

## STANDARD CONTRACT FOR SERVICES

1. **Parties.** This contract for services is made this 2nd day of January 2023 (the “Effective Date”) by and between the State of Vermont, Office of Purchasing & Contracting (hereinafter called “State”), and Comcast Business Communications, LLC., with a principal place of business at 1701 JFK Boulevard, Philadelphia, PA 19103, (hereinafter called “Comcast” or “Service Provider”). Service Provider’s form of business organization is Limited Liability Corporation. It is Service Provider’s responsibility to contact the Vermont Department of Taxes to determine if, by law, Service Provider is required to have a Vermont Department of Taxes Business Account Number. Pages 1 through 4 of this Contract (specifically paragraphs 1 through 12) shall be referred to herein as the “Standard Contract Cover Page”.

2. **Subject Matter.** The subject matter of this contract is services generally on the subject of Telecommunications and Network Services via possible Work Orders, specifically Contractor’s Ethernet Dedicated Internet Services, Ethernet Transport Services (Interstate and Intrastate), Ethernet Trunk Services, Business Internet Services, ActiveCore SD-WAN Services, Wave Services and Video Services.

### 3. **Defined Terms**

**Sales Order or Work Order:** A request to provide the Services to a Service Location(s) submitted by Customer to Comcast on (a) the then current Comcast form designated for such purpose or (b) such other form, or in such other manner, as may be agreed upon by the parties. Customer and Comcast acknowledge and agree that to the extent Service are ordered using a Comcast Sales Order or Work Order, any inclusion of or reference to Comcast terms and conditions referenced therein shall be of no force and effect.

**Service Term:** As specified in a Work Order, the duration of time (which shall commence on the Service Commencement Date) for which Services are ordered. If not specified in a Sales Order, the Service Term shall be one (1) year from the Service Commencement Date.

**Service(s):** Service(s) provided by Comcast pursuant to a Work Order. All Services provided under the Agreement are for commercial, non-residential use only. For the avoidance of doubt, the only Comcast services available to the State under this Contract are Comcast’s Ethernet Dedicated Internet Services, Ethernet Transport Services (Interstate and Intrastate), Ethernet Trunk Services, Business Internet Services, ActiveCore SD-WAN Services, Wave Services and Video Services.

**Service Commencement Date:** With respect to each Service, “Service Commencement Date” shall have the meaning specified in the Product Specific Attachment (which are attached hereto as Attachment F) applicable to such Service, it being understood that a single Work Order containing multiple Service Locations or Services may have multiple Service Commencement Dates.

**Service Location(s):** The Customer location(s) where Comcast provides the Services.

**Maximum Amount.** In consideration of the services to be performed by the Service Provider, the State agrees to pay the Service Provider, in accordance with the payment provisions specified in Attachment B, a sum not to exceed \$1,500,000.00.

4. **Contract Term.** The period of Service Provider's performance shall begin on January 2, 2024, and end on December 31, 2026. This Contract Term may be extended for 2 one-year renewals as may be agreed in writing by the State and Contractor. Notwithstanding the foregoing, if the Service Term applicable to the Services to be provided under a Work Order extends beyond the expiration of the Contract Term, such Work Order shall continue to be governed by the terms and conditions of this Contract.

5. **Prior Approvals.** This Contract shall not be binding unless and until all requisite prior approvals have been obtained in accordance with current State law, bulletins, and interpretations.

6. **Amendment.** No changes, modifications, or amendments in the terms and conditions of this contract shall be effective unless reduced to writing, numbered and signed by the duly authorized representative of the State and the Service Provider.

7. **Termination for Convenience.** This contract may be terminated by the State at any time by giving written notice at least thirty (30) days in advance. In such event, the Service Provider shall be paid under the terms of this contract for all services provided to and accepted by the State prior to the effective date of termination plus any applicable Termination Charges (as defined in Attachment E).

8. **Purchasing Entities.** This Contract may be used by (a) all departments, offices, institutions, and other agencies of the State of Vermont and counties (each a "State Purchaser") according to the process for ordering and other restrictions applicable to State Purchasers set forth herein; and (b) political subdivisions of the State of Vermont and any institution of higher education chartered in Vermont and accredited or holding a certificate of approval from the State Board of Education as authorized under 29 V.S.A. § 902 (each an "Additional Purchaser"). Issues concerning interpretation and eligibility for participation are solely within the authority of the State of Vermont State Contract Administrator. The State of Vermont and its officers and employees shall have no responsibility or liability for Additional Purchasers. Each Additional Purchaser is to make its own determination whether this Contract are consistent with its procurement policies and regulations and negotiate supplemental terms necessary to comply with such Additional Purchaser's requirements. For the avoidance of doubt, non-profit entities are not permitted to purchase under this Contract.

9. **Primary Contacts.** The Parties will keep and maintain current at all times a primary point of contact for this Agreement, which are presently as follows:

**a. For the Service Provider:**

Name: Michelle Barker

Phone: 860-383-9014

Email: [Michelle\\_Barker@comcast.com](mailto:Michelle_Barker@comcast.com)

**b. For the State:**

Name: Frank Costantino

Phone: 802-828-3760

Email: [frank.costantino@vermont.gov](mailto:frank.costantino@vermont.gov)

10. **Attachments.** This contract consists of 164 pages including the following attachments which are incorporated herein:

Attachment A - Statement of Work

Attachment B - Payment Provisions

Attachment C – “Standard State Provisions for Contracts and Grants”

“State of Vermont – Federal Terms Supplement (non-construction)” (only applicable in the event the ordering entity notifies Comcast that a service is subject to Federal funding at the time of order)

Attachment D – Information Technology Professional Services Terms & Conditions

Attachment E – Comcast Enterprise Services General Terms and Conditions (“Comcast Ts&Cs”)

Attachment F – Product Specific Attachments

Attachment G – Service Provider’s Work Order Form

- G1 Sales Order Form – EDI, Ethernet Transport, SD-WAN, DDoS, Mitigation, Trunk, Waves
- G2 Sales Order Form – Business Internet & Video

11. **Order of Precedence.** Any ambiguity, conflict or inconsistency between the documents comprising this contract shall be resolved according to the following order of precedence:

- (1) Standard Contract
- (2) Attachment D
- (3) Attachment C (Standard Contract Provisions for Contracts and Grants)
- (4) State of Vermont – Federal Terms Supplement (non-construction) (the “Federal Supplement”)
- (5) Attachment E (Comcast Terms)
- (6) Attachment F
- (7) Attachment A
- (8) Attachment B
- (9) Attachment G

12. **Existing Sales Orders.** The State and Comcast acknowledge and agree that any Services being provided pursuant to Sales Orders delivered under Contract No. 37301, dated May 4, 2020 (“Existing Orders”), shall, as of the date this contract is executed by both parties, continue under, and be governed by the terms and conditions of, this contract.

**WE THE UNDERSIGNED PARTIES AGREE TO BE BOUND BY THIS CONTRACT**

By the State of Vermont:

By the Contractor: Comcast Business  
Communications LLC

Date: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

Signature: \_\_\_\_\_

Name: Jennifer M.V. Fitch  
Commissioner - Buildings and

Name: \_\_\_\_\_

Title: General Services

Title: \_\_\_\_\_

## **ATTACHMENT A – STATEMENT OF WORK**

The Service Provider shall provide the State of Vermont with the Services as provided herein. The Contractor will perform services as outlined in this Contract via possible Work Orders.

### **Requirements for Ordering.**

- a. The Agency of Digital Services (“ADS”) is responsible for overseeing and incorporating the design, development and installation of flexible cabling infrastructures for all State of Vermont facilities that require voice, data, video and/or multimedia services. The State Contact and ADS Telecommunications shall work closely with the Service Provider and the Agency/Department end users requiring services.
- b. Contractor will accept work requests/orders only from ADS. No department/agency is authorized to contact vendors directly for services required.
- c. There is no designated re-occurring maintenance window. Installation schedules are established through agreements with ADS Telecommunications, contract vendor(s), and department/agency requesting cabling installations, upgrades and/or maintenance.
- d. All work shall be performed Monday through Friday during normal working hours (7:45am-5:00pm local time) unless an occasion may arise which would require work to be performed after normal working hours or on Saturday, Sunday or Holidays.
- e. Orders made under this Contract must include a Purchase Order for the Product and/or Services. If (i) an Order is funded by federal funds and (ii) the State and/or ADS notifies Contractor in writing that the Order funded by federal funds, then the Services provided pursuant to such Order shall be subject to the Federal Supplement.
- f. All orders placed under this Contract must include the Contract Number and Ordering Entity’s Name on the Purchase Order.
- g. The service provider shall maintain a Workbook containing an inventory of existing services in addition to open sale orders. The Workbook will be reviewed periodically on a schedule set by the parties and include, without limitation, the Monthly Recurring Charges, Non-Recurring Charges, Location and Quantity.

### **Contractor Personnel**

The Contractor shall provide a dedicated support team that will provide account general management, technical management, sales engineering, order provisioning, end to end installation support and invoicing services support, it being understood that State shall contact Contractor’s applicable support centers for service-related issues (e.g., service interruptions). Contractor Key Personnel shall include:

Sales Team

Name	Title	Office	E-Mail
Michelle Barker	Strategic Enterprise Account Executive	222 New Park Drive, Berlin, CT 06037	<a href="mailto:Michelle_barker@comcast.com">Michelle_barker@comcast.com</a>

Customer Support Team

Name	Title	Office	E-Mail
Christopher Ready	Sales Engineer	222 New Park Drive, Berlin, CT 06037	<a href="mailto:Christopher_ready@comcast.com">Christopher_ready@comcast.com</a>
Mike Fiorini	Sales Manager	222 New Park Drive, Berlin, CT 06037	<a href="mailto:Mike_fiorini@comcast.com">Mike_fiorini@comcast.com</a>

**Changes in Contractor Personnel.** Contractor shall use reasonable efforts to make available all “Key Personnel” (those listed in table directly above) for the entire life of this Contract. Contractor shall provide the State with written notice should it change any of the Key Personnel. Notwithstanding the foregoing, the State acknowledges that Key Personnel may become unavailable due to termination of employment for any reason, through disability or death, illness, or through leave of absence such as FMLA or National Guard duty for example. In such circumstances, Contractor shall promptly notify the State in writing of the impending or actual departure of any Key Personnel and of the qualifications and identity of proposed replacement Key Personnel. The State has the right to reasonably disapprove of any replacement Key Personnel.

**Control of Contractor Personnel.** Contractor shall be fully responsible for the management, compensation, and performance of all its employees, and the filing of any and all returns and reports and the withholding and/or payment of all applicable federal, State, and local wage tax, or employment-related taxes, including, but not limited to, income taxes, gross receipt taxes, taxes measured by income, social security taxes, and unemployment taxes for Contractor and Contractor's employees. Notwithstanding the foregoing, Contractor's employees shall adhere to the State's reasonable policies and procedures, of which Contractor is made aware while on State premises and shall behave and perform in a professional manner. The State, may, in its reasonable discretion, require Contractor to replace any Contractor employee, including but not limited to Key Personnel, working hereunder who does not adhere to, behave, and perform consistent with the State's reasonable policies and procedures or a significant and material personality conflict arises with a Contractor employee and employee of the State by written notice to Contractor of the requirement of replacement. Contractor shall use reasonable efforts to promptly and expeditiously replace Key Personnel and replace all other personnel within thirty (30) days of receipt of the written notice of a failure to comply with the State's reasonable policies and procedures or a significant and material personality conflicts arises with a Contractor employee and a State employee, unless otherwise mutually agreed.

All intellectual property of each party shall remain with the respective owner(s) and no right, title or interest will transfer to either party as a result of this Contract or the provision or receipt

of services hereunder.

### **State Facilities**

During the term of this Contract, the State may make available to Contractor space in any State facility applicable to the Services, subject to the conditions that Contractor: (i) other than incidental general Contractor obligations, shall only use such space solely and exclusively for and in support of the Services; (ii) other than incidental general Contractor obligations, shall not use State facilities to provide goods or services to or for the benefit of any third party; (iii) shall comply with the leases and reasonable security, use, rules and agreements applicable to the State facilities provided to Contractor by State in writing; (iv) shall not use State facilities for any unlawful purpose; (v) shall comply with all reasonable policies and procedures governing access to and use of State facilities that are provided to Contractor in writing; (vi) except as may be required to perform the Services, shall not photograph or record, duplicate, disclose, transmit or communicate any State information, materials, data or other items, tangible or intangible, obtained or available as a result of permitted use of State facilities; and (vii) return such space to the State in the same condition it was in at the commencement of this Contract, ordinary wear and tear excepted.

### **Early Termination Liability**

Notwithstanding anything to the contrary herein, any Services that are terminated by the State for convenience within the first twelve (12) months of the Contract Term applicable to such Services will be subject to an early termination equal to (i) the monthly recurring charge applicable to such Service multiplied by the number of months remaining in the first twelve (12) months of the Service Term plus (ii) 100% of any remaining, unpaid Custom Installation Fees (as defined in Attachment E) (collectively the "Termination Charges").

Notwithstanding any contrary language anywhere else in this Contract or any Contractor documents, under no such circumstances will the State be liable for any Termination Charges that exceeds the amount equal to (i) multiplying the applicable monthly service charge by 12 plus (ii) 100% of any remaining, unpaid Custom Installation Fees. Any and all cancellation or termination charges will be due and payable in one lump sum within thirty (30) days of billing. The State remains responsible to pay for all Services provided up to the date of any termination.

For the avoidance of doubt, no early Termination Charges set forth in this Section or elsewhere will apply to a Service that is terminated due to a Chronic Service Interruption (as defined in Attachment E), as a result of Contractor's failure to cure a material breach within thirty (30) days of Contractor's receipt of written notice of such failure, or due to non-appropriation in accordance with Attachment C Section 27.

### **General Expectations**

The Service Provider will be required to attend Monthly Service Support meetings with the Network Engineering personnel. The account should be primarily staffed with individuals dedicated to and preferably based in the State of Vermont. The Service Provider will be expected to present performance statistics, chronic problem situations and status, proactive reviews and solutions, and current project status.

The Service Provider will also be expected to present bi-weekly coordination meetings where all requested work orders from the State Network Engineering group will be reviewed for completeness, accuracy and status.

The Service Provider shall submit quarterly reports detailing the State of Vermont accounts active under this Contract. The reports shall be submitted electronically and sent as an attachment to [ADS.ITPurchasing@vermont.gov](mailto:ADS.ITPurchasing@vermont.gov) and [Frank.Costantino@vermont.gov](mailto:Frank.Costantino@vermont.gov). Reports shall contain accurate information of account numbers, services rendered, service locations and the costs associated with them for the quarter. If there is a change in accounts before the quarter report is due, Service Provider shall send the updated report immediately. Any exception to this mandatory requirement or failure to submit complete reports, or in the format required, may result in corrective action, up to and including termination for cause.

**Reporting Period**

January 1 - March 31  
April 1 - June 30  
July 1 - September 30  
October 1 - December 31

**Report Due**

April 30  
July 31  
October 31  
January 31

**Reporting Period**

January 1 - March 31  
April 1 - June 30  
July 1 - September 30  
October 1 - December 31

**Report Due**

April 30  
July 31  
October 31  
January 31

**Account Management**

The Service Provider must provide a team of representatives to work in conjunction with the State regarding the management of equipment, new installations, service relocations, and functional changes. The team should include members in the following disciplines, all reachable via email and toll-free numbers, with backup resources available in the event of illness or vacation.

