

Master Agreement #: AR2474

State of Tennessee Master Contract # 62011

Contractor: CENTURYLINK

Participating Entity: STATE OF TENNESSEE

The following products or services are included in this Contract portfolio:

Networking
Delta Port
Software-Defined Networking (SD-WAN)
DDoS Mitigation
Wavelength

These products or services fall under the following:

1. Software as a Service
2. Platform as a Service
3. Infrastructure as a Service
4. Value added Services

Definitions shall be as follows or as designated and defined in the terms and conditions of this Participating Addendum:

1. **Agency**. The term "Agency" shall mean each State of Tennessee board, commission, committee, department, officer, or any other unit of the State of Tennessee government.
2. **Cloud Solutions**. The term "Cloud Solutions" shall refer to the products and services offered under NASPO ValuePoint Master Agreement # AR2474.
3. **"Contract"** or **"Agreement"** means this Participating Addendum, including all referenced attachments and documents incorporated by reference, including but not limited to Contractor's ValuePoint Master Agreement #AR2474.
4. **Contractor**. The term "Contractor" shall mean a person or legal entity with the legal capacity to enter into contracts to provide goods or services to the State.
5. **Infrastructure as a Service ("IaaS")**. The term "IaaS" shall refer to the Contractor's capability to provide the State with provision processing, storage, networks, and other fundamental computing resources where the consumer is able

to deploy and run arbitrary software, which can include operating systems and applications.

6. **Platform as a Service ("PaaS")**. The term "PaaS" shall refer to the Contractor's capability to provide the State with deployment onto the cloud infrastructure consumer created or acquired applications created using programming languages and tools supported by the provider.
7. **Purchasing Entity**. The term "Purchasing Entity" shall mean a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a purchase order against the ValuePoint Master Agreement # AR2474 and becomes financially committed to the purchase.
8. **Services**. The term "Services" shall refer to the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Participating Addendum.
9. **Software as a Service ("SaaS")**. The term SaaS shall refer to the capability of the Contractor to provide the State with applications running on a Contractor's infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser or a program interface.
10. **Strategic Technology Solutions "STS"**. The term "STS" refers to a division within the State of Tennessee, Finance and Administration.
11. **ValuePoint Master Agreement**. The term "ValuePoint Master Agreement" # AR2474 shall refer to the contract reached between the State of Utah and CenturyLink.

Master Agreement Terms and Conditions:

1. **Scope**: This Participating Addendum covers the network Services identified in Section 8 hereof that are part of the **Cloud Solutions** led by the State of Utah for use by state agencies and other entities located in the State of Tennessee authorized by that State's statutes to utilize State contracts with the prior approval of the State's Chief Procurement Official.
2. **Participation**: This NASPO ValuePoint Master Agreement will only be used by STS or by use of Agencies with prior STS approval.
3. **Access to Cloud Solutions Services Requires State CIO Approval**: Unless otherwise stipulated in this Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Solutions by state executive branch agencies are subject to the authority and prior approval of the State Chief Information

Officer's Office. The State Chief Information Officer means the individual designated by the state Governor within the Executive Branch with enterprise-wide responsibilities for leadership and management of information technology resources of a state.

4. **Primary Contacts:** The primary contact individuals for this Participating Addendum are as follows (or their named successors):

Contractor

Name:	Levi Lohnes, Global Relationship Manager
Address:	51 Century Blvd, Ste 110, Nashville, TN 37214
Telephone:	615-454-8462
Fax:	615-986-2735
Email:	levi.lohnes@centurylink.com

Participating Entity

Name:	Sharon Pope, Category Specialist
Address:	312 Rosa L. Parks Avenue, Nashville, TN 37243
Telephone:	615-741-9588
Email:	sharon.pope@tn.gov

5. PARTICIPATING ENTITY MODIFICATIONS OR ADDITIONS TO THE MASTER AGREEMENT

These modifications or additions apply only to actions and relationships within the Participating Entity.

Participating Entity must check one of the boxes below.

☐ No changes to the terms and conditions of the Master Agreement are required.

☒ The following changes are modifying or supplementing the ValuePoint Master Agreement #AR2474 terms and conditions.

- 6.1 The following numbered sections in Master Agreement Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions are deleted in their entirety and replaced with the following:

Section 4, "Amendments" is deleted and replaced with the following:

4. **Modification and Amendment.** This Participating Addendum may be modified only by a written amendment signed by all Parties hereto and approved by all applicable State officials.

Section 5, "Assignments/Subcontracts" is deleted and replaced with the following:

5. **Assignment and Subcontracting.** The Contractor shall not assign this Participating Addendum or enter into a subcontract for any of the goods or

services provided under this Participating Addendum without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Participating Addendum. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Participating Addendum in whole or in part or the use of subcontractors in fulfilling the Contractor's obligations under this Participating Addendum.

Section 7, "Termination" is deleted and replaced with the following:

- 7.1. Termination for Convenience.** The State may terminate this Participating Addendum for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date; provided that any existing Orders will remain in place for the duration of the Order, subject to the terms of this Contract. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the State or for satisfactory, authorized services completed as of the termination date. Compensation to Contractor shall include actual, direct, and incurred costs of providing services not reasonably covered by fees previously paid by the State. In no event shall the State be liable to the Contractor for compensation for any goods neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Participating Addendum for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Participating Addendum.
- 7.2. Termination for Cause.** If the Contractor fails to properly perform its obligations under this Participating Addendum, or if the Contractor materially violates any terms of this Participating Addendum ("Breach Condition"), the State shall provide written notice to Contractor specifying the Breach Condition. If within thirty (30) days of notice, the Contractor has not cured the Breach Condition, the State may terminate the Participating Addendum and withhold payments in excess of compensation for completed services or provided goods. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any breach of this Participating Addendum by the Contractor and the State may seek other remedies allowed at law or in equity for breach of this Participating Addendum.

Section 8, "Confidentiality, Non-Disclosure, and Injunctive Relief" is deleted and replaced with the following:

8. **Confidentiality of Records.** Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law.

Section 9, "Right to Publish" is deleted and replaced with the following:

9. **Prohibited Advertising or Marketing.** The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Participating Addendum.

Section 12, "Force Majeure" is deleted and replaced with the following:

12. **Force Majeure.** "Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Participating Addendum. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Participating Addendum arising from a Force Majeure Event is not a default under this Participating Addendum or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Participating Addendum is not a Force Majeure Event under this Participating Addendum. Contractor will promptly notify the State of any delay caused by a Force

Majeure Event (to be confirmed in a written notice to the State as soon as the delay is known) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: cease payment of the fees until Contractor resumes performance of the affected obligations. Contractor will not increase its charges under this Participating Addendum or charge the State any fees other than those provided for in this Participating Addendum as the result of a Force Majeure Event.

Section 13, "Indemnification and Limitation of Liability" is deleted and replaced with the following:

13. Hold Harmless

a. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all third party claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity for any death, injury, or damage to property arising from the negligence or willful misconduct on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Participating Addendum. The Contractor further agrees it shall be liable for the reasonable cost of attorneys for the State to enforce the terms of this Participating Addendum.

In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

b. **Intellectual Property Indemnity.** The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor notice of any such claim or suit, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State's failure to

give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.

Section 16, "Insurance" is deleted and replaced with the following:

- 16. Insurance.** Contractor shall maintain insurance coverage as specified in this Section. The State reserves the right to amend or require additional insurance coverage, coverage amounts, and endorsements required under this Participating Addendum. Contractor's failure to maintain or submit evidence of insurance coverage, as required, is a material breach of this Participating Addendum. If Contractor loses insurance coverage, fails to renew coverage, or for any reason becomes uninsured during the Term, Contractor shall immediately notify the State. All insurance companies providing coverage must be: (a) authorized to do business in the State of Tennessee; (b) authorized by the Tennessee Department of Commerce and Insurance ("TDCI"); and (c) rated A- / VII or better by A.M. Best. All coverage must be on a primary basis and noncontributory with any other insurance or self-insurance carried by the State. Contractor agrees to name the State as an additional insured on any insurance policy with the exception of workers' compensation (employer liability) and professional liability (errors and omissions) insurance. All policies must contain an endorsement for a waiver of subrogation in favor of the State. The deductible or SIR and any premiums are the Contractor's sole responsibility. The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Participating Addendum including any indemnification or hold harmless requirements.

To achieve the required coverage amounts, a combination of an otherwise deficient specific policy and an umbrella policy with an aggregate meeting or exceeding the required coverage amounts is acceptable. For example: If the required policy limit under this Participating Addendum is for two million dollars (\$2,000,000) in coverage, acceptable coverage would include a specific policy covering one million dollars (\$1,000,000) combined with an umbrella policy for an additional one million dollars (\$1,000,000). If the deficient underlying policy is for a coverage area without aggregate limits (generally Automobile Liability and Employers' Liability Accident), Contractor shall provide a copy of the umbrella insurance policy documents to ensure that no aggregate limit applies to the umbrella policy for that coverage area. In the event that an umbrella policy is being provided to achieve any required coverage amounts, the umbrella policy shall be accompanied by an endorsement at least as broad as the Insurance Services Office, Inc. (also known as "ISO") "Noncontributory—Other Insurance Condition" endorsement or shall be written on a policy form that addresses both the primary and noncontributory basis of the umbrella policy if the State is otherwise named as an additional insured.

Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified in this Section. The COI must be on a form approved

by the TDCI (standard ACORD form preferred). The COI must list each insurer's National Association of Insurance Commissioners (NAIC) number and be signed by an authorized representative of the insurer. The COI must list the State of Tennessee – CPO Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 as the certificate holder. Contractor shall provide the COI ten (10) business days prior to the Effective Date and shall use best efforts to notify the State at least fifteen (15) calendar days upon renewal or replacement of coverage. Contractor shall provide the State evidence that all subcontractors maintain the required insurance or that subcontractors are included under the Contractor's policy. At any time, the State may require Contractor to provide a valid COI. The parties agree that failure to provide evidence of insurance coverage as required is a material breach of this Participating Addendum. If Contractor self-insures, then a COI will not be required to prove coverage. Instead Contractor shall provide a certificate of self-insurance or a letter, on Contractor's letterhead, detailing its coverage, policy amounts, and proof of funds to reasonably cover such expenses.

The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor or its insurer, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.

The insurance obligations under this Participating Addendum shall be: (1)—all the insurance coverage and policy limits carried by the Contractor; or (2)—the minimum insurance coverage requirements and policy limits shown in this Participating Addendum; whichever is greater. Any insurance proceeds in excess of or broader than the minimum required coverage and minimum required policy limits, which are applicable to a given loss, shall be available to the State. No representation is made that the minimum insurance requirements of the Participating Addendum are sufficient to cover the obligations of the Contractor arising under this Participating Addendum. The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits.

a. Commercial General Liability ("CGL") Insurance

- 1) The Contractor shall maintain CGL, which shall be written on an ISO Form CG 00 01 occurrence form (or a substitute form providing equivalent coverage) and shall cover liability arising from property damage, premises and operations products and completed operations, bodily injury, personal and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract). The Contractor shall maintain single limits not less

than one million dollars (\$1,000,000) per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this policy or location of occurrence or the general aggregate limit shall be twice the required occurrence limit.

b. Workers' Compensation and Employer Liability Insurance

- 1) For Contractors statutorily required to carry workers' compensation and employer liability insurance, the Contractor shall maintain:
 - i. Workers' compensation in an amount not less than one million dollars (\$1,000,000) including employer liability of one million dollars (\$1,000,000) per accident for bodily injury by accident, one million dollars (\$1,000,000) policy limit by disease, and one million dollars (\$1,000,000) per employee for bodily injury by disease.
- 2) If the Contractor certifies that it is exempt from the requirements of Tenn. Code Ann. §§ 50-6-101 – 103, then the Contractor shall furnish written proof of such exemption for one or more of the following reasons:
 - i. The Contractor employs fewer than five (5) employees;
 - ii. The Contractor is a sole proprietor;
 - iii. The Contractor is in the construction business or trades with no employees;
 - iv. The Contractor is in the coal mining industry with no employees;
 - v. The Contractor is a state or local government; or
 - vi. The Contractor self-insures its workers' compensation and is in compliance with the TDCI rules and Tenn. Code Ann. § 50-6-405.

c. Automobile Liability Insurance

- 1) The Contractor shall maintain automobile liability insurance which shall cover liability arising out of any automobile (including owned, leased, hired, and non-owned automobiles).
- 2) The Contractor shall maintain bodily injury/property damage with a limit not less than one million dollars (\$1,000,000) per occurrence or combined single limit.

d. Technology Professional Liability (Errors & Omissions)/Cyber Liability Insurance

- 1) The Contractor shall maintain technology professional liability (errors & omissions)/cyber liability insurance appropriate to the Contractor's profession in an amount not less than ten million dollars (\$10,000,000) per occurrence or claim and ten million dollars (\$10,000,000) annual aggregate, covering all acts, errors, omissions, negligence, infringement of intellectual property (except patent and trade secret); network security and privacy risks, including but not limited to unauthorized access, failure of security, information theft, damage to destruction of or alteration of electronic information, breach of privacy perils, wrongful disclosure and release of private information, collection, or other negligence in the handling of confidential information, and including coverage for related regulatory fines, defenses, and penalties.
 - 2) Such coverage shall include data breach response expenses, in an amount not less than ten million dollars (\$10,000,000) and payable whether incurred by the State or Contractor, including but not limited to consumer notification, whether or not required by law, computer forensic investigations, public relations and crisis management firm fees, credit file or identity monitoring or remediation services and expenses in the performance of services for the State or on behalf of the State hereunder.
- e. Umbrella Liability
- 1) The Contractor shall maintain an umbrella liability policy with limits no less than five million dollars (\$5,000,000) per occurrence or claim, and five million dollars (\$5,000,000) policy aggregate.
- f. Crime Insurance
- 1) The Contractor shall maintain crime insurance, which shall be written on a "loss sustained form" or "loss discovered form" providing coverage for third party fidelity, including cyber theft and extortion. The policy must allow for reporting of circumstances or incidents that may give rise to future claims, include an extended reporting period of no less than two (2) year with respect to events which occurred but were not reported during the term of the policy, and not contain a condition requiring an arrest or conviction.
 - 2) Any crime insurance policy shall have a limit not less than one million dollars (\$1,000,000) per claim and one million dollars (\$1,000,000) in the aggregate. This insurance may be written on a claims made basis, but in the event that coverage is cancelled canceled or non-renewed, the Contractor shall purchase an extending reporting or "tail coverage" of at

least two (2) years after the term.

Section 26, "Records Administration and Audit" is deleted and replaced with the following:

- 26. Records.** The Contractor shall maintain documentation for all charges under this Participating Addendum. The books, records, and documents of the Contractor, for work performed or money received under this Participating Addendum, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.

Section 31, "Warranty" is deleted and replaced with the following:

- 31. Warranty.** Contractor represents and warrants that the term of the warranty ("Warranty Period") shall be the greater of the Term of this Participating Addendum or any other warranty general offered by Contractor, its suppliers, or manufacturers to customers of its goods or services.

Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Participating Addendum.

Contractor will perform materially as described in this Participating Addendum, Master Agreement, SLA, and any SOW throughout any applicable Warranty Period.

Contractor represents and warrants that the State is authorized to possess and use all equipment, materials, software, and deliverables provided under this Participating Addendum.

Contractor represents and warrants that all goods or services provided under this Participating Addendum shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Contractor's industry.

Contractor warrants that the Products it provides under this Participating Addendum are free of malware as of the date of delivery of such Products. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

DISCLAIMER OF WARRANTIES.



EXCEPT AS EXPRESSLY PROVIDED IN ANY APPLICABLE SERVICE EXHIBIT, INCLUDING ANY SERVICE LEVEL AGREEMENT AND REMEDIES THEREUNDER, ALL SERVICES, SOFTWARE, AND PRODUCTS ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. CONTRACTOR MAKES NO REPRESENTATIONS OR WARRANTIES WHATSOEVER REGARDING USE OF THE SOFTWARE, AND MAKES NO WARRANTY THAT THE SOFTWARE OR USE THEREOF WILL BE UNINTERRUPTED, ERROR-FREE, OR VIRUS-FREE. CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, OR ANY WARRANTY OF NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. THE STATE ACKNOWLEDGES THAT THE SOFTWARE MAY INCLUDE VERSIONS OF SOFTWARE, APPLICATION PROGRAMMING INTERFACES, BUGS, VIRUSES AND OTHER ERRORS, MAY HAVE LIMITED FUNCTIONALITY, MAY BE SUBJECT TO INTERRUPTIONS OR DELAYS, MAY NOT PROCESS DATA PROPERLY, MAY NOT OPERATE IN ACCORDANCE WITH ANY SPECIFICATIONS OR DOCUMENTATION, AND/OR MAY NOT SUPPORT CUSTOMER'S BUSINESS REQUIREMENTS ("ERRORS"). ANY DOCUMENTATION, USER'S MANUALS, SPECIFICATIONS, AND OTHER MATERIALS SUPPLIED BY CONTRACTOR PERTAINING TO THE CLIENT SOFTWARE MAY CONTAIN INACCURACIES OR TYPOGRAPHICAL ERRORS. CONTRACTOR MAKES NO WARRANTIES OR REPRESENTATIONS ABOUT THE ACCURACY, RELIABILITY, OR COMPLETENESS OF ANY MATERIALS SUPPLIED IN CONNECTION WITH THE SOFTWARE OR ACCURACY OF ANY RESULTS OR OUTPUT RENDERED BY THE CLIENT SOFTWARE OR THAT THE CLIENT SOFTWARE IS ERROR-FREE, AND THE STATE AGREES THAT CONTRACTOR SHALL NOT BE LIABLE FOR ANY DAMAGE SUFFERED BY THE STATE IN CONNECTION WITH THE STATE'S USE OF THE CLIENT SOFTWARE, OR CAUSED BY SUCH ERRORS. THE STATE'S USE OF THE CLIENT SOFTWARE IS AT THE STATE'S OWN RISK. IF ANY EQUIPMENT OR SOFTWARE NOT PROVIDED BY CONTRACTOR IMPAIRS THE STATE'S USE OF ANY SERVICE, THE STATE WILL NONETHELESS BE LIABLE FOR PAYMENT FOR ALL SERVICES PROVIDED BY CONTRACTOR. FURTHERMORE, THE STATE UNDERSTANDS AND AGREES THAT AS A CONSEQUENCE OF THE OPERATION OF THE SERVICE, CONTRACTOR MAKES NO WARRANTY, GUARANTEE, OR REPRESENTATION, EXPRESS OR IMPLIED, THAT ALL LEGITIMATE COMMUNICATIONS WILL BE RECEIVED BY THE STATE.

IN ADDITION TO ANY OTHER DISCLAIMERS OF WARRANTY STATED IN THE AGREEMENT, CONTRACTOR MAKES NO WARRANTY,

GUARANTEE, OR REPRESENTATION, EXPRESS OR IMPLIED, THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED, THAT CONTENT WILL BE BLOCKED OR ALLOWED IN ACCORDANCE WITH THE STATE'S POLICIES, OR THAT THE PERFORMANCE OF THE SERVICES WILL RENDER THE STATE'S NETWORK AND COMPUTER SYSTEMS SAFE FROM INTRUSTIONS AND INVULNERABLE TO SECURITY BREACHES. THE STATE IS RESPONSIBLE FOR THE STATE'S OWN NETWORK SECURITY POLICY AND SECURITY RESPONSE PROCEDURES. CONTRACTOR MAKES NO GUARANTEE THAT THE SERVICES HEREUNDER WILL BE INVULNERABLE TO MALICIOUS CODE, DELETERIOUS ROUTINES, AND OTHER TECHNIQUES AND TOOLS EMPLOYED BY COMPUTER "HACKERS" AND OTHER THIRD PARTIES TO CREATE SECURITY EXPOSURES.

Section 35, "Debarment" is deleted and replaced with the following:

- 35. Debarment and Suspension.** The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals:
- a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;
 - b. have not within a three (3) year period preceding this Participating Addendum been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;
 - c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and
 - d. have not within a three (3) year period preceding this Participating Addendum had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals are excluded, disqualified, or presently fall under any of the prohibition of sections a-d.

Contractor shall use commercially reasonable efforts to obtain the certifications listed in this Section from the principals of any subcontractor that might perform services under this Participating Addendum. Contractor

shall not utilize any subcontractor whose principals are unable to comply with the requirements in this Section.

Section 37, "Governing Law and Venue" is deleted and replaced with the following:

- 37. Governing Law.** This Participating Addendum shall be governed by and construed in accordance with the laws of the State of Tennessee. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Participating Addendum. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Participating Addendum shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 407.

Contractor's AUP. Any reference to Contractor's Acceptable Use Policy in the Master Agreement is deleted and replaced with the following:

Acceptable Use Policy. The Parties acknowledge and agree that Contractor's Acceptable Use Policy ("AUP"), applies to the use of Contractor's network, websites, systems, facilities, products and services by the State. During the Term of this Participating Addendum, the State shall comply with such AUP. The AUP, as of the Effective Date of this Participating Addendum, is incorporated herein and specified in Attachment C attached hereto. In the event Contractor updates its AUP, the State may propose an amendment to the Participating Addendum to incorporate such modified AUP to this Participating Addendum.

6.2 See Attachment A attached hereto for additional terms and conditions that supplement the NASPO Master Agreement.

- 6. Subcontractors:** All contactors, dealers, fulfillment partners and resellers authorized in the State of Tennessee, as shown on the dedicated Contractor (cooperative contract) website, are approved to provide sales and service support to participants in the NASPO ValuePoint Master Agreement. The Contractor's dealer participation will be in accordance with the terms and conditions set forth in the aforementioned Master Agreement.
- 7. Orders:** Any order placed by a Participating Entity or Purchasing Entity for a product and/or service available from this Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such order.

8. Contractor Service Exhibits.

The following Contractor Service Exhibits, are incorporated herein and attached hereto as Attachment D to this Participating Addendum:

- (1) CenturyLink Domestic IQ Networking Service Exhibit
- (2) CenturyLink Local Access Service Exhibit
- (3) CenturyLink Software-Defined WAN
- (4) CenturyLink DDoS Mitigation Service Exhibit
- (5) CenturyLink Domestic Optical Wavelength
- (6) Level 3 Internet Service Schedule
- (7) Level 3 Wavelength Service Schedule
- (8) CenturyLink Delta Ports

The Service Level Agreements (SLAs) that apply to the Services listed above are incorporated herein and attached hereto as Attachment E.

9. Security Requirements

- a. The Contractor will have periodic security audits and penetration analysis performed by a third-party company against the Century Link infrastructure and equipment that is managed by the Contractor and used to deliver the services. The State CISO reserves the right to conduct full security audits for all facets of CenturyLink infrastructure directly connected to State-managed networks excluding aspects of the CenturyLink infrastructure utilized by user equipment. Audits will be conducted in accordance with Contractor's security guidelines and limited to once annually upon mutually agreed terms as to scope, location and timing. The Contractor shall develop a secure architecture designed to protect the CenturyLink infrastructure used to deliver the services provided under this agreement which shall include: (i) physical security; (ii) network-based attacks; and (iii) unauthorized access.
- b. The Contractor shall maintain operating systems, middle ware and databases supporting customer facing applications that are used in support or use of the CenturyLink services to versions that are supported with available emergency or critical hot-patches.
- c. The Contractor shall keep all network components to versions that are supported with available emergency or critical hot-patches.
- d. The Contractor shall provide a security incident response plan and escalation procedures to the State CISO for rapid response to violations and/or breaches.

CLOUD SOLUTIONS 2016-2026
Led by the State of Utah

IN WITNESS WHEREOF, the parties have executed this Addendum as of the date of execution by both parties below.

	Contractor:
Signature:  Digitally signed by Mike Perry DN: cn=Mike Perry, o=Chief Procurement Officer, ou=Department of General Services, email=mike.perry@tn.gov, c=US Date: 2019.03.27 10:42:31 -0500	Signature: <u>Steve Arneson</u> Steve Arneson (Mar 26, 2019)
Name: Michael F. Perry	Name: Steve Arneson
Title: Chief Procurement Officer	Title: Manager - Offer Management
Date: March 27, 2019	Date: Mar 26, 2019

[Additional signatures may be added if required by the Participating Entity]

For questions on executing a participating addendum, please contact:

NASPO ValuePoint

Cooperative Development Coordinator:	Shannon Berry
Telephone:	775-720-3404
Email:	sberry@naspovaluepoint.org

***Please email fully executed PDF copy of this document
to
PA@naspovaluepoint.org
to support documentation of participation and posting
in appropriate data bases.***

Attachment A

State of Tennessee
("State," "Participating Entity," or "Purchasing Entity")

NASPO ValuePoint Cloud Solutions 2016-2026

Supplemental Terms and Conditions



Standard Terms and Conditions

1. **Required Approvals.** The State is not bound by this Participating Addendum until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Participating Addendum, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.
2. **Subject to Funds Availability.** The Participating Addendum is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Participating Addendum upon 30 days written notice to the Contractor. The State's exercise of its right to terminate this Participating Addendum shall not constitute a breach of Participating Addendum by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Participating Addendum. If the State terminates this Participating Addendum due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Participating Addendum due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount.

3. **Conflicts of Interest.** The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Participating Addendum.

The Contractor acknowledges, understands, and agrees that this Participating Addendum shall be null and void if the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.

4. **Prohibition of Illegal Immigrants.** The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any participating addendum to supply goods or services to the State of Tennessee, shall be a material provision of this Participating Addendum, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Participating Addendum.
- a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Participating Addendum and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Participating Addendum. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment B, semi-annually during the Term. If the Contractor is a party to more than one Participating Addendum with the State, the Contractor may submit one attestation that applies to all Participating Addendums with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.
 - b. Prior to the use of any subcontractor in the performance of this Participating Addendum, and semi-annually thereafter during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Participating Addendum and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Participating Addendum. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.
 - c. The Contractor shall maintain records for all personnel used in the performance of this Participating Addendum. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable written notice by the State.
 - d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.

- e. For purposes of this Participating Addendum, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Participating Addendum.
5. **Monitoring.** The Contractor's activities conducted and records maintained pursuant to this Participating Addendum shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.
6. **Progress Reports.** The Contractor shall submit brief, periodic, progress reports to the State as requested in writing.
7. **Strict Performance.** Failure by any Party to this Participating Addendum to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Participating Addendum shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Participating Addendum shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.
8. **Limitation of State's Liability.** The State shall have no liability except as specifically provided in this Participating Addendum. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, participating addendum, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Participating Addendum or otherwise. The State's total liability under this Participating Addendum (including any exhibits, schedules, amendments or other attachments to the Participating Addendum) or otherwise shall under no circumstances exceed the Maximum Liability as defined herein. This limitation of liability is cumulative and not per incident.
9. **Limitation of Contractor's Liability.** In accordance with Tenn. Code Ann. § 12-3-701, the Contractor's liability for all claims arising under this Participating Addendum shall be limited to an amount equal to two (2) times the Maximum Liability amount detailed in Section 12 of the State's Special Terms and Conditions contained herein and as may be amended. This limitation of liability is cumulative and not per incident. Except as set forth below, in no event will the Contractor be liable to the State or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. PROVIDED THAT in no event shall this Section limit the liability of the Contractor

for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Participating Addendum providing for liquidated damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death.

10. HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Participating Addendum.

- a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Participating Addendum.
- b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Participating Addendum so that both parties will be in compliance with the Privacy Rules.
- c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Participating Addendum is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.
- d. Subject to Contractor's Maximum Liability in Section 9 of this Attachment A to this Participating Addendum, the Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.

11. Tennessee Consolidated Retirement System. Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, *et seq.*, the law governing the Tennessee Consolidated Retirement System ("TCRS"), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, *et seq.*, accepts State employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Participating Addendum to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Participating Addendum is that of

“employee/employer” and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.

12. Tennessee Department of Revenue Registration. The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Participating Addendum.

13. Severability. If any terms and conditions of this Participating Addendum are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Participating Addendum shall not be affected and shall remain in full force and effect. The terms and conditions of this Participating Addendum are severable.

14. Headings. Section headings of this Participating Addendum are for reference purposes only and shall not be construed as part of this Participating Addendum.

15. Incorporation of Additional Documents. Each of the following documents is included as a part of this Participating Addendum by reference. In the event of a discrepancy or ambiguity regarding the Contractor’s duties, responsibilities, and performance under this Participating Addendum, these items shall govern in order of precedence below:

- a. any amendment to this Participating Addendum, with the latter in time controlling over any earlier amendments;
- b. this Participating Addendum;
- c. the attachments and exhibits (excluding the items listed at subsections c. through f., below), which includes Attachments A - E of this Participating Addendum;
- d. any clarifications of or addenda to the Contractor’s Proposal, including Contractor’s response documents, including attachments to the State’s Solicitation seeking this Participating Addendum;
- e. the State Solicitation, as may be amended, including the documents used by the State to solicit Contractor’s Proposal for Goods, Custom Deliverables, or Services identified in this Participating Addendum;
- f. any technical specifications provided to proposers during the procurement process to award this Participating Addendum; and
- g. Contractor’s ValuePoint Master Agreement #AR2474.

16. Iran Divestment Act. The requirements of Tenn. Code Ann. § 12-12-101 et.seq., addressing contracting with persons as defined at T.C.A. §12-12-103(5) that engage in

investment activities in Iran, shall be a material provision of this Participating Addendum. The Contractor certifies, under penalty of perjury, that to the best of its knowledge and belief that it is not on the list created pursuant to Tenn. Code Ann. § 12-12-106.

17. **Major Procurement Contract Sales and Use Tax.** Pursuant to Tenn. Code Ann. § 4-39-102 and to the extent applicable, the Contractor and the Contractor's subcontractors shall remit sales and use taxes on the sales of goods or services that are made by the Contractor or the Contractor's subcontractors and that are subject to tax.
18. **Printing Authorization.** The Contractor agrees that no publication coming within the jurisdiction of Tenn. Code Ann. §§ 12-7-101, *et. seq.*, shall be printed pursuant to this Participating Addendum unless a printing authorization number has been obtained and affixed as required by Tenn. Code Ann. § 12-7-103 (d).
19. **State Ownership of Goods.** All licenses and ownership of any Deliverables provided pursuant to this Contract are as described in the applicable CenturyLink Service Exhibit or as otherwise set forth in a Statement of Work.
20. **Software License Warranty.** Contractor grants a license to the State to use all software provided under this Participating Addendum in the course of the State's business and purposes.
21. **Software Support and Maintenance Warranty.** Contractor shall provide to the State all software upgrades, modifications, bug fixes, or other improvements in its software that it makes generally available to its customers.
22. **Extraneous Terms and Conditions: Statement of Work.** If Contractor accepts a purchase order submitted by the State under this Participating Addendum, then Contractor shall deliver all goods and services associated with such Purchase Order in accordance with the terms of this Participating Addendum and any Statement of Work. Unless otherwise agreed to by the parties, no Purchase Order, invoice, or other documents associated with any sales, orders, or supply of any good or service under this Participating Addendum shall contain any terms or conditions other than as set forth in the Participating Addendum. Any such extraneous terms and conditions shall be void, invalid and unenforceable against the State. Any refusal by Contractor to supply any goods or services under this Participating Addendum conditioned upon the State submitting to any extraneous terms and conditions shall be a material breach of the Participating Addendum. Notwithstanding the foregoing, the parties agree, based on the nature of services available under the NASPO Master Agreement and how each service is provided, certain non-legal terms may be modified upon mutual agreement of the parties in a Statement of Work.
23. **Public Accountability.** If the Contractor is subject to Tenn. Code Ann. §§ 8-4-401, *et seq.*, or if this Participating Addendum involves the provision of services to citizens by the Contractor on behalf of the State, the Contractor agrees to establish a system through which recipients of services may present grievances about Contractor's operation of the service

program. The Contractor shall also display in a prominent place, located near the passageway through which the public enters in order to receive contract-supported services, a sign at least eleven inches (11") in height and seventeen inches (17") in width stating the following:

NOTICE: THIS AGENCY IS A RECIPIENT OF TAXPAYER FUNDING. IF YOU OBSERVE AN AGENCY DIRECTOR OR EMPLOYEE ENGAGING IN ANY ACTIVITY THAT YOU CONSIDER TO BE ILLEGAL, IMPROPER, OR WASTEFUL, PLEASE CALL THE STATE COMPTROLLER'S TOLL-FREE HOTLINE: 1-800-232-5454

The sign shall be of the form prescribed by the Comptroller of the Treasury. The contracting state agency shall request copies of the sign from the Comptroller of the Treasury and provide signs to contractors.

- 24. Contractor Commitment to Diversity.** The Contractor shall comply with and make reasonable business efforts to exceed the commitment to diversity in this Participating Addendum.

The Contractor shall assist the State in monitoring the Contractor's performance of this commitment by providing, as requested, a monthly report of participation in the performance of this Participating Addendum by small business enterprises and businesses owned by minorities, women, service-disabled veterans, and persons with disabilities. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the TN Diversity Software available online at:

<https://tn.diversitysoftware.com/FrontEnd/StartCertification.asp?TN=tn&XID=9810>.

- 25. Unencumbered Personnel.** The Contractor shall not restrict its employees, agents, subcontractors or principals who perform services for the State under this Participating Addendum from performing the same or similar services for the State after the termination of this Participating Addendum either as a State employee, an independent contractor, or an employee, agent, subcontractor or principal of another contractor with the State.

- 26. Personally Identifiable Information.** While performing its obligations under this Participating Addendum, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Participating Addendum, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not knowingly do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Participating Addendum, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical

and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. As described below, Contractor shall promptly notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Participating Addendum; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify that Contractor is in full compliance with its obligations under this Participating Addendum in relation to PII. Upon termination or expiration of the Participating Addendum or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Participating Addendum and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made promptly by the Contractor after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. If a data breach is a direct result of Contractor's breach of its contractual obligations to prevent its release as determined by the State, then Contractor shall, subject to Contractor's Liability in Section 9 of this Attachment A to this Participating Addendum, bear the costs associated with a credit monitoring service to which shall not exceed the average per record per person cost calculated for data breaches in the United States. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Participating Addendum or otherwise available at law.

- 27. State and Federal Compliance.** The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Participating Addendum.
- 28. Nondiscrimination.** The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the basis of any classification protected by federal, Tennessee State constitutional, or statutory law. The Contractor shall, upon request, show proof of such nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.
- 29. Administrative Fees.** The Contractor shall pay the State an Administrative Fee of one (1) and one half (0.5) percent (1.5% or 0.015) in accordance with the Terms and Conditions of the Master Agreement no later than 60 days following the end of each calendar quarter. The

State's Administrative Fee shall be submitted quarterly and is based on sales of products and services (less any charges for taxes or shipping).

Period End	Admin Fee Due
March 31	May 31
June 30	August 31
September 30	November 30
December 31	February 28

The administrative fee shall be submitted to the following address:

Ron Plumb, Director of Financial Management
Department of General Services
W.R. Snodgrass TN. Tower 24th Floor
312 Rosa L. Parks Avenue
Nashville, TN 37243

30. Survival. The terms, provisions, representations, and warranties contained in this Participating Addendum which by their sense and context are intended to survive the performance and termination of this Participating Addendum, shall so survive the completion of performance and termination of this Participating Addendum.

Special Terms and Conditions

- 1. Inspection and Acceptance.** The State shall have the right to inspect all goods or services provided by Contractor under this Participating Addendum. If, upon inspection, the State determines that the goods or services are defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30) days following delivery of goods or performance of services the State does not provide a notice of any defects, the goods or services shall be deemed to have been accepted by the State.
- 2. Term of Participating Addendum.** This Participating Addendum shall be effective for the period beginning on April 15, 2019 ("Effective Date") and ending on December 31, 2022 ("Term"), unless sooner terminated by either party in accordance with the terms of the this Participating Addendum. The State shall have no obligation for goods delivered or services provided by the Contractor prior to the Effective Date.
- 3. Participating Addendum Term Extension.** The State may extend the Term an additional period of time, not to exceed one hundred-eighty (180) days beyond the expiration date of this Participating Addendum, under the same terms and conditions, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.

4. **Travel Compensation.** The Contractor shall not be compensated or reimbursed for travel time, travel expenses, meals, or lodging.
5. **Invoice Requirements.** The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in the terms of this document. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than thirty (30) days after goods or services have been provided to the following address:

Department of Finance and Administration,
Strategic Technology Solutions
901 5th Ave N
Nashville, TN 37243

- a. Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):

- (1) Invoice number (assigned by the Contractor);
- (2) Invoice date;
- (3) Contract number (assigned by the State);
- (4) Customer account name: Department of Finance and Administration, Strategic Technology Solutions;
- (5) Customer account number (assigned by the Contractor to the above-referenced Customer);
- (6) Contractor name;
- (7) Contractor Tennessee Edison registration ID number;
- (8) Contractor contact for invoice questions (name, phone, or email);
- (9) Contractor remittance address;
- (10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;
- (11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;
- (12) Applicable payment methodology (as stipulated in Section C.3.) of each good or service invoiced;
- (13) Amount due for each compensable unit of good or service; and
- (14) Total amount due for the invoice period.

