFFICE SERVICE PROVISIONS.....</b>         | <b>20</b> |

**\*NOTE:** In some prior versions of Provider’s contract documents governing the Services, the title of this Services Addendum was “Service-Specific Terms and Conditions” also referred to as the “Service-Specific T&Cs.” If Customer’s Agreement references Provider’s “Service-Specific Terms and Conditions” and/or the “Service-Specific T&Cs,” all such references shall be deemed to be to this Services Addendum.

## ARTICLE 1 – INTERNET ACCESS SERVICE PROVISIONS

If Customer receives Internet access Services (“**Internet Access Services**”) from Provider, then, in addition to the provisions of the applicable Agreement, Customer’s use of the Internet Access Services is also subject to the terms and conditions of this Article 1:

1.1 End-User Access. Customer must ensure that any persons who use the Internet Access Services through Customer’s equipment and/or Customer’s internal network comply with the terms of the Agreement, this Services Addendum, and Provider’s AUP.

1.2 Acceptance of Risk. Customer expressly acknowledges and agrees that the Internet is a shared network that is not secure and that is not controlled by Provider. Any content that Customer accesses through the Internet Access Services is provided by independent third-party content providers, over which Provider does not exercise control. Provider does not preview, exercise editorial control over, or endorse any opinions or information accessed through the Internet Access Services. Customer expressly understands and agrees that it is possible data or files Customer or any of its employees, contractors, agents, or other end-users send or receive over the Internet may be monitored by third-parties and/or subject to unauthorized access by third-parties. Third-parties may gain access to Customer’s data, including confidential information. Data or files transmitted over the Internet may contain computer viruses, ransomware or other harmful components. Provider has no responsibility and assumes no liability for any such acts or occurrences. Customer expressly assumes the risks inherent in connecting Customer’s internal network and equipment to the Internet and in accessing and using the Internet through the Internet Access Services.

1.3 IP Addresses. Any IP addresses provided to Customer by Provider in connection with the Internet Access Services are and will remain the property of Provider. Customer will not alter, modify, sell, lease, assign, encumber or otherwise tamper with the IP addresses. Provider reserves the right to change addressing schemes at any time.

1.4 Business Class Internet Service. If Customer receives Business Class Internet (“**BCI**”) Service from Provider, Customer expressly acknowledges and agree that BCI is an “up to” bandwidth Service, with the bandwidth specified in Customer’s Agreement being the maximum possible bandwidth. Customer expressly understands and agrees that the actual bandwidth Customer experiences at any time will vary based on numerous factors, such as the type and configuration of Customer’s internal network equipment, the number of devices simultaneously using the BCI Service, the amount of traffic Provider’s network is then-experiencing, and other similar factors. Additionally, Customer understands and agrees that while BCI Service is a fiber-based Service, Provider’s SLA for lit fiber services does not apply to BCI Service. Instead, BCI Service is a “best efforts” Service for which no SLA remedies are available. While Provider will use commercially reasonable efforts to ensure that BCI Service is available to Customer twenty-four (24) hours per day, seven (7) days per week, it is possible that there will be interruptions (e.g., outages) or periods of degradation (e.g., slow transmission) in the BCI Service. While Provider will use commercially reasonable efforts to correct any such interruptions or degradations in a timely manner, Customer expressly acknowledges and agrees that neither service credits nor chronic outage remedies are available to Customer in connection with problems involving BCI Service. Temporary interruptions in or degradation of the BCI Service do not constitute failures on the part of Provider to fulfill its obligations under the Agreement.

1.5 Business Wi-Fi Service. If Customer receives business Wi-Fi Service (“**Business Wi-Fi Service**”) from Provider in connection with Customer’s Internet Access Service, Customer expressly acknowledges and agrees that Business Wi-Fi Service is intended to be used only by Customer’s own personnel; it is not intended to function as a guest Wi-Fi network for temporary guests of Customer’s premises such as patrons at a restaurant or patients at a medical office. As a part of the Business Wi-Fi Service, Provider will install up to five (5) ceiling or wall-mounted wireless devices within Customer’s premises. Customer is responsible for performing any internal wiring work needed in order for Provider to connect Customer’s internal network to the Wi-Fi devices. The wireless Wi-Fi devices are and shall at all times remain Provider’s Equipment. Due to the nature of Wi-Fi technology, each wireless Wi-Fi device inherently has a limited range. Physical obstacles that may be present in Customer’s environment, such as walls, doors, cubicles and other objects may reduce that range. Accordingly, speeds are not guaranteed, and the actual performance of the Business Wi-Fi Service that Customer experiences may vary in different portions of Customer’s premises, as well as at different times during the day, depending on the number of devices simultaneously using Business Wi-Fi Service, the amount of data being transmitted over Customer’s network, and so forth. Customer expressly understands and agrees that no

SLA applies to the Business Wi-Fi Service, even if an SLA does apply to the underlying Internet Access Service Customer receives from Provider. Provider will perform the initial configuration of Business Wi-Fi Service at the time of installation at Customer's location, after which Customer will be responsible for managing the Business Wi-Fi Service just as Customer is responsible for managing any other aspect of its internal network. If Customer subsequently requires assistance from Provider with network management activities (such as resetting the password for its business Wi-Fi network), Provider may charge Customer for such assistance at Provider's then-standard rates for same.

1.6 DDoS Protection Service. If Customer receives DDoS protection Service ("**DDoS Protection Service**") from Provider in connection with Internet Access Service, Customer expressly agrees and understands that the DDoS Protection Service does not guarantee that the Internet Access Service for which the DDoS Protection Service is activated will never be susceptible to or negatively impacted by any distributed denial of service attack or any other type of hostile hacking activity. Instead, the DDoS Protection Service constitutes only one measure of protection against such activities. Provider shall not be liable for any damages or harm of any type or kind that may be suffered by Customer or any of its end-users due to any DDoS attacks or other hostile hacking activity experienced by the Internet Access Service that the DDoS protection Service does not successfully prevent, alleviate or ameliorate.

1.7 Wireless Internet Backup. If Customer receives wireless internet backup Service ("**WIB Service**") from Provider in connection with Customer's primary, wired Internet Access Service, the provisions of this Section 1.7 apply to the provision and use of the WIB Service.

(a) Intended Function. Customer expressly agrees and acknowledges that WIB Service is not intended to function as Customer's primary means of accessing the Internet. Instead, WIB Service is designed to provide Customer with a temporary, back-up, fail-over method of accessing the Internet using the cellular data network in the event that Customer's primary, wired Internet access connection is temporarily interrupted, disrupted or otherwise fails. WIB Service begins to function when Customer's router detects problems with Customer's primary, wired Internet access connection. Once Customer's primary, wired Internet access connection is again transmitting data properly, WIB Service automatically deactivates.

(b) Cost Structure & Data Caps. Because WIB Service uses cellular network wireless data transmission to function, a monthly base data allotment is included in the base price of the WIB Service. **If Customer purchases a WIB Service plan that allows Customer to exceed its monthly base data allotment, then Customer expressly understands and agrees that if its data usage in any given month exceeds the base data allotment, Customer will incur charges for data use overages at the rate specified in the applicable Service Order. Customer will not receive any alert or other notification if its monthly base data allotment is exceeded and Customer begins to incur data use overage charges.** Additionally, if Customer's WIB Service plan involves a maximum monthly data cap, Customer understands and agrees that once its maximum monthly data cap has been reached, its WIB Service will cease transmitting data and will no longer function until the beginning of the next billing period, at which time Customer's data allotment will automatically re-set.

(c) Performance Is Not Guaranteed. Customer expressly understands and agrees that while WIB Service provides a fail-over, back-up solution to temporary disruption of Customer's primary, wired Internet access connection, Provider does not guarantee WIB Service will function as intended or represent that WIB Service is fail-safe or error-free, and Customer further acknowledges and agrees that WIB Service should not be relied upon in situations where error-free or uninterrupted service is essential. The SLA (if any) that applies to the primary, wired Internet Access Service Customer receives from Provider does not apply to WIB Service. Provider will not be responsible for, and Customer expressly assumes all risk of, any losses or damages arising as a result of the failure of WIB Service to function as expected.

1.8 Custom Wi-Fi. If Customer receives Custom Wi-Fi Service ("**CWF Service**") from Provider, the provisions of this Section 1.8 apply to the CWF Service.

(a) Prerequisite Services. As a prerequisite to receive CWF Service, Customer must receive from Provider, at the same Service Site, Dedicated Internet Access or (if approved by Provider) another type of Internet Access Service that Provider

determines to be compatible with CWF Service. Customer acknowledges that without the underlying Internet access Service, CWF Service will not function.

(b) Separate Functionality from Internet Access Service. Customer acknowledges that the underlying Internet Access Service provided by Provider and the CWF Service are complementary but separate from each-other, and that the proper function of the Internet Access Service does not guarantee the proper function of CWF Service.

(c) Performance Is Not Guaranteed; No SLA. Provider does not guarantee CWF Service will function as intended or represent that CWF Service is fail-safe or error-free, and Customer acknowledges that CWF Service should not be relied upon in situations where error-free or uninterrupted service is essential. The SLA (if any) that applies to the primary underlying Internet Access Service Customer receives from Provider with the CWF Service does not apply to CWF Service. Provider will not be responsible for, and Customer expressly assumes all risk of, any losses or damages arising as a result of the failure of CWF Service to function as expected.

(d) Hardware Used to Provide CWF Service. Customer acknowledges that in order to provide CWF Service, Provider must deploy, install, and maintain certain hardware in and on Customer's location(s) where the CWF Service is provided (the "**CWF Hardware**"). Customer agrees to cooperate reasonably with Provider (at Customer's expense) in Provider's deployment, installation, and maintenance of the CWF Hardware, and Customer acknowledges that if it fails to do so, Provider will not be liable to Customer for any related outage, failure, degradation or interruption in or to the CWF Service resulting from problems with the CWF Hardware. Further, Customer acknowledges that upon termination of the CWF Service (regardless of the reason), Provider shall have the right to remove the CWF Hardware from the location(s) where it is installed, and Customer agrees to (i) make the applicable location(s) available to Provider for that purpose, and (ii) cooperate reasonably (at Customer's own expense) with efforts by Provider to remove the CWF Hardware. Unless Provider has expressly agreed with Customer in writing to the contrary, title in and to the CWF Hardware will remain at all times with Provider, and Customer is prohibited from selling, transferring, conveying, removing, or otherwise in any way tampering or interfering with the CWF Hardware, and from attempting or permitting others to do any of the foregoing.