Account General Management: Review contract requirements and ensure that all terms and conditions are enforced.

Account Technical Management: Provide general management responsible to ensure continuous network operations and coordinate service installations, moves and changes.

Sales Engineering: Pre-order support staff, knowledgeable in-service engineering consulting, who can provide detailed itemized quotes for all services when requested.

Order Provisioning: Service Provider staff must be available to interpret State work order requests, work with State contacts to define service needs, and complete any necessary documentation for the Service Provider in order to complete the service implementation. Management of installation due dates, service progress and past dated services will be provided by this area.

Installation Support: Service Provider must provide support, personnel, and equipment for end-to-end connectivity, turn-up and operational verification of all services provided by the Service Provider.

Invoice Services Support: The Service Provider must provide financial representatives who can assist the State in understanding the invoicing system and take corrective actions to resolve billing issues.

**Maintenance Notification**

Contractor shall provide timely notification of maintenance that could impact services provided to the State. A minimum of 72 hours of notice for planned maintenance and, to the extent, practicable, prior notification preferably with a minimum of 24 hours' notice of emergency maintenance.

Contractor shall meet monthly with State, which will include discussions related to technical performance of services, service delivery compliance, operational updates and billing performance.

Contractor and State will discuss/coordinate scheduling failover testing and when/how to provide redundant paths.

**Data Compliance**

In connection with its provision of the Services under this Agreement, the Service Provider shall comply with applicable data security and privacy laws (including any applicable laws pertaining to Contractor's handling of Personally Identifiable Information (PII), notification of security breaches, social security number protection. With respect to Contractor's Ethernet Dedicated Internet Services, Ethernet Transport Services and Business Internet Services provided hereunder, Contractor shall adhere to the standards set forth in:

NIST 800-53 Revisions 4 – Moderate Risk Controls

**Cap on fees or charges for late payment**

The State shall not be liable for charges for late payment, late payment interest, or late payment fees, exceeding in the aggregate the greater of 3% on an annual basis or the then-current applicable federal mid-term rate.

## ATTACHMENT B – PAYMENT PROVISIONS

The maximum dollar amount payable under this contract is not intended as any form of a guaranteed amount. The Contractor will be paid for products or services actually delivered or performed, as specified in Attachment A, up to the maximum allowable amount specified on page 1 of this contract.

1. Prior to commencement of work and release of any payments, Contractor shall submit to the State:
  - a. a certificate of insurance consistent with the requirements set forth in Attachment C, Section 8 (Insurance), and with any additional requirements for insurance as may be set forth elsewhere in this contract; and
  - b. a current IRS Form W-9 (signed within the last six months).
2. Payment terms are Net 30 days from the date the State receives an error-free invoice with all necessary and complete supporting documentation. Invoices shall include such information and/or documentation appropriate and sufficient to substantiate the amount invoiced for payment.
3. Invoices shall be sent to the address identified on the applicable Work Order and shall specify the address to which payments will be sent. The State of Vermont Contract Number, and the name of the purchasing entity, shall appear on each invoice for all purchases placed under this Contract.
4. Contractor shall submit invoices to the State in accordance with the schedule set forth in this Attachment B. Unless a more particular schedule is provided herein, invoices shall be submitted not more frequently than monthly. Notwithstanding the foregoing or anything to the contrary contained in the Contract, the Parties acknowledge and agree that (i) the pricing on Attachment B shall apply to Sales Order placed by the State on or after the Effective Date and (ii) Existing Orders shall continue to be provisioned at their existing pricing.
5. The payment schedule for delivered products, or rates for services performed, and any additional reimbursements, are as provided below. State acknowledges and agree that the below charges are exclusive of any applicable taxes, usage charges (e.g., long distance calling), installation charges, or any fees or payment obligations imposed by governmental or quasi-governmental bodies in connection with the sale, installation, use, or provision of the Services (e.g., applicable franchise fees, right of way fees and Universal Service Fund charges).
6. **Administrative Charges.** An Administrative Charge may be applied if accepted in advance by the State whenever a change is made to the State's Service configuration at State's request. Such changes are defined as those rearrangements necessary to add, delete, or rearrange State's configuration, including changes to State's selected carrier. Although multiple changes may be caused by such actions, only one Administrative Charge will apply per State request and shall not exceed \$100 dollars.

**Ethernet Dedicated Internet (EDI)**

<b>EDI</b>		<b>36mo MRC</b>	<b>E-Rate Price</b>		<b>60mo MRC</b>	<b>E-Rate Price</b>		<b>NRC</b>
5M		\$ 175.00			\$ 150.00			\$ 199.00
10M		\$ 225.00			\$ 200.00			\$ 199.00
15M		\$ 275.00			\$ 250.00			\$ 199.00
20M		\$ 300.00	\$ 300.00		\$ 275.00	\$ 275.00		\$ 199.00
25M		\$ 325.00			\$ 285.00			\$ 199.00
30M		\$ 350.00	\$ 350.00		\$ 300.00	\$ 300.00		\$ 199.00
40M		\$ 375.00			\$ 325.00			\$ 199.00
50M		\$ 400.00	\$ 400.00		\$ 350.00	\$ 350.00		\$ 199.00
60M		\$ 410.00			\$ 360.00			\$ 199.00
70M		\$ 420.00			\$ 370.00			\$ 199.00
80M		\$ 430.00			\$ 380.00			\$ 199.00
90M		\$ 440.00			\$ 390.00			\$ 199.00
100M		\$ 450.00	\$ 450.00		\$ 400.00	\$ 400.00		\$ 199.00
200M		\$ 602.65	\$ 600.00		\$ 542.47	\$ 500.00		\$ 199.00
300M		\$ 764.15	\$ 700.00		\$ 687.82	\$ 600.00		\$ 199.00
400M		\$ 908.65	\$ 750.00		\$ 817.87	\$ 700.00		\$ 199.00
500M		\$ 1,040.40	\$ 850.00		\$ 936.36	\$ 800.00		\$ 199.00
1G		\$ 1,520.65	\$ 1,150.00		\$ 1,368.67	\$ 1,050.00		\$ 199.00
2G		\$ 2,039.15	\$ 1,300.00		\$ 1,835.32	\$ 1,200.00		\$ 199.00
3G		\$ 2,532.15	\$ 1,600.00		\$ 2,279.02	\$ 1,400.00		\$ 199.00
4G		\$ 2,999.65	\$ 1,900.00		\$ 2,699.77	\$ 1,700.00		\$ 199.00
5G		\$ 3,450.15	\$ 2,200.00		\$ 3,105.22	\$ 2,000.00		\$ 199.00
10G		\$ 5,447.65	\$ 3,400.00		\$ 4,902.97	\$ 3,100.00		\$ 199.00

<b>DDoS Unlimited</b>		<b>MRC</b>		<b>NRC</b>
1M - 49M		\$400.00		\$500.00
50M - 499M		\$500.00		\$500.00
500M - 1G		\$800.00		\$500.00
2G - 10G		\$2,400.00		\$500.00

**Ethernet Network Services (ENS)**

<b>Basic ENS</b>	-	<b>36-month MRC</b>	-	<b>60 month MRC</b>	-	<b>NRC</b>		<b>Priority CoS</b>	-	<b>36-month MRC</b>	-	<b>60 month MRC</b>
5M		\$84.00		\$75.60		\$199.00		1M		15.00		13.60
10M		\$134.00		\$120.60		\$199.00		2M		25.00		22.60
15M		\$144.00		\$129.60		\$199.00		3M		36.00		32.40
20M		\$150.00		\$135.00		\$199.00		5M		57.00		51.40
25M		\$160.00		\$144.00		\$199.00		10M		110.00		99.00
30M		\$164.00		\$147.60		\$199.00						
40M		\$180.00		\$162.00		\$199.00		<b>Premium CoS</b>	-	<b>36mo MRC</b>	-	<b>60mo MRC</b>
50M		\$194.00		\$174.60		\$199.00		1M		16.00		14.40
60M		\$210.00		\$189.00		\$199.00		2M		26.00		23.40
70M		\$224.00		\$201.60		\$199.00		3M		37.00		33.40
80M		\$240.00		\$216.00		\$199.00		5M		60.00		50.40
90M		\$254.00		\$228.60		\$199.00		10M		114.00		102.60
100M		\$270.00		\$243.00		\$199.00						
200M		\$388.00		\$349.20		\$199.00						
300M		\$406.00		\$365.40		\$199.00						
400M		\$424.00		\$381.60		\$199.00						
500M		\$442.00		\$397.80		\$199.00						
1G		\$532.00		\$478.80		\$199.00						
5G		\$1,348.00		\$1,213.20		\$199.00						
10G		\$3,180.00		\$2,862.00		\$199.00						

\*5M to 10G Basic MRC included EVC and UNI

\*\*1M to 10M Priority and Premium MRC includes just the EVC

There may be additional one-time construction costs depending on results of fiber construction survey.

**Ethernet Private Line Services (EPL)**

<u>Basic EPL</u>	<u>36-month MRC</u>	<u>60 month MRC</u>	<u>NRC</u>	<u>Priority CoS</u>	<u>36-month MRC</u>	<u>60 month MRC</u>
5M	\$102.00	\$91.80	\$199.00	1M	\$10.00	\$9.00
10M	\$144.00	\$129.60	\$199.00	2M	\$20.00	\$18.00
15M	\$152.00	\$136.80	\$199.00	3M	\$28.00	\$25.20
20M	\$156.00	\$140.40	\$199.00	5M	\$48.00	\$43.20
25M	\$164.00	\$147.60	\$199.00	10M	\$96.00	\$86.40
30M	\$170.00	\$153.00	\$199.00			
40M	\$182.00	\$163.80	\$199.00	<u>Premium CoS</u>	<u>36mo MRC</u>	<u>60mo MRC</u>
50M	\$194.00	\$174.60	\$199.00	1M	\$12.00	\$10.80
60M	\$208.00	\$187.20	\$199.00	2M	\$22.00	\$19.80
70M	\$220.00	\$198.00	\$199.00	3M	\$34.00	\$30.60
80M	\$232.00	\$208.80	\$199.00	5M	\$56.00	\$50.40
90M	\$244.00	\$219.60	\$199.00	10M	\$112.00	\$102.60
100M	\$258.00	\$232.20	\$199.00			
200M	\$488.00	\$439.20	\$199.00			
300M	\$506.00	\$455.40	\$199.00			
400M	\$524.00	\$471.60	\$199.00			
500M	\$542.00	\$487.80	\$199.00			
1G	\$632.00	\$568.80	\$199.00			
2G	\$1,284.00	\$1,155.60	\$199.00			
3G	\$1,428.00	\$1,285.20	\$199.00			
5G	\$1,878.00	\$1,690.20	\$199.00			
10G	\$3,740.00	\$3,366.00	\$199.00			

\*5M to 10G Basic MRC included EVC and UNI

\*\*1M to 10M Priority and Premium MRC includes just the EVC

There may be additional one time construction costs depending on results of fiber construction survey.

**Ethernet Virtual Private Line Services (EVPL)**

<u>Basic EVPL</u>	-	<u>36-month MRC</u>	-	<u>60 month MRC</u>	-	<u>NRC</u>		<u>Priority CoS</u>	-	<u>36-month MRC</u>	-	<u>60 month MRC</u>		
5M		\$93.00		\$83.80		\$199.00		1M		\$21.00		\$19.00		
10M		\$134.00		\$130.60		\$199.00		2M		\$29.00		\$26.20		
15M		\$156.00		\$129.60		\$199.00		3M		\$44.00		\$39.60		
20M		\$150.00		\$135.00		\$199.00		5M		\$66.00		\$59.40		
25M		\$160.00		\$144.00		\$199.00		10M		\$110.00		\$99.00		
30M		\$164.00		\$147.60		\$199.00								
40M		\$180.00		\$162.00		\$199.00		<u>Premium CoS</u>	-	<u>36mo MRC</u>	-	<u>60mo MRC</u>		
50M		\$194.00		\$174.60		\$199.00		1M		\$22.00		\$19.80		
60M		\$210.00		\$189.00		\$199.00		2M		\$30.00		\$27.00		
70M		\$224.00		\$201.60		\$199.00		3M		\$46.00		\$41.40		
80M		\$240.00		\$216.00		\$199.00		5M		\$71.00		\$64.00		
90M		\$254.00		\$226.80		\$199.00		10M		\$114.00		\$102.60		
100M		\$270.00		\$243.00		\$199.00								
200M		\$388.00		\$349.20		\$199.00		<u>Hub Port</u>	-	<u>36mo MRC</u>	-	<u>60mo MRC</u>	-	<u>NRC</u>
300M		\$406.00		\$365.40		\$199.00		10/100		\$30.00		\$27.00		\$199.00
400M		\$424.00		\$381.60		\$199.00		Gig E		\$130.00		\$117.00		\$199.00
500M		\$442.00		\$397.80		\$199.00		10 Gig		\$400.00		\$360.00		\$199.00
1G		\$532.00		\$478.80		\$199.00								
2G		\$898.00		\$808.20		\$199.00								
3G		\$1,016.00		\$914.40		\$199.00								
5G		\$1,348.00		\$1,213.20		\$199.00								
10G		\$3,180.00		\$2,862.00		\$199.00								

**Comcast SD-WAN with ActiveCore**

<b><u>SD-WAN</u></b>	<b><u>MRC</u></b>	<b><u>NRC</u></b>	
SD-WAN	\$199.00	\$0.00	
Installation	\$0.00	\$550.00	
uCPE Medium	\$30.00	\$0.00	
uCPE Large	\$250.00	\$0.00	
Managed SD-WAN	\$50.00	\$300.00	* Service is in addition to SD-WAN fee. If one site is Managed, all sites must be Managed.
Wireless Back Up	\$64.99	\$0.00	
Equipment	\$10.00	\$0.00	
Installation	\$0.00	\$99.99	
<b><u>Cybersecurity</u></b>	<b><u>MRC</u></b>	<b><u>NRC</u></b>	
Versa – Unified Security	\$350.00	\$350.00	
Palo Alto – Unified Secure Access	\$400.00	\$500.00	
Remote Access	\$8.00		Price is per user

**Comcast Wave Services**

<b><u>10G Wave Unprotected</u></b>	<b><u>36-month MRC</u></b>	<b><u>60 month MRC</u></b>	<b><u>NRC</u></b>
Commercial to Commercial	\$2,700.00	\$2,200.00	\$0.00
Commercial to Carrier-Neutral Colo	\$2,400.00	\$1,900.00	\$0.00
Carrier-Neutral Colo to Carrier Neutral Colo	\$2,100.00	\$1,600.00	\$0.00
<b><u>100G Wave Unprotected</u></b>	<b><u>36-month MRC</u></b>	<b><u>60 month MRC</u></b>	<b><u>NRC</u></b>
Commercial to Commercial	\$5,900.00	\$4,400.00	\$0.00
Commercial to Carrier-Neutral Colo	\$4,900.00	\$3,800.00	\$0.00
Carrier-Neutral Colo to Carrier Neutral Colo	\$3,900.00	\$3,200.00	\$0.00
<b><u>10G Wave Protected</u></b>	<b><u>36-month MRC</u></b>	<b><u>60 month MRC</u></b>	<b><u>NRC</u></b>
Commercial to Commercial	\$4,800.00	\$4,300.00	\$0.00
Commercial to Carrier-Neutral Colo	\$3,900.00	\$3,500.00	\$0.00
Carrier-Neutral Colo to Carrier Neutral Colo	\$3,200.00	\$2,700.00	\$0.00