- b. Contractor's invoices shall:

- (1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;

- (2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;
 - (3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and
 - (4) Include shipping or delivery charges only as authorized in this Participating Addendum.
- c. The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this document.
- 6. **Invoice Reductions.** The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Participating Addendum to not constitute proper compensation for goods delivered or services provided.
- 7. **Invoice Payment.** The Contractor/Partner agrees that the timeframe for payment (and any discounts) begins on the invoice date, or when the state/Purchasing Entity is in receipt of a correct invoice meeting the minimum requirements above, whichever is later. It shall be the responsibility of the "bill to" agency to make payment in accordance with the Prompt Payment Act of 1985. Any questions concerning payment should be addressed to the "bill to" agency and not to the Central Procurement Office.
- 8. **Deductions.** The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.
- 9. **Prerequisite Documentation.** The Contractor shall not invoice the State under this Participating Addendum until the State has received the following, properly completed documentation.
 - a. The Contractor shall complete, sign, and present to the State the "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by ACH; and
 - b. The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

10. Contractor Hosted Services and Confidential Data.

- a. "Confidential State Data" is defined as data deemed confidential by State or Federal statute or regulation. If Contractor is given State Data as part of this Contract and unless otherwise modified upon mutual agreement of the parties in a separate Statement of Work, then the Contractor shall protect Confidential State Data as follows:
- (1) The Contractor shall ensure that all Confidential State Data is housed in data centers in the continental United States, inclusive of backup data.
 - (2) The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 validated encryption technologies.
 - (3) The Contractor's processing environment containing Confidential State Data shall be in accordance with at least one of the following security standards: (i) International Standards Organization ("ISO") 27001; (ii) Federal Risk and Authorization Management Program ("FedRAMP"); or (iii) American Institute of Certified Public Accountants ("AICPA") Service Organization Controls ("SOC") 2 Type II certified. The Contractor shall provide proof of current certification annually and upon State request.
 - (4) The Contractor must comply with the State's Enterprise Information Security Policies which is incorporated herein and attached hereto as Attachment F.
 - (5) In the event that the operating system is an integral part of the application, the Contractor agrees to maintain Operating Systems at current, manufacturer supported versions. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.
 - (6) The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Participating Addendum. The Contractor shall make sure that the Application is at all times fully compatible with a manufacturer-supported Operating System; the State shall not be required to run an Operating System that is no longer supported by the manufacturer.

- (7) If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are at all times fully compatible with current versions of the Operating System and Application, to ensure that security vulnerabilities are not introduced.
 - (8) With advance notice from the State, and no more than one (1) time per year the Contractor agrees to allow the State to perform logical and physical audits of the Contractor's facility and systems that are hosting Confidential State Data.
 - (9) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Penetration Tests" shall be in the form of software attacks on the Contractor's computer system, with the purpose of discovering security weaknesses, and potentially gaining access to the computer's features and data. The "Vulnerability Assessment" shall have the goal of defining, identifying, and classifying the security holes (vulnerabilities) in the Contractor's computer, network, or communications infrastructure. The Contractor shall allow the State, at its option, to perform Penetration Tests and Vulnerability Assessments on the Contractor's Processing Environment.
- b. Business Continuity Requirements. The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:
- (1) "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:
 - i. Recovery Point Objective ("RPO"). The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: within 4 hours.
 - ii. Recovery Time Objective ("RTO"). The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: within 4 hours.

- (2) The Contractor shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recover Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.
- c. Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State.
- d. Upon termination of this Participating Addendum and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

11. Destruction of Confidential Data.

Upon termination of this Participating Addendum and in consultation with the State, the Contractor shall destroy all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within thirty (30) business days after destruction.

12. Maximum Liability.

In no event shall the maximum liability of the State under this Contract exceed Fourteen Million Dollars (\$14,000,000) ("Maximum Liability"). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract

after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.

- 13. Memorandum of Understanding.** At its sole discretion, the State may make written requests to the Contractor to add lines, items, or options that are needed and within the scope but were not included in the original Contract. Such lines, items, or options will be added to the Participating Addendum through a Memorandum of Understanding ("MOU"), not an amendment.
- a. After the Contractor receives a written request to add lines, items, or options, the Contractor shall have ten (10) business days to respond with a written proposal. The Contractor's written proposal shall include:
 - (1) The effect, if any, of adding the lines, items, or options on the other goods or services required under the Contract;
 - (2) Any pricing related to the new lines, items, or options;
 - (3) The expected effective date for the availability of the new lines, items, or options; and
 - (4) Any additional information requested by the State and agreed by Contractor.
 - b. The State may negotiate the terms of the Contractor's proposal by requesting revisions to the proposal.
 - c. To indicate acceptance of a proposal, the State will sign it. The signed proposal shall constitute a MOU between the Parties, and the lines, items, or options shall be incorporated into the Contract as if set forth verbatim.
 - d. Only after a MOU has been executed shall the Contractor perform or deliver the new lines, items, or options.

14. Vendor Reporting

Usage Report

Upon request, or at a minimum quarterly, the Contractor shall furnish a usage report delineating the invoiced amounts under the Contract. The format of the report shall be approved by the State and shall disclose, at a minimum, the following for State and non-State governmental entities and all others authorized to use this Contract:

- Purchase Order (PO) Number
- PO Date
- Customer Name (State Agency/Municipality/Other)
- Customer number
- Billing Address & Shipping Address
- Product Type
- Total Price per Invoice



Reporting formats must be submitted to the State for approval within 10 business days after the Addendum start date. Once both parties have agreed to the format of the report, it shall become the standard to follow for the duration of the Contract.



ATTACHMENT B

**ATTESTATION RE PERSONNEL USED IN PARTICIPATING ADDENDUM
PERFORMANCE**

SUBJECT CONTRACT NUMBER:	Participating Addendum Number:
CONTRACTOR LEGAL ENTITY NAME:	CenturyLink
EDISON VENDOR IDENTIFICATION NUMBER:	

The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Participating Addendum and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Participating Addendum.

Steve Arneson
Steve Arneson (Mar 26, 2019)

CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

Steve Arneson

Manager - Offer Management

PRINTED NAME AND TITLE OF SIGNATORY

Mar 26, 2019

DATE OF ATTESTATION

CenturyLink's Acceptable Use Policy

This acceptable use policy ("AUP") defines acceptable practices relating to the use of CenturyLink's network, websites, systems, facilities, products and services (collectively, the "Services") by CenturyLink customers and by users that have gained access to the Services through customer accounts (collectively, "Users"). The Services must be used in a manner that is consistent with the intended purpose of the Services and the terms of the applicable agreement with CenturyLink. By using the Services, Users consent to be bound by the terms of this AUP. For purposes of this AUP, "CenturyLink" includes CenturyLink Communications, LLC and all other affiliates, including direct and indirect subsidiaries of CenturyLink, Inc.

Prohibited Conduct.

- **General.** Users will not use the Services to transmit, distribute or store material in a manner that: (a) violates any applicable law or regulation; (b) may adversely affect the Services or Users; (c) may expose CenturyLink to criminal or civil liability or (d) violate, infringe upon or otherwise misappropriate any third party rights, including intellectual property rights, rights of publicity and privacy rights. Users are prohibited from facilitating the violation of any part of this AUP or applicable third-party policies, including, but not limited to transmitting, distributing, or otherwise making available any product or service that violates this AUP or another provider's policy.
- **Inappropriate Content.** Users will not use the Services to transmit, distribute or store material that CenturyLink reasonably determines is inappropriate, obscene, indecent, defamatory, libelous, tortious, threatening, abusive, hateful, or excessively violent. Users will also not use the Services to host terrorist-related web sites, including sites that advocate human violence and hate crimes based upon religion, ethnicity, or country of origin.
- **Intellectual Property.** Material accessible through the Services may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users will not use the Services in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights. If a domain name is used with any of the Services, it may not be used in violation of the trademark, service mark, or other rights of any third party.
- **Harmful Content.** Users will not use the Services to transmit, distribute or store material that may be harmful to or interfere with the Services or any third party's networks, systems, services, or websites. Such prohibited harmful content includes, but is not limited to, viruses, worms, or Trojan horses, root kits, password crackers, adware, and key stroke capture programs.
- **Fraudulent/Misleading Content.** Users will not use the Services to transmit or distribute material containing fraudulent offers for goods or services, or any advertising or promotional materials that contain false, deceptive, or misleading statements, claims, or representations. In addition, Users are

prohibited from submitting any false or inaccurate data on any order form, contract or online application, including the fraudulent use of credit cards.

- **Email and Unsolicited Messages.** Users will not use the Services to (i) transmit unsolicited e-mail messages, including, without limitation, unsolicited bulk email, where such emails could reasonably be expected to provoke complaints, and (ii) send e-mail messages which are excessive and/or intended to harass or annoy others ("Spam"). Further, Users are prohibited from using the service of another provider to send Spam to promote a site hosted on or connected to the Services. In addition, Users will not use the Services to (a) continue to send e-mail messages to a recipient that has indicated that he/she does not wish to receive them, (b) send e-mail with forged TCP/IP packet header information, (c) send malicious e-mail, including, without limitation, "mail-bombing", (d) send or receive e-mail messages in a manner that violates the use policies of any other Internet service provider, or (e) use an e-mail box exclusively as a storage space for data.
- **Third Party Rules; Usenet.** Users will not use the Services in violation of the rules, guidelines or agreements associated with search engines, subscription Web services, chat areas, bulletin boards, Web pages, USENET, or other services accessed via the Services.
- **Inappropriate Actions.** Users will not use the Services to conduct activities that may be harmful to or interfere with the Services, a User's terminal session or any third party's networks, systems, services, or websites. Users will not engage in any activities designed to harass, or that will preclude or interfere with the use of Service (e.g., synchronized number sequence attacks) by any other User on the CenturyLink network or on another provider's network. In addition, Users will not use the Service (a) by any means or device to avoid payment; (b) to access User's account or CenturyLink Services after User has terminated User's account; (c) on behalf of persons or firms listed in the Spamhaus Register of Known Spam Operations database at www.spamhaus.org; (d) to engage in phishing activities and (e) for purposes of cryptography or similar computational processing to mine or create units of cryptocurrency, such as Bitcoin, Ethereum, Ripple, and Litecoin. Users will not use the Service to engage in any activities that may interfere with the ability of others to access or use the Service or the Internet.
- **Illegal Use:** Customer will not use the Services in a manner that constitutes illegal activities, including but not limited to, death threats, terroristic threats, threats of harm to another individual, multi-level marketing schemes, HYIP or Ponzi schemes, invasion of privacy, credit card fraud, racketeering, defamation, slander, child pornography and violations of the Child Protection Act of 1984, or any other applicable law.
- **Security Breaches and Obligations.** Users are prohibited from violating or attempting to violate the security of the Services or the computers, accounts, or networks of another party, including but not limited to, circumventing the user authentication or security of any host, network or account. Users will not use the Services to cause security breaches or disruptions of Internet communication and/or

connectivity. Security breaches include, but are not limited to, accessing data, accounts or systems without authorization or logging into a server or account that the Customer is not expressly authorized to access and denial of service attacks. Disruptions include port scans, flood pings, email-bombing, packet spoofing, IP spoofing, forged routing information. Customer must use reasonable care in keeping its software on the CenturyLink's servers up-to-date and patched with the latest security updates.

- **IP Allocation.** Users are prohibited from using IP addresses not originally allocated for use or on unassigned VLANs or servers. All IP Addresses are currently owned and registered to CenturyLink and are non-transferable. Customer retains no ownership or transfer rights.

Rights of CenturyLink.

- CenturyLink may suspend or terminate Service of any User which CenturyLink believes has violated any element of this AUP. CenturyLink will suspend Service for violation of the AUP on the most limited basis as CenturyLink determines is reasonably practical under the circumstances to address the underlying violation. CenturyLink will attempt to notify Users via email or other method prior to suspending Service for violation of the AUP; provided, however, CenturyLink may suspend Service without notice if CenturyLink becomes aware of a violation of any applicable law or regulation or activity, including but not limited to a violation of the AUP that exposes CenturyLink to criminal or civil liability or that exposes the CenturyLink network or CenturyLink customers' network or property to harm. Such harm to a network may include, but is not limited to, risk of having an IP address placed on blacklists. CenturyLink may take such further action as CenturyLink determines to be appropriate under the circumstances to eliminate or preclude repeat violations.
- CenturyLink reserves the right to take down any material—or otherwise block access thereto—created or accessible on or through the Services and suspend or terminate any User creating, storing or disseminating such material where CenturyLink becomes aware that the material violates this AUP and/or exposes CenturyLink to civil or criminal liability, including without limitation, under applicable copyright laws. CenturyLink reserves the right to avail itself to the safe harbor provisions of the Digital Millennium Copyright Act.
- Please click [here](#) for information relating to the Service Provider/Designated Agent Information pursuant to the Digital Millennium Copyright Act, 17 U.S.C., Section 512(c).
- Users are responsible for configuring their own systems to provide the maximum possible accountability. CenturyLink shall not be liable for any damage caused by such system configurations regardless of whether such configurations have been authorized or requested by CenturyLink. For example, Users should ensure there are clear "path" lines in news headers so that the originator of a post may be identified. Users should also configure their Mail Transport Agents (MTA) to authenticate (by look-up on the name or similar procedures) any system that connects to perform a mail exchange,

and should generally present header data as clearly possible. As another example, Users should maintain logs of dynamically assigned IP addresses. Users are responsible for educating themselves and configuring their systems with at least basic security. Should systems at a User's site be violated, the User is responsible for reporting the violation and then fixing the exploited system. For instance, should a site be abused to distribute unlicensed software due to a poorly configured FTP (File Transfer Protocol) Server, the User is responsible for re-configuring the system to stop the abuse.

- CenturyLink reserves the right to cooperate with legal authorities and third parties in the investigation of any alleged wrongdoing related to this AUP, including the disclosure of the identity of the User that CenturyLink deems responsible for the wrongdoing. CenturyLink will not be liable for any damages of any nature suffered by any User, or any third party resulting in whole or in part from CenturyLink's exercise of its rights under this AUP.
- CenturyLink reserves the right to install and use, or to have you install and use, any appropriate devices to prevent violations of this Policy, including devices designed to filter or terminate access to the Service. By accepting and using the Service, Users consent to allowing CenturyLink to collect service information and routing information in the normal course of our business, and to use such information for general business purposes. Users may not use the Service to monitor any data, information or communications on any network or system without authorization. Users may not attempt to gain unauthorized access to the user accounts or passwords of other Users.
- In most cases, CenturyLink will notify Users of complaints received by CenturyLink regarding an alleged violation of this Policy. You agree to promptly investigate all such complaints and take all necessary actions to remedy any violations of this Policy. CenturyLink may inform the complainant that you are investigating the complaint and may provide the complainant with the necessary information to contact you directly to resolve the complaint. You shall identify a representative for the purposes of receiving such communications.
- CenturyLink reserves the right to modify this AUP in its discretion at any time. Such modifications will be effective upon posting and use of the Services after such modification constitutes acceptance of such modifications.

Responsibility for Content. CenturyLink takes no responsibility for any material created or accessible on or through the Services and will not exercise any editorial control over such material. CenturyLink is not obligated to monitor such material but reserves the right to do so.

Violations of this AUP may be reported to: abuse@centurylinkservices.net.

Enterprise Information Security Policies



State of Tennessee
Department of Finance and Administration
Strategic Technology Solutions
Information Security Program

Document Version 2.2 – December 14, 2017

Table of Contents

Page 1. EXECUTIVE SUMMARY	Error! Bookmark not defined.
2. INTRODUCTION	2
Scope (2.1)	2
Authority (2.2)	3
Exceptions (2.3)	3
Review (2.4)	3
Document Format (2.5)	4
Policy Maintenance (2.6)	4
3. INFORMATION SECURITY POLICIES	5
Management Direction for Information Security (3.1)	5
Policies for Information Security (3.1.1)	5
Policies for Information Security (3.1.2)	Error! Bookmark not defined.
Policies for Information Security (3.1.3)	Error! Bookmark not defined.
4. OPERATIONS SECURITY	5
Operational Procedures and Responsibilities (4.1)	5
Documented Operating Procedures (4.1.1)	5
Change Management (4.1.2)	5
Change Control Procedures (4.1.2.1)	5
Capacity Management (4.1.3)	6
Separation of Development, Testing and Operational Environments (4.1.4)	6
Protection from Malware (4.2)	6
Malicious Software Control (4.2.1)	6
Backup (4.3)	6
Data Backup (4.3.1)	Error! Bookmark not defined.
Logging and Monitoring 4.4)	6
Event Logging (4.4.1)	6
Availability and Performance Monitoring (4.4.2)	7
Protection of Log Information (4.4.3)	7
Administrator and Logs (4.4.4)	7
Clock Synchronization (4.4.5)	7
Control of Operational Software (4.5)	7
Installation of Software on Operational Systems (4.5.1)	7
Patch Management (4.5.1.1)	7
Software Development Code (4.5.1.2)	8
Review of Application and Operating System Changes (4.5.1.3)	8
Technical and Vulnerability Management (4.6)	8
Management of Technical Vulnerabilities (4.6.1)	8
Restrictions on Software Installation (4.6.2)	Error! Bookmark not defined.
Information Systems Audit Considerations (4.7)	8
Information Systems Audit Controls (4.7.1)	8
5. ACCESS CONTROL	8

Business Requirements of Access Control (5.1)	8
Access Control Policy (5.1.1)	8
Access to Networks and Network Services (5.1.2)	9
Remote Access (5.1.2.1)	9
Information Security Roles and Responsibilities (5.1.3)	9
Segregation of Duties (5.1.4)	9
User Access Management (5.2)	9
User Registration and De-Registration (5.2.1)	9
User Access Provisioning (5.2.2)	9
User Account Naming (5.2.2.1)	Error! Bookmark not defined.
Management of Privileged Access Rights (5.2.3)	10
Management of Secret Authentication of Information Users (5.2.4)	10
Review of User Access Rights (5.2.5)	10
Removal or Adjustment of Access Rights (5.2.6)	10
User Responsibilities (5.3)	10
Use of Secret Authentication Information (5.3.1)	10
System and Application Access Control (5.4)	10
Information Access Restriction (5.4.1)	10
Secure Log-on Procedures (5.4.2)	10
System Administrator Access (5.4.2.1)	11
Logon Banner (5.4.2.2)	Error! Bookmark not defined.
Service Account Use (5.4.2.3)	11
Password Management System (5.4.3)	11
Use of Privileged Utility Programs (5.4.4)	11
Access Control to Program Source Code (5.4.5)	11
Default Configurations (5.4.6)	11
6. ASSET MANAGEMENT	11
Responsibility for Assets (6.1)	12
Inventory of Assets (6.1.1)	12
Ownership of Assets (6.1.2)	12
Acceptable Use of Assets (6.1.3)	12
Return of Assets (6.1.4)	Error! Bookmark not defined.
Asset Identification (6.1.5)	Error! Bookmark not defined.
Data Classification (6.2)	Error! Bookmark not defined.
Classification of Data (6.2.1)	Error! Bookmark not defined.
Labelling of Data (6.2.2)	Error! Bookmark not defined.
Handling and Use of Data (6.2.3)	Error! Bookmark not defined.
Public Data Classification and Control (6.2.3.1)	Error! Bookmark not defined.
Confidential Data Classification and Control (6.2.3.3)	Error! Bookmark not defined.
Confidential Data on Personally Owned Devices (6.2.3.4)	Error! Bookmark not defined.
Confidential Electronic Messages Classification and Control (6.2.3.5)	Error! Bookmark not defined.
Payment Card Information Classification and Control (6.2.3.6)	Error! Bookmark not defined.
Use of Confidential Data (6.2.3.7)	Error! Bookmark not defined.
Media Handling (6.3)	Error! Bookmark not defined.
Management of Removable Media (6.3.1)	Error! Bookmark not defined.
Repair of Removable Media (6.3.1.1)	Error! Bookmark not defined.

Disposal of Removable Media (6.3.2)	Error! Bookmark not defined.
Physical Transfer of Removable Media (6.3.3)	Error! Bookmark not defined.
Workstation Computing (6.4)	Error! Bookmark not defined.
State Provided Workstation Computing Platforms (6.4.1)	Error! Bookmark not defined.
Workstation Platform Reassignment (6.4.2)	Error! Bookmark not defined.
Workstation Platform Disposal (6.4.3)	Error! Bookmark not defined.
Cloud Services (6.4.4)	Error! Bookmark not defined.
7. PHYSICAL AND ENVIRONMENTAL SECURITY	12
Secure Areas (7.1)	12
Physical Security Perimeter (7.1.1)	12
Physical Entry Controls (7.1.2)	12
Securing Offices, Rooms and Facilities (7.1.3)	13
Protecting against External and Environmental Threats (7.1.4)	13
Working in Secure Areas (7.1.5)	13
Delivery and Loading Areas (7.1.6)	13
Equipment (7.2)	13
Equipment Siting and Protection (7.2.1)	13
Supporting Utilities (7.2.2)	13
Cabling Security (7.2.3)	13
Equipment Maintenance (7.2.4)	13
Removal of Assets (7.2.5)	14
Security of Equipment and Assets Off-Premises (7.2.6)	Error! Bookmark not defined.
Secure Disposal or Re-Use of Data Processing Equipment (7.2.7)	14
Unattended User Equipment (7.2.8)	14
Session Time Outs (7.2.8.1)	14
Clear Desk and Clear Screen Policy (7.2.9)	14
8. NETWORK CONNECTIVITY SECURITY	15
Network Security Management (8.1)	15
Network Controls (8.1.1)	15
Security of Network Services (8.1.2)	15
Segregation in Networks (8.1.3)	15
Information Transfer (8.2)	15
Information Transfer Policies and Procedures (8.2.1)	15
Agreements on Data Transfer Policies (8.2.2)	15
Electronic Messaging (8.2.3)	15
Internal Electronic Messages Control (8.2.3.1)	Error! Bookmark not defined.
External Electronic Messages Control (8.2.3.2)	15
Electronic Messaging Management (8.2.3.3)	16
Confidentiality or Non-Disclosure Agreements (8.2.4)	16
9. MOBILE DEVICE SECURITY POLICY	Error! Bookmark not defined.
Mobile Devices and Teleworking (9.1)	Error! Bookmark not defined.
Mobile Device Policy (9.1.1)	Error! Bookmark not defined.
Teleworking (9.1.2)	Error! Bookmark not defined.
10. EXTERNAL PARTY SECURITY	16

Information Security for External Party Relationships (10.1)	16
Information Security Policy for External Party Relationships (10.1.1)	16
Identification of Risk (10.1.2)	16
Addressing Security within External Party Agreements (10.1.3)	16
Reporting of Security Incidents (10.1.3.1)	17
Sub-Contractors Requirements (10.1.3.2)	17
Addressing Security for Access to Citizen Data (10.1.4)	Error! Bookmark not defined.
11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	17
Security Requirements of Information Systems (11.1)	17
Security Requirements of Information Systems (11.1.1)	17
Securing Application Services on Public Networks (11.1.2)	17
Protecting Application Services Transactions (11.1.3)	17
Information Security in Project Management (11.1.4)	18
Security in Development and Support Processes (11.2)	18
Security Requirements of Information Systems (11.2.1)	18
Security in Application Systems Development (11.2.1.1)	18
Input and Data Validation (11.2.1.2)	Error! Bookmark not defined.
Output Data Validation (11.2.1.3)	Error! Bookmark not defined.
Application Authorization (11.2.1.4)	Error! Bookmark not defined.
Inter-process Message Authentication (11.2.1.5)	Error! Bookmark not defined.
Control of Internal Processing (11.2.1.6)	18
System Change Control Procedures (11.2.2)	18
Technical Review of Applications after Operating Platform Changes (11.2.3)	18
Restrictions or Changes to Software Packages (11.2.4)	18
Secure System Engineering Principles (11.2.5)	19
Secure Development Environment (11.2.6)	19
Outsourced Development (11.2.7)	19
System Security Testing (11.2.8)	19
System Acceptance Testing (11.2.9)	19
Test Data (11.3)	19
Protection of Test Data (11.3.1)	19
12. BUSINESS CONTINUITY MANAGEMENT	Error! Bookmark not defined.
Information Business Continuity (12.1)	Error! Bookmark not defined.
Planning Information Systems Continuity (12.1.1)	Error! Bookmark not defined.
Business Impact Analysis (12.1.1.1)	Error! Bookmark not defined.
Critical Applications (12.1.1.2)	Error! Bookmark not defined.
Non-Critical Applications (12.1.1.3)	Error! Bookmark not defined.
Implementing Information Systems Continuity (12.1.2)	Error! Bookmark not defined.
Verify, Review and Evaluate information Systems Continuity (12.1.3)	Error! Bookmark not defined.
Redundancies (12.2)	Error! Bookmark not defined.
Availability of Information Processing Facilities (12.2.1)	Error! Bookmark not defined.
13. INFORMATION SECURITY INCIDENT MANAGEMENT	20
Management of Information Security Incidents and Improvements (13.1)	20
Responsibilities and Procedures (13.1.1)	20

Reporting Information Security Events (13.1.2)	20
Data Breach and Disclosure (13.1.2.1)	Error! Bookmark not defined.
Reporting Information Security Weakness (13.1.3)	20
Assessment of and Decision on Information Security Events (13.1.4)	20
Response to Information Security Incidents (13.1.5)	21
Learning from Information Security Incidents (13.1.6)	21
Collection of Evidence (13.1.7)	Error! Bookmark not defined.
14. CRYPTOGRAPHY	21
Cryptographic Controls (14.1)	Error! Bookmark not defined.
Use of Cryptographic Controls (14.1.1)	Error! Bookmark not defined.
Transmission Integrity (14.1.2)	Error! Bookmark not defined.
Transmission Confidentiality (14.1.3)	Error! Bookmark not defined.
Cryptographic Module Authentication (14.1.4)	Error! Bookmark not defined.
Cryptographic Module Authentication (14.1.5)	Error! Bookmark not defined.
Key Management (14.1.6)	Error! Bookmark not defined.
15. COMPLIANCE	21
Compliance with Legal and Contractual Requirements (15.1)	Error! Bookmark not defined.
Identification of Applicable Legislation and Contractual Requirements (15.1.1)	Error! Bookma
Intellectual Property Rights (15.1.2)	Error! Bookmark not defined.
Protection of Records (15.1.3)	Error! Bookmark not defined.
Privacy and Protection of Personally Identifiable Information (15.1.4)	Error! Bookmark not defi
Regulation of Cryptographic Controls (15.1.5)	Error! Bookmark not defined.
Information Security Reviews (15.2)	Error! Bookmark not defined.
Independent Review of Information Security (15.2.1)	Error! Bookmark not defined.
Compliance with Security Policies and Standards (15.2.2)	Error! Bookmark not defined.
Technical Compliance Review (15.2.3)	Error! Bookmark not defined.
16. HUMAN RESOURCE	21
Prior to Employment (16.1)	21
Screening (16.1.1)	21
Acceptable Use Policy (16.1.2)	21
During Employment (16.2)	21
Management Responsibilities (16.2.1)	21
Information Security Awareness, Education and Training (16.2.2)	21
17. VERSION HISTORY	22
18. TERMS AND DEFINITIONS	23
19. APPENDICES	26

1. EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policies of the State of Tennessee along with the organization and framework/structure required to communicate, implement and support these policies. Information is an asset, which like any other asset owned by the State of Tennessee, has significant value to the stakeholders of the State. Information security is a critical component that is required to enable and ensure the confidentiality, integrity and availability of data, network and processing resources required for the State of Tennessee to perform its business and operational practices. This policy document has been created to establish and uphold the minimum requirements that are necessary to protect information resources (assets) against unavailability, unauthorized or unintentional access, modification, destruction or disclosure as set forth by the Information Systems Council (ISC) of the State of Tennessee.

The scope of this document is intended to cover any information asset owned, leased or controlled by, or operated on behalf of the State of Tennessee. The methodologies and practices of external entities that require access to the State of Tennessee's information resources may be impacted and could be included in this scope. This document seeks to protect:

- All computing platforms, operating system software, middleware or application software under the control of third parties that connect in any way to the State of Tennessee's enterprise computing or telecommunications network.

This document applies to all full- and part-time employees of the State of Tennessee, all third parties, contractors or vendors who work on State premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data.

By establishing the appropriate policy framework and utilizing a documented policy development process that includes all stakeholders, the State envisions maximum voluntary compliance. The policy development and implementation process includes an impact analysis, input from Agency information technology (IT) professionals and approval by the Chief Information Security Officer (CISO) and executive management team within Strategic Technology Solutions, Department of Finance and Administration.

All information resources and any information system owned by the State of Tennessee should be protected from unauthorized disclosure, use, modification or destruction in a manner commensurate with their value, sensitivity and criticality to the business and operation of the State government and those they serve. Access

to information technology assets will be granted using the principle of least privilege.

All of the approved policies will support the requirements of the Information Systems Council of the State of Tennessee.

2. INTRODUCTION

The Information Security Challenge

Information technology (IT) solutions are driven by the demands of our daily business activities. The ability to procure efficient communication, IT resources and technologies that support business processes at a low cost is a foundational component of successful IT programs. This integration moves quickly to align itself with the “just in time” requirements of the business. Given the growth demands of the business along with the associated time sensitive integration strategies, we are presented with new risks at every turn. Organizations will frequently take risks in order to meet those time sensitive business requirements, sometimes bypassing existing processes to meet time demands of the customers whom they serve. This practice, also known as risk management, is a component of any successful business. Modern enterprises will implement risk management and/or information security programs to mitigate these risks.

The State of Tennessee has recognized the need to evaluate risk and has established information security programs. One of the main goals of any successful information security program is to protect the organization's revenues, resources, and reputation. This is accomplished through several means. Some examples are implementing risk management methodologies, security architectures, control frameworks and security policy to list a few.

Security policies are a foundational component of any successful security program. The Enterprise Information Security Policies for the State of Tennessee are based on the International Standards Organization (ISO) 27002 standard framework. The policies are designed to comply with applicable statutes and regulations; however, if there is a conflict, applicable statutes and regulations will take precedence. The policies included in this document are to be considered the minimum requirements for providing a secure operational environment.

Scope (2.1)

The scope of this document is intended to cover the methodologies and practices of external entities that require access to the State of Tennessee's information resources. This document seeks to protect:

- All computing platforms, operating system software, middleware or application software under the control of the State of Tennessee, or by third parties, operated on behalf of the State of Tennessee that connect in any way to the State's enterprise computing or telecommunications network.

All third parties, contractors, or vendors who work on state premises or remotely connect their computing platforms to the State of Tennessee's computing platforms and any cloud provider storing, processing or transmitting State data should adhere to the policies and requirements set forth in this document.

Authority (2.2)

The Information Systems Council (ISC) has authorized the Department of Finance and Administration, Strategic Technology Solutions (STS) to establish and enforce enterprise policies and standards as they are related to information security. These policies and standards include, but are not limited to, network and Internet access, any computing platform attached to the State's enterprise network and any wired or wireless technology attached to the State's enterprise network.

Reference:

Tennessee Code Annotated, Section 4-3-5501, effective, May 10, 1994

ISC Information Resource Policies, Policy 1.00

ISC Information Resource Policies, Policy 13.00

Exceptions (2.3)

All exceptions to any of the security policies will be reviewed, evaluated and processed by a member of the Chief Information Security Officer's staff.

Review (2.4)

Review of this document takes place within Security Advisory Council sessions and will occur on an annual basis at a minimum. Document review can also be requested by sending a request to the Chief Information Security Officer.

The official policy document and supporting documentation will be published on the STS intranet site located at:

Document Format (2.5)

This document generally follows the International Standards Organization (ISO) 27002 (2013) standard framework for information technology security management. Each section starts with a high-level security control category followed by the control objective. Policy statements follow the objectives.

The MINIMUM COMPLIANCE REQUIREMENTS category contains the minimum requirements for compliance criteria that are global and apply to all systems or platforms across the entire enterprise.

X. Section Name

Control Category (x.x) Objective Statement

Policy Name (x.x.x) Policy Statement

Sub-Policy Name (x.x.x.x) Sub-Policy Statement

MINIMUM COMPLIANCE REQUIREMENTS:

Policy Maintenance (2.6)

All policies will be maintained in accordance with the STS policy process documentation.

3. INFORMATION SECURITY POLICIES

Management Direction for Information Security (3.1)

Objective: To provide management direction and support for information security in accordance with agency business requirements and relevant state and federal statute and regulations for the State of Tennessee's computing environments.

Policies for Information Security (3.1.1)

CenturyLink will initiate, control and communicate its own policy framework, organizational and communication framework and security technology framework.

4. OPERATIONS SECURITY

Operational Procedures and Responsibilities (4.1)

Objective: To protect critical State information resource assets, including hardware, software and data from unauthorized use, misuse, or destruction to ensure correct and proper operations.

Documented Operating Procedures (4.1.1)

All vendors or contractors acting on behalf of the State should identify, document and maintain standard security operating procedures and configurations for their respective operating environments and ensure the documentation is available to all CenturyLink users who need it.

Change Management (4.1.2)

Changes to information processing facilities and systems forming the Services provided should be controlled and monitored for security compliance. Formal management responsibilities and procedures should exist to ensure satisfactory control of all changes to equipment, software, configurations or procedures that affect the security of CenturyLink's operational environment. All written documentation generated by the change control policies and procedures should be retained as evidence of compliance.

Change Control Procedures (4.1.2.1)

Change control procedures should include authorization, risk assessment, logging, audit ability, and roll back procedures.

Capacity Management (4.1.3)

The use of resources should be monitored and tuned so that projections of future capacity requirements can be made.

Separation of Development, Testing and Operational Environments (4.1.4)

Development and testing environments should be segregated from production environments in order to reduce the risks of unauthorized access or changes to the production environment. Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and should not be used in development or test environments without authorization from the State. Centurylink undertake not to use the production services provided, for development.

Protection from Malware (4.2)

Objective: Prevent the automated propagation of malicious code and contamination of environments attached to the enterprise network.

Malicious Software Control (4.2.1)

All computing platforms that are attached to the State's enterprise technology infrastructure or operated on behalf of the State should be protected from intentional or unintentional exposure to malicious software. Malicious software includes, but is not limited to, software viruses, worms, Trojan horses, logic bombs and rootkits. Compromised systems should be removed from the operational environment.

Backup (4.3)

Objective: To prevent loss of data and to ensure data availability.

Not applicable.

Logging and Monitoring 4.4)

Objective: To record events and generate evidence.

Event Logging (4.4.1)

All services provided should be configured to support security event logging, recording user activities, exceptions, faults and information security events. Logging levels and monitored elements will be configured in accordance with CenturyLink Security Policy.

Availability and Performance Monitoring (4.4.2)

Mission critical systems should be configured to support Service availability SLAs.

Protection of Log Information (4.4.3)

Logging facilities and log information should be protected against tampering and unauthorized access.

Administrator and Logs (4.4.4)

System administrator activities should be logged and the logs protected and regularly reviewed.

Clock Synchronization (4.4.5)

All non-State provided or managed systems storing, processing or transmitting State data should be synchronized to agreed time synchronization services.

Control of Operational Software (4.5)

Objective: To ensure the integrity of operational systems.

Installation of Software on Operational Systems (4.5.1)

Only software that has been licensed and approved through CenturyLink's change control process should be installed on devices covered by the software's license agreement.

Patch Management (4.5.1.1)

All applications and processing devices that are attached to the State's enterprise technology infrastructure will have critical application, operating system, and/or security related patches made available by the software or hardware vendor applied within 90 calendar days or sooner if an acceptable date can be agreed upon by all affected parties. Emergency patches and updates will be applied as soon as possible following successful validation and testing.

Software Development Code (4.5.1.2)

Software development code cannot be installed on production systems (i.e. non-compiled software programming code)

Review of Application and Operating System Changes (4.5.1.3)

Applications and operating systems should be reviewed and tested to ensure that there is no adverse impact on operations or security when a change has been performed on the operating system. (e.g. patch).

Technical and Vulnerability Management (4.6)

Objective: To prevent the exploitation of technical vulnerabilities.

Management of Technical Vulnerabilities (4.6.1)

Information about technical vulnerabilities on information systems and supporting infrastructure should be obtained in a timely fashion, evaluated for exposure and risk to CenturyLink and appropriate measures implemented to address the associated risk.

Information Systems Audit Considerations (4.7)

Objective: To minimize the impact of audit activities on operational systems.

Information Systems Audit Controls (4.7.1)

Audit requirements and activities involving verification of operational systems should be carefully planned and agreed upon in advance to minimize disruptions to business processes.

5. ACCESS CONTROL

Business Requirements of Access Control (5.1)

Objective: To limit access to information and information processing facilities.

Access Control Policy (5.1.1)

All information processing systems operated on behalf of the State of Tennessee should have an appropriate role-based access

control system that ensures only legitimate users and/or systems have access to data resources that they are explicitly authorized to use.

Access to Networks and Network Services (5.1.2)

All access and connectivity to networks operated on behalf of the State should be granted consistent with the concept of least privilege. Users will only be provided with access to the network and network resources that they have been specifically authorized to use.

Remote Access (5.1.2.1)

All users who access State data on networks operated on behalf of the State should use secure connection methods.

Information Security Roles and Responsibilities (5.1.3)

All information security responsibilities for the provided services should be defined and assigned by CenturyLink.

Segregation of Duties (5.1.4)

Where appropriate, conflicting duties and areas of responsibility should be segregated and assigned to different individuals to reduce opportunities for unauthorized or unintentional modification or misuse.

User Access Management (5.2)

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

User Registration and De-Registration (5.2.1)

A formal user registration and de-registration process should be implemented to enable assignment of access rights and to adjust those rights as the user's role changes.

User Access Provisioning (5.2.2)

User access to information resources should be authorized and provisioned according to CenturyLink provisioning process.

Management of Privileged Access Rights (5.2.3)

Users should have the least privileges required to perform their roles. The allocation and use of privileged access rights should be restricted and controlled.

Management of Secret Authentication of Information Users (5.2.4)

The allocation of secret authentication information should be controlled through a formal management process.

Review of User Access Rights (5.2.5)

A user's access rights should be reviewed, validated and updated for appropriate access on a regular basis or whenever the user's access requirements change (e.g. hire, promotion, demotion, and transfers within and between agencies).

Removal or Adjustment of Access Rights (5.2.6)

All access rights for employees and external entities to information and information processing facilities should be revoked upon termination of their employment, contract, agreement or change of agency by the close of business on the user's last working day.

User Responsibilities (5.3)

Objective: To make users accountable for safeguarding their authentication information.