## ARTICLE 2 – BURSTABLE SERVICE PROVISIONS

If Customer receives burstable Internet Access Services or burstable data transport Services ("**Burstable Services**") from Provider, then, in addition to the provisions of the applicable Agreement, Customer's use of the Burstable Services is also subject to the terms and conditions of this Article 2. Burstable Service allows Customer to increase from the selected base bandwidth up to the specified maximum burstable bandwidth on an as-needed basis when usage spikes. Charges for Burstable Service will be calculated by using the industry standard 95<sup>th</sup> percentile. The 95<sup>th</sup> percentile measurement evaluates the regular and sustained use of a network connection and is measured by sampling usage at 5-minute intervals and ignoring the top 5% of usage samples taken over a month. The 95<sup>th</sup> percentile measure of peak bandwidth will then be compared to the base bandwidth and the incremental usage will be billed at the burst rate in arrears on a monthly basis. Charges for Burstable Service will be measured, calculated and accrued on a monthly basis, and billed in arrears on a monthly basis.

## ARTICLE 3 – ADVANCED SECURITY WITH SD-WAN SERVICES PROVISIONS

If Customer receives Advanced Security with SD-WAN Services ("**Advanced Security with SD-WAN Services**") from Provider, then, in addition to the provisions of the applicable Agreement, Customer's use of the Advanced Security with SD-WAN Services is also subject to the terms and conditions of this Article 3:

3.1 Underlying Internet Connection Required. Customer acknowledges and agrees that the Advanced Security with SD-WAN Services are cloud-hosted Services that require an underlying Internet connection in order to function. The underlying Internet connection does not need to be provided by Provider; it may be provided by any Internet access provider. However, the Advanced Security with SD-WAN Services will not function if Customer does not have an active connection to the Internet.

3.2 Use of Customer Information to Configure Service. In order to configure Advanced Security with SD-WAN Services, Provider must upload certain Customer-provided information regarding Customer's network configuration (e.g., Customer's company name, service site address(es), circuit IDs, etc.) to the cloud-hosted portal through which the Advanced Security with SD-WAN Services will be configured and managed. By ordering Advanced Security with SD-WAN Services from Provider, Customer is authorizing Provider to use information supplied by Customer to establish and configure Customer's account on the cloud-hosted portal.

3.3 Ownership of Equipment. The hardware installed by Provider at Customer's Service Site in connection with Advanced Security with SD-WAN Services is and shall at all times remain the personal property of Provider. Provider shall be responsible for the regular maintenance and repair of all such equipment. Should Customer experience problems with the equipment, Customer must contact Provider, and Provider will use commercially reasonable efforts to repair or replace the malfunctioning equipment as soon as possible after receiving Customer's notification. Provider shall have the right at any time, and from time to time, during the term of the applicable Agreement to substitute different equipment for some or all of the equipment initially installed at Customer's Service Site; provided that the substituted equipment has equivalent or better functionality than the previously installed equipment. Should any equipment require repair or replacement due to Customer's negligent or willful conduct, including the misuse or abuse of same, Customer shall reimburse Provider for the costs of such repair or replacement.

3.4 No Intellectual Property Rights. By using Provider's Advanced Security with SD-WAN Services, Customer will not acquire any rights of, in, or to ownership of copyrights, patents, trade secrets, trademarks or any other intellectual property rights in or to the Advanced Security with SD-WAN Services products, hardware, firmware, software, or the output from the online cloud-hosted portal, all of which are and shall at all times remain owned by Provider or its vendors and suppliers, as applicable. Provider or its vendors and suppliers, as applicable, will retain exclusive ownership in all deliverables created hereunder and will own all intellectual property rights, title and interest in any ideas, concepts, know how, documentation or techniques developed in connection with the Advanced Security with SD-WAN Services.

3.5 No Cyber Security or Network Consulting Services. Provider does not provide cyber security consulting, network security consulting, network management consulting, or any other similar type of professional services. Customer understands and agrees that Provider has not provided Customer with and will not in the future provide Customer with any recommendations, guidance, or advice regarding Customer's use of Advanced Security with SD-WAN Services to configure, optimize, monitor, and/or protect Customer's network. Instead, Customer is at all times fully and solely responsible for configuring, optimizing, monitoring and protecting Customer's network using the Advanced Security with SD-WAN Services provided by Provider as well as any other lawful means Customer, in its sole discretion and independent judgment, deems necessary or appropriate for that purpose. Should Customer, at any time, ask Provider personnel to modify or alter the configuration of Provider's Advanced Security with SD-WAN Services, Customer acknowledges that Provider personnel will not independently assess the advisability of Customer's requested changes. Instead, Provider's only obligation in such situation is to make the specific modifications or alterations requested by Customer.

3.6 Cyber Security Disclaimer. Use of Provider's Advanced Security with SD-WAN Services does not guarantee that Customer's network will never be susceptible to or negatively impacted by any cyber security threats or hostile hacking activity (e.g., viruses, malware, denial of service attacks, ransomware, cryptojacking, phishing, SQL injection, man in the middle attacks, etc.). Instead, the Advanced Security with SD-WAN Services constitute only one measure of protection available for use by Customer to protect against such activities. PROVIDER SHALL NOT BE LIABLE FOR ANY DAMAGES OR HARM OF ANY TYPE THAT MAY BE SUFFERED BY CUSTOMER OR ANY OF ITS EMPLOYEES, CONTRACTORS, AGENTS, BUSINESS PARTNERS, CUSTOMERS, OR END-USERS DUE TO ANY CYBER SECURITY BREACHES OR OTHER HOSTILE HACKING ACTIVITY THAT THE ADVANCED SECURITY WITH SD-WAN SERVICES DO NOT SUCCESSFULLY PREVENT, ALLEVIATE OR AMELIORATE.

#### **ARTICLE 4 – PHONE SERVICE PROVISIONS**

If Customer receives Phone Services (including Hosted Voice Services) ("**Phone Services**") from Provider, then, in addition to the provisions of the applicable Agreement, Customer's use of Phone Services is also subject to the terms and conditions of this Article 4:

4.1 VoIP Services. Provider's Phone Services are provided via Internet Protocol voice network (aka "VoIP"). VoIP services operate using the standard commercial electrical power provided to Customer's Service Site. Provider does not provide a back-up generator, UPS, or other alternate power source for the Phone Services; accordingly, in the event of a power outage at Customer's Service Site, unless Customer has arranged for back-up power, the VoIP services will be unavailable until electrical service is restored. Customer acknowledges and agrees that the VoIP services are not represented as fail-safe and are not designed for use in situations where error-free or uninterrupted service is essential. Provider will not be responsible for, and Customer expressly assumes all risk of, any losses or damages arising as a result of the unavailability of the VoIP services, including the inability to reach 911 or other emergency services, and the inability to contact Customer's security system, fire alarm system, or any remote monitoring service.

4.2 Important Notice Regarding E911 Service. Federal Communications Commission rules require providers of VoIP Phone Services to remind customers of these important E911 facts: (a) Provider needs a complete and correct Service Site address in order to deliver accurate location information to E911; (b) If Customer moves its VoIP phone equipment to a different physical address, Customer must notify Provider immediately and update the location information, otherwise E911 will not have Customer's correct location information on file; (c) VoIP services operate using the standard electrical power provided to the Service Site, so unless Customer has arranged for a back-up power supply, the Phone Service will be unavailable during a power outage (however caused); (d) Customer may not be able to make E911 calls if there is a power outage, network outage or other technical problems, or if Customer's Phone Service is terminated or suspended.

4.3 Other Providers. Unless otherwise expressly agreed to in writing with Customer, Provider has no obligation or responsibility to Customer to arrange for termination or removal of telecommunications services provided by long distance providers. Instead, Customer is and remains responsible for terminating and removing any such unwanted services and circuits provided by other long distance providers. Customer understands that it may designate only one primary interexchange carrier for any one telephone number for state-to-state (interLATA), intrastate and international usage.

4.4 Long Distance Charges. Any long distance rates listed in the applicable Agreement are the rates as of the effective date of that Agreement and may not reflect the actual rates applicable at any given time during the term of the Agreement. All long distance charges are exclusive of applicable taxes, and Provider may add or adjust rates and charges in order to recover amounts it is required or permitted by governmental or quasi-governmental authorities to collect from or pay to others in support of statutory or regulatory programs ("**Governmental Charges**"), plus amounts necessary for Provider to recover reasonable administrative costs associated with such Governmental Charges.

4.5 International Calling Charges. The rates listed in the applicable Agreement do not include charges for international calls. Provider will pass through to Customer all charges for any international calls made via the Phone Services.

4.6 CPNI. Provider will have access to certain proprietary network information of Customer ("**CPNI**"). Under federal law, Customer has a right, and Provider has a duty, to protect the confidentiality of CPNI. CPNI may be useful to tailor services to Customer and to enhance Provider's ability to meet Customer's needs. Customer expressly authorizes Provider, its Affiliates, and/or its sales representatives to use CPNI to determine if Customer could benefit from other Services available from Provider and its Affiliates, and market those Services to Customer. Customer may withdraw its authorization for this use of its CPNI by Provider at any time by informing Provider in writing. Any such withdrawal will not affect the quality of the Services provided to Customer.