**Comcast Business Trunks (PRI) and (SIP)**

<u>PRI</u>	-	<u>36-month MRC</u>	-	<u>60 month MRC</u>	-	<u>NRC</u>			
Full PRI (each)		\$489.00		\$489.00			*200 LD minutes included per Channel		
Equipment fee per site		\$19.95		\$19.95					
Per Site Installation		\$0.00		\$0.00		\$500.00			
<u>SIP Concurrent Call Session</u>	-	<u>36-month MRC</u>	-	<u>60 month MRC</u>	-	<u>NRC</u>			
6 to 9		\$35.00		\$35.00		\$0.00	* MRC per Concurrent Call Session		
10 to 14		\$30.00		\$30.00		\$0.00	*200 LD minutes included per CCS		
15 to 24		\$21.00		\$21.00		\$0.00			
25 to 49		\$14.00		\$14.00		\$0.00			
50 to 99		\$13.00		\$13.00		\$0.00			
100 to 249		\$11.00		\$11.00		\$0.00			
250 to 499		\$10.00		\$10.00		\$0.00			
500 to 749		\$9.00		\$9.00		\$0.00			
750 to 999		\$8.00		\$8.00		\$0.00			
1000		\$7.00		\$7.00		\$0.00			
Equipment Fee per site		\$14.95		\$14.95		\$0.00			
Per Site Installation		\$0.00		\$0.00		\$500.00			
<u>Optional Features</u>		<u>36-month MRC</u>	-	<u>60 month MRC</u>		<u>NRC</u>	<u>PRI &amp; SIP TNs</u>		<u>MRC</u>
Toll Free Number		\$10.00		\$10.00		\$9.95	1 TN Block		\$0.20
Trunk Group		\$0.00		\$0.00		\$0.00	2 TN Block		\$0.40
Busting TG per CCS (SIP)		\$2.00		\$2.00		\$0.00	5 TN Block		\$1.00
Failover TG		\$5.00		\$5.00		\$0.00	10 TN Block		\$2.00
Load Balancing TG		\$5.00		\$5.00		\$0.00	20 TN Block		\$4.00
CNAM at the TN Level		\$0.00		\$0.00		\$0.00	100 TN Block		\$20.00
CFNR per DID		\$1.00		\$1.00		\$0.00	200 TN Block		\$40.00
Unreachable Destination		\$0.00		\$0.00		\$0.00	500 TN Block		\$100.00
DNIS per TG		\$50.00		\$50.00		\$0.00	1000 TN Block		\$200.00
Vanity TN Search		\$0.00		\$0.00		\$0.00	Ported TNs		\$0
Monthly CDR		\$0.00		\$0.00		\$0.00			
DL Non-Listed - Commercial		\$0.00		\$0.00		\$24.95			
DL Non-Published		\$0.00		\$0.00		\$24.95			

<b><u>PRI Long Distance Usage - U.S.</u></b>	<b><u>Per minute Rate</u></b>	
Tier 1 = 0-4,999	\$0.03	
Tier 2 = 5,000-7,499	\$0.03	
Tier 3 = 7,500-9,999	\$0.03	
Tier 4 = 10,000-14,999	\$0.02	
Tier 5 = 15,000-49,999	\$0.02	
Tier 6 = 50,000-99,999	\$0.02	
Tier 7 = 100,000+	\$0.02	
Toll Call Pooled Minutes	\$0.00	*200 per Channel
<b><u>SIP Long Distance Usage - U.S.</u></b>	<b><u>Per minute Rate</u></b>	
Tier 1 = 0-4,999	\$0.03	
Tier 2 = 5,000-7,499	\$0.03	
Tier 3 = 7,500-9,999	\$0.02	
Tier 4 = 10,000-14,999	\$0.02	
Tier 5 = 15,000-49,999	\$0.02	
Tier 6 = 50,000-99,999	\$0.02	
Tier 7 = 100,000+	\$0.02	
Toll Call Pooled Minutes	\$0.00	*200 per Channel

### Comcast Video Services

<b>Video Service</b>	
<b>Private/public view</b>	<b>MRC</b>
TV Basic (C0/BR0)	\$42.95
TV Select (C0.5/BR0.5)	\$47.95
TV Variety (C1.5/BR1.5)	\$64.95
TV Standard (C2/BR2)	\$89.95
TV Preferred (C3/BR3)	\$114.95
Sports & Entertainment package	\$34.95
Public view service charge	\$20.00
<b>Equipment</b>	
Video outlet (primary and additional)	\$9.95
<b>Add-ons</b>	
Music Choice	\$29.95
Canales Selecto	\$15.95

**Option: Comcast Business Internet:**

Broadband Internet		
Product	MRC	NRC
BI Essential - 50 Mbps	\$99.95	\$99.95
BI Standard - 100 Mbps	\$149.95	\$99.95
BI Performance - 250 Mbps	\$199.95	\$99.95
BI Advanced - 500 Mbps	\$249.95	\$99.95
BI Premium - 750 Mbps	\$299.95	\$99.95
BI Gigabit Extra - 1.25 Gbps	\$399.95	\$99.95
BI 2Gig - 2 Gbps	\$499.95	\$99.95
Equipment Fees		
	MRC	
Modem Fee	\$19.95	

Static IPs	
	MRC
1 Static	\$24.95
5 Static	\$29.95
13 Static IP	\$44.95

**Option: Comcast DDoS:**

DDoS Unlimited		
Bandwidth Tier	MRC	NRC (per circuit)
1 Mbps - 49 Mbps	\$400.00	\$500.00
50 Mbps - 499 Mbps	\$500.00	\$500.00
500 Mbps - 1 Gbps	\$800.00	\$500.00
2 Gbps - or higher	\$2,400.00	\$500.00

**Engineering Review.** Each Sales Order submitted by Customer may be subject to an engineering review. The engineering review will determine whether and to what extent the Network must be extended, built or upgraded ("Custom Installation") in order to provide the ordered Services at the requested Service Location(s). Comcast will provide Customer written notification in the event Service installation at any Service Location will require an additional non-recurring installation fee ("Custom Installation Fee"). Custom Installation Fees may also be referred to as Construction Charges on a Sales Order or Invoice. Customer will have five (5) days from receipt of such notice to reject the Custom Installation Fee and terminate, without further liability, the Sales Order with respect to the affected Service Location(s). For certain Services, the Engineering Review will be conducted prior to Sales Order submission. In such case, Customer will have accepted the designated Custom Installation Fee upon submission of the applicable Sales Order

**ATTACHMENT C: STANDARD  
STATE PROVISIONS FOR  
CONTRACTS AND GRANTS  
REVISED DECEMBER 15, 2017**

**1. Definitions:** For purposes of this Attachment, “Party” shall mean the Contractor, Grantee or Subrecipient, with whom the State of Vermont is executing this Agreement and consistent with the form of the Agreement. “Agreement” shall mean the specific contract or grant to which this form is attached.

**2. Entire Agreement:** This Agreement, whether in the form of a contract, State-funded grant, or Federally-funded grant, represents the entire agreement between the parties on the subject matter. All prior agreements, representations, statements, negotiations, and understandings shall have no effect.

**3. Governing Law, Jurisdiction and Venue; No Waiver of Jury Trial:** This Agreement will be governed by the laws of the State of Vermont. Any action or proceeding brought by either the State or the Party in connection with this Agreement shall be brought and enforced in the Superior Court of the State of Vermont, Civil Division, Washington Unit. The Party irrevocably submits to the jurisdiction of this court for any action or proceeding regarding this Agreement. The Party agrees that it must first exhaust any applicable administrative remedies with respect to any cause of action that it may have against the State with regard to its performance under this Agreement. Party agrees that the State shall not be required to submit to binding arbitration or waive its right to a jury trial.

**4. Sovereign Immunity:** The State reserves all immunities, defenses, rights or actions arising out of the State’s sovereign status or under the Eleventh Amendment to the United States Constitution. No waiver of the State’s immunities, defenses, rights or actions shall be implied or otherwise deemed to exist by reason of the State’s entry into this Agreement.

**5. No Employee Benefits For Party:** The Party understands that the State will not provide any individual retirement benefits, group life insurance, group health and dental insurance, vacation or sick leave, workers compensation or other benefits or services available to State employees, nor will the State withhold any state or Federal taxes except as required under applicable tax laws, which shall be determined in advance of execution of the Agreement. The Party understands that all tax returns required by the Internal Revenue Code and the State of Vermont, including but not limited to income, withholding, sales and use, and rooms and meals, must be filed by the Party, and information as to Agreement income will be provided by the State of Vermont to the Internal Revenue Service and the Vermont Department of Taxes.

**6. Independence:** The Party will act in an independent capacity and not as officers or employees of the State.

**7. Defense and Indemnity:** The Party shall defend the State and its officers and employees against all third party claims or suits arising in whole or in part from any act or omission of the Party or of any agent of the Party in connection with the performance of this Agreement. The State shall notify the Party in the event of any such claim or suit, and the Party shall immediately retain counsel and otherwise provide a complete defense against the entire claim or suit. The State retains the right to participate at its own expense in the defense of any claim. The State shall have the right to approve all proposed settlements of such claims or suits.

After a final judgment or settlement, the Party may request recoupment of specific defense costs and may file suit in Washington Superior Court requesting recoupment. The Party shall be entitled to recoup costs only upon a showing that such costs were entirely unrelated to the defense of any claim

arising from an act or omission of the Party in connection with the performance of this Agreement.

The Party shall indemnify the State and its officers and employees if the State, its officers or employees become legally obligated to pay any damages or losses arising from any act or omission of the Party or an agent of the Party in connection with the performance of this Agreement.

Notwithstanding any contrary language anywhere, in no event shall the terms of this Agreement or any document furnished by the Party in connection with its performance under this Agreement obligate the State to (1) defend or indemnify the Party or any third party, or (2) otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or other costs of the Party or any third party.

**8. Insurance:** Before commencing work on this Agreement the Party must provide certificates of insurance to show that the following minimum coverages are in effect. It is the responsibility of the Party to maintain current certificates of insurance on file with the State through the term of this Agreement. No warranty is made that the coverages and limits listed herein are adequate to cover and protect the interests of the Party for the Party's operations. These are solely minimums that have been established to protect the interests of the State.

*Workers Compensation:* With respect to all operations performed, the Party shall carry workers' compensation insurance in accordance with the laws of the State of Vermont. Vermont will accept an out-of-state employer's workers' compensation coverage while operating in Vermont provided that the insurance carrier is licensed to write insurance in Vermont and an amendatory endorsement is added to the policy adding Vermont for coverage purposes. Otherwise, the party shall secure a Vermont workers' compensation policy, if necessary to comply with Vermont law.

*General Liability and Property Damage:* With respect to all operations performed under this Agreement, the Party shall carry general liability insurance having all major divisions of coverage including, but not limited to:

- Premises - Operations

- Products and

- Completed

- Operations

- Personal Injury

- Liability

- Contractual

- Liability

The policy shall be on an occurrence form and limits shall not be less than:

- \$1,000,000 Each Occurrence

- \$2,000,000 General Aggregate

- \$1,000,000 Products/Completed Operations Aggregate

- \$1,000,000 Personal & Advertising Injury

*Automotive Liability:* The Party shall carry automotive liability insurance covering all motor vehicles, including hired and non-owned coverage, used in connection with the Agreement. Limits of coverage shall not be less than \$500,000 combined single limit. If performance of this Agreement involves construction, or the transport of persons or hazardous materials, limits of coverage shall not be less than \$1,000,000 combined single limit.

*Additional Insured.* The General Liability and Property Damage coverages required for performance of this Agreement shall include the State of Vermont and its agencies, departments, officers and employees as Additional Insureds. If performance of this Agreement involves construction, or the transport of persons or hazardous materials, then the required Automotive Liability coverage shall include the State

of Vermont and its agencies, departments, officers and employees as Additional Insureds. Coverage shall be primary and non-contributory with any other insurance and self-insurance.

*Notice of Cancellation or Change.* There shall be no cancellation, change, potential exhaustion of aggregate limits or non-renewal of insurance coverage(s) without thirty (30) days written prior written notice to the State.

**9. Reliance by the State on Representations:** All payments by the State under this Agreement will be made in reliance upon the accuracy of all representations made by the Party in accordance with this Agreement, including but not limited to bills, invoices, progress reports and other proofs of work.

**10. False Claims Act:** The Party acknowledges that it is subject to the Vermont False Claims Act as set forth in 32 V.S.A.

§ 630 *et seq.* If the Party violates the Vermont False Claims Act it shall be liable to the State for civil penalties, treble damages and the costs of the investigation and prosecution of such violation, including attorney's fees, except as the same may be reduced by a court of competent jurisdiction. The Party's liability to the State under the False Claims Act shall not be limited notwithstanding any agreement of the State to otherwise limit Party's liability.

**11. Whistleblower Protections:** The Party shall not discriminate or retaliate against one of its employees or agents for disclosing information concerning a violation of law, fraud, waste, abuse of authority or acts threatening health or safety, including but not limited to allegations concerning the False Claims Act. Further, the Party shall not require such employees or agents to forego monetary awards as a result of such disclosures, nor should they be required to report misconduct to the Party or its agents prior to reporting to any governmental entity and/or the public.

**12. Location of State Data:** No State data received, obtained, or generated by the Party in connection with performance under this Agreement shall be processed, transmitted, stored, or transferred by any means outside the continental United States, except with the express written permission of the State.

**13. Records Available for Audit:** The Party shall maintain all records pertaining to performance under this agreement. "Records" means any written or recorded information, regardless of physical form or characteristics, which is produced or acquired by the Party in the performance of this agreement. Records produced or acquired in a machine readable electronic format shall be maintained in that format. The records described shall be made available at reasonable times during the period of the Agreement and for three years thereafter or for any period required by law for inspection by any authorized representatives of the State or Federal Government. If any litigation, claim, or audit is started before the expiration of the three-year period, the records shall be retained until all litigation, claims or audit findings involving the records have been resolved.

**14. Fair Employment Practices and Americans with Disabilities Act:** Party agrees to comply with the requirement of 21

V.S.A. Chapter 5, Subchapter 6, relating to fair employment practices, to the full extent applicable. Party shall also ensure, to the full extent required by the Americans with Disabilities Act of 1990, as amended, that qualified individuals with disabilities receive equitable access to the services, programs, and activities provided by the Party under this Agreement.

**15. Set Off:** The State may set off any sums which the Party owes the State against any sums due the Party under this Agreement; provided, however, that any set off of amounts due the State of Vermont as taxes shall be in accordance with the procedures more specifically provided hereinafter.

**16. Taxes Due to the State:**

- A.** Party understands and acknowledges responsibility, if applicable, for compliance with State tax laws, including income tax withholding for employees performing services within the State, payment of use tax on property used within the State, corporate and/or personal income tax on income earned within the State.
- B.** Party certifies under the pains and penalties of perjury that, as of the date this Agreement is signed, the Party is in good standing with respect to, or in full compliance with, a plan to pay any and all taxes due the State of Vermont.
- C.** Party understands that final payment under this Agreement may be withheld if the Commissioner of Taxes determines that the Party is not in good standing with respect to or in full compliance with a plan to pay any and all taxes due to the State of Vermont.
- D.** Party also understands the State may set off taxes (and related penalties, interest and fees) due to the State of Vermont, but only if the Party has failed to make an appeal within the time allowed by law, or an appeal has been taken and finally determined and the Party has no further legal recourse to contest the amounts due.