Use of Secret Authentication Information (5.3.1)

Users should follow CenturyLink policy in the use of secret authentication information.

System and Application Access Control (5.4)

Objective: To prevent unauthorized access to systems and applications.

Information Access Restriction (5.4.1)

Access to information and application system function should be restricted in accordance with the defined access control policy.

Secure Log-on Procedures (5.4.2)

Where required by the access control policy, access to systems and application should be controlled by a secure log-on procedure. At a

minimum, user access to protected information resources requires the utilization of User Identification (UserID) and password that uniquely identifies the user. Sharing access credentials intended to authenticate and authorize a single user between any two or more individuals is prohibited.

System Administrator Access (5.4.2.1)

All systems administrators or users with elevated privileges using administrative tools or protocols to access servers located in facilities operated on behalf of the State must use a multifactor VPN solution to obtain access.

Service Account Use (5.4.2.3)

Service accounts should be unique to each application and/or system and should only be used to authenticate systems and/or applications to specific services.

Password Management System (5.4.3)

Password management systems should be interactive and should ensure quality passwords.

Use of Privileged Utility Programs (5.4.4)

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Access Control to Program Source Code (5.4.5)

Access to program source code should be restricted to authorized users.

Default Configurations (5.4.6)

All applications and processing devices that are attached to the State's enterprise technology infrastructure should be deployed with modified configurations for, but not limited to, default accounts, and/or installation paths to minimize the use of default settings to gain unauthorized use, modification or destruction.

6. ASSET MANAGEMENT

Responsibility for Assets (6.1)

Objective: To identify organizational assets and define appropriate protection responsibilities.

Inventory of Assets (6.1.1)

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be created and maintained in order to protect the assets.

Ownership of Assets (6.1.2)

All information resource assets listed in the asset inventory should have an assigned owner or entity

Acceptable Use of Assets (6.1.3)

Rules for the acceptable use of information and assets associated with information and information processing facilities should be identified, documented, implemented and communicated to the employees and contractors who have access to those assets.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Secure Areas (7.1)

Objective: To prevent unauthorized physical access, damage and interference to the State's information and information processing facilities.

Physical Security Perimeter (7.1.1)

All enterprise data processing facilities that process or store data classified as critical or sensitive should have multiple layers of physical security. Each layer should be independent and separate of the preceding and/or following layer(s).

All other processing facilities should have, at a minimum, a single security perimeter protecting it from unauthorized access, damage and/or interference.

Physical Entry Controls (7.1.2)

Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel.

Securing Offices, Rooms and Facilities (7.1.3)

Physical security for offices, rooms and facilities should be designed and applied commensurate with the classification and value of the data being handled or processed.

Protecting against External and Environmental Threats (7.1.4)

Physical protection against natural disaster, malicious attack or accidents should be considered and incorporated in facility design, construction and placement.

Working in Secure Areas (7.1.5)

Procedures for working in secure areas should be created and implemented.

Delivery and Loading Areas (7.1.6)

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled, and if possible, isolated from information processing facilities.

Equipment (7.2)

Objective: To prevent loss, damage, theft or compromise of assets or an interruption to State operations.

Equipment Siting and Protection (7.2.1)

Equipment should be located in secured areas or protected to reduce the opportunities for unauthorized access.

Supporting Utilities (7.2.2)

Infrastructure and related computing equipment should be protected from power failures and other disruptions by failures in supporting utilities.

Cabling Security (7.2.3)

Power and telecommunications cable carrying data or supporting information services should be protected from interception, interference or damage.

Equipment Maintenance (7.2.4)

Equipment should be correctly maintained to ensure its continued availability and integrity.

Removal of Assets (7.2.5)

All equipment, software or information that is a part of State operational systems or processes should not be taken off-site without appropriate approval following CenturyLink processes.

Secure Disposal or Re-Use of Data Processing Equipment (7.2.7)

All data processing equipment including storage devices subject to transfer or reuse should be sanitized in accordance with CenturyLink data classification handling procedures.

Unattended User Equipment (7.2.8)

Users should ensure that unattended data processing equipment has appropriate protection.

Session Time Outs (7.2.8.1)

All systems and devices operated on behalf of the State of Tennessee should be configured to clear and lock the screen or log the user off the system after a defined period of inactivity.

Clear Desk and Clear Screen Policy (7.2.9)

All data classified as confidential must be stored in a locked cabinet or room when unattended. All data processing equipment that provide access to Information Processing Systems will be configured so that a screen-saver, with password protection engaged, or other lock-down mechanism that prevents unauthorized viewing of screen information or unauthorized access to the system will automatically be implemented if the system has been left unattended.

MINIMUM COMPLIANCE REQUIREMENTS:
Redacted for public version of policy

8. NETWORK CONNECTIVITY SECURITY

Network Security Management (8.1)

Objective: To ensure the protection of the State's assets that are accessible by suppliers and vendors.

Network Controls (8.1.1)

Networks should be managed and controlled to protect information in systems and applications.

Security of Network Services (8.1.2)

Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements.

Segregation in Networks (8.1.3)

Information Transfer (8.2)

Objective: To maintain the security of information transferred within network infrastructures manage by on behalf of the State and with any external entity.

Information Transfer Policies and Procedures (8.2.1)

Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.

Agreements on Data Transfer Policies (8.2.2)

Agreements should address the secure transfer of business information between the State and external parties.

Electronic Messaging (8.2.3)

Data involved in electronic messaging should be appropriately protected.

External Electronic Messages Control (8.2.3.2)

E-mail sent through the public Internet must be encrypted if it contains confidential information in the body or attachment of the email. Confidential information should not be placed into the subject line of the message.

Electronic Messaging Management (8.2.3.3)

All electronic messages created, sent or received in conjunction with the transaction of official business should use the State approved gateway(s) to communicate via the Internet.

Confidentiality or Non-Disclosure Agreements (8.2.4)

When exchanging or sharing information classified as Sensitive or Confidential with external parties that are not already bound by the contract confidentiality clause, a non-disclosure agreement should be established between the owner of the data and the external party.

10. EXTERNAL PARTY SECURITY

Information Security for External Party Relationships (10.1)

Objective: To ensure the protection of the State's assets that are accessed, processed, communicated to, or managed by external parties, suppliers or vendors. This includes any external party who has access to physical data processing facilities, logical access to State data processing systems via local or remote access or access via another external party into the State's data processing facilities.

Information Security Policy for External Party Relationships (10.1.1)

Information and physical security requirements for mitigating the risks associated with supplier or vendor access to the State's assets should be agreed upon in writing with the external party.

Identification of Risk (10.1.2)

Risk involving external parties should be identified and proper controls implemented prior to the granting of access to any State of Tennessee information, information technology asset or information process facility.

Addressing Security within External Party Agreements (10.1.3)

All relevant information security requirements should be established and agreed upon with each supplier or vendor that may access, process, store, communicate, or provide IT infrastructure components for the State's processing systems or infrastructure.

Reporting of Security Incidents (10.1.3.1)

External Party Agreements will require external parties to report perceived security incidents that may impact the confidentiality, integrity or availability of State data promptly.

Sub-Contractors Requirements (10.1.3.2)

Primary external parties should require their sub-contractors to abide by State of Tennessee policies and security requirements, as applicable.

11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Security Requirements of Information Systems (11.1)

Objective: To ensure that information security is an integral part of information systems throughout their life cycle. This includes application infrastructure, vendor applications, and information systems which provide services over public networks or the State's internal network.

Security Requirements of Information Systems (11.1.1)

Security requirements should be identified and documented as part of the overall business case for new information systems and for enhancement to existing information systems and should be included early and continuously throughout the lifecycle of the application, including, but not limited to the conception, design, development, testing, implementation, maintenance and disposal phases.

Securing Application Services on Public Networks (11.1.2)

Information involved in application services passing over public networks should be protected from fraudulent activity and unauthorized disclosure or modification.

Protecting Application Services Transactions (11.1.3)

Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Information Security in Project Management (11.1.4)

Information security should be addressed at project initiation and throughout the lifecycle of the project.

Security in Development and Support Processes (11.2)

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

Security Requirements of Information Systems (11.2.1)

Requirements, rules and guidelines for the development of software and systems should be established and applied to all systems development.

Security in Application Systems Development (11.2.1.1)

Input validation, authentication, and authorization should be included in the design, development and implementation of applications.

Control of Internal Processing (11.2.1.6)

Security controls should be included to prevent corruption due to processing errors or deliberate acts.

System Change Control Procedures (11.2.2)

Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.

Technical Review of Applications after Operating Platform Changes (11.2.3)

When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Restrictions or Changes to Software Packages (11.2.4)

Modifications to software packages should be limited to necessary changes, and all changes should be strictly controlled.

Secure System Engineering Principles (11.2.5)

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

Secure Development Environment (11.2.6)

Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

Outsourced Development (11.2.7)

Outsourced system development should be monitored and supervised to ensure CenturyLink's policies and practices are followed and to ensure appropriate security controls are in place.

System Security Testing (11.2.8)

Testing of security functionality should be carried out during development. Applications should be tested periodically throughout their respective lifecycles, at each major version release and prior to assigning public IP addresses or being moved or promoted into the production environment.

System Acceptance Testing (11.2.9)

Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.

Test Data (11.3)

Objective: To ensure the protection of the data used for testing.

Protection of Test Data (11.3.1)

Test data should be selected carefully, protected and controlled. The use of production data for development and testing is prohibited.

13. INFORMATION SECURITY INCIDENT MANAGEMENT

Management of Information Security Incidents and Improvements (13.1)

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Responsibilities and Procedures (13.1.1)

The State of Tennessee will establish a Security Incident Response Team (CIRT). The CIRT will ensure that the State of Tennessee can efficiently and effectively communicate information security incidents to the proper stakeholders and respondents of the State. The CIRT members will be appointed based on their position and capabilities within the organization. Each agency should designate an information security “point of contact” (POC), in accordance with the Information Systems Council’s “Information Resource Policies” requirements. This POC will act as the central communications figure regarding security incidents within the agency. The POC will have responsibility for incident escalations, actions and authority for the administrative oversight of security for the information technology resources under the agency’s control. The POC within each agency will participate as a member of the CSIRT. The CISO of the State of Tennessee will appoint members from within STS to participate in the CIRT.

Reporting Information Security Events (13.1.2)

Information security events should be reported through appropriate channels using CenturyLink Incident response process.

Reporting Information Security Weakness (13.1.3)

Employees and contractors using the State’s information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services to the STS Customer Care Center.

Assessment of and Decision on Information Security Events (13.1.4)

Information security events should be assessed and a determination made on whether to classify the event as an incident in accordance with the Incident Response Plan.

Response to Information Security Incidents (13.1.5)

Information security incidents will be managed in accordance with the documented procedures in the CenturyLink Incident Response Plan.

Learning from Information Security Incidents (13.1.6)

Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

14. RESERVED

15. RESERVED

16. HUMAN RESOURCE

Prior to Employment (16.1)

Objective: To ensure all third parties, contractors, or vendors understand their responsibilities in regards to information security requirements for the State of Tennessee's computing environments.

Reserved (16.1.1)

Acceptable Use Policy (16.1.2)

All provided services are subject to CenturyLink Acceptable Use Policies.

During Employment (16.2)

Objective: To ensure employees and contractors are aware of and fulfill their information security responsibilities.

Management Responsibilities (16.2.1)

Management should ensure that all employees and contractors are aware of and fulfill their information security responsibilities.

Information Security Awareness, Education and Training (16.2.2)

CenturyLink employee and contractors receive annual security awareness training. Individuals in particular positions receive supplementary security training and if a training or testing issue arises (e.g., internal phishing exercises), further guidance is provided.

17. VERSION HISTORY

Version 2.1 – December 15, 2016	<i>Converted Office for Information Resources to Strategic Technology Solutions. Updated policy link in 2.4 Made agency specific policies mandatory for agency specific requirements in 3.1.2. Minor wording changes to sections 13.1.1 and 13.1.2. Updated technology requirement for encryption in 14.1.5. Aligned training periodicity with ISC vote in 16.2.2.</i>
Version 2.2 – December 14, 2017	<i>Updated policy link in 2.4</i>

18. TERMS AND DEFINITIONS

Access Credentials - Access Credentials are issued to users to provide access to particular data or resources. Examples include passwords, badges, and card keys for doors.

Access Granting Authority – The access granting authority is the individual or group that has the responsibility for determining appropriate access and use of resources.

Asset – An asset is anything that can be considered a resource such as employees, computer hardware, computer software, and data.

Authentication – Authentication is the process of ensuring an individual is who they claim to be.

Authorization – Authorization is the process of providing permission to access resources or to perform operations.

Business Continuity – Business Continuity is the ability of an organization to continue its operations and services in the face of a disruptive event.

Business Impact Analysis (BIA) – A Business Impact Analysis is a process that is performed to identify and evaluate the potential impacts of natural and manmade events on business operations.

Cloud Computing – Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Confidential Data – is a generalized term that typically represents **data** classified as Confidential as defined by state or federal statute, regulation or as defined by the Payment Card Industry.

Cryptography - Cryptography is the science of transforming information into a secure form so that it can be transmitted or stored, and unauthorized persons cannot access it.

Custodian – Custodian is the individual or group that is responsible for granting access to data and or network resources.

Data Classification – Data Classification is the process of identifying the levels of protection mechanisms and restrictive access that are required for data based on state or federal statute, regulation and/or criticality and of the data.

Data Validation – Data validation is the process of ensuring that a program operates on clean, correct and useful data.

Hash – A hash is a cryptographic algorithm that can later be decrypted. It is frequently used for comparison purposes to validate the integrity of the data.

Information Systems Council (ISC) – The Information Systems Council is legislatively mandated to provide high level oversight and direction for State of Tennessee information systems and processing.

Input Validation – Input validation is a type of data validation that is applied to data from untrusted sources.

Least Privilege – Least Privilege is a practice where the minimum level of access or privileges required to perform an individual's job duties are granted.

Logic Bomb – A logic bomb is computer code that lies dormant until it is triggered by a specific logical event.

Mobile Device – A mobile device is a computing platform that not meant to be stationary. Examples include but are not limited to laptops, tablets, i-Phones, i-Pads and android devices.

Multifactor Authentication – Multifactor Authentication is using more than one factor to authenticate an individual or resource. Factors include something you know (password), something you have (token or smartcard) and something you are (biometrics such as iris or retinal scans or fingerprints).

Owner – Owner is the individual who is the final authority and decision maker in determining how data and resources are used in State business and what level of access will be granted to them.

Payment Card Industry (PCI) – The Payment Card Industry is comprised of the organizations that transmit, process or store cardholder data. The PCI works with the Payment Card Industry Security Standards Council to develop Payment Card Industry Data Security Standards.

Rootkit – A rootkit is a set of software tools used by an attacker to hide the actions or presence of other types of malicious software.

Salt - A salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase, making the stored data more difficult to crack.

Security Advisory Council – The Security Advisory Council is comprised of the directors in Strategic Technology Solutions.

Security Event – A security event is an event that adversely impacts the established security behavior of an environment or system

Security Incident - A security incident can be accidental or malicious actions or events that have the potential of causing unwanted effects on the confidentiality, integrity and availability of State information and IT assets.

Service Account – A service account is an account that is used by systems, services or applications, not by individuals.

Trojan Horse – A trojan horse (or Trojan) is an executable program advertised as performing one activity, but actually does something else.

Virtual Private Network (VPN) – A VPN extends a private network across a public network, such as the Internet. It enables a computer or wireless enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.

Virus – A computer virus is malicious computer code that reproduces itself on the same computer.

Worm – A computer worm is a malicious program that takes advantage of a vulnerability on one computer and spreads itself to other computers with the same vulnerability.

19. APPENDICES

- Appendix A State of Tennessee Approved Login Banner
- Appendix B Secure Application Development
- Appendix C Information Security Incident Response and Alerting Communications Plan

Enterprise Information Security Policies

State of Tennessee
Department of Finance and Administration
Strategic Technology Solutions

Document Version 2.2

December 14, 2017



Mark Bengel, CIO

Stephanie Dedmon, Deputy CIO

Curtis Clan, CISO

Domestic CenturyLink IQ Networking Service Exhibit

CenturyLink IQ Networking is subject to the Local Access Service Exhibit, the Participating Addendum, and the NASPO ValuePoint Master Agreement #AR2474 between Customer and CenturyLink QCC. Port types that require Rental CPE are also subject to the Rental CPE Service Exhibit. All capitalized terms that are used but not defined in this Attachment are defined in the Agreement or Service Exhibit.

1. General. Domestic CenturyLink IQ® Networking Service ("Service") is provided by CenturyLink QCC under the terms of the Agreement, this Service Exhibit, and any signed quotes between CenturyLink QCC and Customer.

2. Service.

21 Description. Service is a data, IP, and a network management solution that is designed for connectivity between Customer's sites or public Internet connectivity.

22 Ports. CenturyLink offers Service in the following port ("Port") types:

(a) Internet Port. Internet Ports provide public Internet connectivity.

(b) Private Port. Private Ports provide WAN connectivity between Customer sites. Customer may allocate Private Port traffic up to 10 different closed user groups. Customer may request more than 10 point-to-point closed user groups for an additional charge. Quality of service ("QoS") traffic prioritization can be used with Private Ports. Ethernet Private Ports with real-time traffic that require QoS are subject to local access limitations.

(c) CenturyLink IQ+® Port. A CenturyLink IQ+ Port is a bundled solution that includes the following: (i) the functionality of a Private Port, (ii) Local Access, (iii) Monitor and Notification for a CenturyLink provided or approved router, (iv) End-to-End Performance Reporting, and (v) optional CenturyLink provided router as Rental CPE and Priority Queuing. The Local Access and CenturyLink provided router for domestic Service are subject to the Local Access Service Exhibit and CenturyLink Rental CPE Service Exhibit (including the applicable Detailed Description), respectively. Customer may provide a router approved by CenturyLink. Domestic Service with a CenturyLink provided router includes 8x5 NBD maintenance using ProMET® Remote Standard Service or 24x7 on-site maintenance using ProMET® On-Site Premium Service at Customer qualified sites. CenturyLink may use repackaged Rental CPE or substitute the Rental CPE with other CPE. Customer is responsible for any trouble shooting and repair of equipment on Customer's side of the router. Domestically, a CenturyLink IQ+ Port is only available in a CenturyLink determined data center.

(d) CenturyLink IQ+® Cloud Port. A CenturyLink IQ+ Cloud Port is a bundled solution that provides: (i) private connectivity between Customer's Private Port sites and Customer resources in CenturyLink determined data centers and/or cloud service provider environments, (ii) Local Access (Data Center Access), (iii) Monitor and Notification and (iv) End-to-End Performance Reporting. Customer can use all Private Port features defined in the Private Port section above. Access within data centers and cloud service provider environments may include shared or virtualized services where available. Customer understands that cloud-related services are contracted separately.

23 Network Management Service. CenturyLink Network Management Service ("NMS") is a feature available for all Ports. For CenturyLink IQ+ Cloud Ports, the only available type of NMS is Monitor and Notification. Select Management or Comprehensive Management is available with domestic Ports. The feature provides performance reporting, change management, configuration management, fault monitoring, management and notification of CPE and network related issues. Customer may also request NMS management features for devices not associated with a CenturyLink IQ Networking Port in domestic locations with CenturyLink's prior approval. The NMS management types are set forth in more detail below.

(a) Monitor and Notification. Monitor and Notification can be included with CenturyLink IQ+ Ports and CenturyLink IQ+ Cloud Ports and is an optional NMS feature for the other Port types. CenturyLink will monitor the Customer devices 24x7x365 for up/down status using ICMP ping. CenturyLink will notify Customer if no response is received for a designated period. NMS will not provide any troubleshooting and incident resolution for device or network faults. "Monitor & Notification" is the only NMS option available for devices that do not support SNMP and/or are not certified for NMS.

(b) Select Management. Select Management can be included with any eligible domestic Port, except for CenturyLink IQ+ Cloud Ports. CenturyLink will monitor Customer devices 24x7x365 for up/down status as well as provide 24x7x365 remote performance monitoring, reporting, and ticketing via an NMS online portal for devices supported by CenturyLink, fault monitoring, management, and notification (detection, isolation, diagnosis, escalation and remote repair when possible), change management supported by CenturyLink (up to 12 changes per year), asset management (device inventory), and configuration management (inventory of customer physical and logical

Domestic CenturyLink IQ Networking Service Exhibit

configuration). Customer must make change management requests via Control Center at <https://controlcenter.centurylink.com>. Select Management only supports basic routing functions. NMS does not include new CPE initial configuration, lab testing, lab modeling, or on-site work of CPE. The NMS supported device list and a standard change management list are available on request and are subject to change without notice.

(c) Comprehensive Management. Comprehensive Management can be included on any eligible Port, except for CenturyLink IQ+ Cloud Ports. Comprehensive Management includes all of the Select Management features as well as total customer agency and change management (up to 24 configuration changes per year) of complex routing functions within routers, switches, and firewall modules. This includes configuration and management of complex routing, switching, device NIC cards, firewall module configurations, and basic router internal firewall functions. CenturyLink acts as the Customer's single point of contact in managing the resolution of all service, device, and transport faults covered by Comprehensive Management and will work with any third party hardware and/or transport providers the Customer has under contract until all network issues are successfully resolved. With Internet security protocol ("IPSec"), CenturyLink can configure full mesh, partial mesh, or hub-and-spoke topologies with secure tunnels for remote communication between Customer locations. IPSec is only available on approved Cisco and Adtran devices. IPSec opportunities greater than 25 devices or with other manufacturer's devices require CenturyLink approval before submitting an order.

(d) CenturyLink Responsibilities. For NMS, CenturyLink will provide Customer with a nonexclusive service engineer team, which will maintain a Customer profile for the portion of the Customer's network where the devices covered by NMS reside. CenturyLink will work with Customer to facilitate resolution of service affecting issues with Select Management or Comprehensive Management.

(e) Customer Responsibilities.

(i) Customer must provide all information and perform all actions reasonably requested by CenturyLink in order to facilitate installation of NMS. If Customer limits or restricts CenturyLink's read/write access to a device, CenturyLink cannot support configuration backups. Customer is responsible for supporting CenturyLink in access, troubleshooting, and configuration requests made in accordance with normal troubleshooting and repair support activities. For Out-of-Band management related to fault isolation/resolution, Customer will provide and maintain a POTS line for each managed device. "Out-of-Band" means a connection between two devices that relies on a non-standard network connection, such as an analog dial modem, which must be a CenturyLink certified 56k external modem. Additionally, Customer will provide a dedicated modem for each managed device. It is not mandatory that Customer have a POTS line but Customer must understand that CenturyLink will not be able to troubleshoot issues if the device covered by NMS cannot be reached. Service related outages requiring access to the device for troubleshooting and repair purposes will impact the eligibility of any associated SLA credits.

(ii) For Comprehensive Management, Customer must execute the attached Letter of Agency (Attachment 1) to authorize CenturyLink to act as Customer's agent solely for the purpose of accessing Customer's transport services.

(iii) Depending on transport type, Customer's managed devices must comply with the following set of access requirements: (A) for NMS delivered via IP connectivity with an Internet Port or other public Internet service, devices must contain an appropriate version of OS capable of establishing IPsec VPNs; and (B) for NMS delivered with a Private Port, CenturyLink will configure a virtual circuit to access Customer's device at no additional charge. CenturyLink will add the NMS network operations center to the Customer closed user group to manage the devices within Customer's network.

(iv) Customer must provide a routable valid IP address to establish the NMS connection. Customer's primary technical interface person must be available during the remote installation process to facilitate installation of NMS. All Customer devices managed under NMS must be maintained under a contract from a CenturyLink approved onsite CPE maintenance provider. The response times for which Customer contracts with its CPE maintenance provider will affect CenturyLink's timing for resolution of problems involving Customer provided devices. The performance of the CPE maintenance provider is Customer's responsibility.

(v) Customer may not reverse engineer, decompile, disassemble or apply any other process or procedure to alter any CPE, software, or other component of this Service for any purpose.

24 End-to-End Performance Reporting. End-to-End Performance Reporting is a feature included all Ports, except for Ports with VPLS. Customer must include CenturyLink as a member of each closed user group. The feature includes a report based on data collected from Customer's traffic within its closed user groups and measures availability, jitter, latency, and packet delivery between Customer's edge routers, between CenturyLink's routers, and between Customer's edge routers and CenturyLink's routers. The data contained in the report is measured differently

Domestic CenturyLink IQ Networking Service Exhibit

than the goals contained in the SLA applicable to the Service and is for informational purposes only. Customer is not entitled to SLA credits based on the data in the report. Customer may access the report in the Control Center portal. Some quote forms or other associated documents may use "End-to-End Performance Monitoring" to mean "End-to-End Performance Reporting".

25 Multicast. Multicast is an optional feature for Private Ports. The feature enables IP multicast on the CenturyLink IP network. Customer must configure its edge devices with CenturyLink designated multicast protocol specifications and use the CenturyLink designated IP address range for Customer's multicast applications. The standard feature allows up to ten sources of multicast traffic per Customer, but CenturyLink may permit a limited number of additional sources.

26 VPLS. Layer 2 virtual private LAN service ("VPLS") is optional feature for Private Ports only. VPLS is not available for CenturyLink IQ+ Ports or CenturyLink IQ+ Cloud Ports. Private Ports with VPLS are supported on CenturyLink-certified Cisco equipment and are limited to the following connection and encapsulation methods: Ethernet 10 Mbps, 100 Mbps, 1000 Mbps with Ethernet encapsulation; DS1 and DS3 with Frame Relay encapsulation, and OC3 with ATM encapsulation. The following features are not available with Private Ports with VPLS: (a) usage reports; (b) the Precise Burstable or Data Transfer pricing methodologies; (c) the SLA's Reporting Goal; (d) VPN Extensions and (e) End-to-End Performance Reporting.

27 VPN Extensions. A VPN Extension is an optional feature for layer 3 multi protocol label switching ("MPLS") Private Ports. The feature allows Customer to extend its Layer 3 MPLS closed user groups to Customer locations that are not served by CenturyLink's MPLS network ("Remote Location"). Customer can establish a tunnel through the Internet between the Customer's CPE at the Remote Location (separately purchased and managed by Customer) and the CenturyLink network device. The Customer provided CPE must support the CenturyLink service configurations and be installed as designated by CenturyLink or as otherwise agreed upon by the parties. Customer is responsible for the installation, operation, maintenance, use and compatibility of the Remote Location CPE. Customer will cooperate with CenturyLink in setting the initial configuration for the Remote Location CPE interface with the VPN Extension Service. Customer must use IP connectivity at the Remote Location that includes a static public IP address.

(a) Exclusions. CenturyLink will not debug problems on, or configure any internal or external hosts or networks (e.g., routers, DNS servers, mail servers, www servers, and FTP servers). All communication regarding the VPN Extension must be between CenturyLink and a Customer approved site contact that has relevant experience and expertise in Customer's network operations. The following features are not available with VPN Extensions: (i) End-to-End Performance Reporting; (ii) QoS; (iii) VPLS; and (iv) Multicast. VPN Extensions are not subject to the SLA.

28 Backbone Prioritization/Priority Queuing. Backbone Prioritization and Priority Queuing is an optional feature available with individual domestic Private Ports, CenturyLink IQ+ Ports, and CenturyLink IQ+ Cloud Ports. When this feature is configured on such Port, traffic originating from that Port will be designated at a higher class of service to the CenturyLink IP network than traffic originating from such Ports without the feature or Internet Ports. If Customer desires the feature for traffic between two or more such Ports, the feature must be ordered for each such Port. The benefit from this feature is realized during periods of high network congestion. The feature may not be available at all locations or with Multicast in certain circumstances.

3. Ordering. For purposes of this Service Exhibit, "Order Form" means the State purchase order and associated statement of work ("SOW") Subject to availability, CenturyLink will assign /29 Internet address space for Customer during the use of a Port. Neither Customer nor any End Users will own or route these addresses. Upon termination of Service, Customer's access to the IP addresses will cease. If Customer requests special sequencing for Port installation, Customer must designate a Key Port. A "Key Port" is a Port that must be available on the network before adding additional domestic Port locations. The installation of the Key Port will determine the timelines for the installation of other domestic Ports. Customer may designate one Key Port within its CenturyLink IQ Networking network topology by notifying CenturyLink in writing of that request. Unless the parties otherwise agree in writing, Customer has sole responsibility for ordering, securing installation and ensuring proper operation of any and all equipment required to enable Customer to receive the Service.

4. Charges. Customer must pay all applicable MRCs and NRCs set forth in the NASPO ValuePoint Master Agreement #AR2474 or SOW. Charges will commence within five days after the date CenturyLink notifies Customer that Service is provisioned and ready for use ("Start of Service Date"). Customer may order multiple Ports with multiple pricing methodologies in accordance with the pricing methodologies set forth below. Customer may change the pricing methodology (e.g., from Flat Rate to Precise Burstable) of a Port if: (a) the Port's new MRC remains the same or greater than the old MRC, and (b) the Port starts a new Service Term that is equal to or greater than the remaining number of months in the old Service Term, subject to a 12 month minimum. The net rate MRCs set forth in the pricing catalog, SOW, offer attachment or valid signed CenturyLink issued quote. Net rate MRCs are lieu of all other rates, discounts,

Domestic CenturyLink IQ Networking Service Exhibit

and promotions. The End-to-End Performance Reporting, VPN Extension, SIG and Multicast features are provided on a month-to-month basis and either party may cancel a feature with 30 days' prior written notice to the other party. CenturyLink may upon 30 days prior written notice to Customer modify those features, including without limitation, If a CenturyLink IQ+ Port uses Data Center Access as the access type, that Port will be understood to be a CenturyLink IQ+ Cloud Port.

41 Pricing Methodologies.

(a) **Flat Rate.** The Flat Rate pricing methodology bills Customer a specified MRC for a given Port speed regardless of Customer's actual bandwidth utilization.

(b) **Tiered.** The Tiered pricing methodology caps Customer's bandwidth at the tier specified on an Order Form and bills the Customer a fixed MRC based on that bandwidth tier regardless of Customer's actual bandwidth utilization. No more than once per month, Customer may change its specific bandwidth tier (e.g., 2 Mbps to 10 Mbps) within the applicable Port classification (e.g., Ethernet, Fast Ethernet). Customer may not change its bandwidth from one Port classification to another.

(c) **Precise Burstable.** Usage samples are taken every five minutes throughout the monthly billing cycle. Only one sample is captured for each five-minute period, even though there are actually two samples taken; one for inbound utilization and one for outbound utilization. The higher of these two figures is retained. At the end of the billing period, the samples are ordered from highest to lowest. The top 5% of the samples are discarded. The highest remaining sample is used to calculate the usage level, which is the 95th percentile of peak usage. For each Precise Burstable Port, Customer will pay an MRC calculated by multiplying Customer's 95th percentile of peak usage in a given month by the applicable MRC per Mbps. There is a minimum usage amount within each Precise Burstable Port classification ("Precise Burstable Minimum"). Customer will be billed the greater of the Precise Burstable Minimum or the actual charges based upon its 95th percentile of peak usage.

(d) **Data Transfer.** Usage samples are taken every five minutes throughout the Customer's monthly billing cycle. Samples are taken for both in-bound utilization and out-bound utilization. Customer will be billed for the sum total of both inbound and outbound utilization. Charges are applied using a stepped or "metered" methodology such that Customer's traffic will be billed incrementally at each volume tier. For example, if Customer's total volume on a DS1 circuit is 10 GB, the first 7 GB of such total would be billed at the 0-7 GB tier, and the remaining 3 GB would be billed at the 7.01-17 GB tier. For each Data Transfer Port ordered hereunder, Customer will pay an MRC calculated by multiplying Customer's volume of data transferred in a given month (in GBs) by the applicable MRC per GB. Within each Data Transfer Port classification (e.g., DS1, DS3), Customer will be subject to the minimum usage amount set forth in the column heading of the applicable Data Transfer pricing table ("Data Transfer Minimum"). Customer will be billed the greater of the Data Transfer Minimum or the actual charges based upon its actual volume of data transferred. Data Transfer pricing is only available if Customer's premises-based router uses HDLC, PPP, or MLPPP line encapsulation.

5. Term; Cancellation.

51 Term. The term of an individual Port (and associated features/Services, if applicable) begins on the Start of Service Date for that Port and continues for the service term shown on the valid signed CenturyLink issued quote, SOW or the pricing catalog. If Service is installed at multiple Customer locations or with multiple Ports at a Customer location, each separate Port (and associated features/Services) will have its own Start of Service Date. Upon expiration of a Service Term, individual domestic Ports (and associated features/Services) will remain in effect on a month-to-month basis until canceled by either party with 30 days' notice.

52 Cancellation. Cancellation of the Service shall be in accordance with terms and conditions set forth in section 7 of the Participating Addendum.

6. E-mail Notification. Customer acknowledges and agrees that CenturyLink may contact Customer via e-mail at the e-mail address provided to CenturyLink when Customer ordered the Service for any reason relating to the Service, including for purposes of providing Customer any notices required under the Agreement. Customer agrees to provide CenturyLink with any change to its email address.

7. SLA. Ports other than CenturyLink IQ+ Ports or CenturyLink IQ+ Cloud Ports are subject to the CenturyLink IQ Networking Service Level Agreement ("SLA"), CenturyLink IQ+ Ports and CenturyLink IQ+ Cloud Ports are subject to the CenturyLink IQ+ Port SLA and the NMS feature is subject to the NMS SLA. For Customer's claims related to Service or NMS feature deficiencies, interruptions or failures, Customer's remedies are set forth in the applicable SLA. References to CenturyLink IQ+ Ports in the CenturyLink IQ+ SLA will also refer to CenturyLink IQ+ Cloud Ports.

Domestic CenturyLink IQ Networking Service Exhibit

ATTACHMENT 1

COMPREHENSIVE MANAGEMENT

LIMITED LETTER OF AGENCY

between

State of Tennessee ("Customer")

and

CenturyLink Communications, LLC f/k/a Qwest Communications Company, LLC ("CenturyLink")

This limited letter of agency ("LOA") hereby authorizes CenturyLink to act as the Customer's agent for the limited purpose of contacting Customer's designated Local Exchange Carrier ("LEC"), Interexchange Carrier ("IXC"), Internet Service Provider ("ISP"), or customer premises equipment ("CPE") maintenance provider in conjunction with CenturyLink Network Management Service. Network Management Service activities will consist of working with Customer's LEC, IXC, ISP, and/or CPE maintenance provider for the purpose of: (a) extracting information concerning transmission data elements carried over Customer's network connection; (b) identifying Customer's links or data link connection identifiers ("DLCIs"); (c) opening, tracking, and closing trouble tickets with the LEC, IXC, ISP, or CPE maintenance provider on Customer's transport links or CPE when an alarm or fault has been detected; (d) dispatching CPE repair personnel on behalf of Customer to CPE for which a fault has been detected; and (e) discussing fault information with the LEC, IXC or CPE maintenance provider on behalf of Customer to facilitate resolution of the problem.

CenturyLink does not assume any of Customer's liabilities associated with any of the services the Customer may use.

The term of this LOA will commence on the date of execution below and will continue in full force and effect until terminated with 30 days written notice by one party to the other or until the expiration or termination of the Network Management Service.

A copy of this LOA will, upon presentation to LEC, IXC, ISP, and/or CPE maintenance provider, as applicable, be deemed authorization for CenturyLink to proceed on Customer's behalf.

Customer Company Name

Authorized Signature of Customer

Print or Type Name

Title

Date

Local Access Service Exhibit

1 General. CenturyLink QCC will provide Local Access Service ("Service") under the terms of this Service Exhibit, the Agreement and the RSS.

2 Service Description and Availability.

21 Description. Service provides the physical connection between the Service Address and the CenturyLink Domestic Network. Service includes any entrance cable or drop wire to, and equipment maintained by CenturyLink at the Demarcation Point, but does not include CPE, Extended Wiring unless CenturyLink notifies customer that Extended Wiring is included with a service offering, inside wiring, or other equipment not maintained by CenturyLink. Customer is responsible for any additional terminations beyond the Demarcation Point. All equipment owned by CenturyLink remains property of CenturyLink. Customer disclaims any interest in any equipment, property or licenses used by CenturyLink to provide Service. Service is not a standalone service and Customer must purchase the Service in connection with another CenturyLink service for which a local loop is required.

22 Types of Service Technologies. CenturyLink uses the following different technologies to provide Service. Some technologies or speeds may not be available in all areas or with certain types of Service.

(a) Special Access. "Special Access" means Service using digital signal bandwidths DS0, DS1 and DS3 or Optical Carrier signal bandwidths OC3, OC12, OC48 and OC192.

(b) Ethernet Local Access ("ELA"). ELA is available at bandwidths varying from 1 Mbps to 1,000 Mbps (1G) and 10G (Cross-Connect Access only). ELA is available in the following options: Native Single-Class-of-Service (CoS) Low, Native Single-CoS Medium, Native Single-CoS High, Native Multi-CoS, ELA over SONET, or Ethernet Virtual Access ("EVA"). "Native Single-CoS Low" is a layer 2, switched, native service using a standard Ethernet offering from the local access provider. Native Single-CoS Low is not recommended for use with critical applications (i.e. voice), but is ideal for non-critical applications (i.e. Internet and email traffic). "Native Single-CoS Medium" is a layer 2, switched, native service using a better-than-standard Ethernet offering from the local access provider. Native Single-CoS Medium is ideal for a combination of non-critical and/or critical applications; typically varying voice, video, and data. "Native Single-CoS High" is a layer 2, switched, native service using the best Ethernet offering from the local access provider. Native Single-CoS High is ideal for critical applications; typically predictable and reliable voice and data. Native Single-CoS Medium and Native Single-CoS High are only available with the following CenturyLink services: CenturyLink IQ® Networking Internet Port, Private Port or Enhanced Port with Secure Internet Gateway, E-Line, or Ethernet Private Line ("EPL"). Native Single-CoS Medium or Native Single-CoS High circuit speed must match the maximum CenturyLink IQ Networking port, E-Line, or EPL bandwidth. "Native Multi-CoS" is a layer 2, switched, native service closely aligning the CenturyLink IQ Networking QoS and the local access provider's Ethernet class of service offering and is only available with CenturyLink IQ Networking Private Port or Enhanced Port with Secure Internet Gateway. At Customer's discretion, Native Single-CoS Low, Native Single-CoS Medium, Native Single-CoS High, or Native Multi-CoS may be used to support CoS for critical applications (i.e. voice). "ELA over SONET" is a layer 1, SONET-based service. EVA is a layer 2, Ethernet-based service that provides customers with a premium non-oversubscribed connection with Fast E and Gig E connection types. Customer may experience delayed installation intervals due to construction requirements and available bandwidths may be limited due to distance and available Ethernet-supported facilities from the local access provider.