## ARTICLE 5 – HOSTED VOICE SERVICE PROVISIONS

If Customer receives hosted voice Services ("**Hosted Voice Services**") from Provider, then, in addition to the provisions of the applicable Agreement and the provisions regarding Phone Service set forth in Article 4 above, Customer's use of the Hosted Voice Services is also subject to the terms and conditions of this Article 5:

5.1 Leased Hosted Voice Equipment. If Customer is leasing hosted voice equipment (the “**Leased Equipment**”) from Provider, then the Leased Equipment shall at all times be and remain the personal property of Provider. Provider shall be responsible for the regular maintenance and repair of all Leased Equipment. Should Customer experience problems with any of the Leased Equipment, Customer must contact Provider, and Provider will use commercially reasonable efforts to repair or replace the malfunctioning Leased Equipment as soon as reasonably possible after receiving Customer’s notification. For Leased Equipment, Provider shall have the right at any time, and from time to time, during the Service Term to substitute different hosted voice equipment for some or all of the Leased Equipment initially installed at Customer’s Service Site; provided that the substituted Leased Equipment has equivalent or better functionality than the previously installed Leased Equipment. Should any Leased Equipment require repair or replacement due to Customer’s negligent or willful conduct, including the misuse or abuse of same, Customer shall reimburse Provider for the costs of such repair or replacement.

5.2 Purchased Hosted Voice Equipment. If Customer has purchased hosted voice equipment (the “**Purchased Equipment**”) through or from Provider, then upon Customer’s acceptance of the Purchased Equipment, the Purchased Equipment shall be and remain Customer’s personal property. As between Provider and Customer, Customer shall be solely responsible for the repair and maintenance of all Purchased Equipment and any and all obligations and liabilities associated therewith. **CUSTOMER ACKNOWLEDGES THAT THE PURCHASED EQUIPMENT IS NOT MANUFACTURED BY PROVIDER AND THAT PROVIDER DOES NOT SUPPORT AND SHALL HAVE NO MAINTENANCE OR REPAIR OBLIGATIONS OR OTHER LIABILITY REGARDING SAME.** PROVIDER WILL EITHER DELIVER THE MANUFACTURER’S WARRANTY FOR THE PURCHASED EQUIPMENT DIRECTLY TO CUSTOMER OR PASS THE MANUFACTURER’S WARRANTY THROUGH TO CUSTOMER AS-IS, DEPENDING ON THE APPLICABLE MANUFACTURER’S POLICY. PROVIDER HEREBY ASSIGNS TO CUSTOMER ALL OF THE MANUFACTURERS’ WARRANTIES AND INDEMNITIES RELATING TO THE PURCHASED EQUIPMENT TO THE EXTENT PROVIDER IS PERMITTED BY THE MANUFACTURER TO MAKE SUCH ASSIGNMENT. SUCH ASSIGNMENT IS SUBJECT TO ALL OF THE TERMS AND CONDITIONS IMPOSED BY THE MANUFACTURER WITH RESPECT THERETO. CUSTOMER’S REMEDY FOR DEFECTIVE PURCHASED EQUIPMENT SHALL BE AS SET FORTH IN THE APPLICABLE MANUFACTURER’S WARRANTY, WHICH IS CUSTOMER’S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF AN EQUIPMENT WARRANTY. PROVIDER DOES NOT EXTEND ANY WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE, TO CUSTOMER FOR ANY PURCHASED EQUIPMENT, AND PROVIDER SHALL NOT HAVE ANY LIABILITY FOR ANY LOSS, DAMAGE, OR EXPENSE DIRECTLY OR INDIRECTLY ARISING FROM THE USE OF (OR INABILITY TO USE) THE PURCHASED EQUIPMENT. Any questions concerning or requests for maintenance or repair of the Purchased Equipment should be directed to the manufacturer of the Purchased Equipment at issue. If Purchased Equipment impairs or prevents Customer’s access to or use of the Hosted Voice Services, Customer will remain liable for payment to Provider of the applicable Fees for the Hosted Voice Services, including without limitation the MRC and any other Fees specified in the Agreement. If, at Customer’s request, Provider attempts to resolve difficulties caused by Purchased Equipment, Customer will be responsible for payment of Provider’s then-current commercial rates and terms for such consulting services on a time and materials basis.

5.3 Hosted Voice Software. Certain types of Hosted Voice Services, such as virtual seats, mobile clients, and video conferencing solutions, require the installation of third-party software on Customer’s equipment. Additionally, both Leased Equipment and Purchased Equipment may include a limited license to use certain third-party software and/or firmware provided by the vendor or manufacturer of the Leased Equipment or Purchased Equipment. Any such software or firmware provided to Customer in connection with Hosted Voice Services shall be collectively referred to as the “**Hosted Voice Software**.” Customer expressly understands and agrees that, unless otherwise provided to the contrary in any written license agreement or other documentation from the third-party vendor or manufacturer of the Hosted Voice Software, Customer may only use the Hosted Voice Software for the purposes of using and operating the Leased Equipment or Purchased Equipment and receiving the Hosted Voice Services pursuant to the applicable Agreement. Customer understands and agrees that each of the following is prohibited with respect to the Hosted Voice Software: (a) copying the Hosted Voice Software or associated documentation, either in whole or in part; (b) modifying, reverse compiling, reverse assembling or otherwise reverse engineering the Hosted Voice Software, either in whole or in part, or attempting to do any of the foregoing; (c) sub-licensing, leasing, sub-licensing, selling or otherwise distributing the Hosted Voice Software, either in whole or in part, and whether or not for profit, to any third parties; and (d) creating derivative works of, from, based on, using or incorporating all or any portion of the Hosted Voice Software.

5.4 Use of Specific Hosted Voice Features. Hosted Voice Services may include certain features that are enabled by “add-in” software or service components. These features are intended to enhance the functionality of the Hosted Voice Services and to

provide Customer with additional convenience and collaboration tools. Examples of such features include, but are not limited to, SMS messaging, voicemail transcription, voicemail recording and other similar functions, expressly including any additional “add-in” feature enhancements that Provider may make available or incorporate into the Hosted Voice Services in the future. Provider has established its pricing for the Hosted Voice Services based on assumptions of normal business use of the Hosted Voice Services within the United States of America. Should Customer’s use of the Hosted Voice Services, including any of the “add-in” features such as SMS messaging, significantly exceed normal business use, Provider reserves the right to disable the feature(s) at issue and/or impose additional cost-recovery charges for Customer’s excessive use.

5.5 Installation of Hosted Voice Equipment. As a part of the Hosted Voice Services, Provider will install the hosted voice equipment (whether such equipment is Leased Equipment or Purchased Equipment) at the Service Site specified in the applicable Agreement. If Customer’s Service Site contains existing inside wiring, Provider will use Customer’s existing wiring for the installation; provided, that Provider’s use of any existing wiring shall not constitute any type of representation, warranty or guarantee to Customer that the existing wiring is in good condition and/or free from defects and/or otherwise suitable for such use. If Customer’s Service Site does not contain the necessary inside wiring (as determined by Provider in Provider’s commercially reasonable judgment), Provider will so notify Customer, and Customer may elect to install the necessary wiring itself or to request that Provider install the necessary wiring on behalf of Customer. If Provider installs the wiring at Customer’s request, such work shall be performed on a time and materials basis, with the wiring to become Customer’s personal property upon Customer’s acceptance of the Service. If, during the installation process, Provider discovers or uncovers any hazardous materials or substances at Customer’s Service Site: (a) Provider shall have the option to cease work at the Service Site immediately and terminate Customer’s Agreement for Hosted Voice Services, without any liability for or obligation to remove or remediate the hazardous materials so discovered; and (b) Customer shall indemnify, defend and hold Provider harmless from and against any and all claims, costs, damages and expenses incurred by Provider in connection with or as a result of the pre-existing hazardous materials, including attorneys’ and experts’ fees and costs as well as the costs of any environmental assessment or remediation work that may be performed at the Service Site.

5.6 “Bring-Your-Own-Device” Provisions. For certain models and types of devices, Provider has the ability to attempt to connect devices that Customer already owns (the “**Customer Devices**”) to Provider’s Hosted Voice Services, which eliminates the need for Customer to lease or purchase from Provider some or all of the devices necessary to access and use the Hosted Voice Services. If Customer elects to use its own Customer Devices with Provider’s Hosted Voice Services, Customer expressly agrees to the following provisions: (a) Customer must supply the passwords for the Customer Devices to Provider if Provider so requests, otherwise the devices may not be usable with Provider’s network; (b) the process of connecting the Customer Devices to Provider’s network may involve re-setting the Customer Devices to their factory defaults, which will delete all information previously stored on the Customer Devices, including contact lists, speed dial numbers, as well as the configurations established for connectivity to Customer’s previous hosted voice solution; (c) it is possible that attempting to connect the Customer Devices to Provider’s network could render one or more of the Customer Devices unusable, requiring a firmware re-flash. In such event, Provider will have no responsibility or liability for repairing or replacing the Customer Device(s) at issue. Instead, Customer expressly assumes the risk inherent in attempting to attach the Customer Devices to Provider’s hosted voice network; and (d) Provider will be unable to provide support and troubleshooting for Customer Devices after implementation. Provider will be able to troubleshoot problems with Provider’s network, but if the network is functioning properly and there are technical problems with any of the Customer Devices, Customer must seek equipment support from the manufacturer or original vendor of the relevant Customer Devices or other Customer-supplied equipment.

## ARTICLE 6 – VIDEO CONFERENCING SERVICE PROVISIONS

If Customer receives Video Conferencing Services (“**Video Conferencing Services**”) from Provider, then, in addition to the provisions of the applicable Agreement, the provisions regarding Phone Services set forth in Article 4 above, and the provisions regarding Hosted Voice Services set forth in Article 5 above, Customer’s use of the Video Conferencing Services is also subject to the terms and conditions of this Article 6:

6.1 Use of Video Conferencing Service and Customer’s Responsibilities. Provider’s video conferencing solution is a software-based addition to Provider’s Hosted Voice Services that is intended to facilitate group collaboration and remote team



communications. Customer is solely responsible for its use of the Video Conferencing Services, including for all use made of the Video Conferencing Service by Customer's employees, contractors, third-party business partners, and other end-users. Customer's use of the Video Conferencing Services shall at all times comply with all applicable laws, including, but not limited to, laws related to recording, intellectual property, privacy and export control.