**17. Taxation of Purchases:** All State purchases must be invoiced tax free. An exemption certificate will be furnished upon request with respect to otherwise taxable items.

**18. Child Support:** (Only applicable if the Party is a natural person, not a corporation or partnership.) Party states that, as of the date this Agreement is signed, he/she:

- A.** is not under any obligation to pay child support; or
- B.** is under such an obligation and is in good standing with respect to that obligation; or
- C.** has agreed to a payment plan with the Vermont Office of Child Support Services and is in full compliance with that plan.

Party makes this statement with regard to support owed to any and all children residing in Vermont. In addition, if the Party is a resident of Vermont, Party makes this statement with regard to support owed to any and all children residing in any other state or territory of the United States.

**19. Sub-Agreements:** Party shall not assign, subcontract or subgrant the performance of this Agreement or any portion thereof to any other Party without the prior written approval of the State. Party shall be responsible and liable to the State for all acts or omissions of subcontractors and any other person performing work under this Agreement pursuant to an agreement with Party or any subcontractor.

In the case this Agreement is a contract with a total cost in excess of \$250,000, the Party shall provide to the State a list of all proposed subcontractors and subcontractors' subcontractors, together with the identity of those subcontractors' workers compensation insurance providers, and additional required or requested information, as applicable, in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54).

Party shall include the following provisions of this Attachment C in all subcontracts for work performed solely for the State of Vermont and subcontracts for work performed in the State of Vermont: Section 10 ("False Claims Act"); Section 11 ("Whistleblower Protections"); Section 12 ("Location of State Data"); Section 14 ("Fair Employment Practices and Americans with Disabilities Act"); Section 16 ("Taxes Due the State"); Section 18 ("Child Support"); Section 20 ("No Gifts or Gratuities"); Section 22 ("Certification Regarding Debarment"); Section 30 ("State Facilities"); and Section 32.A ("Certification Regarding Use of State Funds").

**20. No Gifts or Gratuities:** Party shall not give title or possession of anything of substantial value (including property, currency, travel and/or education programs) to any officer or employee of the State

during the term of this Agreement.

**21. Copies:** Party shall use reasonable best efforts to ensure that all written reports prepared under this Agreement are printed using both sides of the paper.

**22. Certification Regarding Debarment:** Party certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, neither Party nor Party's principals (officers, directors, owners, or partners) are presently debarred, suspended, proposed for debarment, declared ineligible or excluded from participation in Federal programs, or programs supported in whole or in part by Federal funds.

Party further certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, Party is not presently debarred, suspended, nor named on the State's debarment list at: <http://bgs.vermont.gov/purchasing/debarment>

**23. Conflict of Interest:** Party shall fully disclose, in writing, any conflicts of interest or potential conflicts of interest.

**24. Confidentiality:** Party acknowledges and agrees that this Agreement and any and all information obtained by the State from the Party in connection with this Agreement are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq.

**25. Force Majeure:** Neither the State nor the Party shall be liable to the other for any failure or delay of performance of any obligations under this Agreement to the extent such failure or delay shall have been wholly or principally caused by acts or events beyond its reasonable control rendering performance illegal or impossible (excluding strikes or lock-outs) ("Force Majeure"). Where Force Majeure is asserted, the nonperforming party must prove that it made all reasonable efforts to remove, eliminate or minimize such cause of delay or damages, diligently pursued performance of its obligations under this Agreement, substantially fulfilled all non-excused obligations, and timely notified the other party of the likelihood or actual occurrence of an event described in this paragraph.

**26. Marketing:** Party shall not refer to the State in any publicity materials, information pamphlets, press releases, research reports, advertising, sales promotions, trade shows, or marketing materials or similar communications to third parties except with the prior written consent of the State.

**27. Termination:**

**A. Non-Appropriation:** If this Agreement extends into more than one fiscal year of the State (July 1 to June 30), and if appropriations are insufficient to support this Agreement, the State may cancel at the end of the fiscal year, or otherwise upon the expiration of existing appropriation authority. In the case that this Agreement is a Grant that is funded in whole or in part by Federal funds, and in the event Federal funds become unavailable or reduced, the State may suspend or cancel this Grant immediately, and the State shall have no obligation to pay Subrecipient from State revenues.

**B. Termination for Cause:** Either party may terminate this Agreement if a party materially breaches its obligations under this Agreement, and such breach is not cured within thirty (30) days after delivery of the non-breaching party's notice or such longer time as the non-breaching party may specify in the notice.

**C. Termination Assistance:** Upon nearing the end of the final term or termination of this Agreement, without respect to cause, the Party shall take all reasonable and prudent measures to facilitate any transition required by the State. All State property, tangible and intangible, shall

be returned to the State upon demand at no additional cost to the State in a format acceptable to the State.

**28. Continuity of Performance:** In the event of a dispute between the Party and the State, each party will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.

**29. No Implied Waiver of Remedies:** Either party's delay or failure to exercise any right, power or remedy under this Agreement shall not impair any such right, power or remedy, or be construed as a waiver of any such right, power or remedy. All waivers must be in writing.

**30. State Facilities:** If the State makes space available to the Party in any State facility during the term of this Agreement for purposes of the Party's performance under this Agreement, the Party shall only use the space in accordance with all policies and procedures governing access to and use of State facilities which shall be made available upon request. State facilities will be made available to Party on an "AS IS, WHERE IS" basis, with no warranties whatsoever.

**31. Requirements Pertaining Only to Federal Grants and Subrecipient Agreements:** If this Agreement is a grant that is funded in whole or in part by Federal funds:

**A. Requirement to Have a Single Audit:** The Subrecipient will complete the Subrecipient Annual Report annually within 45 days after its fiscal year end, informing the State of Vermont whether or not a Single Audit is required for the prior fiscal year. If a Single Audit is required, the Subrecipient will submit a copy of the audit report to the granting Party within 9 months. If a single audit is not required, only the Subrecipient Annual Report is required.

For fiscal years ending before December 25, 2015, a Single Audit is required if the subrecipient expends \$500,000 or more in Federal assistance during its fiscal year and must be conducted in accordance with OMB Circular A-

133. For fiscal years ending on or after December 25, 2015, a Single Audit is required if the subrecipient expends

\$750,000 or more in Federal assistance during its fiscal year and must be conducted in accordance with 2 CFR Chapter I, Chapter II, Part 200, Subpart F. The Subrecipient Annual Report is required to be submitted within 45 days, whether or not a Single Audit is required.

**B. Internal Controls:** In accordance with 2 CFR Part II, §200.303, the Party must establish and maintain effective internal control over the Federal award to provide reasonable assurance that the Party is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the award. These internal controls should be in compliance with guidance in "Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States and the "Internal Control Integrated Framework", issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

**C. Mandatory Disclosures:** In accordance with 2 CFR Part II, §200.113, Party must disclose, in a timely manner, in writing to the State, all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. Failure to make required disclosures may result in the imposition of sanctions which may include disallowance of costs incurred, withholding of payments, termination of the Agreement, suspension/debarment, etc.

**32. Requirements Pertaining Only to State-Funded Grants:**

**A. Certification Regarding Use of State Funds:** If Party is an employer and this Agreement is a State-funded grant in excess of \$1,001, Party certifies that none of these State funds will be used to interfere with or restrain the exercise of Party's employee's rights with respect to unionization.

**B. Good Standing Certification (Act 154 of 2016):** If this Agreement is a State-funded grant, Party

hereby represents:

(i) that it has signed and provided to the State the form prescribed by the Secretary of Administration for purposes of certifying that it is in good standing (as provided in Section 13(a)(2) of Act 154) with the Agency of Natural Resources and the Agency of Agriculture, Food and Markets, or otherwise explaining the circumstances surrounding the inability to so certify, and (ii) that it will comply with the requirements stated therein.

(End of Standard Provisions)

STATE OF VERMONT- FEDERAL  
TERMS SUPPLEMENT (Non-Construction)  
**for all Contracts and Purchases of Products and Services Using Federal Funds**  
(Revision date: June 27, 2022)

**PROCUREMENT OF RECOVERED MATERIALS**

In the performance of this contract, the Contractor shall make maximum use of products containing recovered materials that are EPA-designated Items unless the products cannot be acquired-

1. Competitively within a time frame providing for compliance with the contract performance schedule;
2. Meeting contract performance requirements; or
3. At a reasonable price

Information about this requirement, along with the list of EPA-designated items, is available at the EPA's Comprehensive Procurement Guidelines web site, <https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program>.

The Contractor also agrees to comply with all other applicable requirements of section 6002 of the Solid Waste Disposal Act.

**CLEAN AIR ACT AND FEDERAL WATER POLLUTION CONTROL ACT**

1. The contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.
2. The contractor agrees to report each violation to the State of Vermont and understands and agrees that the State of Vermont will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.
3. The contractor agrees to include these requirements in each subcontract supporting services under the Agreement exceeding \$150,000 financed in whole or in part with Federal assistance provided by FEMA.
4. The contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.
5. **a.** Standard. Non-Federal entities and contractors are subject to the debarment and suspension regulations implementing Executive Order 12549, *Debarment and Suspension* (1986) and Executive Order 12689, *Debarment and Suspension* (1989) at 2 C.F.R. Part 180 and the Department of Homeland Security's regulations at 2 C.F.R. Part 3000 (Nonprocurement Debarment and Suspension).

**CONTRACTOR BREACH, ERRORS AND OMISSIONS**

1. Any breach of the terms of this contract, or material errors and omissions in the work product of the contractor must be corrected by the contractor at no cost to the State. .
2. Neither the States' review, approval or acceptance of nor payment for, the services required under this contract shall be construed to operate as a waiver of any rights under this contract or of any cause of action arising out of the performance of this contract.
3. The rights and remedies of the State provided for under this contract are in addition to any other rights and remedies provided by law or elsewhere in the contract.

**TERMINATION FOR CONVENIENCE**

1. General

- a. Any termination for convenience shall be effected by delivery to the Contractor an Order of Termination specifying the termination is for the convenience of the Agency, the extent to which performance of work under the Contract is terminated, and the effective date of the termination.
- b. In the event such termination occurs, without fault and for reasons beyond the control of the Contractor, all (i) completed or partially completed items of work as of the date of termination will be paid for in accordance with the contract payment terms and (ii) all early termination charges will be paid in accordance with the terms of the contract.
- c. No compensation will be allowed for items eliminated from the Contract.
- d. Termination of the Contract, or portion thereof, shall not relieve the Contractor of its contractual responsibilities for work completed and shall not relieve the Contractor's Surety of its obligation for and concerning any just claim arising out of the work performed.

2. Contractor Obligations

After receipt of the Notice of Termination and except as otherwise directed by the State, the Contractor shall immediately proceed to:

- a. To the extent specified in the Notice of Termination, stop work under the Contract on the date specified.
- b. Place no further orders or subcontracts for materials, services, and/or facilities except as may be necessary for completion of such portion(s) of the work under the Contract as is (are) not terminated.
- c. Terminate and cancel any orders or subcontracts for related to the services, except as may be necessary for completion of such portion(s) of the work under the Contract as is (are) not terminated.
- d. Transfer to the State all completed or partially completed plans, drawings, information, and other property which, if the Contract had been completed, would be required to be furnished to the State.
- e. Take other action as may be necessary or as directed by the State for the protection and preservation of the property related to the contract which is in the possession of the contractor and in which the State has or may acquire any interest.
- f. Make available to the State all cost and other records relevant to a determination of an equitable settlement.

3. Claim by Contractor

After receipt of the Notice of Termination from the state, the Contractor shall submit any claim for additional costs not covered herein or elsewhere in the Contract within 120 days of the effective termination date, and not thereafter. Should the Contractor fail to submit a claim within the 120-day period, the State may, at its sole discretion, based on information available to it, determine what, if any, compensation is due the Contractor and pay the Contractor the determined amount.

4. Negotiation

Negotiation to settle a timely claim shall be for the sole purpose of reaching a settlement equitable to both the Contractor and the State. To the extent settlement is properly based on Contractor costs, settlement shall be based on actual costs incurred by the Contractor, as reflected by the contract rates. Consequential damages, loss of overhead, loss of overhead contribution of any kind, and/or loss of anticipated profits on work not performed shall not be included in the Contractor's claim and will not be considered, allowed, or included as part of any settlement.

ATTACHMENT D  
INFORMATION TECHNOLOGY PROFESSIONAL SERVICES  
TERMS AND CONDITIONS (rev. 07/14/2022)

**1. OWNERSHIP AND LICENSE IN DELIVERABLES**

**1.1 Contractor Intellectual Property.** Contractor shall retain all right, title and interest in and to any work, ideas, inventions, discoveries, tools, methodology, computer programs, processes and improvements and any other intellectual property, tangible or intangible, that has been created by Contractor prior to entering into this Contract (“Contractor Intellectual Property”). Should the State require a license for the use of Contractor Intellectual Property in connection with the development or use of the items that Contractor is required to deliver to the State under this Contract, including work product (“Deliverables”), the Contractor shall grant the State a royalty-free license for such development and use. For the avoidance of doubt, Work Product shall not be deemed to include Contractor Intellectual Property, provided the State shall be granted an irrevocable, perpetual, non-exclusive royalty-free license to use any such Contractor Intellectual Property that is incorporated into work product. The parties acknowledge and agree that Contractor is not expected or intended to deliver any work product or Deliverables in connection with the provision of the Services.

**1.2 State Intellectual Property.** The State shall retain all right, title and interest in and to (i) all content and all property, data and information furnished by or on behalf of the State or any agency, commission or board thereof, and to all information that is created under this Contract, including, but not limited to, all data that is generated under this Contract as a result of the use by Contractor, the State or any third party of any technology systems or knowledge bases that are developed for the State and used by Contractor hereunder, and all other rights, tangible or intangible; and (ii) all State trademarks, trade names, logos and other State identifiers, Internet uniform resource locators, State user name or names, Internet addresses and e-mail addresses obtained or developed pursuant to this Contract (collectively, “State Intellectual Property”).

Contractor may not use State Intellectual Property for any purpose other than as specified in this Contract. Upon expiration or termination of this Contract, Contractor shall return or destroy all State Intellectual Property and all copies thereof, and Contractor shall have no further right or license to such State Intellectual Property.

Contractor acquires no rights or licenses, including, without limitation, intellectual property rights or licenses, to use State Intellectual Property for its own purposes. In no event shall the Contractor claim any security interest in State Intellectual Property.

**2. CONFIDENTIALITY AND NON-DISCLOSURE; SECURITY BREACH REPORTING**

**2.1** For purposes of this Contract, confidential information will not include information or material which (a) enters the public domain (other than as a result of a breach of this Contract);

(b) was in the receiving party's possession prior to its receipt from the disclosing party; (c) is independently developed by the receiving party without the use of confidential information; (d) is obtained by the receiving party from a third party under no obligation of confidentiality to the disclosing party; or (e) is not exempt from disclosure under applicable State law.

**2.2 Confidentiality of Contractor Information.** The Contractor acknowledges and agrees that this Contract and any and all Contractor information obtained by the State in connection with this Contract are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq. The State will not disclose information for which a reasonable claim of exemption can be made pursuant to 1 V.S.A. § 317(c), including, but not limited to, trade secrets, proprietary information or financial information, including any formulae, plan, pattern, process, tool, mechanism, compound, procedure, production data, or compilation of information which is not patented, which is known only to the Contractor, and which gives the Contractor an opportunity to obtain business advantage over competitors who do not know it or use it.