(c) Wavelength Local Access. "Wavelength Local Access" means Service using wave division multiplexing technology. Wavelength Local Access is available at bandwidths of 1 GbE, 10 GbE LAN PHY, 2.5 G (OC48), 10 GbE WAN PHY (OC192), 40G, OTU1, OTU2, OTU3, 1G, 2G, 4G and 10G.

(d) DSL Local Access. "DSL Local Access" means Leased Access using digital subscriber line ("DSL") technology. DSL Local Access is available at bandwidths varying from 128 kbps/64 kbps to 15000 Mbps/1000 Mbps. Customer may experience delayed installation intervals due to Construction requirements and available bandwidths may be limited due to distance and available DSL-supported facilities from the local access provider.

2.2.1 Use of IP Connection. In some locations, CenturyLink will enable the Local Access component of your service using "IP Connection" which is a Layer 3, symmetrical functionality that utilizes established IP and MPLS transport technologies. In such cases, Customer agrees that it will use IP Connection functionality only for the provision of either: (i) wireline broadband Internet access (as defined in applicable Federal Communications Commission orders and regulations), or (ii) wireline broadband Internet access plus additional information services, with wireline broadband Internet access constituting a principal use. CenturyLink can provision IP Connection functionality over multiple designs with MPLS transport supporting speeds up to 1G/1G.

Local Access Service Exhibit

23 Types of Service. CenturyLink offers the following three types of Service: CenturyLink Provided Access, Customer Provided Access or Cross-Connect Access.

23.1 CenturyLink Provided Access. "CenturyLink Provided Access" or "CLPA" means either On-Net Access or Leased Access.

(a) On-Net Access. For On-Net Access, Customer must be located in a CenturyLink designated building in which On-Net Access is generally available. On-Net Access is generally available as Special Access (except at the DS0 bandwidth), ELA, and Wavelength Local Access. Depending on the Service Address, On-Net Access may be provided through an existing CPOP, newly built CPOP, existing intra-building local loop facilities, or connections to a third party provider where CenturyLink coordinates the connectivity between CenturyLink facilities and facilities of a service provider with whom CenturyLink is interconnected.

(b) Leased Access. Leased Access is generally available as Special Access, ELA, Wavelength Local Access, and DSL Local Access at the bandwidths described in this Service Exhibit for those access types. Customer may request a Preferred Provider for Leased Access from a list of available providers with whom CenturyLink has interconnect agreements. CenturyLink will attempt to use Customer's Preferred Provider, but both final routing and the provider actually used will be chosen by CenturyLink. Where available for Special Access, ELA and Wavelength Local Access, Customer may request CenturyLink to provide a separate fiber facility path for a protection system between the local access provider's serving wire center and the Service Address ("Protect Route"). Protect Route uses backup electronics and two physically separate facility paths in the provisioning of Service. If the working facility or electronics fail, or the Service performance becomes impaired, the facility is designed to automatically switch to the Service protect path in order to maintain a near-continuous flow of information between locations. Special Access and ELA are also generally available as a central office meet point at a local access provider central office to which Customer has a dedicated connection.

23.2 Customer Provided Access. "Customer Provided Access" or "CPA" means a local loop that Customer orders from a local access provider to connect Customer's premises to the CenturyLink Domestic Network at a connection point specified by CenturyLink. CenturyLink will provide Customer with a limited letter of agency ("LOA"), which is incorporated by this reference, authorizing Customer to act as CenturyLink's agent so that Customer's local access provider will connect Customer's premises to the CenturyLink Domestic Network. Customer will also need to execute a CPA-DAR Addendum for CPA POP with ELA or Wavelength Local Access. Customer will pay a CPA charge to CenturyLink when Customer uses the following: (a) Special Access CPA dedicated facilities or ELA CPA virtual local area network ("VLAN"), both of which are dedicated entrance facilities CenturyLink leases from a local access provider and that carry traffic only from CenturyLink; or (b) ELA CPA POP, which requires CenturyLink to provide space and power for the local access provider to install Ethernet equipment; or (c) Wavelength Local Access. Customer will pay a CPA charge to CenturyLink when Customer uses Special Access CPA non-dedicated facilities owned by local access providers and that carry traffic from multiple carriers, including CenturyLink, if the provider charges CenturyLink for those facilities. CPA ELA VLAN is an access type where CenturyLink will provision and assign an Ethernet virtual circuit from a CenturyLink POP to a Customer designated Ethernet facility leased from a common Ethernet service provider. This access will be used to connect to a CenturyLink VLAN assignment on a CenturyLink IQ Networking Internet or Private Port or E-Line. CenturyLink will not bill Customer a CPA charge for an IP layer 3 expansion site because Customer, not CenturyLink, is responsible for ordering a cross-connect from the IP layer 3 expansion site manager to meet CenturyLink in the IP layer 3 expansion site's meet-me-room. CPA is the responsibility of Customer and CenturyLink will not pay for or troubleshoot components of CPA.

23.3 Cross-Connect Access. "Cross-Connect Access" or "XCA" means: (a) an intra-POP connection between certain Customer facilities with direct access to the CenturyLink Domestic Network and the CenturyLink backbone access point either (i) located within CenturyLink's transport area where CenturyLink allows Customer to bring its own fiber directly to the CenturyLink fiber under an executed Direct Connect Agreement ("Direct Connect") or (ii) in an area where Customer has leased space in a CPOP, a remote collocation site, or a collocation hotel under a Telecommunications Collocation License Agreement or (b) a connection between a CenturyLink-determined data center and a CenturyLink IQ Networking Port, Optical Wavelength Service ("OWS"), or E-Line ("Data Center Access") under an executed CenturyLink TS Service Exhibit with a CenturyLink IQ Networking, OWS or E-Line Service Exhibit. Data Center Access is available in bandwidths of 100 Mbps, 1G, and 10G (CenturyLink IQ Networking and OWS only). Direct Connect requires splicing of Customer and CenturyLink fibers and cross-connection of individual circuits.

24 RSS. Customer understands that Service is an interstate telecommunications service, as defined by Federal Communications Commission regulations and represents while using the Service, more than 10% of its usage will be interstate usage.

Local Access Service Exhibit

3. Ordering. Upon receipt of a State purchase order for a Service, CenturyLink will notify Customer of CenturyLink's target date for the delivery of that Service ("Estimated Availability Date"). Once CenturyLink notifies Customer of the Estimated Availability Date for a Service, cancellation fees or Cancellation Charges set forth in the Cancellation section below will apply to any cancellation of that order. If Customer fails to respond to CenturyLink's requests to arrange for the installation of a Service when CenturyLink is ready, CenturyLink may consider the affected Service order canceled. CenturyLink will use commercially reasonable efforts to install each such Service on or before the Estimated Availability Date, but the inability of CenturyLink to deliver Service by such date is not a default under the Agreement or this Service Exhibit.

4. Charges. Customer will pay the rates set forth in a quote or SOW for Service issued by CenturyLink if the rates for Service at a particular Service Address are not included in the pricing catalog. CenturyLink invoices MRCs in advance and NRCs in arrears. If the Start of Service Date for any Service falls on any day other than the first day of the month, the first invoice to Customer will consist of: (a) the pro-rata portion of the applicable MRC covering the period from the Start of Service Date to the first day of the subsequent month; and (b) the MRC for the following month. Charges for Service will not be used to calculate Contributory Charges. Customer will receive the rates for Service as shown on the pricing catalog regardless of whether an NPA/NXX split or overlay occurs.

4.1 Ancillary Charges. Ancillary charges applicable to Service include but are not limited to those ancillary services set forth in this section. If an ancillary charge applies in connection with provisioning a particular Service, CenturyLink will notify Customer of the ancillary charge to be billed to Customer. Customer may either approve or disapprove CenturyLink providing the ancillary service.

(a) Expedite. A local loop expedite charge applies to orders where Customer requests the delivery of Service one or more days before the Estimated Availability Date. Customer may only request to expedite CenturyLink Provided Access of Special Access and ELA orders (where underlying local access provider allows CenturyLink QCC to order an expedited service.)

(b) Extended Wiring. "Extended Wiring" means additional wiring from the Demarcation Point to Customer's network interface equipment. Customer may only request Extended Wiring for (i) Special Access ordered as Leased Access, (ii) DSL Local Access, and (iii) Ethernet Local Access (where available). Extended Wiring could entail electrical or optical cabling into 1) existing or new conduit or 2) bare placement in drop down ceilings, raised floors, or mounted to walls/ceilings. Once Service is accepted by Customer, the Extended Wiring then becomes property of and maintained by Customer. CenturyLink will maintain Service to the Demarcation Point only.

(c) Construction. Construction charges apply if; (i) special construction is required to extend Service to the Demarcation Point; or (ii) other activities not covered by Extended Wiring are required beyond the Demarcation Point, that cause CenturyLink to incur additional expenses for provisioning the Service ("Construction"). If Customer does not approve of the Construction charges after CenturyLink notifies Customer of the charges, the Service ordered will be deemed cancelled.

(d) Multiplexing. Customer may request multiplexing for Special Access where available. CenturyLink will multiplex lower level local loop into a higher local loop, or vice-versa, for an additional charge. CenturyLink offers multiplexing at a CPOP, at an On-Net Access building or at an ILEC/CLEC facility providing the Leased Access. For multiplexing at a CenturyLink On-Net Access building, CenturyLink provides multiplexed circuit handoffs to Customer at the same On-Net Access Service Address. For multiplexing at ILEC/CLEC facility, CenturyLink facilitates the delivery of multiplexed circuit handoffs to Customer at a single Service Address or at multiple Service Addresses per Customer's request. Multiplexing is generally available at DS1 and OCn circuit levels. Pricing for multiplexing at an ILEC/CLEC facility is on an individual case basis.

(e) Changes. Ancillary change charge applies where Customer requests CenturyLink to change a local loop to a different Service Address that is within the same Customer serving wire center as the existing local loop, but a Cancellation Charge does not apply.

5. Term; Cancellation.

5.1 Term. The term of an individual Service begins on the Start of Service Date for that Service and continues for the number of months specified in a SOW for a particular Service Address or a quote for Service issued by CenturyLink if the rates for Service at particular Service Address are not included in the pricing catalog ("Initial Service Term"). Excluding voice loops and Data Center Access with a month-to-month Initial Service Term, the Initial Service Term will not be less than 12 months.

Local Access Service Exhibit

52 Cancellation. Cancellation of the Service shall be in accordance with terms and conditions set forth in section 7 of the Participating Addendum.

6. Grooming. If CenturyLink plans to groom a circuit on which Service is provided, CenturyLink will provide a grooming notice to Customer. For CPA dedicated facilities grooming, Customer will provide a signed LOA to CenturyLink so that CenturyLink can order the necessary changes. Within 20 calendar days after receipt of that notice, Customer will: (a) notify CenturyLink of its approval, which may not be unreasonably withheld; (b) state its reason for refusing; or (c) request that CenturyLink provide Customer with an LOA so Customer can order the necessary changes. Customer's failure to respond within the 20-day period will constitute approval of the groom. If the groom results in Customer incurring additional NRCs from its local access provider and Customer provides sufficient proof of the local access provider charge, CenturyLink will issue a credit to Customer equal to the local access provider NRC for each groomed circuit. If Customer refuses the groom for On-Net Access, CenturyLink will, upon 20 calendar days' prior written notice, cancel the Service on that circuit and assess a Cancellation Charge. When Customer does not respond to a CPA dedicated facilities grooming notice or refuses a CPA dedicated facilities groom, Customer must either: (a) provide CenturyLink with a LOA/CFA so that CenturyLink can have the local access provider cancel the circuit; or (b) work directly with the local access provider to cancel the circuit. If Customer does neither of these things, CenturyLink will pass through to Customer any costs incurred by CenturyLink from the local access provider as a result of the circuit remaining in place. "CFA" means circuit facility assignment of the CenturyLink facility, as identified by CenturyLink, to which Customer must order a local loop for connection to the CenturyLink Domestic Network.

7. Definitions. Capitalized terms not defined in this Service Exhibit are defined in the Agreement.

"CenturyLink Domestic Network" means the CenturyLink network located within the contiguous U.S. states and Hawaii, which is comprised only of physical media, including switches, circuits, and ports that are operated by CenturyLink.

"CPOP" means a CenturyLink-owned physical point of presence that lies directly on the CenturyLink Domestic Network where direct interconnection between the CenturyLink Domestic Network and a local access provider's network is possible.

"Demarcation Point" means the CenturyLink designated interface between the CenturyLink Domestic Network or the Leased Access provider network and Customer's telecommunications equipment. The Demarcation Point is typically located at a suitable location in the basement or on the first floor of a Service Address where provision is made for termination of the local access provider's outside distribution network facilities.

"Leased Access" means local backbone access circuits ordered and leased by CenturyLink from a local access provider chosen by CenturyLink.

"On-Net Access" means local backbone access circuits provided solely on CenturyLink owned and operated facilities.

"Preferred Provider" or "PP" means a specific local access provider requested by Customer for Leased Access.

"Service Address" means the business building where Customer receives the Service.

"Start of Service Date" for each circuit is the date Customer accepts the circuit, following notification by CenturyLink that the local loop is ready. The ready notification will be via phone call or e-mail. Customer has five days from CenturyLink's ready notification in which to inform CenturyLink if the circuit fails to operate error-free. Within the five-day timeframe, if Customer neither informs CenturyLink about errors nor accepts the circuit, the circuit will be considered to have been accepted and the Start of Service Date to have commenced on the fifth day following CenturyLink's ready notification, regardless of whether Customer placed traffic over the circuit. If Customer informs CenturyLink of circuit errors within the five-day timeframe, CenturyLink will promptly take necessary, reasonable action to correct the errors, and upon correction, notify Customer that the circuit is ready.

1. Applicability. This Service Exhibit applies when Customer orders SD-WAN Service ("SD-WAN Service") which may be designated as "SD-WAN" or "Hybrid-WAN Connectivity" in the Customer Order, pricing catalog, SOW, Order acceptance, service delivery, billing and related documents, and the associated Access Services as described herein (collectively, the "Services"). This Service Exhibit incorporates the terms of the Participating Addendum and NASPO ValuePoint Master Agreement #AR2474 pursuant to which CenturyLink provides services to Customer (collectively, the "Agreement"). Terms used but not defined herein shall have the meaning set forth in the Agreement. Customer expressly agrees that CenturyLink may use third party suppliers to provide the Service, provided that CenturyLink remains responsible to Customer hereunder.

2.1 SD-WAN Service Description. SD-WAN Service is a management overlay that uses software, deployed on a CenturyLink-provided CPE appliance at Customer's location ("SD-WAN Device"), enabling Customer to build a homogeneous private network through different types of network connections. The CPE associated with SD-WAN is provided on a rental basis. The SD-WAN Device establishes logical connections with other Customer edge CPE appliances across a physical WAN. CenturyLink supports SD-WAN Service using diverse network controllers (collectively "Controller") and a password-protected management portal ("Management Portal"). The Controller provides an endpoint for Customer's locations by authenticating the site and assisting to establish a secure channel between such Customer locations. The Management Portal provides centralized configuration and management. If changes in applicable law, regulation, rule, or order materially affect delivery of Service, the parties will negotiate appropriate changes to this Service Exhibit and any such changes will be in accordance with the NASPO ValuePoint Master Agreement #AR2474. If CenturyLink does so, Customer may terminate the affected Service on notice to CenturyLink delivered within 30 days of the cost increase taking effect.

SD-WAN Service supports private networking over the top of site to site networking and local internet breakout with firewall. SD-WAN Service includes a small CPE rental device that CenturyLink or its supplier configures and ships to the Customer site. In some cases, repackaged or substitute CPE may be used. The CPE device can be upgraded to a medium or large CPE rental device at additional charge. Customer may order Security Upgrade at an additional charge. Security Upgrade provides a set of firewall, web filtering, intrusion prevention, and localized DDOS features. Customer may order two SD-WAN Service packages at the same site to create a high-availability resilient network design. Subject to availability, On-Site Installation and On-Site Maintenance may be ordered at an additional charge for each location. The On-Site Installation option will provide a CenturyLink technician at the Customer premises to support the SD-WAN Device activation. The On-Site Maintenance option will provide a CenturyLink technician at the Customer premises to support the replacement of an SD-WAN Device in the event of a device failure.

2.2 CenturyLink Procured Third Party Provided Broadband and Cellular Back-Up Service Descriptions. In conjunction with SD-WAN, Customer may purchase CenturyLink procured broadband access service and/or cellular back-up access service ("Access Services", "Delta Port Internet Connection", or "Wireless Backup Service" as applicable) if available. Broadband access service is an unsecure local internet broadband connection. Cellular back-up access service leverages third party cellular network connectivity and is established utilizing CPE (internal modem or an external enterprise-class cellular-to-Ethernet bridge) in a back-up only or failover situation. If Customer purchases Access Services, those services are subject to the terms of this Service Schedule. If Customer purchases Delta Port Internet Connection for broadband service or Wireless Backup Service for cellular back-up access service, Customer must order and contract for those services separately.

3. Administration and Management. CenturyLink and the Customer will be able to perform ongoing management, monitoring, and reporting of the SD-WAN Service. Customer can submit up to 15 – 20 configuration changes per month per site. CenturyLink reserves the right to charge Customer \$275 for each configuration request over that amount. CenturyLink or its supplier will maintain global administrative access to SD-WAN Service at all times and will maintain the root password for all functions. Customer may have the option to co-manage SD-WAN Service configuration via the Management Portal. However, CenturyLink is not responsible for outages or security incidents that occur due to Customer changes or configuration. CenturyLink is not responsible for any services, systems, software, or equipment Customer uses with SD-WAN Service which are not provided by CenturyLink. CenturyLink will not debug problems on, or configure, any internal or external hosts or networks (examples include, but are not limited to the following: routers, DNS servers, mail servers, WWW servers, and FTP servers).

4. Charges. Customer shall pay the monthly recurring charges ("MRCs"), non-recurring charges ("NRCs"), and usage charges (related to Access Services, if any) set forth in the Order, CenturyLink-issued quote, SOW or the NASPO ValuePoint Master Agreement #AR2474. The SD-WAN Service MRC includes the rental CPE MRC, which may be separately identified in invoices. Customer agrees to pay and/or reimburse CenturyLink for its additional time for fees, costs and expenses resulting from the Customer's failure to comply with the terms of this Service Exhibit and/or Customer's request for changes in Service, unless such change is due to an act or omission of CenturyLink. Cancellation of Service will

be in accordance with the terms and conditions set forth in section 7 of the Participating Addendum.

5. Service Levels.

(a) **SD-WAN Service.** If CenturyLink or its supplier causes Downtime which is not isolated to an issue with the SD-WAN Device, CenturyLink will provide Customer with a credit of one day's charges, prorated from the MRC for the affected SD-WAN Service, for each cumulative hour of Downtime in a calendar month. Total monthly credits will not exceed fifty percent (50%) of the charges for the affected SD-WAN Service for that month. If Downtime is caused by an issue with the SD-WAN Device, Customer will not be entitled to any monetary remedy. Instead, CenturyLink will use commercially reasonable efforts to ship a replacement CPE device to Customer within the following time frames: (i) for locations within the continental U.S., next business day if Customer notifies CenturyLink by 2 pm mountain time the prior business day; and (ii) for locations outside the continental U.S., within five (5) business days from the time Customer notifies CenturyLink.

(b) **Access Services.** CenturyLink does not provide any service level credits for Service Unavailability for broadband access without cellular back-up service. The availability service level of broadband access is 99.99% when combined with cellular back-up service. In the event that CenturyLink fails to achieve the availability SLA, Customer shall be entitled to a credit as a percentage of its MRC for the affected broadband access service as follows:

<u>Cumulative Unavailability (in hrs:mins:secs)</u>	<u>% of broadband access MRC</u>
00:00:01 – 00:04:18 (99.99%)	No credit
00:04:19 – 00:43:00	10%
00:43:01 – 04:00:00	15%
04:00:01 – 12:00:00	30%
12:00:01 or greater	50%

(c) **Definitions.**

(i) "Downtime" is an interruption of SD-WAN Service (for reasons other than an Excused Outage or caused by an issue with Customer's underlying transport) which is confirmed by CenturyLink. Downtime is measured from the time Customer opens a trouble ticket with CenturyLink to the time the SD-WAN Service is restored.

(ii) "Excused Outage" is defined as any event that adversely impacts the Service that is caused by: (a) the acts or omissions of Customer, its employees, contractors or agents, or its end users; (b) the failure or malfunction of equipment, applications, or systems not owned or controlled by CenturyLink or its third party providers; (c) scheduled maintenance, alteration, or implementation; (d) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information; (e) CenturyLink's lack of access to the Customer premises where reasonably required to restore the Service; (f) Customer's failure to release the Service for testing or repair and continuing to use the Service on an impaired basis; (g) CenturyLink's termination of Service for Cause or Customer's use of Service in an unauthorized or unlawful manner; (h) improper or inaccurate specifications provided by Customer; or (i) Force Majeure events.

(iii) "Service Unavailability" is defined as the complete inability (for reasons other than an Excused Outage) of Customer to deliver IP packets from an individual Customer site over both (a) the broadband access and (b) cellular back-up service.

6. Ownership. For the SD-WAN Service and rental CPE, no license is conveyed nor is any right, title, or interest in any intellectual property or other proprietary right transferred to Customer. CenturyLink's intellectual property and proprietary rights include any skills, know-how, modifications or other enhancements developed or acquired in the course of configuring, providing, or managing the Service. Each party agrees that it will not, directly or indirectly, reverse engineer, disassemble, decompile, reproduce, or otherwise attempt to derive source code, trade secrets, or other intellectual property from any information, material, software, or technology of the other party, its licensors, or suppliers. The software and all copyrights, patent rights, and all intellectual property rights related thereto are the sole and exclusive property of CenturyLink or its licensors. Customer is hereby provided a non-exclusive, limited, non-transferrable, personal, revocable (at CenturyLink's sole discretion), non-sublicenseable, non-assignable right to access and/or use the software solely in association with the Service hereunder; provided, however, Customer shall not remove any disclaimers, copyright attribution statements or the like from the software. Export restrictions must be followed for encryption technology. End user licenses cannot be transferred. Customer has the right to use the software until the expiration or termination of the applicable Service Term.

CPE is the personal property of CenturyLink or its supplier. Notwithstanding that, the CPE, or any part thereof, may be affixed or attached to Customer's real property or any improvements thereon. Customer has no right or interest to the CPE other than as provided herein and will hold the CPE subject and subordinate to the rights of CenturyLink or its supplier. Customer will: (a) at its own expense, keep the CPE free and clear of any claims, liens, and encumbrances of any kind; and (b) make no alterations or affix any additions or attachments to the CPE, except as approved by CenturyLink in writing. Customer will not remove, alter, or destroy any labels on the CPE and will allow CenturyLink or its supplier to inspect the CPE at any time. Customer must use not less than a reasonable standard of care to store and protect CPE and shall be responsible for providing a safe and secure environment for the equipment in accordance with CenturyLink's specifications. Customer agrees to: (i) not alter, move, or disconnect CPE and (ii) notify CenturyLink as soon as Customer is aware of any circumstances that may adversely affect the CPE or its operation. As between CenturyLink and Customer, Customer will bear the entire risk of loss, theft, casualty, destruction, or damage to the CPE following delivery from any cause whatsoever (collectively, "Loss"), until returned to CenturyLink. Customer agrees to advise CenturyLink in writing within five business days of any such Loss. In no event will such Loss relieve Customer of the obligation to pay CenturyLink of any underlying service or for any rental fee. Customer shall be responsible for paying CenturyLink the fair market value of any such loss through coordination of insurance and any other necessary payments. CenturyLink shall be subject to the above conditions, provide customer with CPE. All CPE is subject to the terms and conditions set forth in the manufacturer's or publisher's warranty or end-user license.

7. Insurance. While the CPE is in the care, custody and control of Customer, Customer agrees to secure insurance coverage for casualty losses to the CPE and without limiting the liabilities or obligations of Customer, Customer will, at its own cost and expense, maintain during the term of this Agreement, such insurance as required hereunder. The insurance coverage will be from a company, or companies, with an A.M. Best's rating of A-VII and authorized to do business in each state or country where CPE is located. Customer may obtain all insurance limits through any combination of primary and excess or umbrella liability insurance. If local and/or regional laws stipulate higher values than those defined herein, then Customer must comply with the applicable higher value as required by law.

(a) Commercial General Liability with limits not less than \$1,000,000 (USD) or local currency equivalent per occurrence and aggregate.

(b) "All-Risk" property insurance on a replacement cost basis in an amount sufficient to cover the CPE, including CenturyLink or a third party provider designated by CenturyLink, as loss payee as their interests may appear.

CenturyLink, its affiliates, subsidiaries, and parent, as well as the officers, directors, employees, and agents of all such entities will be included as additional insureds on the Commercial General Liability policy. Policies will be primary and not contributory to insurance which may be maintained by CenturyLink, subject to any and all indemnification provisions of this Agreement. Prior to commencement of work under the Agreement, Customer will make available to CenturyLink evidence of the insurance required herein.

8. Customer Responsibilities.

(a) Customer is responsible for providing design specifications, including authentication methods and user role information. Customer is solely responsible for all equipment and other facilities used with the Service which are not provided by CenturyLink. Customer will designate one primary and up to two additional Customer security contacts, and provide email and telephone contact details for each such contact (the "Customer Security Contacts"). Customer will ensure that CenturyLink is informed of any changes to the designation of, and contact details for, the Customer Security Contacts. Customer will ensure that at least one Customer Security Contact is available to be contacted by CenturyLink at any given time (24x7x365). Unless Customer purchases On-Site Installation, Customer is responsible for installation of service and integration into Customer's network. Customer shall ensure CenturyLink and its representatives have access to Customer sites for installation and maintenance (if purchased) and removal of equipment and Services as scheduled, including obtaining all landlord approvals or letters of agency. Customer will timely perform all inside wiring, outside plant, work, cabling, openings, connections, and/or building alterations and provide standard AC power to enable delivery of the Service and CPE. Customer may not resell the Services and may use the Services only within Customer's sites. CenturyLink may provide Customer with guidelines for Customer's network minimum system requirements, compatibility, and other information necessary to use the Access Service. Customer must notify CenturyLink of any move or relocation of SD-WAN Service.

Software-Defined WAN Service Exhibit

(b) Use Restrictions. Customer will not use Services: (i) for fraudulent, abusive, or unlawful purposes or in any other unauthorized or attempted unauthorized manner, including unauthorized or attempted unauthorized access to, or alteration, or abuse of, information; (ii) in any manner that causes interference with CenturyLink's or another's use of the CenturyLink-provided network or infrastructure. Customer will cooperate promptly with CenturyLink to prevent third parties from gaining unauthorized access to the Services, including via Customer's facilities, if applicable; or (iii) in violation of CenturyLink's Acceptable Use Policy. Customer will ensure that all Customer data stored, transmitted, or processed via the Service complies with applicable law and reasonable information security practices, including those involving encryption.

If Customer orders Access Services, Customer shall not use the cellular access service other than in back-up capacity. Without limitation to CenturyLink's other remedies under the Agreement, CenturyLink reserves the right to charge, and Customer agrees to pay, for any misuse of cellular access services or its components, and/or for such usage in excess of CenturyLink's established data pool for Customer, separately at the rates then charged to CenturyLink by the third party cellular provider. Additionally, if CenturyLink provides Customer notice of such use of which CenturyLink becomes aware, CenturyLink may terminate the cellular access service within 10 days of such notice if such use does not cease. Any use of the cellular access service in a primary or non-back-up manner will give CenturyLink the right to immediately suspend such service and Customer shall be liable to CenturyLink for any overage fees that may be charged to CenturyLink for use of the cellular access service beyond a failover. CenturyLink is not responsible, however, for monitoring for such usage by Customer.

(c) CPE Return or Replacement. CenturyLink will provide Customer with instructions on return of CPE. Customer will deliver CPE to CenturyLink in the same condition it was on delivery to Customer, normal wear and tear excepted, and give CenturyLink written notice of such return. If CPE is not returned within 30 calendar days of termination, Customer will become owner of and bear all responsibility for the terminated or replaced CPE and CenturyLink may invoice Customer the then-current value of the applicable CPE model ("Replacement Cost"). Where CPE rented from CenturyLink is replaced due to loss or damage (for example, damage from accident, misuse, or abuse), Customer will pay: (i) the Replacement Cost for the damaged CPE, and (ii) a one-time charge to cover CenturyLink's cost to ship the new CPE. If On-Site Maintenance is not available and Customer requires on-site assistance from CenturyLink to install the replacement CPE, an additional dispatch charge will apply. CenturyLink will quote the charges in advance, obtain Customer's approval, and invoice the charges within 60 days. Customer is responsible for any claim for reimbursement from its insurance carrier. Replacement CPE may or may not be the same model, but will provide equivalent functionality in either case.

(d) To the extent required by law, Customer acknowledges and agrees that it is solely responsible for: (i) notifying its employees, vendors, contractors, or other users that network communications/transmissions on the Customer's network may be monitored, screened, and/or logged by Customer or CenturyLink on Customer's behalf and (ii) obtaining the consent of such employees, vendors, contractors, or other users to such monitoring and/or logging (which may include, where sufficient at law, implied consent).

9. Customer's Security Policies. Customer is responsible for Customer's own network security policy and security response procedures. Customer acknowledges that CenturyLink will implement security policies as reasonably directed by the Customer and, accordingly, that Customer maintains overall responsibility for maintaining the security of Customer's network and computer systems. Customer will ensure that its systems and networks will have up-to-date security controls and patches and that its systems and networks that connect with those included with SD-WAN Service, or that use common network features, have appropriate security controls. Customer agrees to notify CenturyLink in advance of any network changes or activities that could impact Service or reasonably interfere with the monitoring of the Service, such as planned outages, configuration changes, maintenance, or systems changes.

10. Special Terms for Access Services.

(a) CenturyLink will use reasonable efforts to procure the Access Service type per Customer site as

Software-Defined WAN Service Exhibit

identified in the Order. However, CenturyLink does not commit that a certain access service type or technology will be available at a Customer site.

(b) If the specific Access Service type set forth in an Order is not available, CenturyLink will so notify Customer and the Order for Access Services at that Customer site (and only that Customer site) will be cancelled (other Customer sites under such Order will not be impacted). Additionally, if the MRC or NRC must be increased and/or additional construction costs may apply, CenturyLink will request Customer confirmation of such costs, which confirmation may be provided via e-mail and will be binding on Customer. If Customer fails to provide such confirmation within 10 business days, the Order for Access Services at that specific Customer site shall be deemed cancelled.

(c) CenturyLink reserves the right to commence billing Customer, and Customer shall pay for the Access Service MRCs, if and to the extent that (i) such access has been installed; (ii) CenturyLink is incurring charges from the supplier; and (iii) the remaining completion of service installation cannot occur due to Customer delay, inaction, or failure to perform the Customer obligations hereunder.

(d) To the extent that suppliers of Access Service have the right to change the terms and conditions upon which such access is provided, including but not limited to the right to terminate the service and/or to modify rates or charges, notwithstanding anything to the contrary in the Agreement, CenturyLink expressly reserves the right to make corresponding changes with Customer for such services. CenturyLink will provide Customer with as much advanced notice as is reasonable, given the notification provided to CenturyLink from such supplier. In the event of a termination, CenturyLink and Customer will work together in good faith to agree upon and expediently procure another type of Access Service at such Customer site.

(e) Stated speeds for access may not be achieved. Actual speeds may vary and are not guaranteed. Effective throughput may be affected by several factors including but not limited to: physical layer line issues, overhead from encryption of network traffic, congestion within the public Internet, congestion within the underlying supplier access network, TCP window fragmentation, application performance, server loads, or performance and latency from inefficient routing paths within the Internet.

11. Modification or Termination of Access Services by CenturyLink. CenturyLink reserves the right to modify any features or functionalities of the Access Services upon 90 days prior notice to Customer. In the event that such modification materially affects the features or functionality of these services, then Customer, may cancel the affected cellular and/or broadband access service without termination liability, as long as Customer notifies CenturyLink in writing of such termination within 60 days of such notice from CenturyLink. Additionally, CenturyLink may upon written notice terminate the cellular and/or broadband access service at a site (either before or after Service delivery) if CenturyLink determines that the bandwidth and/or coverage is insufficient to support the service at such site. In such case, CenturyLink will notify Customer via e-mail of termination of service at such site and Customer shall not be billed for service at that location.

12. E-mail Notification. Customer acknowledges and agrees that CenturyLink may contact Customer via e-mail at the e-mail address provided to CenturyLink when Customer ordered the Service for any reason relating to the Service, including for purposes of providing Customer any notices required under the Agreement. Customer agrees to provide CenturyLink with any change to its e-mail address.

DDoS MITIGATION SERVICE EXHIBIT

1. General. CenturyLink QCC will provide DDoS Mitigation Service ("Service") under the terms of the Agreement and this Service Exhibit.

2. Service.

21 Service Description. Service consists of Proactive Shared DDoS Mitigation and Reactive Shared DDoS Mitigation. "DDoS" means a distributed denial-of-service attack in which many systems attack a single target, thereby causing denial of service for users of the targeted system. This typically results in the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system. Service is only available in conjunction with Customer's separately purchased CenturyLink IQ® Networking Internet Port or CenturyLink-provided Network-Based Security.

(a) Proactive Shared DDoS Mitigation. Proactive Shared DDoS Mitigation includes: (i) monitoring of Customer's network traffic on a 24x7 basis; and (ii) CenturyLink-supplied equipment and capacity for Mitigation that is shared among multiple customers. Customer also has direct access to CenturyLink's support team on a 24x7 basis. CenturyLink will analyze Customer's network traffic to establish baselines for normal traffic patterns. Once baselines are established, CenturyLink will determine if an Event is taking place. If Events are determined to be Incidents, CenturyLink will forward reports to Customer. Customer may request CenturyLink to notify Customer through either a phone call or e-mail for Proactive Shared DDoS Mitigation alerts. Customer will work with CenturyLink to validate an attack and provide either verbal permission for each Incident or pre-authorized permission for CenturyLink to initiate Mitigation.

(b) Reactive Shared DDoS Mitigation. Reactive Shared DDoS Mitigation includes CenturyLink-supplied equipment and capacity for Mitigation that is shared among multiple customers. Customer also has direct access to CenturyLink's support team on a 24x7 basis. CenturyLink does not notify Customer about Customer's network traffic anomalies. Customer is solely responsible for notifying CenturyLink of an attack and working with CenturyLink to validate the attack. Customer must provide CenturyLink verbal permission to initiate Mitigation with Reactive Shared DDoS Mitigation.

22 Initiation of Mitigation. For Customer-initiated Mitigation services, Customer must approve Mitigation by: (i) providing verbal permission via phone call for each Incident, or (ii) pre-authorizing CenturyLink to initiate Mitigation. Pre-authorization is only available with Proactive Shared DDoS Mitigation. If Customer selects the pre-authorized permission option, Customer must provide CenturyLink written notice via a change ticket in Control Center of its pre-authorized permission to begin Mitigation. Customer may later withdraw its pre-authorized permission via a change ticket. Change tickets require 24 hours advance notice. Customer will pre-authorize which Mitigation countermeasures CenturyLink may deploy, subject to CenturyLink's approval. Customer understands that additional countermeasures beyond the pre-authorized countermeasures may be required to Mitigate the Incident, which may require CenturyLink to contact Customer's Site Contact. CenturyLink will discontinue Mitigation at the Customer's verbal request or until CenturyLink reasonably determines that the DDoS attack has subsided. When CenturyLink determines that the DDoS attack has subsided, CenturyLink will attempt to notify Customer. If CenturyLink is able to contact Customer, Customer will have the option at that time to discontinue Mitigation or continue Mitigation for up to an additional four hours. At the end of the four hours, CenturyLink will discontinue Mitigation as long as another attack has not occurred. If CenturyLink is unable to contact Customer, CenturyLink will continue Mitigation for another four hours, after which point CenturyLink will discontinue Mitigation as long as another attack has not occurred.

23 Customer Responsibilities.

(a) Customer Information. Customer must provide CenturyLink with: (i) accurate and current contact information for Customer's designated points of contact; (ii) advance notice of any network changes; and (iii) a list of Customer IP addresses that Customer wishes to have subject to the Service. CenturyLink may not be able to provide the Service if Customer's security contact information is out of date or inaccurate or if Customer performs network changes without prior notification to CenturyLink.

(b) Notification Responsibilities. Customer must provide CenturyLink with of all the following notices: (i) 24 hours advance notice of any potential promotional events or other activities that may increase Customer's network or Web site traffic; (ii) immediate notice of any sudden events that may cause significant traffic pattern changes in Customer's network; (iii) 24 hours advance notice of any Customer requests to change the traffic baseline; (iv) immediate notice of any additions or deletions to the list of Customer IP addresses subject to the Service; and (v) immediate notice if Customer believes it is under a DDoS attack.