(a) Registration Information. Customer may be required to provide information about itself and its employees and other end-users of the Video Conferencing Services in order to use the Video Conferencing Services or certain functionality provided by or with the Video Conferencing Services. Customer agrees that all such information shall be accurate. Customer may be asked to choose a user name and password. Customer is entirely responsible for maintaining the security of Customer's username and password and agrees not to disclose same to third-parties.

(b) Customer's Content. Customer agrees that it is solely responsible for the content sent, transmitted, displayed and/or uploaded by Customer, Customer's employees, contractors, third-party business partners, and other end-users of the Video Conferencing Services. Customer represents and warrants that it has the right to transmit and upload its content and that such use does not violate or infringe on the rights of any third party. Under no circumstances will Provider be liable in any way for any: (i) content that is transmitted or viewed while using the Video Conferencing Services, (ii) errors or omissions in the content, or (iii) any loss or damage of any kind incurred as a result of the use of, access to, or denial of access to Customer's content or inability to access to Customer's content. Although Provider is not responsible for Customer's content, Provider may delete any of Customer's content at any time without notice to Customer if Provider becomes aware that Customer's content violates any provisions of the Agreement or applicable law. Customer retains its copyrights and any other intellectual property rights Customer already holds (if any) in Customer's content that is submitted, posted or displayed on, through or using the Video Conferencing Services.

(c) Recordings. Customer is responsible for complying with all recording laws. The host of a video conferencing session can choose to record video conference meetings and webinars. By using the Video Conferencing Services, Customer consents to Provider's storage of recordings for any or all video conference meetings or webinars that Customer and/or any of its employees, contractors, third-party business partners, or other end-users may join, if such recordings are stored in Provider's systems. Customer (and its applicable its employees, contractors, third-party business partners, or other end-users who are using the Video Conferencing Services) will receive a notification (visual or otherwise) when recording is enabled. If any person taking part in a call, webinar, meeting or other event that takes place using the Video Conferencing Services does not consent to being recorded, that person can choose to leave the event.

(d) Prohibited Use. Customer agrees that it will not use, and will not permit any of its employees, contractors, third-party business partners, or other end-users of the Video Conferencing Services to do any of the following: (i) modify, disassemble, decompile, prepare derivative works of, reverse engineer or otherwise attempt to gain access to the source code of the Video Conferencing Services, (ii) knowingly or negligently use the Video Conferencing Service in a way that abuses, interferes with, or disrupts Provider's network or the systems, facilities or equipment used by Provider to provide the Video Conferencing Services, (iii) use the Video Conferencing Services in violation of any Provider policy or in a manner that violates applicable law, including but not limited to anti-spam, intellectual property, export control, privacy, and anti-terrorism laws and regulations; (iv) build or benchmark a competitive product or service, or copy any features, functions or graphics of the Video Conferencing Services, (v) use the Video Conferencing Services to communicate any message or material that is harassing, libelous, threatening, obscene, indecent, or that would give rise to civil liability, or that constitutes or encourages conduct that could constitute a criminal offense under any applicable law or regulation; or (vi) upload or transmit any software, content or code that does or is intended to harm, disable, destroy or adversely affect the performance of the Video Conferencing Services or Provider's network or equipment in any way.

(e) Limitations on Use. Customer may not reproduce, resell, or distribute the Video Conferencing Services or any reports or data generated by the Video Conferencing Services for any purpose unless Customer has been specifically permitted to do so under a separate agreement with Provider. Customer may not offer or enable any third parties to use the Video Conferencing Services purchased by Customer, display on any website or otherwise publish the Video Conferencing Services or any content obtained from the Video Conferencing Services (other than content created and owned by Customer) or otherwise generate

revenue from the Video Conferencing Services. Customer may not use the Video Conferencing Services for the development, production or marketing of a service or product substantially similar to the Video Conferencing Services.

(f) Responsibility for End-Users. Customer is responsible for the activities of all of Customer's employees, contractors, third-party business partners, and other end-users who access or use the Video Conferencing Services through Customer's account, and Customer agrees to ensure that all such employees, contractors, third-party business partners, and other end-users comply with the terms of the Agreement, the provisions of this Services Addendum, and any applicable Provider policies (including without limitation Provider's Acceptable Use Policy). If Customer becomes aware of any violation of the Agreement in connection with the use of the Video Conferencing Services by any person, Customer shall notify Provider immediately. Provider may investigate any complaints and violations that come to its attention and may take any (or no) action that Provider believes is appropriate, including, but not limited to issuing warnings, removing content, terminating accounts and/or user profiles, and/or suspending or terminating the provision of Video Conferencing Services to Customer.

6.2 Not for Use in High Risk Environments. THE VIDEO CONFERENCING SERVICES ARE NOT POSITIONED, INTENDED OR DESIGNED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE COMMUNICATIONS OR CONTROLS, INCLUDING, WITHOUT LIMITATION, THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION/COMMUNICATIONS SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT AND/OR WEAPONS SYSTEMS. CUSTOMER MUST NOT USE THE VIDEO CONFERENCING SERVICES IN ANY HIGH RISK ENVIRONMENT.

6.3 Not Intended for Secure Communications. THE VIDEO CONFERENCING SERVICES ARE NOT POSITIONED, INTENDED OR DESIGNED TO PROVIDE SECURE COMMUNICATIONS AND MUST NOT BE USED IN SITUATIONS WHERE THE CONFIDENTIALITY, PRIVACY OR SECURITY OF THE COMMUNICATION AT ISSUE IS ESSENTIAL OR PARAMOUNT. Provider's Video Conferencing Services contain certain industry-standard features that, when correctly configured and enabled, can increase the security of video conference sessions. Provider strongly recommends that Customer use (and require its employees, contractors, third-party business partners, and other end-users to use) the available security features of the Video Conferencing Services. However, even with proper configuration of video conferencing settings, it is possible that communications made using the Video Conferencing Services may be intercepted by unauthorized third parties, disseminated beyond Customer's intended audience, recorded or altered without Customer's consent, or otherwise compromised by hostile hacking activity. CUSTOMER EXPRESSLY UNDERSTANDS AND AGREES THAT ITS USE OF THE VIDEO CONFERENCING SERVICES IS NOT GUARANTEED TO BE SECURE. INSTEAD, CUSTOMER UNDERSTANDS AND AGREES THAT ITS USE OF THE VIDEO CONFERENCING SERVICE IS AT ITS SOLE RISK. PROVIDER SHALL NOT BE LIABLE FOR ANY BREACHES OF PRIVACY, UNAUTHORIZED DISCLOSURE OF CONFIDENTIAL INFORMATION, OR OTHER DAMAGES OR LOSSES OF ANY TYPE THAT MAY BE SUFFERED BY CUSTOMER OR ANY OF ITS EMPLOYEES, CONTRACTORS, THIRD-PARTY BUSINESS PARTNERS, OR OTHER END-USERS DUE TO ANY SECURITY WEAKNESSES IN THE VIDEO CONFERENCING SOFTWARE OR ANY HOSTILE HACKING ACTIVITY EXPLOITING THE SAME.

6.4 No Warranties; Acceptance of Risk. CUSTOMER UNDERSTANDS AND AGREES THAT THE VIDEO CONFERENCING SERVICES ARE PROVIDED "AS-IS" AND THAT PROVIDER, ITS AFFILIATES AND SUPPLIERS EXPRESSLY DISCLAIM ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. PROVIDER, ITS AFFILIATES AND SUPPLIERS MAKE NO WARRANTY OR REPRESENTATION REGARDING THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE VIDEO CONFERENCING SERVICES, REGARDING THE ACCURACY OR RELIABILITY OF ANY INFORMATION OBTAINED THROUGH THE VIDEO CONFERENCING SERVICES, OR THAT THE VIDEO CONFERENCING SERVICES WILL MEET ANY USER REQUIREMENTS, OR BE UNINTERRUPTED, TIMELY, SECURE OR ERROR FREE. USE OF THE VIDEO CONFERENCING SERVICES IS AT CUSTOMER'S SOLE RISK. ANY MATERIAL AND/OR DATA DOWNLOADED OR OTHERWISE OBTAINED THROUGH USE OF THE VIDEO CONFERENCING SERVICES IS AT CUSTOMER'S OWN DISCRETION AND RISK. CUSTOMER WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO OR HARM SUFFERED BY IT RESULTING FROM THE USE OF THE VIDEO CONFERENCING SERVICES. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE VIDEO CONFERENCING SERVICES IS AND REMAINS WITH CUSTOMER. PROVIDER DOES NOT ASSUME ANY RESPONSIBILITY FOR RETENTION OF ANY USER INFORMATION OR COMMUNICATION BETWEEN USERS. PROVIDER CANNOT GUARANTEE AND DOES NOT PROMISE ANY SPECIFIC RESULTS FROM USE OF THE VIDEO CONFERENCING SERVICES.

## ARTICLE 7 – CLOUD CONTACT CENTER SERVICE PROVISIONS

If Customer receives Cloud Contact Center Services (“**Cloud Contact Center Services**”) from Provider, then, in addition to the provisions of the applicable Agreement, Customer’s use of Provider’s Cloud Contact Center Services is also subject to the terms and conditions of this Article 7:

7.1 Underlying Internet Connection Required. Provider’s Cloud Contact Center Services are cloud-hosted Services. All users of the Cloud Contact Center Services must have an underlying Internet connection in order to access and use the Cloud Contact Center Services. The underlying Internet connection does not necessarily need to be provided by Provider. In some situations, Provider may require Customer to purchase the underlying Internet connectivity from Provider in order to receive Provider’s Cloud Contact Center Services. In other situations, Provider may allow Customer to use Internet access purchased from a different provider (a “**Third-Party Provider**”) as the underlying connection to Provider’s Cloud Contact Center Services. In either event, Customer expressly understands and acknowledges that it will not be able to use the Cloud Contact Center Services without an active connection to the Internet.