The State shall immediately notify Contractor of any request made under the Access to Public Records Act, or any request or demand by any court, governmental agency or other person asserting a demand or request for Contractor information. Contractor may, in its discretion, seek an appropriate protective order, or otherwise defend any right it may have to maintain the confidentiality of such information under applicable State law within five (5) business days of the State's notifying Contractor of any such request. Contractor agrees that it will not make any claim against the State if the State makes available to the public any information in accordance with the Access to Public Records Act or in response to a binding order from a court or governmental body or agency compelling its production. Contractor shall indemnify the State for any costs or expenses incurred by the State, including, but not limited to, attorneys' fees awarded in accordance with 1 V.S.A. § 320, in connection with any action brought in connection with Contractor's attempts to prevent or unreasonably delay public disclosure of Contractor's information if a final decision of a court of competent jurisdiction determines that the State improperly withheld such information and that the improper withholding was based on Contractor's attempts to prevent public disclosure of Contractor's information.

The State agrees that (a) it will use the Contractor information only as may be necessary in the course of performing duties, receiving services or exercising rights under this Contract; (b) it will provide at a minimum the same care to avoid disclosure or unauthorized use of Contractor information as it provides to protect its own similar confidential and proprietary information; (c) except as required by the Access to Records Act, it shall not disclose Contractor information to any third party without Contractor's written consent; provided, that, the State may disclose Contractor information to its agents and representatives who have a need to know for the purpose of the State's performance under this Agreement and using the Services so long as such agents and representatives are subject to a written confidentiality agreement that contains restrictions and safeguards at least as restrictive as those contained in this Contract; (d) it will take all reasonable precautions to protect the Contractor's information; and (e) it will not otherwise appropriate such information to its own use or to the use of any other person or entity.

Contractor may affix an appropriate legend to Contractor information that is provided under this Contract to reflect the Contractor's determination that any such information is a trade secret, proprietary information or financial information at time of delivery or disclosure.

### **2.3 RESERVED.**

## **3. SECURITY OF STATE INFORMATION.**

**3.1 Security Standards.** In connection with the provision of the Services under the Agreement, Comcast shall comply with the Comcast Cybersecurity Information Security Program Summary attached to the agreement as Attachment D-1. Without limitation to the foregoing, Comcast shall implement and maintain reasonable and appropriate administrative, physical and technical safeguards consistent with industry standards to protect the security, privacy, confidentiality and integrity of the Contractor Services and the State Confidential Information within Comcast control, in each case, from unauthorized access, disclosure, modification, destruction and use (collectively, "Unauthorized Use").

**3.2 Security Breach Notice and Reporting.** Comcast will maintain a plan for appropriate security incident management and response that covers the Unauthorized Use of State Confidential Information within Comcast's control (each, a "Security Incident"). Comcast will provide notification of a Security Incident as soon as practicable but not more than seventy-two (72) hours after confirmation of the Security Incident. For any Security Incident, Comcast will provide regular updates to You, and will use commercially reasonable efforts to cooperate with You or Your regulators in Your efforts to investigate the Security Incident.

The Contractor agrees to comply with all applicable laws, as such laws may be amended from time to time (including, but not limited to, Chapter 62 of Title 9 of the Vermont Statutes (if applicable) and all applicable State and federal laws, rules or regulations) that require notification in the event of unauthorized release of personally-identifiable information or other event requiring notification.

## **4. CONTRACTOR'S REPRESENTATIONS AND WARRANTIES**

**4.1 General Representations and Warranties.** The Contractor represents and warrants that:

- (i) The Contractor has all requisite power and authority to execute, deliver and perform its obligations under this Contract and the execution, delivery and performance of this Contract by the Contractor has been duly authorized by the Contractor.
- (ii) To its knowledge, as of the Effective Date, there is no outstanding litigation, arbitrated matter or other dispute to which the Contractor is a party which, if decided unfavorably to the Contractor, would reasonably be expected to have a material adverse effect on the Contractor's ability to fulfill its obligations under this Contract.
- (iii) The Contractor will comply with all laws material to its performance of the services and otherwise to the Contractor in connection with its obligations under this Contract.

- (iv) The Contractor (a) owns, or has the right to use under valid and enforceable agreements, all intellectual property rights reasonably necessary for and related to delivery of the services and provision of the services as set forth in this Contract; (b) shall be responsible for and have full authority to license all proprietary and/or third party software modules, including algorithms and protocols, that Contractor incorporates into its product.

## **5. PROFESSIONAL LIABILITY AND CYBER LIABILITY INSURANCE COVERAGE**

In addition to the insurance required in Attachment C to this Contract, before commencing work on this Contract and throughout the term of this Contract, Contractor agrees to procure and maintain (a) Technology Professional Liability insurance for any and all services performed under this Contract, with minimum third party coverage of \$1,000,000.00 per claim, \$2,000,000.00 aggregate. To the extent Contractor has access to, processes, handles, collects, transmits, stores or otherwise deals with State Data, Contractor shall maintain first party Breach Notification Coverage of not less than \$1,000,000.00.

Before commencing work on this Contract the Contractor must provide certificates of insurance to show that the foregoing minimum coverages are in effect.

- 6. REMEDIES FOR DEFAULT.** In the event either party is in default under this Contract, the non-defaulting party may, at its option, pursue any or all of the remedies available to it under this Contract, including termination for cause, and at law or in equity.

## **7. TERMINATION**

**7.1** Contractor shall reasonably cooperate with other parties in connection with all services to be delivered under this Contract, including without limitation any successor provider to whom State Intellectual Property or other State information and materials are to be transferred in connection with termination. Contractor shall assist the State in exporting and extracting any and all State data, in a format usable without the use of the Services and as agreed to by State, at no additional cost. Any transition services requested by State involving additional knowledge transfer and support may be subject to a contract amendment for a fixed fee or at rates to be mutually agreed upon by the parties.

If the State determines in its sole discretion that a documented transition plan is necessary, then no later than sixty (60) days prior to termination, Contractor and the State shall mutually prepare a Transition Plan identifying transition services to be provided.

**7.2 Return of Property.** Upon request, Contractor shall promptly deliver to State all State Intellectual Property that is in the possession or under the control of Contractor/.

## **8. Net Neutrality Standards**

This contract includes provision of broadband Internet access service to the State. Provider hereby certifies that, as required in 3 V.S.A. § 349, except and to the extent it has been granted a waiver from the Secretary of Administration, it is in compliance with the consumer protection and net neutrality standards established in 3 V.S.A. § 348 in providing broadband Internet access service in the State of Vermont. The foregoing certification does not constitute a waiver of Comcast's ability to challenge the applicability or validity of 3 V.S.A. § 348 & 349 via the judicial process. To the extent 3 V.S.A. § 348 and/or 349 are subsequently determined to be invalid or unenforceable as applied to Comcast, this provision shall no longer be of any force and of effect.

- 9. SOV Cybersecurity Standard Update 2023-01:** Contractor confirms that all products and services provided to or for the use of the State under this Agreement shall be in compliance with *State of Vermont Cybersecurity Standard 23-01*, which prohibits the use of certain branded products in State information systems or any vendor system that is supporting State information systems, and is available on-line at:

<https://digitalservices.vermont.gov/cybersecurity/cybersecurity-standards-and-directives>

**10. Agreed Modifications to Attachment C:**

Section 7 of Attachment C is deleted and replace with the following:

**Defense and Indemnity:** Without limitation to the indemnification obligations specified in the Comcast Ts&Cs, Contractor shall indemnify, defend and hold harmless the State and its officers and employees against all third-party claims or suits arising from the negligence, breach, or misconduct of Contractor or any of its agents in connection with the performance of this Agreement. The State shall notify the Contractor in the event of any such claim or suit, and the Party shall immediately retain counsel and otherwise provide a complete defense against the entire claim or suit. The State retains the right to participate at its own expense in the defense of any claim. The State shall have the right to approve all proposed settlements of such claims or suits, such consent not to be unreasonably withheld, to the extent such settlement requires the State to take or refrain from taking any action or purports to obligate the State. Notwithstanding anything to the contrary in this Section 7 or the Agreement, (i) the Contractor's indemnification obligations in this Section 7 shall only apply with respect to (1) the State (including any State Purchaser) and (2) such Additional Purchasers that are entitled to or benefit from sovereign immunity under applicable law and (ii) Contractor's indemnification obligations with respect to Additional Purchasers that are not entitled to or do not benefit from sovereign immunity under applicable law shall be as set forth in the Comcast Ts&Cs.

After a final judgment or settlement in connection Section 7, Contractor may request recoupment of specific defense costs and may file suit in Washington Superior Court requesting recoupment. Contractor shall be entitled to recoup costs only upon a showing that such costs were entirely unrelated to the defense of any claim arising from an act or omission of the Party in connection with the performance of this Agreement.

Notwithstanding any contrary language anywhere, in no event shall the terms of this Agreement

or any document furnished by the Party in connection with its performance under this Agreement obligate the State to (1) defend or indemnify the Party or any third party, or (2) otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or other costs of the Party or any third party.

Section 19, Sub-Agreements, of Attachment C is modified by the addition of the following:

Comcast shall be deemed to satisfy the obligations in Section 19(C) so long as its subcontracts with its subcontractors that it utilizes to perform the Services substantively address the clauses identified in Section 19(c) (i.e., the referenced clauses don't need to be included verbatim in the subcontracts).

**CONTRACTOR**  
**GENERAL TERMS AND CONDITIONS**  
**("General Terms and Conditions")**

**ARTICLE 1: DEFINITIONS**

For purposes of these General Terms and Conditions, the following terms shall have the meanings specified below. Terms used but not otherwise defined herein shall have the meanings ascribed to such terms in the Contract to which these General Terms and Conditions are attached.

**Affiliate:** With respect to each party, any entity that controls, is controlled by or is under common control with such, party.

**Agreement:** Collectively, these General Terms and Conditions, the Contract to which these General Terms and Conditions are attached, any applicable Product Specific Attachment and each binding Sales Order.

**Comcast:** The operating Affiliate of Comcast that provides the Services. References to Comcast in Article 5 and Article 6 shall also include its Affiliates and their respective directors, officers, employees, agents, suppliers, licensors, successors, and assigns, as the case may be.

**Comcast Equipment:** – Any and all facilities, equipment or devices provided by Comcast or its authorized contractors at the Service Location(s) that are used to deliver the Services. Notwithstanding the foregoing, inside telephone wiring within a Service Location, whether or not installed by Comcast, shall not be considered Comcast Equipment.

**Confidential Information:** All information regarding either party's business which has been marked or is otherwise communicated as being "proprietary" or "confidential" or which reasonably should be known by the receiving party to be proprietary or confidential information. Without limiting the foregoing, Confidential Information shall include, even if not marked, the Agreement, all Licensed Software, promotional materials, proposals, quotes, rate information, discount information, subscriber information, network upgrade information and schedules, network operation information (including without limitation information about outages and planned maintenance) and invoices, as well as the parties' communications regarding such items.

**Customer-Provided Equipment:** Any and all facilities, equipment or devices supplied by a party other than Comcast or its authorized contractors for use in connection with the Services.

**Network:** The Comcast Equipment, facilities, fiber optic or coaxial cable associated with electronics and other equipment used to provide the Services.

**Product Specific Attachment(s) or PSA(s):** The additional terms and conditions applicable to the Services and which are attached to the Contract as Attachment E.

**"Website"** – means the Comcast website where the the Privacy Policy and the Use Policies are posted. The current URL for the Website is <https://business.comcast.com/terms-conditions-ent> (as the same may be updated by Comcast from time-to-time).

**ARTICLE 2. DELIVERY OF SERVICE**

**2.1 Orders.** To request Service at a Service Location(s), Customer shall submit a properly completed Sales Order to Comcast. Such Sales Order shall become binding on the parties upon the earlier of (i) Comcast's notice to Customer that it accepts such Sales Order, (ii) Comcast begins providing the Service described in the Sales Order or (iii) Comcast begins installation or construction for delivery of the Services. Each Sales Order submitted by Customer may be subject to an engineering review which will determine whether and to what extent the Network must be extended, built or upgraded in order to provide the ordered Services. Comcast will provide Customer written notification in the event Service installation at any Service Location will require an additional non-recurring installation fee ("Custom Installation Fee" or "Construction Charges"). Notwithstanding anything to the contrary contained in this Article 2.1, Customer shall have five (5) days from receipt of such notice to reject the Custom Installation Fee and terminate the affected Service Location(s). For certain Services, the Engineering Review will be conducted prior to Sales Order submission. In such case, Customer shall be deemed to have accepted the designated Custom Installation Fee upon submission of the applicable Sales Order.

**2.2 Access.** In order to deliver Services to Customer, Comcast may require access, right-of-way, conduit, and/or common room space ("Access") within and/or outside each Service Location. Within the Service Location, Customer shall be solely responsible for securing and maintaining such Access as Comcast may require to deliver the Services. In the event that Customer fails to secure or maintain such Access, Comcast (i) may cancel or terminate Service at such Service Location pursuant to Article 4.3 and (ii) shall be excused from its obligations with respect to the Service(s) at such Service Location (including any obligation to issue service credits) until such time as Customer provides Comcast with the necessary Access. If Comcast is unable to secure or maintain Access outside a particular Service Location, which Access is needed to provide Services to such Service Location, Customer or Comcast may cancel or terminate Service at such Service Location, without further liability beyond the termination date, upon a minimum thirty (30) days' prior written notice to the other party.

**2.3 Hazardous Materials.** If the presence of asbestos or other hazardous materials exists or is detected at a Service Location or within the building where the Service Location is located, Comcast may immediately stop providing and/or installing Services until such materials are removed. Customer shall be responsible for any additional expense incurred by Comcast as a result of encountering, or in the avoidance of, hazardous materials.

**2.4 Equipment**

**A. Comcast Equipment.** Comcast may, in its sole discretion, remove or change Comcast Equipment. Customer shall not move, rearrange, disconnect, remove, attempt to repair, or otherwise tamper with any Comcast Equipment or permit others to do so, and shall not use the Comcast Equipment for any purpose other than as authorized by the Agreement. Customer shall (i) provide an adequate environmentally controlled space and such electricity as may be required for installation, operation, and maintenance of the Comcast Equipment and (ii) be responsible for damage to, or loss of, Comcast Equipment caused by its acts or omissions, or by fire, theft or other casualty at the Service Location(s), unless caused by the gross negligence or willful misconduct of Comcast. Comcast shall maintain, at its cost, Comcast Equipment during the term of this Agreement; provided, however, that such maintenance shall be at Customer's cost to the extent it is related to causes other than the ordinary and proper use of the Comcast Equipment. Upon termination or expiration of this Agreement and/or any Sales Order, Customer shall be responsible for the return of all applicable Comcast Equipment. Until such time as the Comcast Equipment is returned to Comcast, Comcast may continue to invoice Customer for the monthly fee applicable to such Comcast Equipment. If any returned Comcast Equipment has been damaged and/or destroyed other than by Comcast or its agents, normal wear and tear excepted, Comcast may, in its sole discretion, invoice Customer for the manufacturer's list price of such Comcast Equipment or the cost of repair.