(c) Installation/Setup. Customer will cooperate with CenturyLink by: (i) providing CenturyLink with all information concerning the Service reasonably requested by CenturyLink; and (ii) providing a primary and secondary site contact with relevant experience and expertise in Customer's network operations ("Site Contact"). Customer will provide data parameters that will allow CenturyLink to determine the proper threshold levels in an attempt to diagnose a DDoS attack. CenturyLink may periodically require Customer to allow traffic monitoring to determine proper threshold levels.

24 Consent to Access and Use Customer Information. Customer authorizes CenturyLink or its authorized vendor to access and use Customer's information associated with Customer's IP-network traffic (including Content) from domestic locations and, if applicable, from international ones. Customer also understands and agrees that CenturyLink will provide its findings regarding a DDoS attack to law enforcement as required by law. "Content" means information about Customer's IP-network traffic, including header and content information associated with packets. Content could include, for example, images, documents, email messages, or Web content.

DDoS MITIGATION SERVICE EXHIBIT

3. Charges. Customer will pay all applicable MRCs and NRCs set forth in the NASPO ValuePoint Master Agreement #AR2474. Charges will commence within five days of the date CenturyLink notifies Customer that Service is provisioned and ready for use ("Start of Service Date").

4. Term; Cancellation. This Service Exhibit remains in effect until terminated. Either party may terminate this Service Exhibit with at least 30 days prior written notice to the other party. Cancellation of Service will be in accordance with the terms and conditions set forth in Section 7 of the Participating Addendum.

5. E-mail Notification. Customer acknowledges and agrees that CenturyLink may contact Customer via e-mail at the e-mail address provided to CenturyLink when Customer ordered the Service for any reason relating to the Service, including for purposes of providing Customer any notices required under the Agreement. Customer agrees to provide CenturyLink with any change to its e-mail address.

6. AUP. All use of the Services must comply with the AUP.

7. SLA. Service is subject to the DDoS Mitigation service level agreement ("SLA"), attached to the Participating Addendum as Attachment E. For Customer's claims related to Service deficiencies, interruptions or failures, Customer's exclusive remedies are limited to those remedies set forth in the SLA.

8. Definitions. Capitalized terms not defined in this Service Exhibit are defined in the Agreement.

"Event" means a security occurrence detected and reported by the CenturyLink DDoS Mitigation Service. An Event does not necessarily constitute an actual security incident, and must be investigated further to determine its validity.

"Incident" means any single Event or collection of Events that have been determined by a CenturyLink analyst reviewing the data to potentially be of security consequence. Incidents may include Events that are currently being investigated and actual attacks that may be in progress.

"Mitigation" means the mitigation of DDoS attacks by using CenturyLink-supplied mitigation equipment located in CenturyLink's network.

CENTURYLINK DOMESTIC OPTICAL WAVELENGTH SERVICE EXHIBIT

1. General; Definitions. Capitalized terms not defined in this Service Exhibit are defined in the Agreement. CenturyLink QCC will provide Domestic Optical Wavelength Private Line Service ("Service" or Domestic Optical Wavelength Private Line Service") under the terms of the Agreement, RSS, and this Service Exhibit.

"Demarcation Point" means the termination point of the POP at the applicable service address.

"Net Rate" is in lieu of all other rates, discounts, and promotions.

"POP" means a CenturyLink designated point of presence at a location where direct interconnection between the CenturyLink network and the network of another carrier is possible.

"SDH" means synchronous digital hierarchy.

"SLA" means the service level agreement specific to the Service, which is attached to the Participating Addendum as Attachment E.

"SONET" means synchronous optical network.

"Start of Service Date" for each circuit is the date Customer accepts the circuit, following notification by CenturyLink that the circuit is ready. The ready notification will be via phone call or e-mail. Customer has five days from CenturyLink's ready notification in which to inform CenturyLink if the circuit fails to operate error-free. Within the five-day timeframe, if Customer neither informs CenturyLink about errors nor accepts the circuit, the circuit will be considered to have been accepted and the Start of Service Date to have commenced on the fifth day following CenturyLink's ready notification, regardless of whether Customer placed traffic over the circuit. If Customer informs CenturyLink of circuit errors within the five-day timeframe, CenturyLink will promptly take necessary, reasonable action to correct the errors, and upon correction, notify Customer that the circuit is ready.

2. Service.

2.1 Description.

(a) Service is a Dense Wave Division Multiplexing ("DWDM" or "wavelength") solution with metro and long haul transport applications. The speed selected is shown on the SOW. Protection is not currently available at all speeds. Service supports SONET and SDH protocols.

(b) The Service will extend to and include the equipment maintained by CenturyLink at the Demarcation Point but will not include CPE, extended wiring, inside wiring, or other equipment not maintained by CenturyLink at a service address. The SLA provides Customer's sole remedy for service interruptions or service deficiencies of any kind whatsoever for Service.

2.2 RSS. Customer understands that Service is an interstate telecommunications service, as defined by Federal Communications Commission regulations and represents that during the Service Term, more than 10% of its traffic will be interstate traffic.

2.3 Obligations Of Customer. Customer will perform those duties outlined in this Exhibit, in the Agreement, and in the Order Forms. Unless otherwise agreed to by CenturyLink in writing, Customer will have sole responsibility for installation, testing, and operation of any services and equipment other than the Service specifically provided by CenturyLink under this Exhibit. Customer is required to have the CenturyLink Local Access Service Exhibit in conjunction with this Service Exhibit.

2.4 Provisioning Of Domestic Optical Wavelength Private Line Services.

(a) Upon acceptance of an Order Form, CenturyLink will notify Customer of its target date for the delivery of the Service ("Estimated Availability Date"). CenturyLink will use reasonable efforts to install the Service on or before the Estimated Availability Date, but the inability of CenturyLink to deliver Service by such date will not be a default under this Exhibit. If CenturyLink fails to make the Service available within 60 calendar days of the Estimated Availability Date with respect to such Service, Customer's remedy will be to cancel the Order Form which pertains to such Service by giving CenturyLink 10 calendar days written notice prior to the Service's delivery to Customer by CenturyLink; provided however, for metro and long haul applications that Customer will reimburse CenturyLink for any third party charges incurred by CenturyLink as a result of its efforts to install the Service.

(b) "POP Pairs" means: (i) the originating and terminating POPs for long haul; and (ii) the POP location where the two loops are cross-connected for metro.

3. Term; Cancellation. The term of this Service Exhibit will begin on the Effective Date of the Agreement (or, if applicable, an amendment to the Agreement if Customer adds this Service Exhibit after the Effective Date of the Agreement) and will continue until the expiration or cancellation of the last to expire (or cancel) Service ordered under this Service Exhibit. Each Service ordered during the term will commence on the Start of Service Date and continue for the term specified in the SOW ("Term"). Cancellation will be in accordance with the terms and conditions set forth in Section 7 of the Participating Addendum.

4. Charges. Customer will pay the Net Rates set forth in the NASPO ValuePoint Master Agreement #A2474. Recurring charges will be invoiced by CenturyLink on a monthly basis in advance and nonrecurring charges will be invoiced in arrears. If the Start of Service Date for any Service falls on any day other than the first day of the month, the first invoice to Customer will consist of: (a) the pro-rata

CENTURYLINK DOMESTIC OPTICAL WAVELENGTH SERVICE EXHIBIT

portion of the applicable monthly recurring charge covering the period from the Start of Service Date (as defined in this Service Exhibit) to the first day of the subsequent month; and (b) the monthly recurring charge for the following month. The Net Rates will be used to calculate Contributory Charges. For metro only, the loop charge is bundled with the Domestic Optical Wavelength Private Line Service charge. For long haul, the loop charge will appear as a separate line item.

Level 3 Internet Service Exhibit

1 Applicability. This Service Exhibit is applicable where Customer orders Level 3® Internet Services (which may also be called Dedicated Internet Access, Internet Services, High Speed IP, or IP Transit Services on ordering, invoicing or other documentation). The Service is also subject to the Participating Addendum and NASPO ValuePoint Master Agreement #AR2474 pursuant to which CenturyLink provides services to Customer (collectively, the "Agreement"). Subject to section 5 of the Participating Addendum, Level 3 may subcontract the provision of the Service in whole or part, provided that Level 3 remains responsible for the Service to Customer as set forth herein. Capitalized terms used but not defined herein have the definitions given to them in the Agreement.

2 Service Description. Level 3® Internet Services are high speed symmetrical Internet services providing access to the Level 3 IP network and the global Internet ("Service"). The Service is generally available via Ethernet connections from 10/100 Mbps ports to 100Gbps ports, as well as T1/E1, DS3/E3, and SONET connections from OC3/STM1 to OC48/STM16. Additional features and functionality may include:

- a. **IP Addresses.** IP Address space with proper justification.
- b. **Primary DNS / Secondary DNS.** Primary or Secondary DNS as requested.
- c. **Static routing / BGP peering.** Static routing or BGP peering options available.
- d. **On-line bandwidth utilization reports.** On-line bandwidth utilization reports available through the customer portal.
- e. **Basic security service.** Subject to Customer having Level 3-approved routers, included as part of the Services is a one-time per 12-month period ability to request Level 3 to temporarily (i.e. for up to 24 hours): (i) apply a temporary access control list (ACL) with up to 10 rules on such routers; (ii) set up firewall filters specifying IPs, subnets, ports and protocols, and (iii) configure null routes. Requests that exceed this duration or frequency will be charged at \$1000 per hour. Customer is encouraged to order additional Services as outlined below.

The following services may be available at an additional charge to be set forth in an Order and pursuant to the separate Service Exhibits for such services:

- a. **Distributed Denial of Service (DDoS) Mitigation Service.** Level 3's DDoS Mitigation Service provides layers of defense through network routing, rate limiting and filtering that can be paired with advanced network-based detection and mitigation scrubbing center solutions.

3 Charges. Customer shall be billed non-recurring charges ("NRC") and monthly recurring charges ("MRC") for Service as set forth in Order(s) or Statement of Work. NRC includes applicable installation charges for local-access circuit, port connection and bandwidth. MRC includes local-access charges, port connection charges, and bandwidth charges. Other charges, including but not limited to usage-based charges, may apply as stated in Order(s). The Services are available with fixed-rate or burstable billing types.

Fixed-rate. Service with fixed-rate billing provide a set amount of bandwidth at a fixed-rate MRC. No usage element applies. Customer will not be permitted to exceed the contracted bandwidth level, provided that if Customer also orders Dynamic Capacity (where available) bandwidth and the associated charges may be adjusted as set forth in the separate terms for Dynamic Capacity.

Burstable. For Service provided with burstable bandwidth, the MRC is based on Committed Information Rate ("CIR") (which is also called a Committed Data Rate ("CDR")). The CIR/CDR is the minimum Internet bandwidth that will be billed to Customer each month regardless of lower actual usage. Usage charges for any usage in excess of the CIR/CDR (burstable usage) will apply on a per Mbps basis at the rate stated in the Order. Burstable usage is billed on a 95th percentile basis. Usage levels are sampled every five minutes, for the previous 5-minute period, on both inbound and outbound traffic. At the end of the bill cycle, the highest 5% of the traffic samples for each inbound and outbound, will be discarded, and the higher of the resulting inbound and outbound values will be used to calculate any applicable usage. If available and identified in the applicable Order, a Peak Information Rate (PIR) or Peak Data Rate (PDR) may apply, which is the maximum available bandwidth.

Burstable Services may also be provided on an aggregated basis. For aggregate burstable Service the bandwidth MRC is based on the aggregate Committed Information Rate ("ACIR") (which is also called an aggregate Committed Data Rate ("ACDR")). The ACIR/ACDR is the minimum bandwidth that will be charged to Customer each month, regardless of lower actual usage. Usage charges for any usage in excess of the ACIR/ACDR (burstable usage) will apply on a per Mbps basis at the rate stated in the Order. Burstable usage is calculated on a 95th percentile basis across all included ports. If available and identified in the applicable Order, an aggregated Peak Information Rate (APIR) or aggregated Peak Data Rate (APDR) may apply, which is the maximum available bandwidth across all included ports.

4 Customer Responsibilities. Customer is solely responsible for all equipment and other facilities used in connection with the Service which are not provided by Level 3. All IP addresses, if any, assigned to Customer by Level 3 shall revert to Level 3 upon termination of Service, and Customer shall cease using such addresses as of the effective date of termination.

5 On-Net and Off-net Access. Access services provided entirely on the Level 3 owned and operated network ("Network") are "On-Net Access Services". Additionally, Level 3 may use third parties to reach Customer's site from the Level 3 Network ("Off-Net Access Services"), but not before receiving written approval by the State (Central Procurement Office on behalf of agency) as shown in a SOW.

Level 3 Internet Service Exhibit

6. **Service Levels and Service Credits.** The following service level agreements (SLAs) apply as set forth below.
- Availability Service Level. Level 3's availability SLA in the United States and Canada is 99.99%. Outside the United States and Canada, the availability SLA is 99.98% for On-Net Access Services and 99.9% for Off-Net Access Service.
 - Network Packet Delivery Service Level. The packet delivery SLA on the Level 3 Network is 99.95%.
 - Network Latency Service Levels. The latency SLAs on the Level 3 Network are set forth below and are average round-trip.

Table A: Network Latency

Route	Network Latency Metrics Round-Trip
Intra-North America	< 50 ms*
Intra-Europe	< 35 ms
Intra-Asia	< 110 ms
Intra-Latin America	< 120 ms
North America to Europe	< 80 ms**
North America to Asia	< 185 ms**
North America to Latin America	< 140ms**
Europe to Asia	< 345 ms**
Europe to Latin America	< 210 ms**
Asia to Latin America	< 315 ms**

* Additionally, add 90ms from/to the Mexico IP Hub and add 30ms from/to Hawaii to the west coast of the continental United States.

** Additionally, add the applicable "intra-region" latency parameter for the region in which the applicable Customer Site is located.

- Credits for SLAs above:** All SLA credits will be calculated after deducting any discounts and other special pricing arrangements. Credit percentages are applied to the MRC of the CIR/CDR rate, port charge, and local access circuits for applicable sites only. In no event will SLA credits in any calendar month exceed 100% of the total MRCs for Services hereunder for the affected site(s).
- Availability Service Credit:** Service is "Unavailable" (except in the case of an Excused Outage) if the Customer port at a Customer site is unable to pass traffic. Service Unavailability is calculated from the timestamp Level 3 opens a trouble ticket following the report of a problem by the Customer until the time the ticket is closed. If credits are due under this SLA, no other SLAs apply to the same event. If Service is Unavailable for reasons other than an Excused Outage, Customer will be entitled to a service credit off of the MRC for the affected Service based on the cumulative Unavailability of the Service in a given calendar month as set forth in the tables below.

Table B: Availability Service Credit - United States and Canada

Cumulative Unavailability (hrs:mins:secs)	Service Level Credit
00:00:01 – 00:05:00	No Credit
00:05:01 – 00:43:00	5%
00:43:01 – 04:00:00	10%
04:00:01 – 8:00:00	20%
08:00:01 – 12:00:00	30%
12:00:01 – 16:00:00	40%
16:00:01 – 24:00:00	50%
24:00:01 or greater	100%

Level 3 Internet Service Exhibit

Table C: Availability Service Credit - On-Net Access Services outside the U.S. and Canada

Cumulative Unavailability (hrs:mins:secs)	Service Level Credit
00:00:01 – 00:10:00	No Credit
00:10:01 – 00:43:00	5%
00:43:01 – 04:00:00	10%
04:00:01 – 8:00:00	20%
08:00:01 – 12:00:00	30%
12:00:01 – 16:00:00	40%
16:00:01 – 24:00:00	50%
24:00:01 or greater	100%

Table D: Availability Service Credit- Off-Net Access Services outside the U.S. and Canada

Cumulative Unavailability (hrs:mins:secs)	Service Level Credit
00:00:01 – 00:43:00	No Credit
00:43:01 – 04:00:00	10%
04:00:01 – 8:00:00	20%
08:00:01 – 12:00:00	30%
12:00:01 – 16:00:00	40%
16:00:01 – 24:00:00	50%
24:00:01 or greater	100%

- ii. **Network Packet Delivery Service Credits.** Packet Delivery SLAs are based on monthly average performance between Level 3 designated points of presence (“POPs”). Customer will be entitled to a service credit off of the MRC for the affected Service as set forth below for the Service parameter(s) not met for reasons other than an Excused Outage. Customer will not be entitled to credits under the packet delivery SLA for the affected Service where such failure is related to Unavailability under the Availability SLA.

Table E: Packet Delivery Service Credit

Packet Delivery Metrics	Percentage Credit
99.95% or greater	No Credit
99.94% - 99.0%	10%
98.99% - 96.0%	30%
95.99% or less	50%

- iii. **Network Latency Service Credits.** Network latency SLAs are based on monthly average performance between Level 3 designated points of presence (“POPs”). Customer will be entitled to a service credit off of the MRC for the affected Service as set forth below for the Service parameter(s) not met for reasons other than an Excused Outage. Customer will not be entitled to credits under the network latency SLA for the affected Service where such failure is related to Unavailability under the Availability SLA.

Level 3 Internet Service Exhibit

Table F: Network Latency Service Credit

Delay Exceeding Network Latency Metrics	Percentage Credit
1- 10 ms	10%
11- 25 ms	30%
26 ms or greater	50%

- e. **Chronic Outage.** In addition to any other termination rights contained in the Agreement, Customer may elect to terminate an affected Service, or if applicable an affected Converged Voice-Internet Service, hereunder prior to the end of the Service Term without termination liability if, for reasons other than an Excused Outage, such Service becomes Unavailable (as defined in Section 6(d)(i) above) twice during a 30-day period, and becomes Unavailable a third time within 30 days following the second event. Customer may terminate such Service that is Unavailable as described above, and must exercise its right to terminate the affected Service under this Section, in writing, within 30 days after the event giving rise to the termination right. For clarification, termination of a Converged Voice-Internet Service will result in termination of all applicable Services bundled together as the Converged Voice-Internet Service under the Order.
- f. **Installation Service Level.** Level 3 will exercise commercially reasonable efforts to install any Service on or before the Customer Commit Date for the particular Service. This installation SLA shall not apply to Orders that contain incorrect information supplied by Customer or Orders that are altered at Customer's request after submission and acceptance by Level 3. In the event Level 3 does not meet this installation SLA for reasons other than an Excused Outage, Customer will be entitled to a service credit for each day of delay equal to the charges for 1 day of the pro rata share of the MRC associated with the affected Service up to a monthly maximum credit of 10 days. For Services billed on an Aggregate CIR/CDR basis, the charges for 1 day of the pro rata share of the MRC will be calculated based on the average MRC per port for the aggregate.

7. Resale Restriction. Notwithstanding anything to the contrary in the Agreement, Customer is prohibited from reselling any Internet Service or any ports provided hereunder as a stand-alone service to a third party without the express written consent of Level 3, provided, however that Customer may bundle any Internet Service or any ports provided pursuant to this Service Schedule with any other Level 3 services (to the extent resale of those service is allowed) or the services of Customer and resell such bundled service to Customer's subscribers and its customers. The Parties agree that the preceding is not applicable to Converged Voice-Internet Service, and Customer is prohibited from reselling any Converged Voice-Internet Service unless the parties enter into an amendment signed by authorized representatives of both parties.

8. Level 3 Arranged Third Party Procured Internet Services. In accordance with section 5 of the Participating Addendum, for certain Service locations (including but not limited to where Level 3 may lack relevant licenses to provide such service), Level 3 may agree to arrange Internet services using third party providers ("Third Party Internet Service"). Service options vary on a country by country basis and may include access to the Internet via overbooked and/or non-overbooked connections, DSL technology, private leased circuits (fixed or wireless) and/or Satellite. Specific service details (access type, e.g. downstream/upstream speed, customer premises equipment requirements and number of IP addresses) also differ on a country by country basis. Customer understands and acknowledges that Third Party Internet Service will, if requested by Customer, be provided by third party subcontractor(s) to Level 3 and accordingly, is provided on a best effort and as-is basis. Notwithstanding the foregoing, Customer may report faults and/or outages in Third Party Internet Access to Level 3 on a 24x7 basis and in such circumstances Level 3 will contact the applicable third party service provider with a view to restoring service as quickly as possible. Customer will reasonably cooperate with the requests of such providers of Third Party Internet Service to enable installation, maintenance, repair and disconnection of Services.

Level 3 WAVELENGTH SERVICE SCHEDULE

1. **Applicability.** This Service Schedule is applicable only where Customer orders Level 3® Intercity Wavelength Service, Level 3® Metro Wavelength Service, or Level 3® International Wavelength Service (collectively "Level 3 Wavelength Service") on a lease basis. With respect to Services provided in Latin America, Customer agrees that it (or its local Affiliate) will enter into a separate local country addendum/agreement (as approved by local authorities) ("LCA") with the respective Level 3 Affiliate which provides the local Service(s), containing terms necessary to comply with local laws/regulations, and such Level 3 Affiliate will invoice the Customer (or its local Affiliate) party to the LCA for the respective local Service(s).
2. **Definitions.** Any capitalized terms used herein and not otherwise defined shall have the meanings set forth in the Agreement.
 - (A) "Customer Commit Date" means the date by which Level 3 will install Service. The Customer Commit Date is established following Level 3's acceptance of a Customer Order.
 - (B) "E2E" means end to end, and includes the On-Net and Off-Net components of Services in the United States and European Union, taken together.
 - (C) "On-Net" means Service provided on the network owned (or operated and controlled) by Level 3 between two locations that are served directly by Level 3 owned (or operated and controlled) fiber and Level 3 owned equipment. Services that are not On-Net are Off-Net.
 - (D) "Protected" shall mean any Service that includes a Level 3 managed protection scheme that allows traffic to be re-routed in the event of a fiber cut or equipment failure.
 - (E) "Termination Node" shall mean the locations within Level 3's facilities or within Customer Premises in each of the cities in which termination is available. Each Level 3 Wavelength Service shall contain two (2) Termination Nodes, the exact location of which will be set forth in the Customer Order.
 - (F) "Unavailable" or "Unavailability" means the duration of a break in transmission measured from the first of ten (10) consecutive severely erred seconds ("SESS") on the affected Level 3 Wavelength Service until the first of ten (10) consecutive non-SESSs.
 - (G) "Unprotected" shall mean any Service that does not include a Level 3 managed protection scheme that would allow traffic to be re-routed in the event of a fiber cut or equipment failure.
3. **Service Description.** Level 3 Wavelength Service is a dedicated, transparent, optical wave signal for transport of high bandwidth between two Termination Nodes offered on a Protected or Unprotected basis. Customer interface consists of 2.5Gb, 10Gb, 40Gb, 1GbE, 10GbE, 40GbE and 100GbE, OTU1, OTU2, OTU2e, OTU3, OTU4 and 1Gb, 2Gb, 4Gb, 8Gb, and 10Gb Fibre Channel.
4. **Interconnection.**
 - (A) **Demarc.** To use the Level 3 Wavelength Service, Customer must provide to Level 3, at each Termination Node, a SONET or SDH-framed 2.5Gb, 10Gb or 40Gb signal, as defined by Telcordia GR-253-CORE, a 1Gb, 10Gb, 40Gb or 100Gb Ethernet signal, as defined by IEEE 802.3ae, a OTU1, OTU2, OTU2e, OTU3, OTU4 signal, as defined by ITU G.709, or a 1Gb, 2Gb, 4Gb, 8Gb, or 10Gb Fibre Channel signal, as defined by T11 Technical Committee within INCITS (the International Committee for Information Technology Standards (collectively, "Traffic"), which Traffic will thereafter be delivered by Level 3, in like format, to the opposite and corresponding Termination Node.

The demarcation point for the Level 3 Wavelength Service shall be the Level 3 OSX or fiber termination panel at the Termination Node. Customer shall be solely responsible for providing all interconnection equipment used both to deliver Traffic to, or to accept Traffic from, Level 3 in the formats described above and for any and all protection schemes Customer chooses to implement respecting the Traffic. For a Termination Node at a location other than a Level 3 Gateway, Customer shall provide Level 3 with space and power (at no charge to Level 3), as reasonably requested by Level 3, for placement and operation of an OSX, fiber termination panel or other equipment within the Customer Premises.
 - (B) **Construction of Facilities.** With respect to construction of facilities to the Customer Premises and installation, maintenance and repair of facilities within the Customer Premises, Customer shall provide Level 3 with access to and the use of Customer's entrance facilities and inside wiring, and/or shall procure rights for Level 3 allowing the placement of facilities necessary for installation of facilities to deliver the Level 3 Wavelength Service to the Customer Premises. All costs associated with procuring and maintaining rights needed to obtain entry to the building (and the real property on which the building is located) within which the Customer Premises are located, and costs to procure and maintain rights within such building to the Customer Premises, shall be borne by Customer.
 - (C) **Third Party Providers.** Subject to Section 5 Assignment and Subcontracting of the Participating Addendum, where Level 3 Wavelength Service is being terminated Off-Net at the Customer Premises through a third party provider to be provisioned by Level 3 on behalf of Customer, the charges set forth in the Customer Order for such Level 3 Wavelength Service assumes that such Level 3 Wavelength Service will be terminated at a pre-established demarcation point or minimum point of entry (MPOE)

Level 3 WAVELENGTH SERVICE SCHEDULE

in the building within which the Customer Premises is located, as determined by the local access provider. Where the local access provider determines that it is necessary to extend the demarcation point or MPOE through the provision of additional infrastructure, cabling, electronics or other materials necessary to reach the Customer Premises, (i) Level 3 may charge Customer additional non-recurring charges and/or monthly recurring charges not otherwise set forth in the Customer Order for such Level 3 Wavelength Service, (ii) installation of Service may be delayed and (iii) Section 5(A) of this Service Schedule shall not apply. Level 3 will notify Customer of any additional non-recurring charges and/or monthly recurring charges after Level 3 is notified by the local access provider of the amount of such charges.

In addition, where Level 3 Wavelength Service is being terminated Off-Net at the Customer Premises through an Off-Net Local Loop to be provisioned by Level 3 on behalf of the Customer, the charges and the Service Term set forth in the Customer Order for such Level 3 Wavelength Service assumes that such Level 3 Wavelength Service can be provisioned by Level 3 through the local access provider selected by Level 3 (and/or Customer) for the stated Service Term. In the event Level 3 is unable to provision such Level 3 Wavelength Service through the selected local access provider or the selected local access provider requires a longer Service Term than that set forth in the Customer Order, Level 3 reserves the right, regardless of whether Level 3 has accepted the Customer Order, to suspend provisioning of such Level 3 Wavelength Service and notify Customer in writing of any additional non-recurring charges, monthly recurring charges and/or Service Term that may apply. Upon receipt of such notice, Customer will have five (5) business days to accept or reject such changes. If Customer does not respond to Level 3 within the five (5) business day period, such changes will be deemed rejected by Customer. In the event Customer rejects the changes (whether affirmatively or through the expiration of the five (5) business day period), the affected Level 3 Wavelength Service will be cancelled without cancellation or termination liability of either party. Level 3 does not guarantee that any Level 3 Wavelength Service will be provided by a specified local access provider.

5. Service Levels.

- (A) Installation Service Level. Level 3 will exercise commercially reasonable efforts to install any On-Net Level 3 Wavelength Service on or before the Customer Commit Date specified for the particular Level 3 Wavelength Service. This Installation Service Level shall not apply to Customer Orders that contain incorrect information supplied by Customer, or Customer Orders that are altered at Customer's request after submission and acceptance by Level 3. In the event Level 3 does not meet this Installation Service Level for a particular Level 3 Wavelength Service for reasons other than an Excused Outage, Customer will be entitled to a service credit off of one month's monthly recurring charges ("MRC") (after application of discounts and other special pricing arrangements, if any) for the affected Level 3 Wavelength Service as set forth in the following table:

Installation Delay Beyond Customer Commit Date	Service Level Credit (MRC)
1 – 5 business days	5%
6 – 20 business days	10%
21 business days or greater	15%

- (B) Availability Service Level. In the event that a particular Level 3 Wavelength Service becomes Unavailable for reasons other than an Excused Outage, Customer will be entitled to a service credit off of the MRC (after application of discounts and other special pricing arrangements, if any) for the affected Level 3 Wavelength Service based on the cumulative Unavailability for the affected Level 3 Wavelength Service in a given calendar month as set forth in the following table:

For On-Net Unprotected Service

Cumulative Unavailability (in hrs:mins:secs)	Service Level Credit
00:00:01 – 4:00:00	No Credit
4:00:01 – 6:00:00	10% of the MRC
6:00:01 – 10:00:00	25% of the MRC
10:00:01 or greater	50% of the MRC

For On-Net Protected Service

Cumulative Unavailability (in hrs:mins:secs)	Service Level Credit
--	----------------------

Level 3 WAVELENGTH SERVICE SCHEDULE

00:00:01 - 00:05:00	No Credit
00:05:01 – 01:00:00	10% of the MRC
01:00:01 – 6:00:00	25% of the MRC
6:00:01 or greater	50% of the MRC

For E2E Protected Service

Cumulative Unavailability (in hrs:mins:secs)	Service Level Credit
00:00:01 to 3:30:00	No Credit
03:30:01 – 6:00:00	10% of the MRC
6:00:01 – 12:00:00	25% of the MRC
12:00:01 or greater	50% of the MRC

For E2E Unprotected Service

Cumulative Unavailability (in hrs:mins:secs)	Service Level Credit
00:00:01 to 8:00:00	No Credit
8:00:01 – 10:00:00	10% of the MRC
10:00:01 – 16:00:00	25% of the MRC
16:00:01 or greater	50% of the MRC

- (C) Service Level Limitations. Except with respect to E2E Service, for any Off-Net Service, Level 3 will pass-through to Customer any service levels and associated credits (or other express remedies) provided to Level 3 by the applicable third party carrier. Service Levels do not apply to Service interruptions attributable to long-haul international access circuits between a Level 3 point of presence in one country and a Customer premises in a different country.
- (D) The credits and any other remedies specified in Sections 5(A), 5(B) and Section 6 below set forth the remedies of Customer for any interruptions or delays of any Level 3 Wavelength Service or other Service-related issues.

6. **Chronic Outage.** In addition to any other termination rights contained in the Agreement, Customer may elect to terminate any affected Wavelength Service prior to the end of the Service Term without termination liability if, for reasons other than an Excused Outage, the Service is Unavailable for more than 12 consecutive hours in each of 3 consecutive calendar months, or for more than 36 hours in the aggregate in any calendar month, or more than 5 outages related to the same issue in any calendar month. The termination right must be exercised within 30 days of the event giving rise to it.

CENTURYLINK IQ® DELTA PORT™ WITH IP CONNECTION BUNDLE OFFER ATTACHMENT

This offer attachment ("Attachment") is subject in all respects to the domestic CenturyLink IQ® Networking Service Exhibit, the Local Access Service Exhibit, the Rental CPE Service Exhibit, the Network-Based Security ("NBS") Service Exhibit if applicable ("Service Exhibits"), the Participating Addendum, and the NASPO ValuePoint Master Agreement #AR2474. All capitalized terms that are used but not defined in this Attachment are defined in the Agreement or Service Exhibit.

1 Scope. Customer may purchase a Delta Port™ with IP Connection Bundle under this Attachment. Unless otherwise stated in this Attachment, Offer Pricing is exclusive of, and may not be combined with, any other offers, promotions, or discounts, and will only be applied in lieu of any such discounts. All other rate elements not specifically set forth in this Attachment are as stated in the Agreement and Service Exhibits. Customer's Agreement must include all of the applicable Service Exhibits. However, CenturyLink may, in its sole discretion, accept orders and quotes beyond that date, and any such orders and quotes will be subject to the terms of this offer.

2 Description, Eligibility, and Restrictions.

21 A "Delta Port with IP Connection Bundle" is a bundled solution that includes a CenturyLink IQ® Networking Ethernet Internet Port or Private Port, a Local Access IP Connection, Rental CPE, and NBS (if Private Port is used).

(a) Delta Port with IP Connection Bundles must use IP Connection. Service is subject to availability and is only available in qualified locations where CenturyLink facilities exist and Customer's locations meet specific network conditions. Availability is determined by CenturyLink.

(b) Delta Port with IP Connection Bundles are not eligible for any service credits set forth in the SLA referenced in the domestic CenturyLink IQ Networking Service Exhibit.

(c) Limited support hours are available with Delta Port with IP Connection Bundles.

(d) CenturyLink may modify the underlying Service with new or different technology with the same or improved functionality as the existing technology if such new or different technology becomes commercially available by CenturyLink. CenturyLink reserves the right to modify Delta Port with IP Connection Bundle rates after the completion of the Service Term.

(e) When purchasing IP Connection, Customer agrees that it will use the IP Connection attached to a CenturyLink IQ Networking Internet Port only for the provision of either: (i) wireline broadband Internet access (as defined in applicable Federal Communications Commission orders and regulations), or (ii) wireline broadband Internet access plus additional information services, with wireline broadband Internet access constituting a principal use. If the IP Connection is attached to a CenturyLink IQ Networking Private Port, Customer must, so long as the Private Port is used, have entered into an agreement or amendment directing Customer to the NBS Service Exhibit and use at least one NBS instance per CUG (closed user group) that includes that Private Port. Customer agrees the arrangement will be configured so that each Private Port connection will be used consistent with the wireline broadband Internet access usage limitations noted above.

22 Customer Support. Customer Support is limited to 5 days per week, nine hours per day, excluding holidays. The Customer support hours must be the same hours each day.

Customer Support Days	Customer Support Hours (local time, based on the location of the Delta Port with IP Connection Bundle)
TBD	TBD

23 Service Escalations. Customer is allowed to request one customer support escalation for each Delta Port with IP Connection Bundle each month. An escalation means any customer support that occurs outside of the established nine hour time frame. If Customer requests more than the allotted customer service escalations in a given month, CenturyLink will charge \$100 for each service escalation that is in addition to the allotted amount.

31 Term. Subject to any cancellation rights of Customer in the Master Agreement or Participating Addendum and subject to expiration of the Term of the Master Agreement or Participating Addendum, Customer must have an Agreement Term of 24 or 36 months and Customer must agree to use each required Service that is included in the Delta Port with IP Connection Bundle for the minimum number of months associated with the Offer Pricing selected ("Service Term"). The Service Term is indicated in the quote. Customer must order all the applicable Delta Port with IP Connection Bundle Service elements at the same time. If CenturyLink or Customer cancels any of the Services that comprise a Delta Port with IP Connection Bundle, the entire Delta Port with IP Connection Bundle must be terminated at the same time. Each Delta Port with IP Connection Bundle will have its own Service Term commencing on the Start of Service Date for that bundle and continue for the number of months remaining in the Term of the Agreement. Should CenturyLink continue to provide Service after the expiration of the Term, Service will continue on a month-to-month basis, terminable by either party with 30 days' advanced written notice to the other party. "Start of Service Date" means the date CenturyLink notifies Customer that the Delta Port with IP Connection Bundle is provisioned and ready for use

32 Cancellation. Termination will be in accordance with sections 7.1 and 7.2 of the PA.

4. Upgrades; Migration to another CenturyLink Service; Waiver of Cancellation Charges.

41 Upgrades: Customer may upgrade to a higher bandwidth at the same location if: (a) Customer has had the Delta Port with IP Connection Bundle for three months or longer; (b) Customer's location qualifies for the higher bandwidth, and (c) if CenturyLink approves the upgrade. If Customer upgrades to a higher bandwidth, then: (d) CenturyLink will waive the Cancellation Charges associated with the Delta Port with IP Connection Bundle that is canceled; (e) Customer must start a new Service Term for the upgraded Delta Port with IP Connection Bundle and shall continue for the number of months remaining in the Term of the underlying Agreement, (f) Customer must pay the applicable MRCs for the upgraded Delta Port with IP Connection Bundle, and (g) Customer might be required to pay a speed-change charge at then-current time and material rates.

42 Migration to Another Service CenturyLink will waive a Delta Port with IP Connection Bundle's Cancellation Charges if Customer migrates to standard CenturyLink IQ Networking Service or to a CenturyLink IQ® Data Bundle or Managed Data Bundle if available ("Migration"). The MRC for the new CenturyLink IQ Networking Service or Data Bundle solution must be equal to or greater than the MRCs of the Delta Port with IP Connection Bundle being terminated, the new minimum service term is at least as long as the then remaining Service Term of the Delta Port with IP Connection Bundle being terminated and the new Service is available.

5. Offer Pricing.

51 Delta Port with IP Connection Bundle. Customer must pay all applicable MRCs set forth in Appendix A of the NASPO ValuePoint Master Agreement #AR2474.

52 Network-Based Security. NBS rates are set forth in the Network-Based Security Service Exhibit. Delta Port with IP Connection Bundle customers that order the Essential security type with the Basic support level are eligible to receive a 10 Mbps security bandwidth level at rate equal to the 1 Mbps security bandwidth level MRC, as shown in Appendix A.

6. Services.

61 CenturyLink IQ Networking Service. Delta Port with IP Connection Bundles are available with CenturyLink IQ Networking Internet Port and Private Ports at the following bandwidths: 3 Mbps, 5 Mbps, 7 Mbps, 10 Mbps, 20 Mbps, 30 Mbps, 40 Mbps, 60 Mbps, 80Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, or 1 Gbps.

62 Local Access IP Connection. IP Connection is included in the Delta Port with IP Connection Bundle MRC. Other Local Access types such as Customer Provided Access, Cross Connect, or CO Meet Points may not be used with Delta Port with IP Connection Bundles.

63 Rental CPE. Rental CPE will not be offered under this Master Agreement and Participating Addendum.

64 Network Based Security. NBS provides an Internet gateway between Customer's CenturyLink IQ Networking Private Port network and the Internet. CenturyLink will configure the CenturyLink Network Based Security policies based on information that is submitted to CenturyLink by Customer. Customer is responsible for providing accurate information. CenturyLink will provide the Customer with detailed configuration information upon request. Customer may upgrade the security bandwidth level and select from security and support levels rates within NBS.