7.2 When Underlying Internet Connectivity Is Provided by a Third-Party Provider. If Customer is using Internet connectivity provided by a Third-Party Provider to access and use Provider’s Cloud Contact Center Services, Customer expressly acknowledges and agrees to each of the following:

- (a) Provider is not responsible for and has no control over the Internet access service Customer receives from any Third-Party Provider. Customer must contact its Third-Party Provider for any technical support issues Customer experiences with its underlying Internet connection.
- (b) In order for the Cloud Contact Center Services to function as intended, the underlying Internet connection must meet certain minimum technical and other relevant characteristics. As between Provider and Customer, Customer is solely responsible for determining whether the Internet access service it receives from its Third-Party Provider has the technical and other applicable characteristics (such as sufficient stability, throughput, low latency, etc.) necessary to support Customer’s use of Provider’s Cloud Contact Center Services in the manner in which the Cloud Contact Center Services are designed to function. Provider has no obligation whatsoever to modify the Cloud Contact Center Services to make them compatible with Internet access service Customer receives from any Third-Party Provider.
- (c) IF CUSTOMER’S ABILITY TO ACCESS AND USE THE CLOUD CONTACT CENTER SERVICES IS DEGRADED, INTERRUPTED OR OTHERWISE ADVERSELY IMPACTED BY THE POOR TECHNICAL PERFORMANCE AND/OR UNAVAILABILITY OF THE UNDERLYING INTERNET CONNECTION CUSTOMER RECEIVES FROM A THIRD-PARTY PROVIDER, CUSTOMER SHALL NONETHELESS REMAIN FULLY OBLIGATED TO PAY PROVIDER FOR THE CLOUD CONTACT CENTER SERVICES DURING SUCH PERIOD. IN NO EVENT SHALL PROVIDER BE LIABLE FOR ANY PROBLEMS CUSTOMER MAY EXPERIENCE IN USING THE CLOUD CONTACT CENTER SERVICES DUE TO THE INTERNET CONNECTION PROVIDED BY A THIRD-PARTY PROVIDER, OR FOR ANY OUTAGES, DEGRADATION, OR INTERRUPTION OR OTHER PROBLEMS CUSTOMER MAY EXPERIENCE WITH ANY INTERNET ACCESS SERVICE CUSTOMER RECEIVES FROM A THIRD-PARTY PROVIDER.
- (d) CUSTOMER’S DECISION TO USE AND ACCESS PROVIDER’S CLOUD CONTACT CENTER SERVICES VIA AN INTERNET CONNECTION CUSTOMER RECEIVES FROM A THIRD-PARTY PROVIDER IS UNDERTAKEN AT CUSTOMER’S SOLE AND EXCLUSIVE RISK.

7.3 Installation and Use of Cloud Contact Center Software. Provider’s Cloud Contact Center Services are provided in partnership with Provider’s vendor, Intermedia.net, Inc. (“**Intermedia**”). In order to access and use the Cloud Contact Center Services, Customer must download and install certain software provided by Intermedia (the “**Cloud Contact Center Software**”).

To use the Cloud Contact Center Software, Customer must accept and agree to the terms and conditions of Intermedia’s end-user license agreement, which is posted on the Intermedia website at the following URL: <https://intermedia.com/end-user-license-agreement> (the “**Cloud Contact Center EULA**”). If Customer does not agree to the terms and conditions of the Cloud Contact Center EULA, Customer may not use the Cloud Contact Center Software or the Cloud Contact Center Services. The terms and conditions of the Cloud Contact Center EULA are incorporated into and constitute a part of this Services Addendum. **CUSTOMER ACKNOWLEDGES THAT THE CLOUD CONTACT CENTER SOFTWARE IS NOT MANUFACTURED OR PUBLISHED BY PROVIDER AND THAT PROVIDER DOES NOT SUPPORT AND SHALL HAVE NO MAINTENANCE OBLIGATIONS OR OTHER LIABILITY OR OBLIGATION REGARDING THE CLOUD CONTACT CENTER SOFTWARE.** Further, Customer acknowledges and agrees that it may use the Cloud Contact Center Software only for the purpose of using and operating the Cloud Contact Center Services as contemplated by the applicable Agreement with Provider, and that each of the following is prohibited with respect to the Cloud Contact Center Software: (a) copying the Cloud Contact Center Software or associated documentation, either in whole or in part; (b) modifying, reverse compiling, reverse assembling or otherwise reverse engineering the Cloud Contact Center Software, either in whole or in part, or attempting to do any of the foregoing; (c) sub-licensing, leasing, sub-licensing, selling or otherwise distributing the Cloud Contact Center Software, either in whole or in part, and whether or not for profit, to any third parties; and (d) creating derivative works of, from, based on, or using or incorporating all or any portion of the Cloud Contact Center Software.

7.4 Cloud Contact Center Services SLA. Provider’s normal SLA for lit fiber services does not apply to the Cloud Contact Center Services. Instead, the service level agreement applicable to the Cloud Contact Center Services is posted on the Intermedia website at the following URL: <https://www.intermedia.com/assets/pdf/legal/sla-contact-center.pdf> (the “**Cloud Contact Center SLA**”).

7.5 Cloud Contact Center EULA and Cloud Contact Center SLA Are Subject to Future Updates. Both the Cloud Contact Center EULA and the Cloud Contact Center SLA may be updated at any time and from time to time without notice to Customer. Customer understands and agrees that it is Customer’s responsibility to review both the Cloud Contact Center EULA and the Cloud Contact Center SLA with reasonable frequency to keep abreast of any changes. Customer’s continued use of the Cloud Contact Center Services at any time shall constitute Customer’s agreement to the most recently revised terms and conditions of the Cloud Contact Center EULA and/or the Cloud Contact Center SLA, as applicable.

## ARTICLE 8 – VIDEO SERVICE PROVISIONS

If Customer receives video Services (“**Video Services**”) from Provider, then, in addition to the provisions of the applicable Agreement, Customer’s use of the Video Services is also subject to the terms and conditions of this Article 8:

8.1 Price Increases. After the first twelve (12) months of the Initial Service Term, the MRC for the Video Services is subject to increase; provided, that in no event shall any such increase exceed Provider’s increased direct costs to deliver the Video Services. Should Provider elect to increase the price of some or all of the Video Services provided to Customer, Provider shall give Customer at least thirty (30) days’ advance written notice specifying the amount of the price increase.

8.2 Additional Charges. The MRC for Video Services that is specified on Customer’s Service Order does not include Applicable Taxes, franchise fees, FCC regulatory fees, broadcast station retransmission fees (aka RTC fees), certain sports programming fees or any charges or fees imposed by a governmental authority on the provision of the Video Services, all of which shall be passed through to Customer as additional line items on Provider’s monthly invoice to Customer for the Video Services.

8.3 Channel Line-Up. Provider may at any time and from time to time change the number and/or identity of the signals comprising the Video Services and/or the placement of those signals (aka the “channel line-up”). In connection with providing the Video Services to Customer, Provider and/or its authorized agents and equipment manufacturers may send code updates to Customer’s equipment including, but not limited to, cable modems, digital interactive televisions with CableCARDS, MTAs, HD DTAs or other similar equipment at any time. Such code updates may change, add or remove features or functionality of any such equipment or the Video Services.

8.4 Restricted Viewing in Public Areas. Pursuant to the provisions of one or more of Provider’s programming agreements with video content providers, Customer may be restricted from showing certain channels available to it via the Video Services in

public areas (e.g., meeting rooms, lobbies, exercise rooms, restaurants, etc.). Customer agrees not to display the Video Services in public areas. Provider shall not be liable to Customer or to any third party should Customer violate this restriction.

8.5 Separate Music Licenses. Customer may be required by law to obtain separate music performance license(s) if Customer uses the audio component of the Video Services in public areas (e.g., meeting rooms, lobbies, exercise rooms, restaurants, etc.). Customer is solely responsible for: (a) investigating and determining the need for such license(s); and (b) taking all steps necessary to obtain and pay for such license(s).

8.6 No Unauthorized Distribution. The Video Services provided to Customer are for the sole benefit of Customer and its employees, contractors, agents, and/or end-users who occupy the Service Site. Customer shall not re-sell or allow redistribution of the Video Services to any third party or to any other location, either in whole or in part, whether directly or indirectly, and whether on an integrated or unintegrated basis. Customer is responsible for all access to and use of the Video Services by means of Customer's equipment and/or internal wiring, whether or not Customer has actual knowledge of or authorizes such access or use. Customer agrees to implement commercially reasonable security measures to prevent unauthorized use of, access to, or redistribution of the Video Services.

8.7 Performance; Technical Support. Provider shall use commercially reasonable efforts in keeping with normal industry standards to ensure that the Video Services are available twenty-four (24) hours per day, seven (7) days per week. It is possible, however, that there will be interruptions of the Video Services. Customer understands and agrees that the Video Services may be unavailable from time to time either for scheduled or unscheduled maintenance, technical difficulties, or for other reasons beyond Provider's reasonable control. Temporary service interruptions for such reasons, as well as all service interruptions caused by Customer's employees, contractors, agents, or end-users, will not constitute failures by Provider to perform its obligations under the Agreement. If Provider responds to a request from Customer for technical support and Provider determines that the problem was due to or caused by Customer or its employees, agents, or end-users, or by Customer's equipment, rather than any aspect of Provider's network or equipment, then Customer shall compensate Provider for its time spent troubleshooting the problem at Provider's then-current rates.

8.8 Right to Audit. Provider may, at any time during the Service Term, upon reasonable advance notice to Customer, enter onto the Service Site to perform an audit verifying that Customer's use of the Video Services complies with the provisions of the applicable Agreement and this Services Addendum. Should Provider reasonably determine, whether through an audit or otherwise, that Customer's use of the Video Services has violated any provision of the Agreement or this Services Addendum, Customer agrees to immediately correct the violation.

8.9 Cooperation with Technology Upgrades. During the Service Term it is possible that technological changes, improvements or enhancements will make it necessary for Provider to substitute new/different equipment at Customer's Service Site in order for Customer to continue receiving the Services. Customer agrees to reasonably cooperate with Provider in connection with any such technology upgrades.