**B. Customer-Provided Equipment.** Customer shall have sole responsibility for providing maintenance, repair, operation and replacement of all Customer-Provided Equipment, inside telephone wiring and other Customer equipment and facilities on the Customer's side of the demarcation point (i.e., the point of interconnection between the Network and Customer-Provided Equipment located at a Service Location). Neither Comcast nor its employees, Affiliates, agents or contractors shall (i) have any obligation to install, operate, or maintain Customer-Provided Equipment or (ii) be liable for any damage, loss, or destruction to Customer-Provided Equipment, unless caused by the gross negligence or willful misconduct of Comcast. Customer-Provided Equipment shall at all times be compatible with the Network. Customer shall be responsible for the payment of service charges for visits by Comcast's employees or agents to a Service Location when the service difficulty or trouble report results from Customer-Provided Equipment.

## **2.5 Network, Intellectual Property and IP Addresses.**

**A.** All intellectual property of each party shall remain with the respective owner(s) and no right, title or interest will transfer to either party as a result of this Contract or the provision or receipt of services hereunder.

**B.** The Network is and shall remain the property of Comcast regardless of whether installed within, upon,

overhead, above, or underground at or near the Service Location and shall not be considered a fixture or an addition to the land or the Service Location(s) located thereon. Customer agrees that it shall take no action that directly or indirectly impairs Comcast's title to the Network, or any portion thereof, or exposes Comcast to any claim, lien, encumbrance, or legal process, except as otherwise agreed in writing by the parties. Nothing in this Agreement shall preclude Comcast from using the Network for services provided to other Comcast customers. For a period of twelve (12) months following Comcast's discontinuance of Service to the Service Location(s), Comcast retains the right to remove the Network. To the extent Comcast removes such portion of the Network it shall be responsible for returning the Service Location(s) to its prior condition, reasonable wear and tear excepted.

**C.** Customer acknowledges that use of the Services does not give it any ownership or other rights in any telephone number or Internet/online addresses provided in connection with such Services, including, but not limited to, Internet Protocol addresses, e-mail addresses and web addresses.

**D.** Title and intellectual property rights to (i) the Services and (ii) any computer software or code provided by Comcast to use the Services, including, but not limited to, associated documentation, and all updates thereto ("Licensed Software") are, in each case, owned by Comcast, its agents, suppliers or affiliates or their licensors or otherwise by the owners of such material. The copying, redistribution, bundling or publication of the Services, in whole or in part, without the express prior written consent of Comcast or other owner of such material, is prohibited.

**E.** The Agreement provides no right to use any party's or its Affiliates' trademarks, service marks, or trade names, or to otherwise refer to the other party in any marketing, promotional, or advertising materials or activities.

**2.6 License Grant.** If Customer requires the use of Licensed Software from Comcast in order to use the Services, Customer shall have a nonexclusive, nontransferable, and limited license to use such Licensed Software in object code only and solely to the extent necessary to use the applicable Service during the corresponding Service Term. Customer may not claim title to, or an ownership interest in, any Licensed Software (or any derivations or improvements thereto), and Customer shall execute any documentation reasonably required by Comcast, including, without limitation, end-user license agreements for the Licensed Software. Customer shall not: (i) copy the Licensed Software (or any upgrades thereto or related written materials) except for emergency back-up purposes or as permitted by the express written consent of Comcast; (ii) reverse engineer, decompile, or disassemble the Licensed Software; (iii) sell, lease, license, or sublicense the Licensed Software; or (iv) create, write, or develop any derivative software or any other software program based on the Licensed Software. Customer acknowledges that the use of Service may

periodically require updates and/or changes to the Licensed Software resident in the Comcast Equipment or Customer Provided-Equipment. Customer hereby consents to, and shall provide free access for, such updates deemed reasonably necessary by Comcast.

### **ARTICLE 3. BILLING AND PAYMENT**

#### **3.1 Charges; Changes to MRC; Taxes.**

A. Customer agrees to pay all charges associated with the Services, including, but not limited to, (i) any fees or payment obligations in connection with the Services imposed by governmental or quasi-governmental bodies in connection with the sale, installation, use, or provision of the Services (e.g., applicable franchise fees, right of way fees and Universal Service Fund charges) regardless of whether Comcast or its Affiliates pay the fees directly or are required or permitted by law to collect them from Customer and (ii) charges incurred as the result of fraudulent or unauthorized use of the Services. Any failure on the part of Customer to be ready to receive Service, or any refusal on the part of Customer to receive Service, shall not relieve Customer of its obligation to pay charges for any Service that is otherwise available for use. For the avoidance of doubt, Comcast shall not be responsible for any purchases made by Customer or its end users while using the Services.

#### **B. RESERVED**

C. Except to the extent Customer provides a valid tax exemption certificate prior to the delivery of Service, Customer shall be responsible for the payment of any and all applicable local, state, and federal taxes or fees (however designated). Customer shall also be responsible to pay any Service fees, payment obligations and taxes that become applicable retroactively.

#### **3.2 Payment Terms; Disputes**

A. Comcast will invoice Customer in advance on a monthly basis for all monthly recurring charges and fees arising under the Agreement. All other charges will be billed monthly in arrears, including without limitation, certain usage based charges and third party pass through fees. Payment is due upon presentation of an invoice and will be considered timely made to Comcast if received within thirty (30) days after the date Customer receives the invoice. If a Service Commencement Date is not the first day of a billing period, Customer's first monthly invoice shall include any pro-rated charges for the Services, from the Service Commencement Date to the start of the next billing period. Partial payment of any bill will be applied to the Customer's outstanding charges in amounts and proportions solely determined by Comcast. Except to the extent otherwise prohibited by law, Customer will be assessed a service charge up to the full amount permitted under applicable law for any check or other instrument used to pay for the Services that has been rejected by the bank or other financial

institution. Any payment not made when due will be subject to a late charge equal to the lower of (i) 1.5% per month and (ii) the highest rate allowed by law. No acceptance of partial payment(s) by Comcast shall constitute a waiver of any rights to collect the full balance owed under the Agreement.

B. If Customer disputes any portion of an invoice, Customer shall pay the undisputed portion of the invoice and submit a written claim, including all substantiating documentation, to Comcast for the disputed amount of the invoice by the invoice due date. The parties shall negotiate in good faith to resolve any billing dispute submitted by Customer pursuant to this Article 3.2(B). Under no circumstances may Customer submit a billing dispute to Comcast later than ninety (90) days following Customer's receipt of the applicable invoice.

### **ARTICLE 4. TERM & TERMINATION**

4.1 **Sales Order Term.** Upon the expiration of the Service Term applicable to a Sales Order, each Sales Order shall automatically renew for successive periods of one (1) year each (each, a "Renewal Term"), unless prior written notice of non-renewal is delivered by either party to the other at least thirty (30) days before the expiration of the Service Term or the then current Renewal Term. To the extent the initial Service Term or a Renewal Term applicable to a Sales Order extends beyond the expiration date of the Contract Term, such Sales Order shall continue to be governed by the terms and conditions of the Agreement.

4.2 **Reserved.**

4.3 **Reserved.**

4.4 **Effect of Expiration/Termination of a Sales Order.** Upon the expiration or termination of a Sales Order for any reason (i) Comcast shall disconnect the applicable Service, (ii) Comcast may delete all applicable data, files, electronic messages, or other information stored on Comcast's servers or systems and (iii) Comcast may assess and collect from Customer applicable Termination Charges. Termination by either Party of a Sales Order does not waive any other rights or remedies that it may have under this Agreement. The non-defaulting Party shall be entitled to all available legal and equitable remedies for such breach.

### **ARTICLE 5. LIMITATION OF LIABILITY; DISCLAIMER OF WARRANTIES**

#### **5.1 Limitation of Liability.**

A. **THE AGGREGATE LIABILITY OF COMCAST FOR ANY AND ALL LOSSES, DAMAGES AND CAUSES ARISING OUT OF THE AGREEMENT, INCLUDING, BUT NOT LIMITED TO, THE PERFORMANCE OF**

SERVICE, AND NOT OTHERWISE LIMITED HEREUNDER, WHETHER IN CONTRACT, TORT, OR OTHERWISE, SHALL NOT EXCEED DIRECT DAMAGES EQUAL TO THE SUM TOTAL OF PAYMENTS MADE BY CUSTOMER TO COMCAST DURING THE THREE (3) MONTHS IMMEDIATELY PRECEDING THE EVENT FOR WHICH DAMAGES ARE CLAIMED. THIS LIMITATION SHALL NOT APPLY TO COMCAST'S INDEMNIFICATION OBLIGATIONS AND CLAIMS FOR DAMAGE TO PROPERTY AND/OR PERSONAL INJURIES (INCLUDING DEATH) ARISING OUT OF THE GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF COMCAST WHILE ON THE CUSTOMER SERVICE LOCATION.

**B. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THE AGREEMENT, IN NO EVENT SHALL THE AGGREGATE LIABILITY OF COMCAST UNDER THIS AGREEMENT FOR ALL INDEMNIFICATION OF IP CLAIMS UNDER SECTION 6(i) OF THESE GENERAL TERMS AND CONDITIONS EXCEED THE GREATER OF (I) ONE (1) MILLION DOLLARS (\$1,000,000) AND (II) THE AGGREGATE AMOUNT OF FEES RECEIVED BY COMCAST FROM CUSTOMER DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE DATE ON WHICH THE IP CLAIM FIRST AROSE.**

**C. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THE AGREEMENT, IN NO EVENT SHALL COMCAST BE LIABLE FOR ANY LOSS, DAMAGE OR CLAIM ARISING OUT OF OR RELATED TO: (1) STORED, TRANSMITTED, OR RECORDED DATA, FILES, OR SOFTWARE; (2) ANY ACT OR OMISSION OF CUSTOMER, ITS USERS OR THIRD PARTIES; (3) INTEROPERABILITY, INTERACTION OR INTERCONNECTION OF THE SERVICES WITH APPLICATIONS, EQUIPMENT, SERVICES OR NETWORKS PROVIDED BY CUSTOMER OR THIRD PARTIES; OR (4) LOSS OR DESTRUCTION OF ANY CUSTOMER HARDWARE, SOFTWARE, FILES OR DATA RESULTING FROM ANY VIRUS OR OTHER HARMFUL FEATURE OR FROM ANY ATTEMPT TO REMOVE IT. CUSTOMER IS SOLELY RESPONSIBLE FOR BACKING UP ITS DATA, FILES, AND SOFTWARE PRIOR TO THE INSTALLATION OF SERVICE AND AT REGULAR INTERVALS THEREAFTER.**

**D. NOTWITHSTANDING ANYTHING TO CONTRARY CONTAINED IN THIS AGREEMENT, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INCIDENTAL, INDIRECT, SPECIAL, COVER, PUNITIVE OR CONSEQUENTIAL DAMAGES, WHETHER OR NOT FORESEEABLE, OF ANY KIND INCLUDING BUT NOT LIMITED TO ANY LOSS**

**REVENUE, LOSS OF USE, LOSS OF BUSINESS, OR LOSS OF PROFIT WHETHER SUCH ALLEGED LIABILITY ARISES IN CONTRACT OR TORT; PROVIDED, THAT, THE FOREGOING LIMITATION SHALL NOT LIMIT CUSTOMER'S LIABILITY FOR AMOUNTS OWED FOR THE SERVICES, FOR ANY EQUIPMENT OR SOFTWARE PROVIDED BY COMCAST, OR FOR TERMINATION CHARGES.**

**5.2 Disclaimer of Warranties.** Services shall be provided pursuant to the terms and conditions in the applicable PSA and Service Level Agreement, and are in lieu of all other warranties, express, implied or statutory, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement. **TO THE MAXIMUM EXTENT ALLOWED BY LAW, COMCAST EXPRESSLY DISCLAIMS ALL SUCH EXPRESS, IMPLIED AND STATUTORY WARRANTIES.** Without limiting the generality of the foregoing, and except as otherwise identified in a PSA or Service Level Agreement, Comcast does not warrant that the Services, Comcast Equipment, or Licensed Software will be uninterrupted, error-free, or free of latency or delay, or that the Services, Comcast Equipment, or Licensed Software will meet customer's requirements, or that the Services, Comcast Equipment, or Licensed Software will prevent unauthorized access by third parties. Customer acknowledges and agrees that the Services are not fail-safe and are not designed or intended for use in situations requiring fail-safe performance or in which an error or interruption in the Services could lead to severe injury to business, persons, property or environment.

**5.3 Exclusive Remedies.** Customer's sole and exclusive remedies are as expressly set forth in the Agreement. In those states where Customer's remedies cannot be so limited, the liability of Comcast is limited to the maximum extent permitted by law.

## **ARTICLE 6. INDEMNIFICATION**

**6.1 Comcast's Indemnification Obligations.** Subject to Sections 5.1(B), 5.1(C) and 5.1(D) and any other limitations contained in the Agreement, Comcast shall indemnify defend, and hold harmless Customer, its Affiliates and their respective employees, directors, officers, and agents (the "Customer Indemnified Parties") from and against all , actions, causes of actions, damages, liabilities, losses, and expenses (including reasonable attorneys' fees) arising out of (i) infringement of U.S. patent or copyright law based solely on Comcast Equipment or Licensed Software; provided, that, Comcast shall have no liability for any claim of infringement arising from: (a) Comcast's compliance with any designs, specifications, or instructions of Customer; (b) modification or alteration of the Licensed Software or Comcast Equipment by Customer or a third party without the prior knowledge and written approval of an authorized officer of Comcast; (c) use of the Licensed Software or Comcast Equipment in a way not authorized in writing by an authorized officer of

Comcast; and/or (d) Customer's failure to use an updated version of the Licensed Software or Comcast Equipment which has been provided, or made available, to Customer and (ii) damage to tangible personal property or real property, and personal injuries (including death) arising out of the negligence or willful misconduct of Comcast.

## **6.2 RESERVED**

**6.3 Indemnification Procedures.** To the extent a party may be entitled to indemnification under this Agreement (an "Indemnified Party"), such Indemnified Party shall (i) promptly notify the other Party (the "Indemnifying Party") in writing of any pending or threatened claim or demand that the Indemnified Party has determined has given or would reasonably be expected to give rise to such right of indemnification (an "Action") and (ii) cooperate in every reasonable way to facilitate the defense or settlement of such Action. The Indemnifying Party shall assume the defense of any Action with counsel reasonably satisfactory to the Indemnified Party. The Indemnified Party may employ its own counsel in any such case, and shall pay such counsel's fees and expenses. The Indemnifying Party shall have the right to settle any claim for which indemnification is available; provided, however, that to the extent that such settlement requires the Indemnified Party to take or refrain from taking any action or purports to obligate the Indemnified Party, then the Indemnifying Party shall not settle such claim without the prior written consent of the Indemnified Party, which consent shall not be unreasonably withheld, conditioned or delayed.

## **ARTICLE 7. CONFIDENTIAL INFORMATION AND PUBLICITY**

**7.1 Disclosure and Use.** All Confidential Information disclosed by either party shall, during the term of the Agreement and for two (2) years after the expiration or termination thereof (or such longer period as may be required by law), be kept by the receiving party in strict confidence and shall not be disclosed to any third party without the disclosing party's express written consent. Notwithstanding the foregoing, (i) such information may be disclosed (A) to the receiving party's employees, affiliates, and agents who have a need to know for the purpose of performing under this Agreement, using the Services and rendering the Services (provided that in all cases the receiving party shall take appropriate measures prior to disclosure to its employees, affiliates, and agents to assure against unauthorized use or disclosure) or (B) as otherwise authorized by this Agreement and (ii) each party's confidentiality obligations hereunder shall not apply to information that: (A) is already known to the receiving party without a pre-existing restriction as to disclosure, (B) is or becomes publicly available without fault of the receiving party; (C) is rightfully obtained by the receiving party from a third party without restriction as to disclosure, or is approved for release by written authorization of the disclosing party, (D) is developed independently by the receiving party without use of the disclosing party's

Confidential Information or (E) is required to be disclosed by law or regulation, including, but not limited to, pursuant to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq. Each party agrees to treat all Confidential Information of the other in the same manner as it treats its own proprietary information, but in no case using less than a reasonable degree of care. Notwithstanding anything to the contrary contained in this Article 7.1 or the Agreement, Customer acknowledges and agrees that Comcast shall have no liability or responsibility for content received or distributed by Customer or its users through the Service.