7. Miscellaneous. All other terms not specifically set forth in this Attachment, including, without limitation, any other rate elements, are as stated in the Agreement and Service Exhibits. The Delta Port with IP Connection Bundle rates will become effective as soon as practicable, but in no event later than the second full billing cycle following the Agreement or Amendment Effective Date. All other terms set forth in the Agreement will remain in effect. This Attachment, the CenturyLink IQ Networking Service Exhibit, the Local Access Service Exhibit, the Rental CPE Service Exhibit, the Network-Based Security Service Exhibit (if applicable), and the NASPO ValuePoint Master Agreement #AR2474 set forth the entire understanding between the parties as to the subject matter herein and supersede any prior written or verbal statements, representations, and agreements concerning the subject matter hereof.

**LEVEL 3® DISTRIBUTED DENIAL OF SERVICE MITIGATION SERVICE
SERVICE EXHIBIT**

1. Applicability. This Service Exhibit is applicable only where Customer orders Level 3® Distributed Denial of Service Mitigation Service ("Service"). Level 3® Distributed Denial of Service Mitigation Service may be designated as "DDoS," "Denial of Service," "Distributed DoS Service," "DDoS Mitigation Service" or "Distributed DoS Mitigation Service" in Customer Orders, Order acceptance, service delivery, billing and related documents. This Service Exhibit incorporates the terms of the Agreement under which Level 3 provides Services to Customer (the "Agreement").

2. Definitions. Any capitalized terms used herein and not otherwise defined herein shall have the meanings set forth in the Agreement.

"Always-On" refers to an option for DDOS Mitigation Direct, DDOS Mitigation Internet Direct Service, DDOS Mitigation GRE Service, or DDOS Mitigation Proxy Service that continually diverts Customer's inbound internet traffic through the Level 3 Mitigation Infrastructure. For DDOS Mitigation Proxy Service it also continuously diverts Customer's outbound internet traffic through the Level 3 Mitigation Infrastructure.

"Clean (Post-Mitigation) Traffic Capacity" means the level of traffic using standard DDoS Mitigation Service that is returned to the Customer "clean" following the mitigation process.

"Cloud Signaling" means that Application Monitoring and Mitigation Service hardware deployed at the Customer premises utilizes automated monitoring tools to detect anomalies in IP traffic patterns and signals a potential Denial of Service Attack to Level 3's cloud infrastructure.

"Customer Disaster Recovery Site" ("DR Site") means an alternative backup site that is used when a primary location becomes unusable due to failure or disaster. Customer will not use the DDoS Mitigation service with production traffic at the DR Site except when use of the Customer primary site fails.

"Customer-Initiated Mitigation" is an optional feature for Direct Service, DDOS Mitigation Internet Direct Service or GRE Service that allows customers to initiate mitigation via specific BGP route announcements to Level 3 rather than calling the Level 3 Security Operations Center ("SOC"). Customer-Initiated Mitigation is equivalent to Customer approval to route traffic to the Mitigation Infrastructure for purposes of the Time to Mitigate Service Level. Customer-Initiated Mitigation is subject to Level 3 availability based on its network configuration. If available, Customer must dynamically advertise the preferred prefixes into the clean return tunnels and the advertised prefixes automatically propagate from the Level 3 Mitigation Infrastructure to the Internet and the Service automatically begins scrubbing the advertised traffic. The maximum number of prefixes that can be advertised via Customer-Initiated Mitigation is subject to technical constraints. Customer-Initiated Mitigation is only available to a customer that purchases the Always-On option.

"DDoS Mitigation Direct Service" or "Direct Service" means the DDoS mitigation solution which is implemented using BGP route advertisements as a mechanism to re-route legitimate and attack traffic through the Level 3 Mitigation Infrastructure. Clean traffic is routed back to the Customer data center over IPVPN/EVPL logical connections between the Mitigation Infrastructure and Customer's border router(s).

"DDoS Mitigation Internet Direct Service" or "Internet Direct Service" means the DDoS mitigation solution which is implemented using BGP route advertisements as a mechanism to re-route legitimate and attack traffic through the Level 3 Mitigation Infrastructure. Clean traffic is delivered back to the Customer data center over a separate VLAN logical connection on a Level 3 provided Internet Service circuit only.

"DDoS Mitigation GRE Service" or "GRE Service" means the DDoS mitigation solution which is implemented using BGP route advertisements as a mechanism to re-route legitimate and attack traffic through the Level 3 Mitigation Infrastructure. Clean traffic is routed back to the Customer data center using a GRE tunnel.

"DDoS Mitigation Proxy Service" or "Proxy Service" means the DDoS mitigation solution which utilizes DNS entry updates as a mechanism to redirect legitimate and attack traffic through the Level 3 Mitigation Infrastructure. Clean traffic and Customer's protected web server outbound traffic are delivered between Customer's protected web based server and Mitigation Infrastructure over public Internet. Proxy Service is subject to Level 3 availability.

"Distributed Denial of Service Attack" or "Attack" is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

"Level 3 Mitigation Infrastructure" or "Mitigation Infrastructure" is defined as a collection of Level 3 devices designed to filter malicious attack traffic and pass through legitimate traffic in order to mitigate the potential disruptions caused by a Distributed Denial of Service Attack.

"On-Demand" refers to an option for DDOS Mitigation Direct, DDOS Mitigation Internet Direct Service or DDOS Mitigation GRE Service that diverts Customer's inbound internet traffic through the Level 3 Mitigation Infrastructure using BGP networking only when Customer traffic is under Attack or suspected of being under Attack.

**LEVEL 3® DISTRIBUTED DENIAL OF SERVICE MITIGATION SERVICE
SERVICE EXHIBIT**

“Regularly Scheduled Maintenance” means any scheduled maintenance performed to the Mitigation Infrastructure. Regularly Scheduled Maintenance will not normally result in Service interruption. If Regularly Scheduled Maintenance requires an interruption, Level 3 will: (a) provide Customer seven (7) days’ prior written notice, (b) work with Customer to minimize such interruptions, (c) use commercially reasonable efforts to perform such maintenance between midnight and 6:00 a.m. local time where the Mitigation Infrastructure is located on which such maintenance is performed and (d) work with Customer to remove Always-On Customer traffic from the Mitigation Infrastructure during such maintenance to avoid interruption. Emergency maintenance may be performed on less or no notice. Regularly Scheduled Maintenance, emergency maintenance and Force Majeure Events, and unavailability of the DDoS Mitigation Service due to malfunction of the public Internet are “Excused Outages.”

“Service Validation” means the process by which DDoS Mitigation Service is confirmed as available for GRE Service, DDOS Mitigation Internet Direct Service and Direct Service as a part of the provisioning process enabling Level 3 to obtain a profile of Customer’s traffic. Customer will coordinate to schedule such Service Validation when contacted by Level 3 to do so. Service Validation is conducted over two (2) windows during which traffic is routed through the Mitigation Infrastructure as follows: (a) an initial 2 hour “test” window, and (b) a 24-hour validation window. Service Validation must be completed for all or a subset of protected Class C subnet prior to routing traffic through the Mitigation Infrastructure.

“Special Unavailability” means unavailability of the DDoS Mitigation Service due to (a) Customer misuse; (b) other negligent or unlawful acts by Customer or Customer Representatives; (c) network unavailability, including telecommunications failures outside of the Mitigation Infrastructure or Level 3 network; (d) problems with Customer’s servers or equipment; (e) Customer’s sustained traffic load reaching a point that causes material degradation to or outage of the underlying Level 3 Internet infrastructure not directly related to the Mitigation Infrastructure; (f) any other action or inaction by a third party; or (g) a Force Majeure Event, as defined in the Agreement. Whether Special Unavailability is present shall be determined by Level 3 in its good faith discretion supported by records, data and other evidence.

“SSL Mitigation” means the DDoS mitigation solution that inspects encrypted web traffic to determine if the traffic is legitimate or compromised. SSL Mitigation is available only if GRE Service, Direct Service or Internet Direct Service is or has been ordered and SSL Mitigation is not available as a standalone feature. Clean traffic is routed back to the Customer data center over the selected DDoS Mitigation Service clean traffic return path.

“Suspension” means Level 3’s suspension of the DDoS Mitigation Service to Customer as permitted by this Service Exhibit or as otherwise allowed under the Agreement.

3. Service Description. The DDoS Mitigation Service is available on Customer’s Internet services as described herein. The Customer Order form will specify the type of Mitigation Services and whether those Services are Always-On or On-Demand, as applicable. Notwithstanding anything in the Agreement to the contrary, Level 3 may upon prior approval of Customer, in its sole and absolute discretion, subcontract any or all of the work to be performed under this Service Exhibit, including but not limited to, installation, detection, and mitigation services, provided that Level 3 will remain responsible for the performance of Level 3’s obligations hereunder Services other than the DDoS Mitigation Services provided by Level 3 to Customer that work in conjunction with DDoS Mitigation Services (such as IPVPN Service) are subject to separate Service Exhibits. DDoS Mitigation Service is available in 4 cloud-based options that Customer will select and that will be identified in the Customer Order: (i) Direct Service, (ii) DDOS Mitigation Internet Direct Service, (iii) GRE Service, or (iv) Proxy Service.

In the event Customer has Level 3 Managed Network Service, by ordering DDoS Service, Customer expressly grants Level 3 permission to make configuration changes to any Customer Premises Equipment (regardless of ownership) managed by Level 3 for DDoS service activation and ongoing maintenance.

Direct Service is activated by BGP route advertisement, with logical private line connections over IPVPN/EVPL between the Mitigation Infrastructure and Customer’s border router(s). BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack.

Internet Direct Service is activated by BGP route advertisement delivering mitigated traffic from the Mitigation Infrastructure to Customer’s border router(s) via a separate VLAN on a Level 3 provided Internet connectivity. BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack.

GRE Service is activated by BGP route advertisement and is based upon the GRE protocol with virtual tunnel connections constructed to Customer’s border router(s). BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure, enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack. Customers directly connected to the Level 3 AS IP network can advertise a /32 subnet. Non-Level 3 IP customers must advertise a /24 subnet as a minimum.

Proxy Service is an Always-On service which mitigates specific internet-based Attacks and allows legitimate internet based traffic to the Customer’s protected web based server. For Proxy Service, Level 3 will assign virtual IP addresses (“VIPs”) that the Customer will point to either directly or via another DNS record. Customer is responsible to update Customer’s DNS entries to Level 3-provided information which redirects Customer’s web traffic via Proxy Service. Each Proxy Service will terminate to only one (1) Customer hosted

**LEVEL 3® DISTRIBUTED DENIAL OF SERVICE MITIGATION SERVICE
SERVICE EXHIBIT**

IP address and will send clean traffic to and receive outbound internet traffic from Customer's server. Proxy Service works with standard TCP based Web (i.e., HTTP, HTTPS) application layer protocols. Customer acknowledges that Proxy Service can be setup to open HTTPS traffic for deep packet inspection if Customer elects HTTPS packet inspection at the application Layer 7 level on a per domain, per SSL certificate basis. This optional Proxy Service component requires Customer to provide Level 3 with a SSL certificate to be loaded on to Proxy Service platform for the traffic which shall be subject to HTTPS packet inspection.

Routing under either the Direct Service, Internet Direct Service, or the GRE Service is asymmetric, with outgoing traffic from Customer to the Internet being forwarded as normal to Customer's Internet Service Provider, without passing through Mitigation Infrastructure. For Proxy Service both incoming and outgoing Customer web application Internet traffic configured to use the Proxy Service passes through the Mitigation Infrastructure.

For On-Demand Service, once the Mitigation Infrastructure is engaged, if an identifiable Attack is not seen by Level 3 within 48 hours, Level 3 will coordinate with Customer and obtain consent from Customer (which shall not be unreasonably withheld) to return Customer to normal conditions. Upon receipt of Customer consent, Level 3 may continue to maintain traffic on Mitigation Infrastructure for an agreed-upon limited time period.

For Always-On Service, the diverted traffic entering Level 3's Mitigation Infrastructure will be inspected and filtered of attack traffic based on predefined filters agreed upon by Level 3 and Customer. Customer must report to Level 3 any new attacks not effectively blocked by predefined filters. Level 3 will respond to new requests for mitigation in accordance with the "Time To Mitigate SLA."

For On-Demand Service, upon confirmation of an Attack and with the cooperation of Customer, Level 3 shall route Customer's IP traffic to the Mitigation Infrastructure designed to filter malicious Attack traffic and pass through legitimate traffic in order to mitigate the potential disruptions caused by an Attack. However, due to the varying nature of Attacks, Level 3 cannot guarantee that all Attacks will be detected and/or mitigated; nor does Level 3 guarantee that all IP traffic patterns that initially appear to be Attacks are actual Attacks.

Customer must promptly notify Level 3 if it believes it is under Attack and provide Level 3 with reasonable assistance to reroute the IP traffic to the Mitigation Infrastructure in order for the DDoS Mitigation Service to function properly.

Monitoring options for the DDoS Mitigation Service provide proactive detection of DDoS events ("Attack Monitoring Services"). Attack Monitoring Services are available only to Customers with management access to their Customer Premises Equipment ("CPE") who purchase DDoS Mitigation Services and to Customers with Level 3 Internet Service that choose monitoring from Level 3 provided edge routers directly. There are two types of available Attack Monitoring Services as follows:

(a) Flow Based Monitoring ("FBM") Service provides 24x7 monitoring of Customer's border router(s) or Level 3 provided edge routers directly and alerts for large flood-based Attacks. FBM Service requires a reliable feed of netflow sampling and SNMP specific to the Customer's traffic. To the extent Customer purchases the FBM Service with the On-Demand Service, Level 3 will proactively notify Customer about DDoS mitigation system generated alarms that Level 3 determines are caused by DDoS Attacks. For Attacks that are not detected by the DDoS mitigation system, Customer must contact the Level 3 SOC to initiate mitigation. There will be an MRC and an NRC for each Customer router when monitoring occurs from Customer's border router(s) or for each logical circuit when monitoring occurs from Level 3 provided edge routers directly from which the FBM Service collects netflow sampling.

(b) Application Monitoring and Mitigation for Customer owned and managed equipment ("AMM Cloud Signaling") Service means that a hardware based DDoS detection and mitigation solution is implemented at the Customer premises to monitor the Customer's perimeter network and issues alerts for layer 7 or "application layer" Attacks. AMM Cloud Signaling Service includes CPE hardware that is installed on the Customer premises. Customer may order AMM Cloud Signaling Service only with Customer-owned and managed CPE. In such event Customer must be able to provide Cloud Signaling from its CPE to Level 3's Cloud Signaling endpoint and Customer must utilize an equipment manufacturer, model, software code and other applicable items approved by Level 3. Customer is responsible for technical support, service and maintenance of the CPE. Customer will have full administrative access to the CPE and Level 3 will have no access to the CPE. There will be an MRC and an NRC for each piece of equipment utilizing the AMM Cloud Signaling Service.

Notwithstanding the foregoing, Level 3 reserves the right at any time by notification by email, SMS or phone call to the Customer to: (i) change or supplement the monitoring tools and the mitigation techniques (including but not limited to modifying the Mitigation Infrastructure); (ii) increase or decrease the monitoring tools' sensitivity to anomalous IP traffic patterns; and (iii) modify the definition of anomalous IP traffic patterns that may indicate an Attack.

4. Charges. For DDoS Mitigation Services, Customer will be billed monthly in advance based on a fixed rate for mitigation up to a predefined bandwidth level. The manner of billing selected will be set forth in the Customer Order. Fixed rate charges for DDoS Mitigation Service consist of 2 components: (a) a non-recurring charge ("NRC") and (b) a monthly recurring charge ("MRC"). The Service Commencement Date begins upon issuance of a Level 3 Connection Notice. The Connection Notice will be issued on the first to occur of: (i) successful completion of Service Validation or (ii) five (5) business days after Level 3 notifies Customer that it has provisioned all components of the Service that Level 3 can provision without Customer's assistance. In the event there are multiple locations, billing will begin with the Service Commencement Date for the initial location (unless other locations are not available due to the fault of Level 3).

**LEVEL 3® DISTRIBUTED DENIAL OF SERVICE MITIGATION SERVICE
SERVICE EXHIBIT**

Customer may seek expedited "turn-up" of DDoS Mitigation Service for a one-time charge ("Expedited Service"). Level 3 will exercise good faith efforts to turn up Expedited Service for GRE Service in one (1) business day however this is a nonbinding objective. For DDoS Mitigation Service other than GRE Service, the order will be processed in a prioritized manner. No Service Levels will apply to Expedited Service during the first seven (7) days of service.

5. IP Addresses. In the event that Level 3 assigns to Customer an IP address as part of the provision of Service, such IP address shall (upon Level 3's request and to the extent permitted by law) revert to Level 3 after termination of the applicable Customer Order for any reason whatsoever, and Customer shall cease using such address. At any time after such termination, Level 3 may re-assign such address to another user.

In the event that Level 3 does not assign to Customer an IP address as part of the provision of Service, Customer represents and warrants that all title, right and interest in and to each IP address used by Customer in connection with the DDOS Mitigation Service is owned exclusively by Customer and/or Customer has all permissions necessary from the owner to enable Level 3 and Customer to perform their obligations hereunder.

6. Clean Bandwidth. Level 3 will provide to Customer Clean (Post Mitigation) Traffic Capacity up to the level set forth in the Customer Order.

7. Service Levels and Remedies.

The following Service Levels are not available prior to the completion of Service Validation. To receive credits, Customer must immediately notify Level 3 in writing of a Service issue, but in no event later than 30 calendar days after the incident. Whether an incident constitutes an event for Service credit purposes will be determined by Level 3 in its good faith discretion supported by records, data and other evidence. Credits are only available against the MRC for the affected DDoS Mitigation Service. The Service Levels stated in Sections A - D below apply to the mitigation aspect of DDoS Mitigation Service. Service Levels do not apply to Excused Outages. The availability of credits shall not affect any of Customer's rights or remedies available under the Master Agreement and/or the Participating Addendum.

(A) DDoS Mitigation Service Levels, Service Credits and Chronic Termination Rights. Level 3 shall use commercially reasonable efforts to make the Level 3 Mitigation Infrastructure available to Customer one hundred percent (100%) of the time once Customer's IP traffic is routed to the Level 3 Mitigation Infrastructure in response to a confirmed Denial of Service Attack until Customer's IP traffic is re-routed back to normal following cessation of such Attack (the "Mitigation SLA"). For purposes of this Mitigation SLA, a "Mitigation Service Outage" means that the Level 3 Mitigation Infrastructure is unavailable to Customer to the extent that Customer is routing traffic through such Mitigation Infrastructure (i.e., the Customer cannot pass traffic through the Level 3 Mitigation Infrastructure) for more than 60 consecutive seconds, except during an Excused Outage, periods of Special Unavailability or periods of Suspension. The duration of the Mitigation Service Outage shall be determined by Level 3 (including through the use of third party monitoring of Customer provided URL availability, in the case of Proxy Service) in its good faith discretion using information collected from Level 3 trouble tickets and/or data collected on the Mitigation Infrastructure.

In the event a Mitigation Service Outage lasts 4 or less consecutive hours, upon Customer request Level 3 will provide a service credit to Customer equal to 3 days of the MRC associated with the DDoS Mitigation Service at the affected location (the MRC of the affected location ÷ 30 calendar days x 3).

If a particular Mitigation Service Outage reported by Customer lasts more than 4 consecutive hours, upon Customer request Level 3 will provide a service credit to Customer equal to 5 days of the MRC associated with the DDoS Mitigation Service at the affected location (MRC of the affected location ÷ 30 calendar days x 5).

In no event will Customer receive a credit for more than 1 incident per day pursuant to the terms of this Section 7(A), regardless of the number of times Level 3 fails to comply with the Mitigation SLA during that day.

In addition to Customer being entitled to the above credit(s), as Customer's sole remedy for any non-performance of the Service, the additional termination rights apply:

(i) in the event a Mitigation Service Outage extends for 10 or more consecutive days, Customer shall have the right, for 30 days following the start of such Mitigation Service Outage, to terminate the affected DDoS Mitigation Service under the applicable Order without early termination liability;

(ii) in the event of 7 separate occurrences of Mitigation Service Outage each lasting at least 60 minutes in a 90 day period, Customer shall have the right, for 30 days following the 7th such occurrence, to terminate the affected DDoS Mitigation Service under the applicable Order without early termination liability; and

(iii) if Customer has procured from Level 3 an IPVPN circuit or Level 3 Internet Service circuit as part of the DDoS Mitigation Service, Customer's termination rights hereunder extend to such IPVPN Service or Level 3 Internet Service.

**LEVEL 3® DISTRIBUTED DENIAL OF SERVICE MITIGATION SERVICE
SERVICE EXHIBIT**

(B) Time to Mitigate Service Level. Level 3 agrees to deploy mitigation following Customer approval (which may be verbal) and Customer properly routing traffic to the Mitigation Infrastructure during an Attack. The Time to Mitigate is measured from the time Level 3 obtains Customer approval and Customer properly routing traffic to the Mitigation Infrastructure during an Attack until Level 3 deploys countermeasures to initiate mitigation. The applicable Service Level for each type of Attack is set forth below.

<u>Attack Type</u>	<u>Time to Mitigate Service Level</u>
▪ UDP/ICMP Floods	10 minutes
▪ SYN Floods	10 minutes
▪ TCP Flag Abuses	10 minutes
▪ DNS Reflection	10 minutes
▪ DNS Attack	10 minutes
▪ HTTP GET/POST Attacks*	10 minutes

*HTTP Attack mitigation requires a subscription to Proxy Service.

In the event the Time to Mitigate Service Level ("TTM SLA") is not achieved, the following remedies apply:

<u>Duration of Single Event</u>	<u>Service Credit</u>
>10 minutes - 60 minutes	1 day of the MRC
>60 minutes - 6 hours	2 days of the MRC
>6 hours	7 days of the MRC

Customer is deemed to have pre-approved mitigation for Proxy Service or Always-On and the SOC does not have to call Customer to deploy the same. Certain mitigation countermeasures related to FBM Service may be pre-authorized by Customer. If a countermeasure is required that has not been pre-authorized (e.g. in addition to the pre-authorized countermeasures), verbal approval is required from Customer to deploy such countermeasure.

Mitigation requiring traffic analysis and custom signature development are not covered under the TTM SLA.

(C) Attack Monitoring Services Time to Notify Service Level (FBM and AMM Cloud Signaling Services only)

If Customer orders FBM Service or AMM Cloud Signaling Service, a credit as set forth below will be provided if an Attack Monitoring Failure to Notify Event ("FTN Event") occurs. An FTN Event is an event in which an Attack Monitoring DDoS alert occurs but steps to notify Customer within a period of 15 minutes from the time that Level 3 receives a "Type DDoS" alert are not taken. Timely efforts to notify Customer whether via email or phone satisfy the requirement to take such steps whether or not the Customer can be reached.

For each FTN Event that occurs during a calendar month, Customer will be entitled to receive a service credit equal to the pro-rated charges for 3 days of the MRC applicable to the affected site(s). If 3 or more FTN Events occur during a calendar month, in lieu of service credits, Customer shall have the right, for 30 days following the third FTN Event, to terminate the applicable Service without liability.

(D) General Terms for all Service Levels

Credits shall only apply for DDoS Mitigation Service provided pursuant to an MRC, and will not apply to any other DDoS Mitigation Service, including, without limitation, any custom service. Duplicative credits (e.g., for both a Mitigation SLA and a TTM SLA) will not be awarded for a single incident. In the event a single incident triggers both the Mitigation SLA and TTM SLA, Customer will be entitled to receive the higher of the two credits. The aggregate credits under subparts (A), (B) and (C) above to be provided in any calendar month shall not exceed 100% of the MRC of the affected DDoS Mitigation Service. Customer must maintain with Level 3 up to date contact information and an up to date escalation list for Service Levels to apply. Any non-emergency changes or service design changes that may be required outside of an Attack event such as prefix additions and migration from On-Demand to Always-On require a change order. Level 3's objective is to complete change requests within two (2) business days. The change request objective is non-binding and does not constitute a ServiceLevel.

8. Customer Responsibilities. Customer must provide to Level 3 an up-to-date point of contact with 24x7 availability who Level 3 will coordinate with upon detection of an Attack. Customer is solely responsible for updating such point of contact information, as necessary.

Customer must cooperate with Level 3 and Level 3's partners or subcontractors in coordinating setup of the DDoS Mitigation Service, including but not limited to, placing the necessary routing device at the edge of Customer's environment and cooperating with Level 3 in the rerouting of IP traffic to the Level 3 Mitigation Infrastructure during an Attack.

For the Direct Service, Customer must procure from Level 3 connectivity between the Level 3 network and the Customer Site (border routers) per the following criteria: (i) the demarcation point is the physical network port of the Mitigation Infrastructure, (ii) the connectivity must consist of at least one (1) IPVPN circuit directly to the port on the Mitigation Infrastructure from each of Customer's data centers, and (iii) any Ethernet circuit must support 802.1Q. Provisioning begins upon confirmation of IPVPN circuit availability.

**LEVEL 3® DISTRIBUTED DENIAL OF SERVICE MITIGATION SERVICE
SERVICE EXHIBIT**

Level 3 may suspend Direct Services if Level 3 determines that any Customer provided equipment is causing interference with the Level 3 network or other customers. Any IPVPN circuit provided by Level 3 will be subject to service levels as set forth in Level 3's standard service exhibit for such service or as otherwise agreed in writing by Customer and Level 3.

For the Internet Direct Service, Customer must procure from Level 3 connectivity between the Level 3 network and the Customer Site (border routers) per the following criteria: (i) the demarcation point is the physical network port of the Mitigation Infrastructure, (ii) the connectivity must consist of at least one (1) Level 3 Internet Service circuit capable of connecting to the port on the Mitigation Infrastructure from each of Customer's data centers (subject to availability), and (iii) any Ethernet circuit must support 802.1Q for delivery of Internet and scrubbed traffic on two (2) separate VLANs. Provisioning begins upon confirmation of Level 3 Internet Service circuit availability. Level 3 may suspend Internet Direct Services if Level 3 determines that any Customer provided equipment is causing interference with the Level 3 network or other customers. Any Level 3 Internet Service circuit provided by Level 3 will be subject to service levels as set forth in Level 3's standard service exhibit for such service or as otherwise agreed in writing by Customer and Level 3.

Customer is required to redirect traffic off of the Level 3 Mitigation Infrastructure within 48 hours of notification that there is no longer any observed Attack traffic.

Customer must promptly notify Level 3 of any events that may cause significant IP traffic pattern changes for the Customer network being monitored through the DDoS Mitigation Service.

Customer must promptly notify Level 3 if it believes it is under an Attack in order for the DDoS Mitigation Service to be activated effectively.

Customer must establish and consistently maintain reasonable and adequate security policies and devices for defense of its assets. Customer acknowledges that DDoS Mitigation Service is regarded as a tool that can be used as part of the Customer's overall security strategy, but not as a total solution.

In relation to Proxy Service and SSL Mitigation, Customer is solely responsible to ensure, and hereby represents, that the provision of any SSL certificate to Level 3 and Level 3's use of the same to provide the Services hereunder does not violate any laws, security policies or regulations.

Customer understands and expressly consents that in the performance of its obligations hereunder, notwithstanding any other requirements in the Agreement between Level 3 and Customer, Level 3 (or its subcontractor) may route Customer traffic to Level 3 Mitigation Infrastructure which is located in a country other than the country of origination and/or destination of such traffic.

In the event Customer or Level 3 determine that the DDoS Mitigation Service is being affected by a continuing error, conflict or trouble report, or similar issue (in each case a "Chronic Problem") caused by the Customer, Customer shall resolve any Chronic Problem by taking whatever steps are deemed necessary to rectify the same, including, but not limited to: (i) removing or modifying the existing DDoS Mitigation Service configuration (or requesting Level 3 to remove the same); or (ii) replacing Customer's equipment providing distributed denial of service Mitigation should that be deemed necessary. If Customer has not remedied the Chronic Problem within 30 days of request by Level 3, then Level 3 may suspend or terminate the DDoS Mitigation Service.

9. Policies. The DDoS Mitigation Service is subject to Level 3's then-current acceptable use and privacy policies as incorporated in Attachment C of the Participating Addendum.

10. Restrictions. If Level 3 provides Customer with portal access in connection with the DDoS Mitigation Service, Customer will use such access solely as for use with the DDoS Mitigation Service in accordance with this Service Exhibit and the Agreement, and Customer will be responsible for any unauthorized access to or use thereof. A charge will apply to any Customer users in excess of ten (10) Customer users of the DDoS Mitigation Service portal. The DDoS Mitigation Service uses two-factor authentication ("2FA") for access to the portal. The 2FA tokens will be disabled for accounts that have not been active in more than six (6) months requiring such users to request new tokens if they wish to reestablish access. Customer understands and acknowledges that the DDoS Mitigation Service is not suitable for the maintenance or processing (apart from mere transmission) of protected health information consistent with the Health Insurance Portability and Accountability Act (HIPAA), as amended or any other applicable laws in the matter.

11. Disclaimer. Notwithstanding any language in the Agreement to the contrary, Level 3 shall not be obligated to provide any defense, indemnity or hold harmless obligations with regard to any actual or alleged claim, liability, damage, expense or fees arising in connection with Customer's use of the DDoS Mitigation Service (or any associated software or Services) or otherwise arising in connection with this Service Schedule. The DDoS Mitigation Service and associated steps or countermeasures are configured to reduce disruption of Customer's legitimate traffic. The DDoS Mitigation Service is provided on a "best efforts" basis and is designed to provide protection from most DDoS Attacks. Accordingly, there can be no assurance or guarantee with respect to the efficacy of the DDoS Mitigation Service or that the DDoS Mitigation Service will provide protection in all or most cases. If a DDoS Attack is impacting, or may impact, the Level 3 network or other Level 3 customers, or if it exceeds the amount of Clean Traffic Capacity or Attack protection purchased, Level 3 may take any action, including but not limited to "blackhole" filtering or "null routing" Customer's traffic, which filtering or "null routing" would result in all traffic destined to Customer being dropped. In such event Level 3 may also offer Customer, for an additional charge, a higher level of Clean Traffic Capacity or Attack protection in line with the Clean Traffic Capacity or Attack bandwidth level to enable potential protection. Because DDoS Mitigation Service is provided using shared Mitigation Infrastructure, such Mitigation Infrastructure may be unavailable or impaired in the event of large scale Attacks (including to other customers of Level 3).

**LEVEL 3® DISTRIBUTED DENIAL OF SERVICE MITIGATION SERVICE
SERVICE EXHIBIT**

12. Additional Terms and Conditions Associated with the Service.

Level 3 may terminate any Customer Order in the event that Level 3 cannot maintain any required regulatory approvals, despite its reasonable efforts to do so. Level 3 may temporarily suspend any DDoS Mitigation Service immediately in the event Level 3 has a good faith belief that such suspension is reasonably necessary to mitigate damage or liability that may result from Customer's continued use of the DDoS Mitigation Service. In the event of any expiration or termination of any Service, Customer's access to the applicable Services will end and Level 3 will not be responsible for assisting Customer with any transition to an alternative provider, notwithstanding anything to the contrary in the Agreement. In the event of any such termination, Customer shall have no further liability. Nothing in this Service Schedule or the Agreement grants Customer any rights to, and Customer is expressly prohibited from, reselling the DDoS Mitigation Service or using any component of the DDoS Mitigation Service or Proprietary Materials to create or offer derivative versions of the DDoS Mitigation Service either directly, or through a third party, as a standalone service offering, as bundled with Customer's services or products, or on a service-bureau basis.

NETWORK-BASED SECURITY SERVICE EXHIBIT

1. **General.** CenturyLink QCC will provide Network-Based Security Service ("NBS" or "Service") under the terms of the Agreement and this Service Exhibit.

2. **Service Description.** NBS is a CenturyLink security service that manages and monitors traffic between the Internet and Customer's separately purchased CenturyLink IQ® Networking Private Port network. CenturyLink will provide Service from a CenturyLink network facility, such as a POP or data center, which is determined by CenturyLink and is subject to relocation. Security features associated with NBS are implemented within CenturyLink's network. Customer may choose among various categories of security types, support levels, and security bandwidths. Service also includes a Web portal that is designed to assist Customer with certain self management and reporting functions. Unless the parties otherwise agree in writing, Customer has sole responsibility for ordering, securing installation and ensuring proper operation of any and all equipment required to enable Customer to receive the Service.

2.1 **Security Features.** The NBS security features are described below.

(a) **Firewall.** The managed firewall feature includes a set of related functions designed to allow or deny certain hosts or networks to communicate to each other, based on Customer's security policy. The managed firewall feature includes a network-based firewall instance, installation, configuration support, logging, reporting, and 24x7 monitoring of the firewall infrastructure.

(b) **VPN.**

(i) The virtual private network ("VPN") feature uses a variety of specialized protocols to support private encrypted communications through the Internet from a Customer location to the NBS platform. Customer is responsible for the provision and management of the equipment at its location that connects to the NBS platform and of the encrypted tunnel between the Customer-provided equipment and the NBS platform. Customer's use of CenturyLink technical support in connection with the VPN feature is limited to CenturyLink facilitating the encrypted connection between Customer equipment and the NBS platform.

(ii) If Customer or its End Users use remote access SSL VPN to access the NBS platform, Customer is responsible for procuring, installing and testing client VPN software on Customer's End User computers. A SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol. CenturyLink will configure user credentials for use with the Service to enable End User access to the NBS platform. There is a 20 End User limit if the End Users are provisioned directly on the NBS platform. For deployments exceeding 20 End Users, Customer must provide an authentication server, with the maximum number of End Users subject to CenturyLink's approval. Customer is responsible for the management (e.g., adding or deleting End Users) and security of the authentication server.

(iii) The parties will provide each other with necessary configuration information required for Customer to establish the VPN connection.

(c) **Windows Active Directory (AD) Integration for Single Sign-On.** The Windows AD Integration feature provides single sign-on capabilities to users with the help of agent software. The agent software sends information about user logins to the NBS platform. With user information such as IP address and user group membership, security policies can allow authenticated network access to users who belong to the appropriate user groups without requesting their credentials again. In addition to single sign-on, AD integration is beneficial as NBS reports provide better detail with regards to user and group information.

(d) **Intrusion Detection and Prevention.**

(i) The network intrusion detection and prevention features of the Service ("IDS/IPS") monitor Customer's network traffic on 24x7 basis for a list of attack and misuse signatures according to a pre-defined security policy specific to Customer's network environment. The policy may have an option to block and report on misused traffic.

(ii) The security policy is submitted by Customer to CenturyLink and is subject to CenturyLink's approval. The security policy categorizes intrusion Events as either "low priority level," "medium priority level," or "high priority level." An "Event" means any security occurrence detected and reported by the IDS/IPS feature. An Event does not necessarily constitute an actual security incident. CenturyLink may update the security policy from time-to-time in order to address industry-wide changes in security needs. Customer may view the Event detail (including timestamp, attack type) on the NBS Web portal. Such reports contain information relating to low, medium, and high priority Events, including the time of the Event, the Event name, and a summary of attack statistics. Low, medium, and high priority Events are described below:

- **Low Priority.** A low priority Event identifies activity on a network that is not necessarily suspicious or malicious in nature, but may indicate a need for a more secure means of network implementation. An example of a low priority Event includes poor security practices.
- **Medium Priority.** A medium priority Event identifies activity that is suspicious in nature and may warrant investigation. An example of a medium priority Event includes network reconnaissance by an unknown source.
- **High Priority.** A high priority Event identifies activity that is potentially malicious in nature and requires immediate attention. An example of a high priority Event includes attempts to compromise Customer's network or attempts to gain privileged access to Customer's network.

(iii) CenturyLink will analyze high priority Events to determine if an Incident has occurred. An "Incident" means any single Event or collection of Events that have been determined by a CenturyLink IDS/IPS analyst reviewing the data to potentially be of security consequence. Incidents may include Events that are currently being investigated and actual attacks that may be in progress. If, upon investigation, an Event or series of Events is determined to be a high priority level Incident, CenturyLink will attempt to notify Customer

NETWORK-BASED SECURITY SERVICE EXHIBIT

via telephone or e-mail (as agreed upon between the parties) within fifteen minutes after such determination to consult with Customer to determine the most appropriate response to the Incident.

(e) Content Filtering. The content filtering feature is designed to block Web content based on Customer's policy settings. Customer is responsible for defining content filtering policies. Content Filtering events are detected, logged, and viewable by Customer on the NBS Web portal.

(f) DLP. Data leak prevention ("DLP") is a feature that is designed to detect, report and optionally block potential data leakage incidents by intercepting and inspecting traffic that is traversing between the Internet and Customer's Private Port network. The DLP feature is able to block or allow End User traffic that matches pre-defined data patterns and is based on Customer's rules and policies. DLP supports only certain protocols and file types.

2.2 Security Types. Service is available in three security types. Each security type contains a fixed set of NBS security features. The following table describes the NBS security features that are available for each security type.

Security Type (D, E, or F)	Features that are included in the security type
Next Generation Internet (D)	Firewall and VPN features
Content Filtering (E)	Firewall, VPN, Remote User SSL VPN, Windows AD Integration and Content Filtering features
Complete Security (F)	Firewall, VPN, Remote User SSL VPN, Windows AD Integration, Content Filtering, IDS/IPS and DLP features

2.3 Support Levels. Support levels apply to Customer's security type, and not to each security feature. The following table describes each support level.