## ARTICLE 9 – CLOUD HOSTING SERVICE PROVISIONS

If Customer receives Cloud Hosting Services ("**Cloud Hosting Services**") from Provider, then, in addition to the provisions of the applicable Agreement, Customer's use of Provider's Cloud Hosting Services is also subject to the terms and conditions of this Article 9:

9.1 Incorporation of 11:11 Systems Documents. Provider's Cloud Hosting Services are provided through and by a third-party provider called 11:11 Systems. Customer's use of the Cloud Hosting Services is subject to the following policies established by 11:11 Systems, which are incorporated herein by this reference:

- (a) The Service Schedule posted on the 11:11 Systems website at the following URL: <https://1111systems.com/legal/service-schedule> (the "**Cloud Hosting Service Schedule**"); and

- (b) The Acceptable Use Policy posted on the 11:11 Systems website at the following URL: <https://1111systems.com/legal/acceptable-use-policy/> (the “Cloud Hosting AUP”).

For purposes of this Services Addendum, all references in the Cloud Hosting Service Schedule and the Cloud Hosting AUP to “11:11 Systems” shall be deemed to be references to “Provider.” Both the Cloud Hosting Service Schedule and the Cloud Hosting AUP may be updated at any time and from time to time without notice to Customer. Customer understands and agrees that it is Customer’s responsibility to review both the Cloud Hosting Service Schedule and the Cloud hosting AUP with reasonable frequency to keep abreast of any changes. Customer’s continued use of the Cloud Hosting Services after any update to the Cloud Hosting Service Schedule and/or the Cloud Hosting AUP shall constitute Customer’s agreement to the revised terms and conditions of the Cloud Hosting Service Schedule and/or the Cloud Hosting AUP, as applicable.

9.2 Potential Price Increases. Provider retains the right, at any time during the Service Term of an Agreement for Cloud Hosting Services, to increase the MRC for the Cloud Hosting Services to pass-through price increases imposed on Provider; provided, that in no event shall any such increase exceed Provider’s increased direct costs to deliver the Cloud Hosting Services to Customer. Provider shall give Customer at least thirty (30) days’ advance written notice of any such price increases.

9.3 Software Licenses; Audit Rights. Customer expressly acknowledges that in connection with Customer’s use of the Cloud Hosting Services and/or as a requirement for Customer to be able to use the Cloud Hosting Services, Provider may provide Customer with a license or the right to use certain software under the terms of a separate license from a third-party licensor. **CUSTOMER EXPRESSLY ACKNOWLEDGES THAT ITS RIGHTS TO USE SUCH SOFTWARE ARE LIMITED TO THE RIGHTS PROVIDED BY THE THIRD PARTY LICENSOR AND THAT ANY AND ALL CLAIMS THAT CUSTOMER MAY HAVE CONCERNING OR RELATING TO SUCH SOFTWARE REGARDING THE PERFORMANCE OR FUNCTIONALITY OF SUCH SOFTWARE OR ANY SERVICES RELATED THERETO SHALL BE BROUGHT EXCLUSIVELY AGAINST THE THIRD PARTY LICENSOR OF SUCH SOFTWARE AND NOT AGAINST PROVIDER. PROVIDER DOES NOT MAKE ANY WARRANTIES CONCERNING THE PERFORMANCE OR FUNCTIONALITY OF ANY SOFTWARE (INCLUDING ANY RELATED SERVICES THAT MAY BE AVAILABLE FROM THE THIRD-PARTY LICENSOR OR OTHERWISE) DISTRIBUTED BY PROVIDER IN CONNECTION WITH THE CLOUD HOSTING SERVICES, AND PROVIDER HEREBY DISCLAIMS AND EXCLUDES ALL SUCH WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES FOR MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, OR SATISFACTORY QUALITY, WHETHER AT COMMON LAW, IN CONTRACT OR TORT OR BY STATUTE, OR OTHERWISE.** At reasonable intervals and upon at least five (5) days’ prior notice to Customer, Provider shall have the right to audit the records of Customer that document software licenses purchased or used by Customer in connection with Customer’s use of the Cloud Hosting Services. Customer shall cooperate reasonably (and at its own expense) with Provider’s exercise of the audit rights set forth in this Section.

9.4 Compliance with Laws; Data Protection Laws. Customer’s use of the Cloud Hosting Service shall at all times comply with all applicable laws, rules and regulations of any governmental authority having valid jurisdiction over Customer, including without limitation Data Protection Laws, as defined below.

(a) Definitions. For purposes of the Cloud Hosting Services, the following terms shall have the meanings set forth below:

- (i) “**Data Protection Laws**” means (A) all governmental laws, codes, rules, orders, and regulations applicable to the collection, storage, use, and other processing of Customer information (including without limitation data privacy laws applicable to Customer or Customer Data); and (B) all industry standards, codes of conduct, and best practices applicable to the collection, storage, use, and other processing of Customer information, including Payment Card Industry (PCI) standards. Data Protection Laws include, without limitation, Massachusetts Regulation 201 CMR 17.00; California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018(CCPA)); California Proposition 24 (also known as the California Privacy Rights Act (CPRA)); the U.S. Health Insurance Portability and Accountability Act of 1996; the Gramm-Leach-Bliley Act (GLBA); the U.S. Health Information Technology for Economic and Clinical Health Act (in each case as amended repealed,

consolidated or replaced from time to time); and any other data protection laws and regulations relating to data protection and privacy that apply to Customer's handling or use of Protected Information.

- (ii) **"Customer Data"** means all Customer data (including Protected Information) and software hosted or otherwise stored by Provider in connection with the provision of the Cloud Hosting Services.
- (iii) **"Protected Information"** means personally identifiable information (including, without limitation, credit card numbers, individuals' dates of birth, and tax identification numbers) that is transmitted or maintained in any form or medium by Customer in connection with the Cloud Hosting Services and which is subject to Data Protection Laws.

(b) Compliance with Data Protection Laws. Customer acknowledges that at all times it is responsible for understanding and complying with applicable Data Protection Laws in its use of the Cloud Hosting Services. In addition, and consistent with (and without limiting) this general obligation, Customer further agrees that:

- (i) Customer shall use the Cloud Hosting Services to store or transmit Protected Information only in compliance with applicable Data Protection Laws;
- (ii) Customer shall not use the Cloud Hosting Services for the storage or transmission of Protected Information unless the Protected Information has been secured by Customer so as to render it unusable, unreadable, or indecipherable to unauthorized individuals through the use of valid encryption processes or other applicable safeguards; and
- (iii) Customer shall utilize processes on all Protected Information to be transmitted or stored using the Cloud Hosting Services to ensure that the Protected Information is encrypted (1) during transmission to and from storage using the Cloud Hosting Services, and (2) at all times while stored using the Cloud Hosting Services.

(c) Indemnification by Customer of Provider. Customer shall defend, indemnify, and hold Provider and its Affiliates and its and their respective officers, directors and employees harmless from any and all claims under Data Protection Laws relating to Customer's use of Provider's networks and services (including the Cloud Hosting Services) for the storage and processing or other usage of any kind of Protected Information or any other Customer Data (including Protected Information).

#### 9.5 Recommendation to Maintain Other Cop(y/ies) of Customer Data.

(a) Acknowledgement of Recommendation. Customer acknowledges that the Cloud Hosting Services are not intended to be used as the sole repository for any Customer data or information (including, without limitation, Customer Data and Protected Information) or software, and that Customer is advised to maintain a separate copy or copies of all Customer data and information (including, without limitation, Customer Data and Protected Information) and software stored by Provider in connection with the Cloud Hosting Services on servers other than those provided or maintained by Provider (or Provider's contractor(s)) in connection with the provision of the Cloud Hosting Services.

(b) No Liability for Lost or Damaged Data. NOTWITHSTANDING ANYTHING TO THE CONTRARY SET FORTH ELSEWHERE IN THE AGREEMENT FOR CLOUD HOSTING SERVICES, UNDER NO CIRCUMSTANCES SHALL PROVIDER HAVE ANY LIABILITY TO CUSTOMER FOR OR IN RESPECT OF (i) THE COSTS OF RELOADING, REPLACING, OR RECREATING ANY LOST OR DAMAGED INFORMATION, DATA OR SOFTWARE (INCLUDING, WITHOUT LIMITATION, ANY CUSTOMER DATA AND/OR PROTECTED INFORMATION), OR (ii) THE LOSS OF ANY INFORMATION, DATA OR SOFTWARE IN ANY WAY TRANSMITTED OR STORED USING PROVIDER'S NETWORKS OR SERVICES (INCLUDING, WITHOUT LIMITATION, THE CLOUD HOSTING SERVICES).

9.6 Early Termination by Provider Due to Termination by Hosting Vendor. In addition to the provisions of the Agreement regarding early termination of the Cloud Hosting Services, in the event that, at any time during the Service Term for Cloud Hosting

Services, 11:11 Systems (the third-party vendor that is providing the Cloud Hosting Services to Provider), terminates the services it provides to Provider for any reason, then Provider may terminate the Cloud Hosting Services it is providing to Customer by giving Customer at least sixty (60) days’ advance written notice of termination. In the event Provider terminates the Cloud Hosting Services pursuant to this Section 9.6, Customer will pay to Provider all outstanding NRC and the MRC (and any other applicable amounts then due to Provider pursuant to the Agreement) for the Cloud Hosting Services provided by Provider prior to the date of termination, and thereafter neither Party will have any further liability to the other with respect to the terminated Cloud Hosting Services.