**7.2 Publicity.** Neither party shall issue any publication or press release relating to, or otherwise disclose the existence of, the terms and conditions of any contractual relationship between Comcast and Customer without the prior written consent of the other party.

**7.3 Remedies.** Notwithstanding any other Article of this Agreement, the non-breaching party shall be entitled to seek equitable relief to protect its interests pursuant to this Article 7, including, but not limited to, injunctive relief.

## **ARTICLE 8. PROHIBITED USES; USE AND PRIVACY POLICIES**

**8.1 Prohibited Uses; Comcast Use Policies.** Customer is prohibited from using, or permitting the use of, any Service (i) for any purpose in violation of any law, rule, regulation, or policy of any government authority; (ii) in violation of any Use Policy (as defined below); (iii) for any use as to which Customer has not obtained all required government approvals, authorizations, licenses, consents, and permits; or (iv) to interfere unreasonably with the use of Comcast service by others or the operation of the Network. Customer is responsible for the compliance of its users with the provisions of the Agreement. Customer may not sell, resell, sublicense, assign, license, sublicense, share, provide, or otherwise utilize in conjunction with a third party (including, without limitation, in any joint venture or as part of any outsourcing activity) the Services or any component thereof. Customer acknowledges and agrees that Customer's and its users' use of Services shall be subject to Comcast's acceptable use policies ("AUPs") and security policies (together with the AUPs, the "Use Policies") that may limit Customer's and its users' use of the Services. The Use Policies are posted on the Website, and are incorporated into this Agreement by reference. Comcast reserves the right to act immediately and without notice to (i) terminate or suspend the Services and/or to remove from the Services any information transmitted by or to Customer or users, if Comcast determines that such use or information is in violation of this Article 8.1 or the Use Policies and (ii) terminate or suspend the Services in the event of fraudulent use of Customer's Services. Customer acknowledges and agrees that Comcast may, but is not obligated to, detect or report unauthorized or fraudulent use of the Services to Customer.

**8.2 Privacy Policy.** Comcast's commercial privacy policy (the "Privacy Policy") applies to Comcast's handling of Customer confidential information. The Privacy Policy is available on the Website. Notwithstanding the foregoing or anything to the Contrary contained in the Agreement or the Privacy Policy, Comcast is not responsible for any information provided by Customer to third parties and Customer assumes all privacy and other risks associated with providing personally identifiable information to third parties via the Services.

## **ARTICLE 9. MISCELLANEOUS TERMS**

**9.1 Chronic Service Interruption.** Notwithstanding anything to the contrary contained in the Agreement (including any PSA), Customer shall have the right to terminate the interrupted portion of a Service prior to the end of the applicable Service Term, without payment of any applicable Termination Charges, and without further liability or penalty on the part of Comcast: (i) if such portion of Service experiences a Service Interruption on three (3) or more separate occasions of more than four (4) hours each in any thirty (30) day period and (ii) following written notice thereof from Customer to Comcast, that portion of Service experiences a Service Interruption of more than twelve (12) hours at any time within the twelve (12) month period immediately following said notice; or (iii) subsequent to the events of "(i)", if such portion of the Service experiences a Service Interruption in excess of seventy-two (72) continuous hours, (each a "Chronic Service Interruption"). Notwithstanding anything to the contrary contained in this Paragraph, Customer acknowledges and agrees that outages resulting from Force Majeure events, Planned Service Interruptions, Customer's actions or inactions, or the actions or inactions of third parties not under the control of Comcast, shall not qualify as a Service Interruption for the purposes of this Section 9.1.

**9.2 Assignment or Transfer.** Neither party shall assign any right, obligation or duty, in whole or in part, nor of any other interest hereunder, without the prior written consent of the other party, which shall not be unreasonably withheld. Notwithstanding the foregoing, Comcast may assign the Contract (i) to any Affiliate or any entity that purchases all or substantially all of the assets to which the Contract pertains or (ii) in connection with a corporate reorganization, in each case, without the Customer's consent. All obligations and duties of either party hereunder shall be binding on all successors in interest and permitted assigns of such party.

**9.3 Notices.** Except as otherwise identified herein, any notice sent pursuant to the Agreement shall be deemed given and effective when sent by facsimile (confirmed by first-class mail), or when delivered by overnight express or other express delivery service, in each case, to the following addresses (or to such other addresses as a party may designate by written notice to the other party): (i) with respect to Customer, the point of contact set forth in Section 9 of the Standard Contract (Primary

Contacts);; or (ii) with respect to Comcast, to: Vice President of Sales Operations (Comcast Business), One Comcast Center, 1701 JFK Blvd., Philadelphia, PA 19103, with a copy to Cable Law Department, One Comcast Center, 50<sup>th</sup> Floor, 1701 JFK Blvd., Philadelphia, PA 19103. Alternatively, Customer may send termination notice to Comcast through the Comcast disconnection portal found at the following URL: <https://business.comcast.com/landingpage/disconnect> (as the same may be updated by Comcast from time-to-time).

**9.4 Amendments; Changes to the Agreement.** The Agreement may not be amended except by a written agreement executed by the parties; provided, that, notwithstanding the foregoing, Comcast may change or modify the Use Policies and Privacy Policy from time to time ("Revisions") by posting such Revisions to the Website. The Revisions are effective upon posting to the Website. Customer will receive notice of any Revisions in the next applicable monthly invoice. Customer shall have thirty (30) calendar days from the invoice notice of such Revisions to provide Comcast with written notice that the Revisions adversely affect Customer's use of the Service(s). If, after such notice, Comcast is able to verify such adverse effect but is unable to reasonably mitigate the Revision's impact on such Services, then Customer may terminate the impacted Service(s) without further obligation to Comcast beyond the termination date, including Termination Charges, if any. This shall be Customer's sole and exclusive remedy for any Revisions. Terms or conditions contained in any Sales Order, or restrictive endorsements or other statements on any form of payment, shall be void and of no force or effect.

**9.5 Tariffs.** Notwithstanding anything to the contrary in the Agreement, Comcast may elect or be required to file with regulatory agencies tariffs for certain Services. In such event, the terms set forth in the Agreement may, under applicable law, be superseded by the terms and conditions of the tariffs. Without limiting the generality of the foregoing, in the event of any inconsistency with respect to rates, the rates and other terms set forth in the applicable Sales Order shall be treated as individual case based arrangements to the maximum extent permitted by law, and Comcast shall take such steps as are required by law to make the rates and other terms enforceable. If Comcast voluntarily or involuntarily cancels or withdraws a tariff under which a Service is provided to Customer, the Service will thereafter be provided pursuant to the Agreement and the terms and conditions contained in the tariff immediately prior to its cancellation or withdrawal. In the event that Comcast is required by a governmental authority to modify a tariff under which Service is provided to Customer in a manner that is material and adverse to either party, the affected party may terminate the applicable Sales Order upon a minimum thirty (30) days' prior written notice to the other party, without further liability.

**9.6 Entire Understanding; Construction; Survival; Headings; No Waiver.** The Agreement supersedes all prior agreement between the parties with respect to its subject matter

and constitutes a complete and exclusive statement of the terms of the agreement between the parties with respect to the subject matter hereof. In the event that any portion of the Agreement is held to be invalid or unenforceable, the parties shall replace the invalid or unenforceable portion with another provision that, as nearly as possible, reflects the original intention of the parties, and the remainder of the Agreement shall remain in full force and effect. The rights and obligations of either party that by their nature would continue beyond the termination or expiration of the Agreement shall survive termination or expiration of the Agreement. The article headings used herein are for reference only and shall not limit or control any term or provision of this Agreement or the interpretation or construction thereof. No failure by either party to enforce any right(s) hereunder shall constitute a waiver of such right(s). The Agreement may be executed in counterpart copies. Each party represents and warrants that the persons who executes the Agreement on its behalf are duly authorized to do so.

**9.7     Reserved.**

**9.8     No Third Party Beneficiaries; Independent Contractors.** This Agreement does not expressly or implicitly provide any third party (including users) with any remedy, claim, liability, reimbursement, cause of action, or other right or privilege. The parties to this Agreement are independent contractors. Neither party is an agent, representative, or partner of the other party. Neither party shall have any right, power, or authority to enter into any agreement for, or on behalf of, or incur any obligation or liability of, or to otherwise bind, the other party. This Agreement shall not be interpreted or construed to create an association, agency, joint venture, or partnership between the parties or to impose any liability attributable to such a relationship upon either party.

## ATTACHMENT F

### COMCAST ENTERPRISE SERVICES PRODUCT-SPECIFIC ATTACHMENT ETHERNET DEDICATED INTERNET SERVICES

The following additional terms and conditions are applicable to Sales Orders for Comcast's Ethernet Dedicated Internet Service:

#### **DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

**"Estimated Availability Date"** means the target date for delivery of Service.

**"HFC Network"** means a hybrid fiber coax network

**"Interconnection Facilities"** means transmission capacity provided by Comcast, Customer or a third-party supplier to extend the Comcast Equipment from a Comcast terminal to any other location (e.g., a local loop provided by a local exchange company or other communications company).

**"Off-Net"** means geographical locations that are outside of Comcast's service area and/or geographical locations that are within Comcast's service area generally, but are not readily accessible by Comcast network facilities. All Off-Net Services are provided by third-party service providers. Off-Net Services provisioned over a fiber optic network are referred to as **"Off-Net Fiber."**

**"On-Net"** means geographical locations where Comcast currently provides Services through its Comcast network. On-Net Services may be provisioned over a fiber optic network ("On-Net Fiber"), or via a HFC Network ("On-Net HFC"), as available through Comcast.

**"Service(s)"** means Ethernet Dedicated Internet Services.

#### **ARTICLE 1. SERVICES**

This attachment shall apply to Ethernet Dedicated Internet Service. A further description of the Service is set forth in **Schedule A-1** hereto which is incorporated herein by reference.

#### **ARTICLE 2. PROVIDER**

On-Net Service shall be provided by Comcast Business Communications, LLC.

On-Net Service provided over the HFC Network and Off-Net Services are available in a limited number of markets. For information on service availability, call 866-429-0152.

#### **ARTICLE 3. CUSTOM INSTALLATION FEES**

Once Comcast accepts a Sales Order for Services, Comcast will invoice Customer for all Custom Installation Fee(s). Customer will pay the Custom Installation Fee(s) within thirty (30) days of the invoice date unless a payment schedule is specified in the applicable Sales Order.

#### **ARTICLE 4. PROVISIONING INTERVAL**

Following its acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Services on or before the Estimated Availability Date; provided, however, that Comcast's failure to provision by said date shall not constitute a breach of the Agreement.

#### **ARTICLE 5. SERVICE COMMENCEMENT DATE**

Comcast shall inform Customer when Service is available and performing in accordance with the "Technical Specifications" set forth in Schedule A-1 hereto ("Availability Notification"). Charges for Service shall begin to accrue as of the Service Commencement Date. The Service Commencement Date shall be earliest of: (A) the date on which Customer confirms receipt of and concurrence with the Availability Notification; (B) five (5) business days following the date of the Availability Notification, if Customer fails to notify Comcast that the Service does not comply materially with the Technical Specifications (defined in Article 8); or (C) the date on which Customer first uses the Service. In the event that a Service Term has not been expressly set forth in a Sales Order, the Service Term for such Sales Order shall be twelve (12) months

#### **ARTICLE 6. PORTABILITY; UPGRADES**

**6.1 Portability.** Customer may terminate an existing On-Net Service (an "Existing Service") and turn up a replacement On-Net Service (*i.e.*, activate Service with termination points on Comcast's network that are different than those of the Existing Service) (a "Replacement Service") without incurring Termination Charges with respect to the Existing Service, provided that: (a) the Replacement Service must have a Service Term equal to or greater than the remaining Service Term of the Existing Service, but in no event less than twelve (12) months; (b) the Replacement Service must have monthly recurring charges equal to or greater than the monthly recurring

charges for the Existing Service; (c) Customer submits a Sales Order to Comcast for the Replacement Service within ninety (90) days after termination of the Existing Service and that Sales Order is accepted by Comcast; (d) Customer reimburses Comcast for any and all installation charges that were waived with respect to the Existing Service; and (e) Customer pays the actual costs incurred by Comcast in installing and provisioning the Replacement Service.

**6.2 Upgrades.** Customer may upgrade the speed or capacity of an Existing Service without incurring Termination Charges, provided that: (a) the upgraded Service (the “Upgraded Service”) must assume the remaining Service Term of the Existing Service, but in no event less than twelve (12) months; (b) the Upgraded Service must have the same points of termination on Comcast’s network as the Existing Service; (c) Customer submits a Sales Order to Comcast for the Upgraded Service and that Sales Order is accepted by Comcast; (d) Customer pays Comcast’s applicable nonrecurring charges for the upgrade; and (e) Customer agrees to pay the applicable monthly recurring charges for the Upgraded Service commencing with the upgrade. Upgrades to Off-Net Services are subject to the applicable third party service provider rules and availability. Comcast has no obligation to upgrade Customer’s Off-Net Service.

## **ARTICLE 7. ADDITIONAL INFORMATION**

As necessary for the interconnection of the Service with services provided by third parties, Comcast may request (as applicable), and Customer will provide to Comcast, circuit facility assignment information, firm order commitment information, and design layout records necessary to enable Comcast to make the necessary cross-connection between the Service and Customer’s other service provider(s). Comcast may charge Customer nonrecurring and monthly recurring cross-connect charges to make such connections.

## **ARTICLE 8. TECHNICAL SPECIFICATIONS; SERVICE LEVEL AGREEMENT**

The technical specifications applicable to the Service are set forth in Schedule A-1 hereto (“Technical Specifications”). The service level agreement applicable to the Service is set forth in a Schedule A-2 hereto and incorporated herein by reference.

**COMCAST ENTERPRISE SERVICES**  
**PRODUCT-SPECIFIC ATTACHMENT**  
**ETHERNET DEDICATED INTERNET SERVICES**

**SCHEDULE A-1**  
**SERVICE DESCRIPTIONS AND TECHNICAL SPECIFICATIONS**  
**COMCAST ETHERNET DEDICATED INTERNET SERVICES**

Comcast's Ethernet Dedicated Internet Service will be provided in accordance with the service descriptions and technical specifications set forth below:

**Service Descriptions**

**Ethernet Dedicated Internet Service ("EDI")**. EDI provides reliable, simple, and flexible access to the Internet. The Service is offered in the Ethernet User-to-Network Interfaces ("UNI") increments identified in Figure 1 below and is available in Committed Information Rate ("CIR") speed increments starting at 1Mbps, subject to available capacity. The Service provides an Ethernet Virtual Connection ("EVC") from the Customer Service Location to a Comcast Internet Point of Presence ("POP") router.