Support Level	Description of support included with the applicable support level
Standard (5) Available only with Next Generation Internet (D) and Content Filtering (E)	- CenturyLink-managed review of high priority Events - Policy change timeframe is 24 hours - Maintenance window for policy changes - One year log retention* - Co-management option is available Security Type: Next Generation Internet - 15 policy changes per 12-month period (beginning from the Start of Service Date) - Maximum of five site-to-site VPNs Security Type: Content Filtering - 20 policy changes per 12-month period (beginning from the Start of Service Date) - Maximum of ten site-to-site VPNs
Unlimited (6) Available only with Complete Security (F)	- CenturyLink managed review of high priority Events - Unlimited policy changes per month - Policy change timeframe is 8 hours - Two urgent policy changes per month - CenturyLink will respond within two hours after an urgent policy change request - Maintenance window for policy changes - One year log retention* - Co-management option is available - 25 or more site-to-site VPNs, subject to CenturyLink's approval & platform bandwidth limits

* CenturyLink does not retain logs after the log retention period has been completed.

2.4 Security Bandwidth. The security bandwidth level that Customer selects will be the maximum throughput for Customer traffic passing between Customer's CenturyLink IQ Network Private Port network and the Internet. CenturyLink may limit the maximum security bandwidth level available for purchase for a particular Service instance based on the security type, the security features, and the complexity of the policies selected.

2.5 Web Portal. Service includes access to a Web portal via Control Center that a Customer Administrator can access for information such as inventory, trouble ticketing, billing information and reports. CenturyLink will provide Customer up to three security tokens for access to the NBS Web portal. If Customer requests more than three security tokens, CenturyLink will provide the additional security tokens for an additional charge. Real-time logs are available for up to 30 days. Offline log retention periods are as specified in the Support Level table.

2.6 Co-Management Option. Customer may elect to co-manage the Service. CenturyLink will provide the designated Customer Administrators the ability to modify Service configurations via the Web portal. Change requests by CenturyLink will continue to be processed as per the applicable support level. Customer must notify CenturyLink of its intent to participate in the co-management option. The SLA does not apply if an SLA Goal is missed as a result of a Customer-initiated configuration.

NETWORK-BASED SECURITY SERVICE EXHIBIT

2.7 CenturyLink Responsibilities.

- (a) During deployment and initiation, CenturyLink will work with Customer to deploy new Service. CenturyLink will send Customer a welcome e-mail and conduct a kickoff call to introduce CenturyLink deployment specialists to Customer contacts and begin to assess Customer requirements.
- (b) CenturyLink will gather detailed information for the initial setup of Service and associated Service features. Most of the questions will be technical in nature and help determine the layout of Customer's network, including hosts on the network and desired security policies. A portion of the requested data will reflect Customer organization, and will include security contacts and escalation paths. Using the provided information, CenturyLink will work with Customer to understand the existing Customer environment and work with Customer to build a configuration and security policy used with NBS.
- (c) CenturyLink will provide ongoing service support, policy management, and record retention of all changes in accordance with the applicable support level.
- (d) CenturyLink will provide management of the NBS platform, system patches and upgrades, troubleshoot problems on the NBS platform.
- (e) CenturyLink will perform service configuration and implementation remotely.

2.8 Customer Responsibilities. CenturyLink may not be able to provide the Service if Customer's responsibilities are not met.

- (a) During deployment, Customer will work with CenturyLink to deploy Service.
- (b) Customer will provide CenturyLink with: (i) accurate and current contact information for Customer's designated points of contact; (ii) a primary and a secondary Customer contact; and (iii) an escalation path through the organization in the event that CenturyLink must contact Customer.
- (c) Customer will participate in a scheduled kickoff call to introduce team members, set expectations, and begin the assessment process.
- (d) Customer will be required to complete a form to provide detailed information about the network configuration and must work with CenturyLink in good faith to accurately assess Customer's network and environment.
- (e) Customer is required to provide hands on assistance for the purposes of troubleshooting and/or diagnosing technical difficulties.
- (f) On an annual basis, Customer agrees to work with CenturyLink to review configuration of the Service and identify required updates.
- (g) Customer is responsible for making agreed to changes to the network environment.
- (h) Customer is responsible for ensuring the desired network traffic and applicable segments are configured to route network traffic through the Service.
- (i) Customer must appropriately safeguard its login credentials to the Web portal, including not disclosing to any third party, and promptly notify CenturyLink if a compromise of credentials is suspected. Customer will ensure that its systems and networks will have up-to-date security controls and patches and that its systems and networks that connect with those included with NBS, or that use common network features, have appropriate security controls.
- (j) Customer agrees to notify CenturyLink in advance of any network changes or activities that could impact Service or reasonably interfere with the monitoring of the Service, such as planned outages, configuration changes, maintenance, or systems changes.
- (k) Customer represents and warrants that it has notified (including by means of appropriate internal use policies, where applicable, and by means of screen banners displayed on system log-in) its employees, vendors, contractors and other of its email network that communications or transmissions on the Customer's network are subject to monitoring, filtering, screening, or logging, and that to the extent required by law, such employees, vendors, contractors and other users have consented to such monitoring, filtering, screening or logging (which may include, where sufficient at law, implied consent). Customer is responsible for compliance with the laws and regulations applicable to such monitoring, filtering, screening or logging of network communications performed on its behalf by CenturyLink in any jurisdiction in which the Customer utilizes the Service, which may include prior consulting and informing of employee representative and regulatory registrations, such as with any relevant data protection authority (an "Authority"). CenturyLink will rely on this representation as evidence that all users of Customer's network have been made aware of such monitoring, filtering, screening or logging.
- (l) The parties agree that Service may not be ordered or provided outside of the United States.

2.9 Administrative Access. CenturyLink will exclusively maintain global administrative access to NBS platform at all times. CenturyLink maintains the root password for all security functions. All remote CenturyLink administration functions occur via an encrypted session. The Customer Administrator will only have administrative access to portions of Service relating to Customer's instance of Service. "Customer Administrator" means up to three designated Customer contacts that have relevant experience and expertise in Customer's network operations and the authority to access or modify content via the Web portal.

NETWORK-BASED SECURITY SERVICE EXHIBIT

2.10 Ongoing Management, Monitoring, and Reporting. CenturyLink performs ongoing management, monitoring, and reporting. After NBS is installed on Customer's network, change requests are processed as set forth in the applicable support level that Customer has selected. Requests must be initiated by an approved Customer Administrator and will be submitted via the NBS Web portal or by calling the CenturyLink security operations center.

2.11 Consent to Access and Use Customer Information. Customer authorizes CenturyLink or its authorized vendor to access and use Customer's information associated with Customer's IP-network traffic (including content) from domestic locations and, if used, from international locations to provide NBS. Customer is responsible for complying with all laws and regulations in connection with its use of the Services, including, but not limited to: (a) with respect to personally identifiable information sent or received by Customer or its End Users, all privacy laws and regulations and (b) when traffic from an international location will sent to the NBS platform, advising End Users that their content or personal information is being transferred outside an international location and receiving any required consents. Additional requirements regarding Customer consent related to use of the Service in the EU will be provided at the time Customer places an order for such Service.

2.12 Data Compilation. Customer consents to CenturyLink's use of deep packet inspection methods to collect, gather and compile security event log data to look at trends, real or potential threats, and in order to provide and improve Service. CenturyLink may compile or otherwise combine this security event log data with similar data of other customers so long as such data is compiled or combined in a manner that will not in any way reveal the data as being attributable to Customer. Aggregated data may be used to market and communicate to customers or shared to assist in mitigating suspected cybersecurity incidences. Customer specific data will not be shared without Customer's consent unless otherwise required by law. CenturyLink may retain security event log data for as long as necessary or useful for its uses consistent with this Service Exhibit and with no obligation to provide to Customer beyond the retention periods outlined in the Support Levels section. Additional requirements regarding Customer consent related to use of the Service in the EU will be provided at the time Customer places an order for such Service.

2.13 Excluded Services. CenturyLink is not responsible for any services, systems, software or equipment Customer uses with NBS. CenturyLink will not: (a) debug problems on, or configure any internal or external hosts or networks (examples include, but are not limited to the following: routers, DNS servers, mail servers, WWW servers, and FTP servers); and (b) act as an end-user help desk to Customer's employees or End Users. All communication regarding the NBS will be between CenturyLink and Customer's approved Customer Administrator only.

3. Charges. Customer must pay all applicable MRCs and NRCs set forth in the attached pricing attachment or offer attachment. All charges are in U.S. dollars unless otherwise stated. Charges will commence within five days after the date CenturyLink notifies Customer that Service is provisioned and ready for use ("Start of Service Date"). The rates set forth in the applicable pricing attachment or offer attachment will be used to calculate Contributory Charges. Taxes are based on the location of the CenturyLink network location from where NBS is provisioned. Customer understands that Service is provided from a CenturyLink-designated POP or data center in CenturyLink's network and in certain circumstances, CenturyLink may find it necessary to relocate Service to another POP or data center in a different network location. Customer acknowledges that as a result of a relocation to a new Service location, the tax portion of Customer's bill could change to reflect Taxes based on the new location from which CenturyLink provides Service.

4. Term; Cancellation. The term for each new NBS Service instance will begin on the Start of Service Date and will continue for the number of months remaining in the Term of the Agreement ("Service Term"). A Service instance means a Service combination that includes a security type, a support level and a security bandwidth. Customer may increase the security bandwidth, security type and/or support level of a Service instance at any time without restarting the Service Term. Customer may also decrease a Service instance's security bandwidth one time per 12-month period (as measured from the Start of Service Date) without restarting the Service Term. Should CenturyLink continue to provide Service after the expiration of the Service Term, Service will continue on a month-to-month basis unless either party elects to cancel the Service by providing 30 days prior written notice of such cancellation to the other party. Cancellation of Service will be in accordance with the terms and conditions set forth in Section 7 of the Participating Addendum.

5. E-mail Notification. Customer acknowledges and agrees that CenturyLink may contact Customer via e-mail at the e-mail address provided to CenturyLink when Customer ordered the Service for any reason relating to the Service, including for purposes of providing Customer any notices required under the Agreement. Customer agrees to provide CenturyLink with any change to its e-mail address.

6. SLA. Service is subject to the Network-Based Security service level agreement ("SLA"), located in Attachment E of the Participating Addendum. For Customer's claims related to Service deficiencies, interruptions or failures, Customer's exclusive remedies are limited to those remedies set forth in the applicable SLA.

7. AUP. All use of the Services must comply with the AUP as incorporated in Attachment C of the Participating Addendum.

**CENTURYLINK IQ® NETWORKING
RETAIL SERVICE LEVEL AGREEMENT**

(not applicable to services offered under the CenturyLink Wholesale and Enhanced Services Agreements)

This Service Level Agreement ("SLA") is effective as of the first day of the second month after initial installation of Services. "Service" includes the applicable components of CenturyLink IQ Networking Service and Dedicated Hosting Collocation Service. This SLA applies to Service ordered by CenturyLink's customer pursuant to an agreement ("Agreement") with CenturyLink Communications, LLC f/k/a Qwest Communications Company, LLC d/b/a CenturyLink QCC ("CenturyLink"). On April 1, 2014, Qwest Communications Company, LLC completed a name change to CenturyLink Communications, LLC. References in supporting agreements or other documents, to Qwest Communications Company, LLC or its predecessors are replaced with "CenturyLink Communications, LLC." For Customer's claims related to Service deficiencies, interruptions or failures, Customer's exclusive remedies are limited to those remedies set forth in this SLA.

1. Network and Port Components.

1.1 Components. The SLA Goal measurement includes: (a) all network components of the CenturyLink IP network; (b) all network components of the CenturyLink ATM and Frame Relay networks as incorporated into the Service; and (c) CenturyLink Provided Access for the domestic Network Availability and Installation goals only. The CenturyLink IP, ATM, and Frame Relay networks include routers, switches, fiber and any other facilities that are owned by CenturyLink or other providers specifically designated by CenturyLink for international IP service ("International Service Providers"). As defined in this SLA, a "POP" means a CenturyLink point of presence location, as determined by CenturyLink, that represents the provider edge of the CenturyLink IP, ATM or Frame Relay network or an International Service Provider POP. "CenturyLink Provided Access" means local backbone access circuits in the continental U.S. (a) ordered and leased by CenturyLink from another carrier on Customer's behalf; or (b) provided solely on CenturyLink owned and operated facilities. This includes Special Access, Ethernet Local Access, Frame Partner Access, and ATM Partner Access technologies, as defined in the Local Access Service Exhibit. "Affected Service" means the particular CenturyLink IQ Networking Port that fails to meet the applicable Goal.

1.2 Regions. A list of international regions (including Customer Service Center support information) and corresponding Tiers is appended to this SLA as Attachment 1, located at <http://www.centurylink.com/legal>.

Domestic Regions	SLA Components:
Intra U.S.	The CenturyLink IP network within the 48 contiguous U.S. states
Hawaii to U.S. West Coast ("Hawaii")	CenturyLink Trans-Hawaii IP network to the continental U.S. CenturyLink IP network in the Los Angeles Metro Area
Alaska to U.S. Pacific Northwest ("Alaska")	CenturyLink Trans-Alaska IP network to the continental U.S. CenturyLink IP network in the Seattle Metro Area

2. Goals.

2.1 Domestic Network and Port-Related Goals. The following domestic service level goals ("Goals") apply to Internet Ports, Private Ports, and Enhanced Ports (collectively, "CenturyLink IQ Networking Ports") purchased from CenturyLink pursuant to an agreement. If a Bandwidth Tier applies, Goals for CenturyLink IQ Networking Ports only apply to the portion of traffic that is within the contracted Bandwidth Tier and will not apply to the CenturyLink IQ Networking Port bandwidth usage that exceeds the Bandwidth Tier. The Goals associated with Latency, Packet Delivery, Jitter, and Black Hole Filtering are measured using monthly averages from the CenturyLink IP network and apply in the listed regions after the ports have been accepted for use. Individual circuit outages of MLPPP (NxDS1) bundles are not subject to the Network Availability or Reporting Goals. International Goals for Availability, Latency, Packet Delivery, and Jitter are appended to this SLA in Attachment 1.

(a) Network Availability. The availability of the Service ("Network Availability") is measured by "Network Downtime," which exists when a particular CenturyLink IQ Networking Port of Customer is unable to transmit and receive data. Network Downtime is measured from the time a trouble ticket is opened by CenturyLink in the CenturyLink trouble management system to the time the affected CenturyLink IQ Networking Port is again able to transmit and receive data. Network Availability for ports with Frame Partner Access or ATM Partner Access is only applicable if Customer provides ready access to associated routers for monitoring purposes.

Region	Goal	Remedy (Credit is applied to MRC of the Affected Service)*
Intra U.S. Hawaii Alaska	100%	Each cumulative hour of Network Downtime qualifies Customer for a credit of one day's charges pro-rated from the MRC.

(b) Latency. The average network transit delay ("Latency") will be measured via roundtrip pings on an ongoing basis every five minutes to determine a consistent average monthly performance level for Latency at all the POPs within the region. Latency is calculated as follows:

$$\frac{\sum (\text{Roundtrip Delay for POP-POP trunks})}{\text{Total Number of POP-POP trunks}} = \text{Latency}$$

Region	Goal	Remedy (Credit is applied as a % of the MRC for the Affected Service)*		
North America				
Intra U.S.	42 ms	43 – 60 ms = 10%	61 – 80 ms = 25%	Greater than 80 ms = 50%
Hawaii Alaska	75 ms	76 – 95 ms = 10%	96 - 120 ms = 25%	Greater than 120 ms = 50%

*subject to requirements and limitations in Section 4

**CENTURYLINK IQ® NETWORKING
RETAIL SERVICE LEVEL AGREEMENT**

(c) Packet Delivery. Packet Delivery will be measured on an ongoing basis every five minutes to determine a consistent average monthly performance level for packets actually delivered between the POPs.

Region	Goal	Remedy (Credit is applied as a % of the MRC for the Affected Service)*		
Intra U.S. Hawaii Alaska	99.90%	99.01 % - 99.89% = 10%	90% - 99% = 25%	Less than 90% = 50%

(d) Jitter. Jitter is a measurement of the interpacket delay variance and packet loss in the CenturyLink IP network, which is measured by generating synthetic user datagram protocol (UDP) traffic. This Goal does not apply if the Internet Port is used in conjunction with DDoS Mitigation Service.

Region	Goal	Remedy (Credit is applied as a % of the MRC for the Affected Service)*		
Intra U.S.	2 ms	2.1 – 3 ms = 10%	3.1 – 4 ms = 25%	Greater than 4 ms = 50%
Hawaii Alaska	4 ms	4.1 – 5 ms = 10%	5.1 – 6 ms = 25%	Greater than 6 ms = 50%

(e) Reporting. The Reporting Goal is measured from the time a Network Downtime trouble ticket is opened to the time CenturyLink reports the Network Downtime to Customer by the agreed upon notification method. This Goal does not apply to Ports that use Ethernet Local Access.

Region	Goal	Remedy (Credit is applied to MRC of the Affected Service)*
Intra U.S. Hawaii Alaska	10 minutes	Each failure to meet the Goal qualifies Customer for a credit of one day's charges pro-rated from the MRC, at a maximum of one such credit accrued per day.

(f) Installation. The Installation Goal measures the installation times for CenturyLink Provided Access ordered in conjunction with CenturyLink IQ Networking Ports only. The Installation Goal only applies if there are existing CenturyLink facilities in the location that supports the Affected Service. Installation is measured from the date CenturyLink Engineering accepts the CenturyLink Provided Access order. If Customer has a designated Key Port, the applicable Installation Goal shown below will apply to that Key Port, and the installation of related non-Key Ports will occur the later of: (i) within 10 business days after that Key Port's Start of Service Date; or (ii) within the normal Installation Goal for that Port, as measured from the date CenturyLink Engineering accepts the order. If no Key Port is designated, CenturyLink will follow normal installation intervals without special sequencing.

Region	Goal	Remedy (Credit is applied to MRC of the Affected Service)*
Intra U.S.	DS-1 22 business days	Each failure to meet the Goal qualifies Customer for a credit of one day's charges pro-rated from the MRC for each day beyond the applicable Goal until the CenturyLink Provided Access is installed, for a maximum of 15 days' charges.
	DS-3 OC-3 OC-12 33 business days	
	Ethernet 10 – 1000 Mbps 66 business days	
Hawaii Alaska	DS-1 22 business days	Each failure to meet the Goal qualifies Customer for a credit of one day's charges pro-rated from the MRC for each day beyond the applicable Goal until the CenturyLink Provided Access is installed, for a maximum of 15 days' charges.
	DS-3 OC-3 OC-12 43 business days	

(g) Black Hole Filtering. Once a suspected Distributed Denial of Service ("D/DoS") attack is determined to be valid, the Black Hole Filtering Goal is measured from the time CenturyLink receives permission and all necessary information from Customer to implement a null-route and the actual placement of a null-route on the affected destination IP address. The Black Hole Filtering Goal is only applicable to Internet Ports and the Internet Port portion of Enhanced Ports.

Region	Goal	Remedy (Credit is applied to MRC of the Affected Service)*
Intra U.S. Hawaii Alaska	15 minutes	Failure to implement a null routing within the Goal qualifies Customer for one day's charges pro-rated from the MRC of the Port of the Affected Service, up to a maximum of one such credit accrued per day.

3. Maintenance.

3.1 Network Normal Maintenance. "Normal Maintenance" means upgrades of hardware or software or upgrades to increase capacity. Normal Maintenance may temporarily degrade the quality of the Service, including possible outages. "Local Time" means the local time in the time zone in which an Affected Service is located. CenturyLink may change the maintenance window times upon posting to the website or other notice to Customer. CenturyLink will undertake Normal Maintenance during the hours and upon the prior notice time period stated below. International Maintenance hours are located in Attachment 1 to this SLA.

Region	Normal Maintenance Hours	Prior Notice
Intra U.S. Hawaii Alaska	Sunday, Tuesday, and Thursday mornings between the hours of 12:00 AM and 6:00 AM Local Time	10 business days

3.2 Network Urgent Maintenance. "Urgent Maintenance" means efforts to correct network conditions that are likely to cause a material Service outage and that require immediate action. Urgent Maintenance may degrade the quality of the Services, including possible outages. Such effects related to Urgent Maintenance will entitle Customer to service credits as set forth in this SLA. CenturyLink may undertake Urgent Maintenance at any time deemed necessary and will provide notice of Urgent Maintenance to Customer as soon as is commercially practicable under the circumstances.

*subject to requirements and limitations in Section 4

**CENTURYLINK IQ® NETWORKING
RETAIL SERVICE LEVEL AGREEMENT**

4. General.

4.1 Remedies. To be eligible for service credits, Customer must be in good standing with CenturyLink and current in its obligations. To receive service credits, Customer must contact the Customer Service Center at 1-800-860-1020 and submit the relevant trouble ticket information within 30 calendar days from the date when the relevant SLA Goal was not met. CenturyLink will determine the credits provided to Customer by applying the applicable remedies set forth in this SLA. A credit will be applied only to the month in which the event giving rise to the credit occurred. The credits will apply to the MRCs of the Affected Service after application of all discounts and do not apply to MRCs of other services, including but not limited to CenturyLink Provided Access. The maximum service credits for CenturyLink IQ Networking Service or Dedicated Hosting Collocation Service issued in any one calendar month will not exceed: (a) for Goals related to Network Availability, Reporting, Installation, and Black Hole Filtering, seven days' charges pro-rated from the MRC of the Affected Service; or (b) for Goals not listed in (a), 50% of the MRCs of the Affected Service less any credits calculated under (a). In no event will the total credit, in the aggregate for all credits issued in one month for CenturyLink IQ Networking Service or Dedicated Hosting Collocation Service exceed the equivalent of 50% of the relevant MRCs for the Affected Service. Cumulative credits in any one month must exceed \$25.00 to be processed. If Customer fails to notify CenturyLink in the manner set forth above with respect to the applicable SLA credits, Customer will have waived its right to such SLA credits for that month.

4.2 Limitations. This SLA will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under this SLA, for any event that adversely impacts the Service that is caused by: (a) the acts or omissions of Customer, its employees, contractors or agents or its end users; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink or its International Service Providers; (c) Force Majeure Events; (d) scheduled service maintenance, alteration or implementation; (e) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information; (f) CenturyLink's lack of access to the Customer premises where reasonably required to restore the Service; (g) Customer's failure to release the Service for testing or repair and continuing to use the Service on an impaired basis; (h) CenturyLink's termination of Service for Cause or Customer's use of Service in an unauthorized or unlawful manner; or (i) improper or inaccurate network specifications provided by Customer.

4.3 Customer Termination Rights. In the Intra U.S., Hawaii, and Alaska regions, Customer may terminate the Affected Service without Cancellation Charges if, in any single calendar month: (a) Network Downtime exists for at least 24 hours in the aggregate; or (b) Network Downtime exists for a period of at least eight consecutive hours. Customer may terminate the Affected Service by providing written notice to the Customer Service Center with a courtesy copy to the attention of CenturyLink's General Counsel within 20 days after either one of the Network Downtime events described in subsections (a) or (b) above occur. Such termination will be effective 45 days after receipt of written notice by CenturyLink. For all other regions, Customer may terminate the Affected Service without early termination charges if CenturyLink is unable to restore the Affected Service to meet the Goals herein within a 60 day cure period. The 60 day cure period will begin after a trouble ticket is opened. Customer may terminate the Affected Service by providing written notice to the Customer Service Center with a courtesy copy to the attention of CenturyLink's General Counsel within 20 days after the 60 day cure period ends. Such termination will be effective upon receipt of written notice by CenturyLink of termination from Customer, unless Customer requests Service to be continued during a transition period and establishes a new termination date. Customer is responsible for all Service charges until the termination date. If Customer fails to notify CenturyLink in the manner set forth in this section with respect to the applicable termination right, Customer will have waived its right to terminate the Affected Service.

**CENTURYLINK ON-NET LOCAL ACCESS
SERVICE LEVEL AGREEMENT**

(not applicable to services offered under the CenturyLink Wholesale and Enhanced Services Agreements)

This Service Level Agreement ("SLA") applies to On-Net Access circuits ("Service") ordered by CenturyLink's customer ("Customer") pursuant to a signed agreement ("Agreement") with CenturyLink Communications, LLC f/k/a Qwest Communications Company, LLC d/b/a CenturyLink QCC ("CenturyLink"). On April 1, 2014, Qwest Communications Company, LLC completed a name change to CenturyLink Communications, LLC. References in supporting agreements or other documents, to Qwest Communications Company, LLC or its predecessors are replaced with "CenturyLink Communications, LLC." Service terminates at the Service Address's common telecommunications facility or meet-me point. This SLA does not apply to local access circuits that are provided by another carrier.

1. Definitions

"Calendar Month" refers to the period beginning at 12:00 midnight on the first day of a month and ending at 11:59 PM on the last day of that month.

"CenturyLink Domestic Network" is the network located within those areas in the 48 contiguous United States of America and District of Columbia where CenturyLink is legally permitted to provide Service to Customer and is comprised only of CenturyLink facilities.

"On-Net Access" means a Special Access (excluding DS0), Ethernet Local Access or Wavelength Local Access circuit provided solely on facilities owned and operated by CenturyLink Communications, LLC.

"Service Address" is the building where Customer receives Service. Only a building that is classified by CenturyLink as a business address can be a Service Address.

2. Availability Objective

CenturyLink offers the following SLA for Service with a minimum one year Service term. The SLA is effective as of the first day of the second month after initial installation and Customer acceptance of Service.

Customer will, subject to the terms, exclusions, and restrictions described in this SLA, be entitled to receive from CenturyLink a credit if the availability of a particular circuit ("Circuit Availability") for any Calendar Month falls below the percentage shown in the applicable credit schedule included in this section. CenturyLink guarantees the Circuit Availability only to the point to which CenturyLink can perform remote loop back testing, even if the demarcation point extends past such point. Service will for purposes of this document be deemed to be unavailable to Customer only if the circuit ("Affected Circuit") is subject to an interruption (other than as noted in this SLA) that results in the total disruption of the Service ("Outage").

The credit ("Outage Credit") to which Customer may be entitled under this section will be equal to the applicable credit percentage identified in the table below of Customer's monthly recurring charges ("MRCs") for the Affected Circuit after application of any credits or discounts ("Eligible Circuit Charges"). The Outage Credit will not include credits on any other MRCs charged to Customer for any other service.

Circuit Availability Percentage is calculated as follows:

$$\left[\frac{(\text{Applicable Days in Calendar Month} \times 24 \times 60) - (\text{Minutes of Outage on Affected Circuit in Calendar Month})}{(\text{Applicable Days in Calendar Month} \times 24 \times 60)} \right] \times 100$$

For purposes of measuring Customer's Circuit Availability, the CenturyLink Trouble Management System determines the number of minutes of an Outage. An Outage will be deemed to commence upon verifiable notification thereof by Customer to the CenturyLink Trouble Management System, and CenturyLink's issuance of a trouble ticket. An Outage will conclude upon the restoration of the Affected Circuit as evidenced by the appropriate network tests conducted by CenturyLink.

Credit Schedule for Service		
Circuit Availability		Amount of Credit (as a % of the Eligible Circuit Charges for the Affected Circuit)
Upper Level	Lower Level	
100%	99.999%	0%
< 99.999%	99.99%	5%
< 99.99%	99.9%	10%
< 99.9%	99.5%	25%
< 99.5%	0%	50%

Subject to the terms, exclusions and restrictions described in this SLA, in the event Customer experiences chronic Outages with respect to any circuit, Customer will be entitled to terminate the Affected Circuit. A circuit suffers from chronic Outages if such circuit, measured over any Calendar Month, experiences more than five Outages, or more than 48 aggregate hours of Outages. Customer may as its sole and exclusive remedy for chronic Outages, upon 30 days' prior written notice to CenturyLink, terminate the Affected Circuit without incurring any early termination charges associated with that Affected Circuit except for all usage charges accrued to the date of termination. Customer must exercise any termination right available to it under this section within 30 days after Customer first becomes

**CENTURYLINK ON-NET LOCAL ACCESS
SERVICE LEVEL AGREEMENT**

(not applicable to services offered under the CenturyLink Wholesale and Enhanced Services Agreements)

eligible to exercise the termination right. In the event Customer fails to comply with the condition set forth in the immediately preceding sentence, Customer will, with respect to the termination right, have waived its right to such termination right.

3. Terms and Conditions

CenturyLink is offering Service in accordance with the CenturyLink Rate and Services Schedule and the applicable CenturyLink agreement. In the event of a conflict between the terms of this document and the Rate and Services Schedule or applicable CenturyLink agreement, the terms of this document will control.

To be eligible for an Outage Credit under this SLA, Customer must, in addition to complying with the other terms included in this SLA, (i) be in good standing with CenturyLink and current in their obligations, other than those invoices that are recognized as being in dispute, and (ii) submit necessary supporting documentation and request reimbursement or credits hereunder within 30 days of the Outage resolution. In the event Customer fails to comply with the condition set forth in the immediately preceding sentence, Customer will, with respect to that remedy, have waived its right to such remedy.

CenturyLink will determine the Outage Credits provided to Customer by totaling the eligible Outage minutes throughout the Calendar Month on an Affected Circuit, subject to the restrictions and exclusions in this SLA. Outage Credits for any Calendar Month must exceed \$25.00 to be processed. In no case will CenturyLink provide credit to Customer for an Affected Circuit that exceeds the monthly recurring charge or the stated applicable maximum credit percentage. Customer may receive Outage Credits for a particular Affected Circuit for a maximum of four months in any 12 month period.

CenturyLink will give notice to Customer of any scheduled maintenance as early as is practicable and a scheduled outage will under no circumstances be viewed as an Outage hereunder.

The remedies included in this SLA are Customer's sole and exclusive remedies for disruption of Service and will apply in lieu of any other Service interruption guarantee or credit, outage guarantee or credit or performance credit for which Customer might have otherwise been eligible. If Customer receives an Outage Credit, Customer is not entitled to receive any other credit that may be available under the local access service provided or ordered by CenturyLink on behalf of Customer for the Affected Circuit in that Calendar Month.

Except as provided in this SLA, the objectives and related remedies set forth herein will not apply to CenturyLink services other than the Service.

4. Restrictions and Exclusions

An Outage will not be deemed to have occurred in the event that the Service is unavailable or impaired due to any of the following:

- (a) Interruptions on a circuit that is not an "Accepted Circuit" where an Accepted Circuit is one that CenturyLink and Customer have tested and mutually agree is working as ordered following provisioning of an order or change order;
- (b) Interruptions caused by the negligence, error or omission of Customer or others authorized by Customer to use or modify Service;
- (c) Interruptions due to failure of power at Customer premises or failure or poor performance of Customer's premises equipment;
- (d) Interruptions during any period in which CenturyLink or its agents are not afforded access to the premises where Service is terminated, provided such access is reasonably necessary to prevent a degradation or to restore Service;
- (e) Interruptions during any period when CenturyLink has posted on the CenturyLink Web site or communicated to Customer in any other manner that Customer's Service will be unavailable for maintenance or rearrangement purposes, or Customer has released Service to CenturyLink for the installation of a customer service order;
- (f) Interruptions during any period when Customer elects not to release the circuit for testing and/or repair and continues to use it on an impaired basis;
- (g) Interruptions resulting from force majeure events beyond the reasonable control of CenturyLink including, but not limited to, acts of God, government regulation, labor strikes, national emergency or war (declared or undeclared);
- (h) Interruptions resulting from Customer's use of Service in an unauthorized or unlawful manner;
- (i) Interruptions resulting from a CenturyLink disconnect for Customer's breach of a term set forth in the Agreement pursuant to which CenturyLink is providing Service to Customer;
- (j) Interruptions resulting from incorrect, incomplete or inaccurate orders from Customer;
- (k) Interruptions due to improper or inaccurate network specifications provided by Customer;
- (l) Interruptions resulting from a failure of a carrier other than CenturyLink providing local access circuits; or
- (m) Special configurations of the Service that have been mutually agreed to by CenturyLink and Customer; provided, however, CenturyLink may provide a separate service level agreement to Customer for those special configurations.

**CENTURYLINK HYBRID SD-WAN BUNDLES
RETAIL SERVICE LEVEL AGREEMENT**

(not applicable to services offered under the CenturyLink Wholesale and Enhanced Services Agreements)

This SLA applies to CenturyLink Hybrid SD-WAN Bundles ordered by CenturyLink's customer ("Customer") pursuant to an agreement ("Agreement") with CenturyLink Communications, LLC f/k/a Qwest Communications Company, LLC d/b/a CenturyLink QCC ("CenturyLink"). On April 1, 2014, Qwest Communications Company, LLC completed a name change to CenturyLink Communications, LLC. References in supporting agreements or other documents, to Qwest Communications Company, LLC or its predecessors are replaced with "CenturyLink Communications, LLC." Capitalized terms not in this SLA are defined in the Agreement. The SLA is effective as of the first day of the second month after initial Service activation and continues through the Service Term because SLA measurement begins after Service activation. For Customer's claims related to Service deficiencies, interruptions or failures, Customer's exclusive remedies are limited to those remedies set forth in this SLA.

1. Definitions

Affected Service. Affected Service is the particular CenturyLink Hybrid SD-WAN Bundle Package at a particular site that fails to meet the applicable SLS or SLO.

CenturyLink IQ Networking Ports. CenturyLink IQ Networking Ports are Private Ports for the purposes of this SLA.

CenturyLink Provided Access. CenturyLink Provided Access means local backbone access circuits in the continental U.S. (a) ordered and leased by CenturyLink from another carrier on Customer's behalf. This includes Ethernet Local Access, as defined in the Local Access Service Exhibit.

Chronic Outage. A Chronic Outage is deemed to have occurred if Network Downtime exists for at least 24 hours in the aggregate over any single calendar month for the Silver and Gold Packages; or if Network Downtime exists for both transport options (CenturyLink IQ Networking and Delta Port Internet Connection) under the Silver and Gold Packages for a period of at least six consecutive hours.

Cut-off Time. Cut-off Time is the time CPE replacement must be identified to be eligible for next business day replacement. 8x5 next business day replacement must be identified by 2 p.m. MT during regular business hours (Monday-Friday, excluding holidays).

Delta Port Internet Connection. Delta Port Internet Connection means local Internet broadband in the domestic U.S. provided by CenturyLink and provisioned by a third-party broadband carrier.

Jitter. Jitter is a measurement of the interpacket delay variance and packet loss in the CenturyLink IP network, which is measured by generating synthetic user datagram protocol (UDP) traffic.

Latency. Latency is the average network transit delay measured via roundtrip pings on an ongoing basis.

Local Time. Local Time means the local time in the time zone in which an Affected Service is located.

MTTR. Mean Time to Repair ("MTTR") is measured by calculating the average time for CenturyLink to repair or restore Service within a given Calendar Month after a qualified trouble ticket has been submitted. A qualified trouble ticket opened by Customer must provide adequate information for CenturyLink to begin the troubleshooting process. If the trouble ticket does not provide adequate information for CenturyLink to begin troubleshooting, CenturyLink will attempt to contact the primary Customer contact to obtain the necessary information to begin troubleshooting. MTTR calculation is listed below.

NBD. NBD means Next Business Day.

Network Availability. Network Availability of the Service is measured by "Network Downtime," which exists when a particular Service is unable to transmit and/or receive Service.

Network Downtime. Network Downtime of the Service is measured from the time a trouble ticket is opened by either CenturyLink or Customer in the CenturyLink trouble management system to the time the Affected Service is again able to transmit and receive Service

Normal Maintenance. Normal Maintenance means upgrades of hardware or software or upgrades to increase capacity of CenturyLink IQ Networking or SD-WAN software capability

Outage. An Outage of the Service begins from Customer verifiable notification to the CenturyLink trouble management system, and CenturyLink's issuance of a trouble ticket. An Outage will conclude upon the restoration of the Service as evidenced by the appropriate network tests conducted by CenturyLink.

Packet Delivery. Packet Delivery is a measurement for packets actually delivered between POPs.

Point of Contact (POC). A person, group of people, or help desk provided to CenturyLink by Customer to serve as the central point of contact for all information exchanged with CenturyLink necessary to troubleshoot or facilitate the Service.

Point of Presence (POP). POP means a CenturyLink point of presence location, as determined by CenturyLink, that represents the provider edge of the CenturyLink IP network.

SD-WAN CPE. SD-WAN CPE is the CenturyLink provided appliance included with the CenturyLink Hybrid SD-WAN Bundles upon which SD-WAN software has been configured.

Service. Service includes the applicable components of CenturyLink Hybrid SD-WAN Bundles.

Service Level Standard (SLS). Service Level Standard is a contractual Service commitment that CenturyLink provides the Customer and has an associated monetary credit if unmet.

**CENTURYLINK HYBRID SD-WAN BUNDLES
RETAIL SERVICE LEVEL AGREEMENT**

Service Level Objective (SLO). Service Level Objective is a goal or target indicating a best-effort time to rectify a Service disruption within a specific time frame. SLOs do not have associated monetary credits if unmet.

Urgent Maintenance. Urgent Maintenance means efforts to correct network conditions that are likely to cause a material Service Outage and that require immediate action.

1.2 Regions.

Domestic Regions	SLA Components:
Intra U.S.	The CenturyLink IP network within the 48 contiguous U.S. states
Hawaii to U.S. West Coast ("Hawaii")	CenturyLink Trans-Hawaii IP network to the continental U.S. CenturyLink IP network in the Los Angeles Metro Area
Alaska to U.S. Pacific Northwest ("Alaska")	CenturyLink Trans-Alaska IP network to the continental U.S. CenturyLink IP network in the Seattle Metro Area

2. Service Components. Each SLS or SLO applies only to the CenturyLink Hybrid SD-WAN Bundle package types specifically set forth in the corresponding Section below. Each SLS or SLO includes only those components of the bundles specifically defined in Section 3 below.