9.7 Effect of Termination.

(a) Destruction of Data Upon Termination. Within ninety (90) days after the expiration or earlier termination of the Agreement for Cloud Hosting Services, Provider will destroy all Customer Data hosted or stored by Provider in connection with the Cloud Hosting Services in accordance with the NIST 800-88 data destruction standards. During the ninety (90) day period between the expiration or earlier termination of the Agreement for Cloud Hosting Services and destruction of the Customer Data, Customer is responsible for migrating the Customer Data to a new location at Customer’s sole risk, cost and expense, and Customer acknowledges that once Customer Data has been destroyed by Provider, it can no longer be recovered or otherwise restored. Upon the expiration or earlier termination of a Service Order for Cloud Hosting Services, Customer may request and prepay Provider for a period not to exceed 90 days during which Provider will not destroy the Customer’s Data (a “**Transition Period**”). Customer may also request that Provider assist with the migration of Customer’s Data either prior to the expiration or earlier termination of the Agreement or during the Transition Period. Provider’s continued hosting or storage of Customer Data during a Transition Period and any migration assistance provided by Provider shall be subject to the Parties’ execution of a new order or an amendment to the original Services Order (either, a “**Transition Services Order**”), and further shall be at Customer’s expense, as provided for in the applicable Transition Services Order. **Customer acknowledges that in the absence of a duly executed Transition Services Order, all Customer Data stored by Provider as part of the Cloud Hosting Services will be irretrievably destroyed in the manner specified in the first sentence of this Section 9.7(a).**

(b) Cessation of Software Use. Immediately upon the expiration or earlier termination of the Agreement for Cloud Hosting Services, Customer shall uninstall and discontinue all use of any software in respect of which a software license was provided by Provider pursuant to the terminated or expired Agreement or otherwise in connection with Customer’s use of the Cloud Hosting Services.

9.8 Service Level Agreement for Cloud Hosting Services. This Section 9.8 constitutes the service level agreement (“**SLA**”) applicable to the Cloud Hosting Services. Customer expressly understands and agrees that Provider’s service level agreements for lit fiber services and/or for wavelength and dark fiber services, do not apply to the Cloud Hosting Services. Instead, the SLA set forth in this Section 9.8 is the only SLA applicable to the Cloud Hosting Services.

(a) Infrastructure and Service Availability. Provider shall use commercially reasonable efforts to make sure that the Cloud and Datacenter Resources are available each calendar month according to the table below.

| Service   | Availability |
|---|--------------|
| Bare Metal  | 100%         |
| Colocation  | 100%*        |
| IaaS (Astound Cloud and Astound Secure Cloud)         | 100%         |
| BaaS (Astound Secure Cloud Backup)                    | 100%         |
| DRaaS (Astound Secure Disaster Recovery as a Service) | 100%         |
| Astound Secure Cloud Backup for Office 365            | 100%         |



|                                     |      |
|-------------------------------------|------|
| Astound Secure Cloud Object Storage | 100% |
|-------------------------------------|------|

\*This colocation availability SLA is exclusively applicable to infrastructure provided by Provider, and it applies only if the Customer provided equipment supports dual power connected to redundant A+B power circuits.

The Cloud Hosting Services will be deemed unavailable if (1) the Customer can neither transmit nor receive data to or from the Cloud Hosting Services (where the inability to transmit or receive data is confirmed by way of Customer documentation that verifies said inability is due to an issue with Provider’s equipment), and (2) such inability has been communicated to Provider in sufficient detail to enable Provider to open a case in respect thereof. The Cloud Hosting Services shall not be deemed unavailable (without limitation) in the event of any one or more of the following:

- (i) Any circumstances whatsoever which are not within the reasonable control of Provider or its subcontractor(s);
- (ii) Force Majeure events;
- (iii) Virus activity and/or hacking attempts;
- (iv) In accordance with a court order or any requirements of any authority or other competent local authority;
- (v) Periods of scheduled or emergency maintenance on Provider-provided infrastructure of which the Customer has been notified;
- (vi) Failure or malfunction of the Customer’s (or Customer’s end-user’s) connection to the Provider Network (e.g. via the public internet or the Customer’s own network) or related problem beyond the Provider Network Demarcation Point;
- (vii) Failure or malfunction of equipment, software, or other technology not owned or controlled by Provider;
- (viii) Failure to comply with any terms of the then-current Cloud Hosting Service Schedule and/or Cloud Hosting AUP;
- (ix) Failure or malfunction caused by Customer over-provisioning Reserved Resources in excess of the specifications set out on the Work Order;
- (x) A malfunction that results from inconsistencies in the environment or unavailability that result from changes in the Customer’s source environment, including either intentional or accidental connection or disconnections to the environment;
- (xi) A malfunction that results from any action or inactions of Customer or any third party;
- (xii) A malfunction that results from anyone gaining access to the Cloud Resources by means of Customer’s passwords or equipment;
- (xiii) Any failure to restore an environment from a Cloud Backup file chain in Astound Cloud Services (Astound Secure Cloud Backup with Veeam only); or
- (xiv) Unavailability of any management console or APIs.

In the event Customer experiences unavailability or any other problems with Customer’s Cloud Hosting Services, Customer must contact Provider’s network operations center (“**NOC**”) and open a Trouble Ticket regarding the problem. The duration of any unavailability or other failure to meet the target metrics set forth in this SLA commences when Customer opens a Trouble Ticket regarding the problem and ends when the problem has been resolved and the Cloud Hosting Services are again functioning properly.

(b) Cloud Storage Service Performance.

(i) Storage Performance Target. Provider may offer different storage types with targeted performance according to the following chart:

| Storage Type                 | Average Performance | Average Response Time Target (Read/Write) |
|------------------------------|---------------------|---|
| Advanced/Accelerated Storage | 500 IOPS per TB     | 1 ms (millisecond)                        |
| SSD Storage                  | 2000 IOPS per TB    | 1 ms (millisecond)                        |

(ii) Storage Performance Limits. The storage is capable of very high IOPS, and that enables Provider to allow Customers to occasionally burst IOPS over the guaranteed aggregated average IOPS for no additional charge. However, if Provider determines, in its sole discretion, that the Customer's IOPS bursting is excessive or detrimental to overall storage performance, then, Provider will notify the Customer about the excessive bursting and work with the Customer to: (1) correct the issue causing the excessive bursting, or (2) upgrade to the next available storage tier. If the Customer and Provider cannot come to a resolution within 30 days after the notice, Provider shall, at its sole discretion, rate limit such IOPS until the Customer can correct the issue causing the excessive bursting.

(c) DRaaS Service Performance.

(i) Recovery Time Objective (RTO). Once the Customer has completed a successful test of the then-current Recovery Plan with Provider's involvement, Provider shall use commercially reasonable efforts to ensure that Failover occurs at the average rate of 1 Virtual Machine per minute; and

(ii) Recovery Point Objective (RPO). Customer's RPO is determined and reflected based on settings in the replication engine software, and, as a result, Provider can only offer guarantee on best efforts in assisting Customer to achieve that RPO dependent on Customer's bandwidth and configuration.

| Type                           | SLA                                     |
|--------------------------------|---|
| Recovery Time Objective (RTO)  | Average of 1 Virtual Machine per Minute |
| Recovery Point Objective (RPO) | Based on Recovery Group settings        |

(d) Technical Ticket Response Service Performance. Provider shall use commercially reasonable efforts to make sure that the Technical Ticket Response Management process adheres to the Targets set out in the chart below.

| Severity   | Description  | Initial Response Target | Resolution Target | Response Target |
|------------|--|-------------------------|-------------------|-----------------|
| Severity 1 | <u>Production system down</u> : A service is "down" or there is a critical impact to the customer's business operations.                                   | < 15 mins               | < 2 hrs           | 100%            |
| Severity 2 | <u>System impaired</u> : Customer's business has moderate loss or degradation of services and can reasonably continue in an impaired or restricted manner. | < 30 mins               | < 4 hrs           | 100%            |

|            |  |         |          |      |
|------------|--|---------|----------|------|
| Severity 3 | <u>General guidance</u> : Customer has a general question or need help using an Astound product/service. | < 2 hrs | < 16 hrs | 100% |
|------------|--|---------|----------|------|

(e) **Billing Credits**. If Provider does not meet its obligations under the terms of this SLA during a particular month during the Service Term, Provider shall, at the Customer’s request, provide the applicable service credit (“**Credit**”) set out in the chart below. The Credits in this Section shall not apply to Customers that have contracted with Provider through either a Veeam Service Agreement or a third party Reseller.

| Condition   | Billing Credit  |
|---|---|
| Monthly Uptime Percentage < 100.00% and >= 99.95% | 1% of Monthly Service Fee Billed for Affected Cloud/Data Center Resource  |
| Monthly Uptime Percentage < 99.95% and >= 99.00%  | 5% of Monthly Service Fee Billed for Affected Cloud/Data Center Resource  |
| Monthly Uptime Percentage < 99.00% and >= 98.00%  | 10% of Monthly Service Fee Billed for Affected Cloud/Data Center Resource |
| Monthly Uptime Percentage < 98.00%                | 15% of Monthly Service Fee Billed for Affected Cloud/Data Center Resource |

The following conditions must be met to be eligible for Credits:

(i) To be eligible for any SLA-related Credit, Customer must be current in its financial obligations to Provider. A Credit shall be applicable and issued only if the aggregate amount of Credits for the applicable monthly billing cycle is greater than ten dollars (\$10 USD). Provider shall only apply Credit against future payments otherwise due from Customer. Credits are not transferable or redeemable for cash. Credits may not be transferred or applied to any other account.

(ii) To request a Credit, the Customer must submit a written request for the Credit to Customer’s account manager within fifteen (15) days after the end of the calendar month in which the incident giving rise to the Credit occurred. Customer’s request must include the following information: (1) Customer name and contact information; (2) Trouble Ticket number(s); (3) the date and beginning/end time of the claimed outage or failed SLA metric; and (4) a brief description of the characteristics of the claimed outage or failed SLA metric. If Customer fails to timely submit, pursuant to the procedure described in this Section, a request for any SLA-related Credit for which Customer might otherwise be eligible under this SLA, Customer shall be deemed to have waived its right to receive such Credit. The Credits provided by this SLA are Customer’s sole and exclusive remedies for any and all claims or complaints regarding the quality and/or availability of any of the Cloud Hosting Services to which this SLA applies.