3. SLS Measurements and Remedies.

3.1 Domestic Network and Port-Related SLSS. The following domestic service level SLSSs apply to Private Ports, ("CenturyLink IQ Networking Ports") purchased from CenturyLink pursuant to an agreement. SLSSs for CenturyLink IQ Networking Ports only apply to the portion of traffic that is within the contracted bandwidth and will not apply to the CenturyLink IQ Networking Port bandwidth usage that exceeds the contracted bandwidth. The SLSSs associated with Latency, Packet Delivery, and Jitter are measured using monthly averages from CenturyLink IP network and apply in the listed regions after the ports have been accepted for use and only on the CenturyLink IQ Networking portion of the service for the CenturyLink Hybrid SD-WAN Silver and Gold Packages.

(a) Network Availability. Network Availability applies to the Hybrid SD-WAN Silver and Gold Packages only. Network Availability is measured by Network Downtime. If Customer is unable to use Service on a Hybrid SD-WAN Gold Package due to a failure in both of the CenturyLink SD-WAN CPE, Customer will be eligible for the SLS and remedy until replacement SD-WAN CPE reaches the Affected Service site. If Customer is unable to use Service on a CenturyLink Hybrid SD-WAN Gold Package due to a failure of both of their SD-WAN CPE, the Hardware Replacement SLR will not apply. If the issue is isolated to one SD-WAN CPE on a Gold or Silver Package, Customer will only be eligible for Hardware Replacement SLS.

Region	SLS	Remedy (Credit is applied to MRC of the Affected Service)*
Intra U.S. Hawaii Alaska	100%	Silver & Gold Packages: Each cumulative hour of Network Downtime qualifies Customer for a credit of two day's charges pro-rated from the MRC if both transport (CenturyLink IQ Networking and Delta Port Internet Connection) paths are unable to transmit and receive data. Gold Package: Each cumulative hour of Network Downtime qualifies Customer for a credit of two day's charges pro-rated from the MRC due to failure of both CenturyLink provided SD-WAN CPE.

(b) Latency. Latency applies to the IQ Networking portion of the Hybrid SD-WAN Silver or Gold Packages only. The average network transit delay ("Latency") will be measured via roundtrip pings on an ongoing basis every five minutes to determine a consistent average monthly performance level for Latency at all the POPs within the region. Latency is calculated as follows:

$$\frac{\sum (\text{Roundtrip Delay for POP-POP trunks})}{\text{Total Number of POP-POP trunks}} = \text{Latency}$$

Region	SLS	Remedy (Credit is applied as a % of the MRC for the Affected Service)*		
North America				
Intra U.S.	42 ms	43 – 60 ms = 10%	61 – 80 ms = 25%	Greater than 80 ms = 50%
Hawaii Alaska	75 ms	76 – 95 ms = 10%	96 - 120 ms = 25%	Greater than 120 ms = 50%

*subject to requirements and limitations in Section 5

(c) Packet Delivery. Packet Delivery applies to the IQ Networking portion of the Hybrid SD-WAN Silver or Gold Packages only. Packet Delivery will be measured on an ongoing basis every five minutes to determine a consistent average monthly performance level for packets actually delivered between the POPs.

Region	SLS	Remedy (Credit is applied as a % of the MRC for the Affected Service)*		
Intra U.S. Hawaii Alaska	99.90%	99.01 % - 99.89% = 10%	90% - 99% = 25%	Less than 90% = 50%

*subject to requirements and limitations in Section 5

(d) Jitter. Jitter applies to the IQ Networking portion of the CenturyLink Hybrid SD-WAN Silver or Gold Packages only. Jitter is a measurement of the interpacket delay variance and packet loss in the CenturyLink IP network, which is measured by generating synthetic user datagram protocol (UDP) traffic. This SLS does not apply if the Internet Port is used in conjunction with DDoS Mitigation Service.

Region	SLS	Remedy (Credit is applied as a % of the MRC for the Affected Service)*		
Intra U.S.	2 ms	2.1 – 3 ms = 10%	3.1 – 4 ms = 25%	Greater than 4 ms = 50%
Hawaii Alaska	4 ms	4.1 – 5 ms = 10%	5.1 – 6 ms = 25%	Greater than 6 ms = 50%

**CENTURYLINK HYBRID SD-WAN BUNDLES
RETAIL SERVICE LEVEL AGREEMENT**

*subject to requirements and limitations in Section 5

3.2 Hardware Replacement SLS. Hardware replacement applies to the CenturyLink-provided SD-WAN CPE. The Hardware Replacement SLS applies to all CenturyLink Hybrid SD-WAN package types. In the event that the service-impacting issue is isolated to the SD-WAN CPE, CenturyLink will drop-ship replacement hardware to the Affected Service site 8x5 NBD. 8x5 NBD replacement must be identified by the Cut-off Time to be eligible for next business day replacement. In the event the Cut-off Time is missed, the device will be replaced by the next full business day. Hardware Replacement will be measured from CenturyLink trouble ticket notation to time replacement hardware is delivered by shipper confirmation.

Region	SLS	Remedy (Credit is applied to MRC of the Affected Service)*
Intra U.S. Hawaii Alaska	8x5 NBD Replacement	Each cumulative day qualifies Customer for a credit of one day's charges pro-rated from the MRC.

*subject to requirements and limitations in Section 5

3.3 Installation SLS. The Installation SLS measures the installation times for: (a) applicable Delta Port Internet Connection and (b) CenturyLink Provided Access ordered in conjunction with CenturyLink IQ Networking Ports. The Installation SLS applies to all CenturyLink Hybrid SD-WAN Bundle package types. The Installation SLS only applies if there are existing Delta Port Internet Connection or CenturyLink facilities, as applicable, in the location that supports the Affected Service. Installation is measured from the date CenturyLink Engineering accepts the CenturyLink Provided Access order or the Delta Port Internet Connection Order, as applicable. If Customer has a designated Key Port, the applicable Installation SLS shown below will apply to that Key Port (often referred to as a hub location), and the installation of related non-Key Ports will occur the later of: (i) within 10 business days after that Key Port's Start of Service Date; or (ii) within the normal Installation Goal for that Port, as measured from the date CenturyLink Engineering accepts the order. If no Key Port is designated, CenturyLink will follow normal installation intervals without special sequencing. To be eligible for the Installation SLS, Customer's locations must be pre-qualified by CenturyLink with the applicable third-party vendors. The Installation SLS does not apply for sites that are not pre-qualified or qualified and require additional construction for installation.

Region	SLS		Remedy (Credit is applied to MRC of the Affected Service)*
Intra U.S.	Bronze Package (Delta Port Internet Connection Only)	52 business days	Each failure to meet the SLS qualifies Customer for a credit of one day's charges pro-rated from the MRC for each day beyond the applicable SLS until the Delta Port Internet Connection or CenturyLink Provided Access, as applicable, is installed, for a maximum of 15 days' charges.
	Silver or Gold Packages CPLA and Delta Port Internet Connection	66 business days	

*subject to requirements and limitations in Section 5

4. SLO Measurements. The following establish nonbinding objectives for the provision of certain features of the Service. CenturyLink reserves the right to modify these SLOs with 30 days' prior written notice.

4.1. Maintenance.

(a) Network Normal Maintenance. "Normal Maintenance" means upgrades of hardware or software or upgrades to increase capacity of CenturyLink IQ Networking or SD-WAN software capability. Normal Maintenance may temporarily degrade the quality of the Service, including possible Outages. CenturyLink may change the maintenance window times upon posting to the website or other notice to Customer. CenturyLink will undertake Normal Maintenance during the hours and upon the prior notice time period stated below.

Region	Normal Maintenance Hours	Prior Notice
Intra U.S. Hawaii Alaska	Sunday, Tuesday, and Thursday mornings between the hours of 12:00 AM and 6:00 AM Local Time	10 business days

(b) Network Urgent Maintenance. "Urgent Maintenance" means efforts to correct network conditions that are likely to cause a material Service Outage and that require immediate action. Urgent Maintenance may degrade the quality of the Services, including possible Outages. Such effects related to Urgent Maintenance will entitle Customer to service credits as set forth in this SLA. CenturyLink may undertake Urgent Maintenance at any time deemed necessary and will provide notice of Urgent Maintenance to Customer as soon as is commercially practicable under the circumstances.

4.2. Policy Change Request SLO. CenturyLink will acknowledge receipt of Customer's policy change request within two business hours of receipt by CenturyLink if placed during regular business hours (Monday-Friday, excluding holidays). This SLO applies to all CenturyLink Hybrid SD-WAN Bundle package types. This SLO is only available for policy change requests submitted by the POC in accordance with the provided procedures.

4.3. Service Request Implementation SLO. CenturyLink will provision service requests for non-billable changes, such as a configuration change, related to the SD-WAN component within the execution times set forth below. This SLO applies to the SD-WAN component of all

CENTURYLINK HYBRID SD-WAN BUNDLES
RETAIL SERVICE LEVEL AGREEMENT

CenturyLink Hybrid SD-WAN Bundle package types. CenturyLink will satisfy 95% of Customer's monthly service requests within the execution times set forth below.

Table: MACD for Network devices

Standard MACD –Hybrid SD-WAN Bundle Package	Execution Time
Bronze	2 Business Days
Silver	1 Business Day
Gold	1 Business Day

The target execution time assumes requests are placed during regular business hours (Monday-Friday, excluding holidays).

4.4 Reporting. The Reporting SLO is measured from the time a Network Downtime trouble ticket is opened to the time CenturyLink reports the Network Downtime to Customer by the agreed upon notification method.

Region	SLO
Intra U.S. Hawaii Alaska	10 minutes

4.5. MTTR. The MTTR SLO, as defined in Section 1 above, applies to all CenturyLink Hybrid SD-WAN Bundle package types.

Severity Levels	Description	SLO
High	Service not available	Less than 4 hours for On-Net** or 8 hours for Off-Net**
Medium	Service degraded performance or functionality	Less than 12 hours for On-Net** or 24 hours for Off-Net**
Low	Intermittent Issues	Less than 24 hours for On-Net** or 48 hours for Off-Net**

* subject to requirements and limitations in Section 6.

** On-net means local access network owned and operated by CenturyLink and Off-Net means a local access network not owned and operated by CenturyLink.

5. General

5.1 Remedies. To be eligible for service credits, Customer must be in good standing with CenturyLink and current in its obligations. To receive service credits, Customer must contact the Customer Service Center at 1-800-860-1020 and submit the relevant trouble ticket information within 30 calendar days from the date when the relevant SLS was not met. CenturyLink will determine the credits provided to Customer by applying the applicable remedies set forth in this SLA. A credit will be applied only to the month in which the event giving rise to the credit occurred. The credits will apply to the MRCs of the Affected Service after application of all discounts and do not apply to MRCs of other services including but not limited to CenturyLink Provided Access. The maximum service credits for CenturyLink Hybrid SD-WAN Bundle Service issued in any one calendar month will not exceed: (a) for SLSs related to Network Availability and Installation, seven days' charges pro-rated from the MRC of the Affected Service; or (b) for SLSs not listed in (a), 50% of the MRC(s) of the Affected Service less any credits calculated under (a). In no event will the total credit, in the aggregate for all credits issued in one month for CenturyLink Hybrid SD-WAN Bundle Service exceed the equivalent of 50% of the relevant MRC(s) for the Affected Service. Cumulative credits in any one month must exceed \$25.00 to be processed. If Customer fails to notify CenturyLink in the manner set forth above with respect to the applicable SLS credits, Customer will have waived its right to such SLS credits for that month. CenturyLink Hybrid SD-WAN Bundle SLSs cannot be combined with any other SLSs that may be related to any of the individual underlying components of the overall bundle.

5.2 Limitations. This SLA will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under this SLA, for any event that adversely impacts the Service that is caused by: (a) the acts or omissions of Customer, its employees, contractors or agents or its end users; (b) the failure or malfunction of equipment, applications or systems not owned, managed, or controlled by CenturyLink; (c) Force Majeure Events; (d) Normal Maintenance, scheduled alteration, or implementation; (e) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information; or (f) CenturyLink's lack of access to the Customer premises where reasonably required to restore the Service; (g) Customer's failure to release the Service for testing or repair and continuing to use the Service on an impaired basis; (h) Customer's failure to comply with all manufacturer environmental requirements; (i) CenturyLink's termination of Service for Cause or Customer's use of Service in an unauthorized or unlawful manner; or (j) improper or inaccurate network specifications provided by Customer. Customer must use all components of the CenturyLink Hybrid SD-WAN Bundle Packages in order to be eligible for the SLAs and SLOs described herein.

5.3 Customer Termination Rights. Customer may terminate the Affected Service without Cancellation Charges if Customer experiences a Chronic Outage in any single calendar month. Customer may only terminate the Affected Service by providing written notice to CenturyLink within 20 days after Customer first becomes eligible to exercise the applicable termination right. Such termination will be effective 45 days after receipt of written notice by CenturyLink. Customer is responsible for all Service charges until the termination date. If Customer fails to notify CenturyLink in the manner set forth in this section with respect to the applicable termination right, Customer will have waived its right to terminate the Affected Service.

**DDOS MITIGATION SERVICE
RETAIL SERVICE LEVEL AGREEMENT**

(not applicable to services offered under the CenturyLink Wholesale and Enhanced Services Agreements)

This Service Level Agreement ("SLA") applies to DDoS Mitigation Service ("Service" or "DDoS") ordered by customers pursuant to an agreement ("Agreement") between the specific customer ("Customer") and CenturyLink and its affiliates ("CenturyLink"). Capitalized terms not defined in this SLA are defined in the Agreement between the specific Customer and CenturyLink. For Customer's claims related to Service deficiencies, interruptions or failures, Customer's exclusive remedies are limited to those remedies set forth in this SLA. The SLA is effective as of the first day of the second month after initial installation of DDoS.

1. Goals. The following service level goals ("Goals") apply to DDoS Mitigation Service, excluding DDoS Appliance Services which are provided on an as available basis with no applicable SLA. Customer will be eligible to receive from CenturyLink a credit subject to the terms, exclusions, and restrictions described in this SLA. DDoS Mitigation SLA times are based on information in the CenturyLink trouble ticketing system.

(a) Time to Notify. The Time to Notify Goal is measured from the time an Incident is detected by a system-generated alarm ("Initial DDoS Alarm") to when CenturyLink attempts to verbally notify Customer of the Incident. Customer may request CenturyLink to notify Customer through either a phone call or e-mail. A phone call notification is available for high priority alerts. E-mail notification is available for low, medium and high priority alerts. The Time to Notify Goal applies only to DDoS Mitigation on Qualifying Internet Services, excluding Reactive DDoS Services.

(b) Time to Mitigate. If Customer has provided all the necessary information to initiate Mitigation, the Time to Mitigate Goal is measured from Customer Approval to the actual initiation of Mitigation. "Customer Approval" means: (i) the time CenturyLink receives verbal permission from Customer to initiate Mitigation or (ii) the Initial DDoS Alarm for DDoS Mitigation Service if Customer has pre-authorized CenturyLink to initiate Mitigation. If Customer has pre-authorized CenturyLink to initiate Mitigation, but additional countermeasures that were not pre-authorized are required to mitigate the Incident, the verbal permission Time to Mitigate Goal will apply to the additional countermeasures that were not previously pre-authorized. Initiation of Customer pre-authorized Mitigation may be done by an authorized CenturyLink employee or as an automated initiation by the system ("Auto-Mitigation"). Customer chooses which mode to use.

Description	Goal	Remedy (Credit is applied as a % of the MRC for the affected Service)	
Time to Notify	15 minutes from Initial DDoS Alarm	16 – 30 minutes = 50%	More than 30 minutes = 100%
Time to Mitigate	15 minutes from Customer's verbal permission to begin Mitigation	16 – 30 minutes = 50%	More than 30 minutes = 100%
	15 minutes from Initial DDoS Alarm (Pre-authorized Mitigation initiated by CenturyLink employee or Auto-Mitigation)	16 – 30 minutes = 50%	More than 30 minutes = 100%

2. Status Reporting and Change Requests. The following Status Reporting and change request objectives are intended to be informational only and do not provide any SLA credits and are not subject to any other Goal in this SLA.

(a) Status Reporting. If requested by Customer, CenturyLink will provide Customer with a status report by telephone, or e-mail within 60 minutes after the initiation of Mitigation.

(b) Change Requests. Customer may request one routine configuration or policy change per 90 day period. CenturyLink will provide the routine configuration and policy change requests within one business day after the request. Customer requests that exceed one request per 90 day period may result in additional charges. A routine change means a change when an attack is not taking place.

3. Maintenance.

31 Normal Maintenance. CenturyLink may periodically upgrade software or hardware to maintain the latest versions in operation. If CenturyLink determines an upgrade is necessary, CenturyLink will work with Customer to schedule a time to make necessary changes, preferably during the normally scheduled CenturyLink maintenance window as follows.

AMERICAS: Saturday 00:00 AM to 05:00 AM; Sunday 00:00 AM to 05:00 AM.
EMEA: Saturday 00:00 AM to 04:00 AM.
ASIA PACIFIC (Except Japan): Saturday 21:00 (GMT) to Sunday 01:00 (GMT)
JAPAN: Sunday 04:00 (JST) to 08:00 (JST)
All times listed are local times and subject to change.

Customer must allow CenturyLink to make these changes within five business days of receipt of the request from CenturyLink, or CenturyLink's obligation to provide this Service and meet any Service SLAs and Goals will be suspended until Customer grants CenturyLink the access CenturyLink requires to make such changes.

32 Urgent Maintenance. "Urgent Maintenance" means efforts to correct conditions that require immediate action. Urgent Maintenance may degrade the quality of the Service. CenturyLink's efforts related to Urgent Maintenance are subject to this SLA

**DDOS MITIGATION SERVICE
RETAIL SERVICE LEVEL AGREEMENT**

and credits may apply to the extent Goals are missed. CenturyLink may undertake Urgent Maintenance at any time deemed necessary and will provide notice of Urgent Maintenance to Customer as soon as is commercially practicable under the circumstances.

4. General.

41 Remedies. To be eligible for SLA credits, Customer must be in good standing with CenturyLink and current in its obligations. To receive SLA credits, Customer must contact CenturyLink Billing Inquiries via the contact information provided on their invoice within 60 calendar days after the date when the relevant SLA Goal was not met. CenturyLink will determine the credits provided to Customer by applying the applicable remedies set forth in this SLA. All performance calculations and applicable Service Credits are based on CenturyLink records and data unless Customer can provide CenturyLink with clear and convincing evidence to the contrary. A credit will be applied only to the month in which the event giving rise to the credit occurred. The credits will apply to the MRCs of the affected Service after application of all discounts and do not apply to MRCs of other services. The maximum service credits issued in any one calendar month will not exceed 100% of the MRCs of the affected Service. Cumulative credits in any one month must exceed \$25.00 to be processed. If Customer fails to notify CenturyLink in the manner set forth above with respect to the applicable SLA credits, Customer will have waived its right to such SLA credits for that month.

42 Limitations. This SLA will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under this SLA, for any event that adversely impacts the Service that is caused by: (a) the acts or omissions of Customer, its employees, contractors or agents or its end users; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink; (c) Force Majeure Events; (d) scheduled service maintenance, alteration or implementation; (e) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information; (f) CenturyLink's lack of access to the Customer premises where reasonably required to restore the Service; (g) Customer's failure to release the Service for testing or repair and continuing to use the Service on an impaired basis; (h) Customer's failure to provide timely approvals and/or consents, including allowing CenturyLink to retune the Service as required for CenturyLink to provide the Service; (i) CenturyLink's termination of Service for Cause or Customer's use of Service in an unauthorized or unlawful manner; (j) improper or inaccurate network specifications provided by Customer; or (k) Customer fails to fulfil any of its responsibilities or obligations as detailed in the Agreement, the SG and/or any other guidelines or policies applicable to the Service.

43 Customer Termination Rights. Customer may terminate the affected Service for its convenience and without cancellation charges or further liability to CenturyLink if CenturyLink is unable to meet the Goals herein within a 60 day cure period. The 60 day cure period will begin after a trouble ticket is opened. Customer may terminate the affected Service by providing written notice per the Agreement within 20 days after the 60 day cure period ends. Such termination will be effective 45 days after receipt of written notice by CenturyLink of termination from Customer, unless Customer requests Service to be continued and establishes a new termination date after 45 days. Customer is responsible for all Service charges until the termination date. If Customer fails to notify CenturyLink in the manner set forth in this section with respect to the applicable termination right, Customer will have waived its right to terminate the affected Service.

**OPTICAL WAVELENGTH SERVICE
RETAIL SERVICE LEVEL AGREEMENT
(not applicable to services offered under the CenturyLink Wholesale and Enhanced Services Agreements)**

This Service Level Agreement ("SLA") applies to CenturyLink Optical Wavelength Private Line Service ("Service" or "Optical Wavelength Private Line Service") ordered by customers pursuant to an agreement ("Agreement") between the specific customer ("Customer") and Qwest Communications Company, LLC d/b/a CenturyLink QCC ("CenturyLink"). In no case will CenturyLink be required to provide duplicate reimbursement or payment to Customer for any Service quality failure incident.

Circuit Availability

Customer will, subject to the terms, exclusions, and restrictions described herein, be entitled to receive from CenturyLink a credit, as outlined in the Outage Credits section of this SLA, if the availability ("Circuit Availability") of a circuit for any calendar month falls below the percentage shown in the relevant credit schedule included in this section ("Outage Credit"). The credit schedule provides availability objectives and related remedies.

Circuit Availability objectives and related remedies are provided for local access or tail circuits used in connection with the service only if these are on CenturyLink-owned network facilities.

The service will for purposes of this SLA be deemed to be unavailable to Customer only if the service on a particular circuit ("Affected Service") is subject to an interruption (other than noted herein) that results in the total disruption of the service ("Outage").

The credit to which Customer may be entitled under this section will be equal to the applicable percentage of Customer's monthly recurring charges ("MRC") for the Affected Service after application of any credits or discounts ("Eligible Service Charges"). The credit will not include credits on any other MRCs charged to Customer for any other service.

Circuit Availability is the measure of Service, expressed in percentage, calculated as Total Time minus Outage Time divided by Total Time. For the purpose of this definition, "Total Time" is the number of seconds in a calendar month. "Outage Time" is the time in seconds the service has had an Outage.

For protected or Domestic Network Diversity Service, Outage Time includes only the amount of time in seconds that both service paths experience concurrent Outage Time. If at any given time any one of the two paths is available it will not be deemed as Outage Time.

1. Outage Credits.

1.1 Optical Wavelength Private Line Service Long Haul (Intercity)

1.1.A Unprotected Service. Service is delivered on CenturyLink-owned network facilities using a single unprotected circuit providing two fiber hand off to the Customer at CenturyLink-designated hand off points.

Credit Schedule for Long Haul Unprotected Service		
Circuit Availability		Amount of Credit (as a % of the Eligible Circuit Charges for the Affected Circuit)
Upper Level	Lower Level	
100%	99.9%	0%
< 99.9%	99.7%	5%
< 99.7%	99.2%	10%
< 99.2%	98.5%	25%
< 98.5%	0%	50%

1.1.B Domestic Network Diversity Service. Service is delivered on CenturyLink-owned network facilities using two diversely routed circuits and providing four fiber hand off to the Customer at CenturyLink-designated hand off points.

Credit Schedule for Long Haul Domestic Network Diversity Service		
Circuit Availability		Amount of Credit (as a % of the Eligible Circuit Charges for the Affected Circuit)
Upper Level	Lower Level	
100%	99.99%	0%
< 99.99%	99.9%	5%
< 99.9%	99.7%	10%
< 99.7%	99.5%	25%
< 99.5%	0%	50%

**OPTICAL WAVELENGTH SERVICE
RETAIL SERVICE LEVEL AGREEMENT**

1.1.C Protected Service Service is delivered on CenturyLink-owned network facilities using two diversely routed circuits between CenturyLink locations with protection switching and providing two fiber hand off to the Customer at CenturyLink-designated hand off points.

Credit Schedule for Long Haul Protected Service		
Circuit Availability		Amount of Credit (as a % of the Eligible Circuit Charges for the Affected Circuit)
Upper Level	Lower Level	
100%	99.99%	0%
< 99.99%	99.9%	5%
< 99.9%	99.7%	10%
< 99.7%	99.5%	25%
< 99.5%	0%	50%

1.2 Optical Wavelength Private Line Service Metro

1.2.A Unprotected Service. Service is delivered on CenturyLink-owned network facilities using a single unprotected circuit providing two fiber hand off to the Customer at CenturyLink-designated hand off points.

Credit Schedule for Metro Unprotected Service		
Circuit Availability		Amount of Credit (as a % of the Eligible Circuit Charges for the Affected Circuit)
Upper Level	Lower Level	
100%	99.9%	0%
< 99.9%	99.7%	5%
< 99.7%	99.2%	10%
< 99.2%	98.5%	25%
< 98.5%	0%	50%

1.2.B Domestic Network Diversity Service. Service is delivered on CenturyLink-owned network facilities using two circuits, diversely routed, and providing four fiber hand off to the Customer at CenturyLink-designated hand off points.

Credit Schedule for Metro Domestic Network Diversity Service		
Circuit Availability		Amount of Credit (as a % of the Eligible Circuit Charges for the Affected Circuit)
Upper Level	Level	
100%	99.99%	0%
<99.99%	99.9%	5%
<99.9%	99.7%	10%
<99.7%	99.5%	25%
<99.5%	0%	50%

1.2.C Core Protected Service. Service is delivered on CenturyLink owned network facilities using two diversely routed circuits between CenturyLink-designated on-net locations along with protection switching and providing two fiber hand off to the Customer at CenturyLink-designated hand off points.

**OPTICAL WAVELENGTH SERVICE
RETAIL SERVICE LEVEL AGREEMENT**

Credit Schedule for Metro Core Protected		
Circuit Availability		Amount of Credit (as a % of the Eligible Circuit Charges for the Affected Circuit)
Upper Level	Lower Level	
100%	99.99%	0%
< 99.99%	99.9%	5%
< 99.9%	99.7%	10%
< 99.7%	99.5%	25%
< 99.5%	0%	50%

1.3 The Outage Credit will apply to the monthly recurring charges for the section of the Service affected by an Outage ("Eligible Monthly Recurring Charge of Affected Services"); provided, however, that if any portion of the affected Service remains beneficially used or useable by Customer between any intermediate terminals (where Customer has installed drop and insert capability) or end terminals, the Outage Credit will not apply to that pro-rata portion of the mileage. The length of each Outage will be calculated in seconds. An Outage will be deemed to have commenced upon verifiable notification thereof by Customer to CenturyLink, or, when indicated by network control information actually known to CenturyLink network personnel, whichever is earlier. Each Outage will be deemed to terminate upon restoration of the affected Service as evidenced by appropriate network tests by CenturyLink. CenturyLink's trouble ticketing system will be the governing source of data for calculating Outage Credits. CenturyLink will give notice to Customer of any scheduled outage as early as is practicable, and a scheduled outage will under no circumstances be viewed as an Outage hereunder.

1.4 Outage Credits will not be granted if the malfunction of any Service is due to:

- (a) Interruptions or times of service degradation during any period in which CenturyLink or its agents are not afforded access to the premises where the access lines associated with Customer's Service are terminated, provided such access is reasonably necessary to prevent a degradation or to restore service;
- (b) Interruptions or times of service degradation during any period when CenturyLink has posted on the CenturyLink web site or communicated to Customer in any other manner that Customer's Service will be unavailable for maintenance or rearrangement purposes, or Customer has released the service to CenturyLink for the installation of a Customer Service order;
- (c) Interruptions or times of service degradation during any period when Customer elects not to release the Service(s) for testing and/or repair and continues to use it on an impaired basis;
- (d) Interruptions or times of service degradation resulting from force majeure events beyond the reasonable control of CenturyLink including, but not limited to, acts of God, government regulation, labor strikes, national emergency, or war (declared or undeclared);
- (e) Interruptions or times of service degradation resulting from Customer's use of the Service in an unauthorized or unlawful manner;
- (f) Interruptions or times of service degradation resulting from a CenturyLink disconnect for Customer's breach of a term set forth in the Agreement;
- (g) Interruptions or times of service degradation resulting from incorrect, incomplete, or inaccurate orders from Customer;
- (h) Interruptions or times of service degradation due to improper or inaccurate network specifications provided by Customer;
- (i) Interruptions or times of service degradation resulting from an outage or other defect occurring in Customer's Interconnection Facilities; or
- (j) Special configurations of the standard Service that have been mutually agreed to by CenturyLink and Customer; provided, however, CenturyLink may provide a separate service level agreement to Customer for those special configurations.

1.5 To be eligible for Outage Credits under this SLA, Customer must submit necessary supporting documentation and request the Outage Credit within 30 days of the conclusion of the service month in which the Outage arose. All approved Outage Credits will be credited on the next monthly invoice for the affected Service after receipt of Customer's request for credit and CenturyLink's approval of the Outage Credit. The total of all Outage Credits applicable to or accruing in any given month will not exceed the amount payable by Customer to CenturyLink for that same month for such Service.

1.6 "Chronic Outage" for purposes of this SLA, means that over a 30 consecutive day period, Service experiences: (a) more than five outages related to the same issue; or (b) more than 48 aggregate hours of outages. If Customer experiences Chronic Outages with respect to the Service, Customer will be entitled to terminate the affected Service without further obligation by providing CenturyLink with written notice following such Chronic Outages (a "Chronic Circuit Cancellation"). Customer must exercise any termination right available to it under this section within 30 days after Customer first becomes eligible to exercise the applicable termination right. In the event Customer fails to comply with the condition set forth in the preceding sentence, Customer will, with respect to the applicable termination right, have waived its right to terminate.

1.7 The Outage Credit and Chronic Circuit Cancellation described in this section will be the sole and exclusive remedy of Customer in the event of any Outage or Chronic Outages, and under no circumstance will either be deemed a default under the Agreement.

2. Performance Objectives

The following assumptions apply to the derived data:

**OPTICAL WAVELENGTH SERVICE
RETAIL SERVICE LEVEL AGREEMENT**

- 1GbE, 2.5G (OC-48), 10G (OC-192 or 10G WAN PHY), 10GbE LAN PHY, 40G (OC768), OTU1 (2.666G), OTU2 (10.709G), OTU3 (43.018G) Fibre Channel 1G, 2G, 4G and 10G circuits originate and terminate on wavelength translators interfacing to CenturyLink's optical Dense Wave Division Multiplexing (DWDM) backbone
- Mean Time To Repair (MTTR) for DWDM, and wavelength translator equipment: 4 hours
- MTTR for fiber optical cable: 8 hours (Bellcore Standard)
- Cable cut rate: 4.39 /year/1,000 sheath miles (Bellcore Standard)
- BER: 1×10^{-12}

3. Acceptance Criteria.

The acceptance criterion is to demonstrate the above-specified BER performance levels measured during a 24-hour test period. If the BER specified (10^{-12}) is observed during the 24-hour test period, the Service is considered accepted.

**NETWORK-BASED SECURITY SERVICE
RETAIL SERVICE LEVEL AGREEMENT**

(Not applicable to services offered under the CenturyLink Wholesale and Enhanced Services Agreements)

This service level agreement ("SLA") applies to Network-Based Security Service ("Service" or "NBS") ordered by customers pursuant to an agreement ("Agreement") between a specific customer and Qwest Communications Company, LLC d/b/a CenturyLink QCC ("CenturyLink"). Capitalized terms not defined in this SLA are defined in the Agreement. For Customer's claims related to Service deficiencies, interruptions or failures, Customer's exclusive remedies are limited to those remedies set forth in this SLA.

1. GOALS.

11 System Availability. Customer will, subject to the terms, exclusions, and restrictions described in this SLA, be eligible to receive from CenturyLink a credit, as outlined in this SLA for an Affected Service. "Affected Service" means a Service instance that fails to meet the applicable Goal. System availability is measured by System Downtime in a calendar month. "System Downtime" exists when the CenturyLink NBS platform is unable to pass customer traffic as a part of performing its security functions. System Downtime is measured from the time a trouble ticket is opened by CenturyLink or Customer in the CenturyLink trouble management system to the time the CenturyLink NBS platform is able to pass customer traffic for the Affected Service. The system availability of a particular Service instance, expressed as a percentage, is calculated as Total Time minus the number of minutes of System Downtime in a calendar month divided by Total Time. "Total Time" is the number of minutes in a calendar month.

Goal	Availability	Remedy (Credit is applied as a % of the Affected Service MRC)
99.9%	97.6% - 99.8%	10%
	95.1% - 97.5%	25%
	95% or less	50%

12 Policy Changes. The following Goals apply to policy change requests available with the applicable NBS support level. Provided Customer has complied with its obligations in the Service Exhibit, CenturyLink will implement Customer's policy change requests as follows.

Support Level	Goal	Remedy (Credit is applied as a % of the Affected Service MRC)
Basic	24 hours	10% for each missed Goal
Value	8 hours	
Prime	8 hours	
Prime - up to 2 urgent policy changes	2 hours	

Support Level	Goal	Remedy (Credit is applied as a % of the Affected Service MRC)
Standard	24 hours	10% for each missed Goal
Unlimited	8 hours	
Unlimited – up to 2 urgent policy changes	2 hours	

2. MAINTENANCE.

21 "Normal Maintenance" means upgrades of hardware or software or upgrades to increase capacity. Normal Maintenance may temporarily degrade the quality of the Service, including possible outages. CenturyLink may change the maintenance window times upon posting to the website or other notice to Customer. CenturyLink will undertake Normal Maintenance during the hours and upon the prior notice time period stated below. Normal Maintenance hours are Sunday, Tuesday, and Thursday mornings between the hours of 12:00 AM and 6:00 AM Local Time. "Local Time" means the local time in the time zone in which an Affected Service is located.

22 In addition to the scheduled Normal Maintenance hours, Customer will provide an additional three-hour maintenance window each month for CenturyLink to perform Normal Maintenance. System upgrades may occur outside of the Normal Maintenance hours and three-hour maintenance window upon permission from Customer's designated Customer Administrator.

23 "Urgent Maintenance" means efforts to correct network conditions that are likely to cause a material Service outage and that require immediate action. Urgent Maintenance may degrade the quality of the Services, including possible outages. Such effects related to Urgent Maintenance will not entitle Customer to service credits as set forth in this SLA. CenturyLink may undertake Urgent Maintenance at any time deemed necessary and will provide notice of Urgent Maintenance to Customer as soon as is commercially practicable under the circumstances.

24 Outages related to Normal Maintenance and Urgent Maintenance will not be considered System Downtime.

**NETWORK-BASED SECURITY SERVICE
RETAIL SERVICE LEVEL AGREEMENT**

3. GENERAL.

31 Remedies. To be eligible for service credits, Customer must be in good standing with CenturyLink and current in its obligations. To receive service credits, Customer must contact the Customer Service Center at 1-800-860-1020 and submit the relevant trouble ticket information within 30 calendar days from the date when the relevant SLA Goal was not met. CenturyLink will determine the credits provided to Customer by applying the applicable remedies set forth in this SLA. A credit will be applied only to the month in which the event giving rise to the credit occurred. The credits will apply to the MRCs of the Affected Service after application of all discounts and do not apply to MRCs of other services. The maximum service credits issued in any one calendar month will not exceed 50% of the MRC of the Affected Service. Cumulative credits in any one month must exceed \$25.00 to be processed. If Customer fails to notify CenturyLink in the manner set forth above with respect to the applicable SLA credits, Customer will have waived its right to such SLA credits for that month.

32 Limitations. This SLA will not apply, and Customer will not be entitled to receive a credit or exercise a termination right under this SLA, for any event that adversely impacts the Service that is caused by: (a) the acts or omissions of Customer, its employees, contractors or agents or its end users; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by CenturyLink or its third party service; (c) Force Majeure Events; (d) Normal Maintenance; Urgent Maintenance or scheduled alteration or implementation; (e) the unavailability of required Customer personnel, including as a result of failure to provide CenturyLink with accurate, current contact information; or (f) CenturyLink's lack of access to the Customer premises where reasonably required to restore the Service; (g) Customer's failure to release the Service for testing or repair and continuing to use the Service on an impaired basis; (h) CenturyLink's termination of Service for Cause or Customer's use of Service in an unauthorized or unlawful manner; or (i) improper or inaccurate network specifications provided by Customer.

33 Customer Termination Rights. Customer may terminate the Affected Service without Cancellation Charges if, in any single calendar month: (a) System Downtime exists for at least 24 hours in the aggregate; or (b) System Downtime exists for a period of at least eight consecutive hours. Customer may only terminate the Affected Service by providing written notice to CenturyLink within 20 days after Customer first becomes eligible to exercise the applicable termination right. Such termination will be effective 45 days after receipt of written notice by CenturyLink. Customer is responsible for all Service charges until the termination date. If Customer fails to notify CenturyLink in the manner set forth in this section with respect to the applicable termination right, Customer will have waived its right to terminate the Affected Service.

Agreement Document from CenturyLink

Final Audit Report

2019-03-27

Created:	2019-03-25
By:	Levi Lohnes (levi.lohnes@centurylink.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAPhBcyNVzaJbFmpdkvKF4bJ6Y5d54wJLe

"Agreement Document from CenturyLink" History



Document created by Levi Lohnes (levi.lohnes@centurylink.com)

2019-03-25 - 4:54:12 PM GMT- IP address: 13.108.254.8



Document emailed to Steve Arneson (pomdirectorsignature@centurylink.com) for signature

2019-03-25 - 4:56:50 PM GMT



Document viewed by Steve Arneson (pomdirectorsignature@centurylink.com)

2019-03-27 - 2:22:57 AM GMT- IP address: 155.70.23.45



Document e-signed by Steve Arneson (pomdirectorsignature@centurylink.com)

Signature Date: 2019-03-27 - 2:26:43 AM GMT - Time Source: server- IP address: 155.70.23.45



Signed document emailed to Levi Lohnes (levi.lohnes@centurylink.com) and Steve Arneson (pomdirectorsignature@centurylink.com)

2019-03-27 - 2:26:43 AM GMT