(iii) All claims for SLA-related Credits and other remedies are subject to evaluation and verification by Provider. Upon receiving a claim for SLA-related Credit or other remedy, Provider will evaluate the claim and respond to Customer within thirty (30) days. If Provider requires additional information in order to evaluate Customer’s claim, Provider will notify Customer by email specifying what additional information is required. Customer will have fifteen (15) days from the date on which it receives Provider’s request for additional information in which to provide the requested information. If Customer fails to provide the additional information within that time period, Customer will be deemed to have abandoned its claim. Provider will promptly notify Customer of Provider’s resolution of each Customer claim. If Customer’s claim for an SLA-related Credit or other remedy is rejected, the notification will specify the basis for the rejection. If Customer’s claim for a Credit is approved, Provider will issue the Credit to Customer’s account, to appear on the next monthly invoice. Provider’s good faith determination regarding whether or not a Credit is due shall be final.

(iv) Total Credits for any given calendar month shall not exceed 100% of the MRC for the affected Cloud Hosting Services. Credits shall not be cumulative with respect to any given incident; instead, if multiple SLAs are violated during a single incident, Customer shall be entitled only to the largest applicable Credit amount. This SLA will not apply and Customer will not be entitled to any Credit under this SLA for any impairment of the Cloud Hosting Services that is caused by or due to any of the following: (i) the acts or omissions of Customer, its agents, employees, contractors, or Customer's end-users, or other persons authorized by Customer to access, use or modify the Cloud Hosting Services; (ii) the failure of or refusal by Customer to reasonably cooperate with Provider in diagnosing and troubleshooting problems with the Cloud Hosting Services; (iii) scheduled service alteration, maintenance or implementation; (iv) the failure or malfunction of network equipment or facilities not owned or controlled by Provider; or (v) Force Majeure Events.

#### **ARTICLE 10 – DARK FIBER SERVICE PROVISIONS**

If Customer receives dark fiber Services ("**Dark Fiber Services**") from Provider, then, in addition to the provisions of the applicable Agreement, Customer's use of Provider's Dark Fiber Services is also subject to the terms and conditions of this Article 10:

10.1 Grant of License. Beginning on the Service Commencement Date for each segment of dark fiber (as determined pursuant to the applicable provisions of the Agreement), and continuing through the Service Term of the Agreement, Provider grants to Customer, and Customer accepts from Provider, a license (the "**License**") to use the specified number of dark fiber strands on the segment(s) specified in the Agreement (the "**Licensed Fibers**") by accessing same solely at the A Location and Z Location end points (the "**End Points**") specified in the Agreement. Customer is not permitted to access the Licensed Fibers at any location other than the End Points. The License does not include any right on Customer's part to: (i) own, control, possess, encumber, repair or maintain, or cause or permit any lien to attach to the Licensed Fibers, any Provider-owned equipment, or any other property of Provider; or (ii) use or access any of the other fiber optic strands that may be in the same cable bundle as the Licensed Fibers.

10.2 Route of Licensed Fibers. Provider shall at all times have full and complete discretion to choose the route along which the Licensed Fibers are installed between the End Points. That route will not necessarily be the most direct route between the End Points. Provider may, from time to time, elect to change the route along which the Licensed Fibers are installed. So long as the technical specifications for each Fiber Route continue to be met, Customer shall have no authority to approve or disapprove of any particular installation route. In the event of any route relocation, Provider shall use commercially reasonable efforts to minimize the disruption to Customer's use of the Licensed Fibers.

10.3 Provider's Retained Rights. Provider retains the exclusive right to provide services using, or to sell or lease to other customers or end-users any fibers (other than the Licensed Fibers) contained in the same cable bundle as the Licensed Fibers. Provider shall not use the Licensed Fibers during the Service Term of the Agreement.

10.4 Standard Technical Specifications. Provider's dark fiber will typically comply with the following specifications: (i) the maximum bi-directional average splice loss shall not exceed 0.15 dB; and (ii) the attenuation shall not exceed 0.25 dB/km when measured at a wavelength of 1550 nm. If the Agreement contains different technical specifications from those listed above, the technical specifications set forth in the Agreement will control.

#### **ARTICLE 11 – REMOTE VIRTUAL OFFICE SERVICE PROVISIONS**

If Customer receives remote virtual office Services ("**Remote Virtual Office Services**") from Provider, then, in addition to the provisions of the applicable Agreement, Customer's use of Remote Virtual Office Services is also subject to the terms and conditions of this Article 11:

11.1 Component Services. Provider's Remote Virtual Office Services comprise a combination of Advanced Security with SD-WAN Services (see Article 3), Hosted Voice Services (see Article 5), Video Conferencing Services (see Article 6), as well as any other optional add-on Services selected by Customer as specified in the applicable Agreement. Accordingly, the provisions of this

Services Addendum that apply to the component Services comprising Remote Virtual Office Services also apply to the Remote Virtual Office Services.

#### 11.2 End-Users.

(a) In General. Provider's Remote Virtual Office Services are available for purchase by Provider's business customers with the intention that the business customer will deploy the individual seat packages to members of its end-user work force. Provider's Remote Virtual Office Services are intended to permit those end-users to perform their work activities from their homes or other locations that are geographically separate from the Customer's office space. Thus, the actual users of Remote Virtual Office Services will generally be the Customer's employees and/or contractors (the "**End-Users**").

(b) No Contractual Relationship Between End-Users and Provider. Notwithstanding that the End-Users will be the actual users of Remote Virtual Office Services, there is no contractual relationship between Provider and any one or more of the End-Users. Instead, the contractual relationship with respect to the Remote Virtual Office Services is solely between Provider and the Customer that executes the Agreement with Provider for the Remote Virtual Office Services. Customer is responsible to Provider for all activities performed by its End-Users using the Remote Virtual Office Services, including any unauthorized or illegal use or activities, and including the repair and/or replacement of any equipment (whether owned by Provider or Customer) that is damaged while in the End-User's possession. Accordingly, it is Customer's responsibility to ensure that all of Customer's End-Users comply with the terms of the Agreement and this Services Addendum, and any other applicable Provider policies.

(c) Technical Support for End-Users. Provider does not provide direct technical support for Remote Virtual Office Services to any End-Users. Instead, Provider will provide any needed technical support only to Customer directly. It is solely Customer's responsibility to provide technical support to its own End-Users.

11.3 Underlying Internet Connection Required. Remote Virtual Office Services are cloud-hosted Services that require an underlying Internet connection in order to operate. The underlying Internet connection does not need to be provided by Provider; it may be provided by any Internet access provider. However, the Remote Virtual Office Services will not function if the End-User does not have an active connection to the Internet. Customer expressly acknowledges and agrees that each End-User is responsible for obtaining and maintaining his/her own underlying Internet access connection, and that Provider has no liability or responsibility whatsoever for any End-User's Internet access connection.

11.4 Performance of Remote Virtual Office Services. Because Remote Virtual Office Services rely on the End-User's Internet connection to operate, the performance each End-User of the Remote Virtual Office Services experiences at any given time may vary and fluctuate depending on the attributes of that End-User's underlying Internet access connection.

11.5 Purchased Equipment. Remote Virtual Office Services may require the purchase of certain auxiliary equipment, such as headsets, HD video cameras, desktop phones, tablets, or other devices (the "**Purchased Equipment**"), that become the property of Customer upon delivery of the equipment to the End-User. Upon the End-User's acceptance of the Purchased Equipment, the Purchased Equipment shall become and remain Customer's personal property. As between Provider and Customer, Customer shall be solely responsible for the repair and maintenance of all Purchased Equipment and any and all obligations and liabilities associated therewith. **CUSTOMER ACKNOWLEDGES THAT THE PURCHASED EQUIPMENT IS NOT MANUFACTURED BY PROVIDER AND THAT PROVIDER DOES NOT SUPPORT AND SHALL HAVE NO MAINTENANCE OBLIGATIONS OR OTHER LIABILITY REGARDING SAME.** PROVIDER WILL EITHER DELIVER THE MANUFACTURER'S WARRANTY FOR THE PURCHASED EQUIPMENT DIRECTLY TO CUSTOMER OR PASS THE MANUFACTURER'S WARRANTY THROUGH TO CUSTOMER AS-IS, DEPENDING ON THE APPLICABLE MANUFACTURER'S POLICY. PROVIDER HEREBY ASSIGNS TO CUSTOMER ALL OF THE MANUFACTURERS' WARRANTIES AND INDEMNITIES RELATING TO THE PURCHASED EQUIPMENT TO THE EXTENT PROVIDER IS PERMITTED BY THE MANUFACTURER TO MAKE SUCH ASSIGNMENT TO CUSTOMER. SUCH ASSIGNMENT IS SUBJECT TO ALL OF THE TERMS AND CONDITIONS IMPOSED BY THE MANUFACTURER WITH RESPECT THERETO. CUSTOMER'S REMEDY FOR DEFECTIVE PURCHASED EQUIPMENT SHALL BE AS SET FORTH IN THE APPLICABLE MANUFACTURER'S WARRANTY, WHICH IS CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF AN EQUIPMENT WARRANTY. PROVIDER DOES NOT EXTEND ANY WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE, EITHER TO CUSTOMER OR TO CUSTOMER'S



**Business Solutions** Powered by **RCN** | **GRANDE** | **WAVE**

END-USERS, FOR ANY PURCHASED EQUIPMENT PURCHASED BY CUSTOMER, NOR SHALL PROVIDER HAVE ANY LIABILITY FOR ANY LOSS, DAMAGE, OR EXPENSE DIRECTLY OR INDIRECTLY ARISING FROM CUSTOMER'S (OR ITS END-USERS') USE OF (OR INABILITY TO USE) THE PURCHASED EQUIPMENT. Any questions concerning or requests for maintenance or repair of the Purchased Equipment should be directed to the manufacturer of the Purchased Equipment at issue. If Purchased Equipment impairs use of the Remote Virtual Office Services by Customer or any End-User, Customer will remain liable for payment of the Fees for the Remote Virtual Office Services. If, at Customer's request, Provider attempts to resolve difficulties caused by Purchased Equipment, Customer will be responsible for Provider's then-current commercial rates and terms for such consulting services on a time and materials basis.