**EDI Technical Specifications.**

**1. Ethernet User-to-Network Interface.** The Service provides the bidirectional, full duplex transmission of untagged Ethernet frames using a standard IEEE 802.3 Ethernet interface (UNI) to attach to the Customer's router. Figure 1 lists the available UNI speed and their UNI Physical Interfaces, and available CIR bandwidth increments and Committed Burst Sizes (CBS). CIR increments of less than 10 Mbps are generally not available in conjunction with Off-Net Services.

UNI Speed	UNI Physical Interface	CIR Increments	CBS (bytes)
		1 Mbps	25,000
100 Mbps	100BaseT	10 Mbps	250,000
1 Gbps	1000Base T or 1000BaseSX	100 Mbps	2,500,000
10 Gbps	10GBase-SR or 10GBase-LR	1 Gbps	25,000,000
100 Gbps	100GBASE-LR4	10 Gbps	25,000,000

**Figure 1: Available UNI interface types and CBS values for different CIR Increments**

**2. Traffic Management.** Comcast's network traffic-policing policies restrict traffic flow to the subscribed, CIR. If the Customer-transmitted bandwidth rate exceeds the subscription rate CIR and CBS, Comcast will discard the non-conformant packets. The Customer's router must shape traffic to the contracted CIR. Traffic management policies associated with any Off-Net portions of Service will conform to the policies enforced by the third-party service provider.

**3. Maximum Frame Size.** The Service supports a maximum transmission unit ("MTU") frame size of 1518 bytes including Layer 2 Ethernet header and FCS.

**4. Layer 2 Control Protocol ("L2CP") Processing.** All L2CP frames are discarded at the UNI.

**5. IP Address Allocation.** IP address space is a finite resource that is an essential requirement for all Internet access services. Comcast assigns up to two (2) routable IP addresses to each customer circuit. Customer can obtain additional IP addresses if required based on American Registry for Internet Numbers ("ARIN") guidelines and by completing an IP address request form; additional charges may apply.

**6. Domain Name Service.** Comcast provides primary and secondary Domain Name Service ("DNS"). DNS is the basic network service that translates host and domain names into corresponding IP addresses, and vice-versa.

7. **Border Gateway Protocol (“BGP”) Routing.** Comcast supports BGP-4 routing (“BGP-4”) as an optional service feature. BGP-4 allows Customers to efficiently multi-home across multiple ISP networks. This optional service feature requires an Autonomous System Number (ASN) be assigned to a customer by the ARIN. Customers should also be proficient in BGP routing protocol to provision and maintain this optional service feature on their router. Additional information and requirements for BGP routing will be provided to the Customer upon request. Comcast supports private peering if the Customer is multi-homed only to Comcast’s network.

## 8. Monitoring, Technical Support and Maintenance

1. **Network Monitoring.** Comcast monitors On-Net Service on a 24x7x365 basis.

2. **Technical Support.** Comcast provides a toll-free trouble reporting telephone number to the Comcast Enterprise Technical Support (“ETS”) center that operates on a 24x7x365 basis. Comcast provides technical support for Service-related inquiries. ETS will not offer consulting or advice on issues relating to CPE or other equipment not provided by Comcast.

A. Escalation. Reported troubles are escalated within the ETS to meet the response/restoration objectives described below (Response and Restoration Standards). Service issues are escalated within Comcast ETS as follows: to a Supervisor at the end of the applicable objective time interval plus one (1) hour; to a Manager at the end of the applicable objective time interval plus two (2) hours, and to a Director at the end of the applicable objective time interval plus four (4) hours.

B. Maintenance. Comcast’s standard maintenance window for On-Net Services is Sunday to Saturday from 12:00am to 6:00am local time. Scheduled maintenance for On-Net Services is performed during the maintenance window and will be coordinated between Comcast and the Customer. Comcast provides a minimum of forty-eight (48) hour notice for non-service impacting scheduled maintenance. Comcast provides a minimum of seven (7) days’ notice for service impacting planned maintenance. Emergency maintenance is performed as needed without advance notice to Customer. Maintenance for Off-Net Services shall be performed in accordance with the applicable third party service provider rules. Therefore, maintenance for Off-Net Service may be performed without advance notice to Customer.

3. Comcast provides certain Comcast Equipment for provisioning its Services and the delivery of the UNI, which will reside on the Customer-side of the Demarcation Point. Comcast will retain ownership and management responsibility for this Comcast Equipment. This Comcast Equipment must only be used for receipt of the Services. Customers are required to shape their egress traffic to the CIR identified in the Sales Order. Comcast will be excused from paying SLA credits, as set forth in Schedule A-2, if the Service Interruption is the result of Customer’s failure to shape their traffic to the contracted CIR or utilizing Comcast Equipment for non-Comcast provided Services.

### Response and Restoration Standards

Comcast has the following response and restoration objectives:

CATEGORY	OBJECTIVE	MEASUREMENT	REMEDIES
<i>Mean Time to Respond Telephonically to Call</i>	15 minutes	Averaged over one Month	Escalation (see above)
<i>Mean Time to Restore On-Net Comcast Equipment</i>	4 hours	Averaged over one Month	Escalation (see above)
<i>Mean Time to Restore Off-Net Equipment</i>	6 hours	Averaged over one Month	Escalation (see above)
<i>Mean Time to Restore On-Net Services</i>	6 hours	Averaged over one Month	Escalation (see above)
<i>Mean Time to Restore Off-Net Services</i>	9 hours	Averaged over one Month	Escalation (see above)

Customer shall bear any expense incurred, e.g., dispatch/labor costs, where a Service Interruption is found to be the fault of Customer, its end users, agents, representatives or third-party suppliers.

**COMCAST ENTERPRISE SERVICES**  
**PRODUCT-SPECIFIC ATTACHMENT**  
**ETHERNET DEDICATED INTERNET SERVICES**

**SCHEDULE A-2**  
**SERVICE LEVEL AGREEMENT**

Comcast's Ethernet Dedicated Internet Service is backed by the following Service Level Agreement ("SLA"):

**A. Definitions**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Ethernet Dedicated Internet Services PSA or the General Terms and Conditions.

**"Planned Service Interruption"** means any Service Interruption caused by planned work such as scheduled maintenance or planned enhancements or upgrades to the network.

**"Service Interruption"** means an interruption in transmission that renders the Service unusable due to a total loss of signal for the Service. The Service shall be "Available" in the absence of a Service Interruption.

**B. EDI Service Level Agreements**

1. Availability SLAs. Comcast's liability, and Customer's sole remedy for Service Interruptions, and errors, omissions, interruptions, delays, outages, or defects in transmission or switching of any Service (individually or collectively, "Liability"), shall be limited to the amounts set forth in the Tables below ("Credit"). For the purposes of calculating credit for a Service Interruption, the "Length of Service Interruption" begins when the Customer reports such Service Interruption and a trouble ticket is opened, and concludes upon the closing of the same trouble ticket or, if sooner, the termination of the Service Interruption less any time Comcast is awaiting additional information or premises testing from the Customer. In no event shall the total amount of Credit issued to Customer's account on a per-month basis exceed 50% of the total monthly recurring charge ("MRC") associated with the impacted portion of the Service set forth in the Sales Order. The Length of Service Interruptions will not be aggregated for purposes of determining Credit allowances. To qualify, Customer must request the Credit from Comcast within thirty (30) days of the beginning of the Service Interruption. Comcast shall not incur any Liability, including Credit, for any failure of the Services caused by force majeure events, Planned Service Interruptions, Customer actions, omission or equipment, CPE, or any other items set forth in the "Exceptions to Credit Allowances" section below.

**TABLE 1: Availability SLA for Services provided over On-Net Fiber (99.99% Availability)**

<b>Length of Service Interruption:</b>	<b>Amount of Credit:</b>
Less than 4 minutes	None
At least 4 minutes but less than 4 hours	5% of Total MRC
At least 4 hours but less than 8 hours	10% of Total MRC
At least 8 hours but less than 12 hours	20% of Total MRC
At least 12 hours but less than 16 hours	30% of Total MRC
At least 16 hours but less than 24 hours	40% of Total MRC
At least 24 hours or greater	50% of Total MRC

**TABLE 2: Availability SLA for Services provided over Off-Net Fiber (99.95% Availability)**

<b>Length of Service Interruption:</b>	<b>Amount of Credit:</b>
Less than 20 minutes	None
At least 20 minutes but less than 4 hours	5% of Total MRC
At least 4 hours but less than 8 hours	10% of Total MRC
At least 8 hours but less than 12 hours	20% of Total MRC
At least 12 hours but less than 16 hours	30% of Total MRC
At least 16 hours but less than 24 hours	40% of Total MRC
At least 24 hours or greater	50% of Total MRC

**TABLE 3: Availability SLA for Services provided over On-Net HFC or Off-Net Non-Fiber Transport (99.9% Availability)**

<b>Length of Service Interruption:</b>	<b>Amount of Credit:</b>
Less than 40 minutes	None
At least 40 minutes but less than 4 hours	5% of Total MRC
At least 4 hours but less than 8 hours	10% of Total MRC
At least 8 hours but less than 12 hours	20% of Total MRC
At least 12 hours but less than 16 hours	30% of Total MRC
At least 16 hours but less than 24 hours	40% of Total MRC
At least 24 hours or greater	50% of Total MRC

THE TOTAL CREDIT ALLOWANCES PER CALENDAR MONTH IS CAPPED AT 50% of THAT MONTH'S MRC FOR THE INTERRUPTED PORTIONS OF SERVICE. SEPARATELY OCCURRING SERVICE INTERRUPTIONS ARE NOT AGGREGATED FOR THE PURPOSES OF DETERMINING CREDIT ALLOWANCES.

### **C. Exceptions and Terms applicable to all SLAs**

#### **Emergency Blocking**

The parties agree that if either Party hereto, in its reasonable and sole discretion, determines that an emergency action is necessary to protect its own network, the Party may, after engaging in reasonable and good faith efforts to notify the other Party of the need to block, block any transmission path over its network by the other Party where transmissions do not meet material standard industry requirements. The Parties further agree that none of their respective obligations to one another under the Agreement will be affected by any such blockage except that the Party affected by such blockage will be relieved of all obligations to make payments for charges relating to the circuit(s) which is so blocked and that no Party will have any obligation to the other Party for any claim, judgment or liability resulting from such blockage.

#### **Remedy Processes**

All claims and rights arising under this Service Level Agreement must be exercised by Customer in writing within thirty (30) days of the event that gave rise to the claim or right. The Customer must submit the following information to the Customer's Comcast account representative with any and all claims for credit allowances: (a) Organization name; (b) Customer account number; and (c) basis of credit allowance claim (including date and time, if applicable). Comcast will acknowledge and review all claims promptly and will inform the Customer by electronic mail or other correspondence whether a credit allowance will be issued or the claim rejected, with the reasons specified for the rejection.

#### **Exceptions to Credit Allowances**

A Service Interruption shall not qualify for the remedies set forth herein if such Service Interruption is related to, associated with, or caused by: scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment; any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers, any power, equipment or services provided by third parties; or an event of force majeure as defined in the Agreement.

#### **Other Limitations**

The remedies set forth in this Service Level Agreement shall be Customer's sole and exclusive remedies for any Service Interruption, Liability, outage, unavailability, delay, or other degradation, or any Comcast failure to meet the service objectives and Mitigation Intervals.

#### **Notice of Outage for On-Net Services**

If Comcast identifies an outage with respect to an On-Net Service, Comcast will notify Customer of such outage, either via email or phone, within thirty (30) minutes of becoming aware of the same.

**/END OF EDI PSA. ETHERNET INTERSTATE TRANSPORT PSA BEGINS ON NEXT PAGE/**

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
ETHERNET TRANSPORT SERVICES**

The following additional terms and conditions are applicable to Sales Orders for Comcast's Ethernet Transport Services:

**DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

**"Estimated Availability Date"** means the target date for delivery of Service.

**"HFC Network"** means a hybrid fiber coax network.

**"Interconnection Facilities"** means transmission capacity provided by Comcast, Customer or a third-party supplier to extend the Comcast Equipment from a Comcast terminal to any other location (e.g., a local loop provided by a local exchange company or other communications company).

**"Off-Net"** means geographical locations that are outside of Comcast's service area and/or geographical locations that are within Comcast's service area generally, but are not readily accessible by Comcast Network facilities. All Off-Net Services are provided by third-party service providers. Off-Net Services provisioned over a fiber optic network are referred to as **"Off-Net Fiber."**

**"On-Net"** means geographical locations where Comcast currently provides Services through its Comcast Network. On-Net Services may be provisioned over a fiber optic network (**"On-Net Fiber"**), or via an HFC Network (**"On-Net HFC"**), as available through Comcast.

**"Service(s)"** means Ethernet Transport Services.

**ARTICLE 1. SERVICES**

This attachment shall apply to Ethernet Transport Services. A further description of these Services is set forth in **Schedule A-1** hereto which is incorporated herein by reference.

**ARTICLE 2. PROVIDER**

On-Net Service provided over Fiber shall be provided by Comcast Business Communications, LLC.

On-Net Service provided over the HFC Network and Off-Net Services are available in a number of Comcast markets. For information on service availability, call 866-429-0152.

**ARTICLE 3. REGULATORY APPROVAL; TRAFFIC MIX**

Comcast's pricing for Service may be subject to FCC, public service commission or other regulatory approval. Further, Customer represents that its use of Service hereunder will be jurisdictionally interstate. Customer agrees to indemnify and hold Comcast harmless from any claims by third parties resulting from or arising out of Customer's failure to properly represent or certify the jurisdictional nature of its use of the Service(s).

**ARTICLE 4. CUSTOM INSTALLATION FEE**

Once Comcast accepts a Sales Order for Service, Comcast will invoice Customer for all Custom Installation Fee(s). Customer will pay the Custom Installation Fee(s) within thirty (30) days of the invoice date unless a payment schedule is specified in the applicable Sales Order.

**ARTICLE 5. PROVISIONING INTERVAL**

Following its acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Service on or before the Estimated Availability Date; provided, however, that Comcast's failure to provision by said date shall not constitute a breach of the Agreement.

**ARTICLE 6. SERVICE COMMENCEMENT DATE**

Comcast shall inform Customer when Service is available and performing in accordance with the "Technical Specifications" set forth in Schedule A-1 hereto (**"Availability Notification"**). Charges for Service shall begin to accrue as of the Service Commencement Date. The Service Commencement Date shall be earliest of: (A) the date on which Customer confirms receipt of and concurrence with the Availability Notification; (B) five (5) business days following the date of the Availability Notification, if Customer fails to notify Comcast that the Service does not comply materially with the Technical Specifications (defined in Article 9) or (C) the date on which Customer first uses the Service. In the event that a Service Term has not been expressly set forth in a Sales Order, the Service Term for such Sales Order shall be twelve (12) months.

**ARTICLE 7. PORTABILITY; UPGRADES**

**7.1 Portability.** Customer may terminate an existing On-Net Service (an "Existing Service") and turn up a replacement On-Net Service (i.e., activate Service with termination points

on Comcast's network that are different than those of the Existing Service) (a "Replacement Service") without incurring Termination Charges with respect to the Existing Service, provided that (a) the Replacement Service must have a Service Term equal to or greater than the remaining Service Term of the Existing Service but in no event less than twelve (12) months; (b) the Replacement Service must have monthly recurring charges equal to or greater than the monthly recurring charges for the Existing Service; (c) Customer submits a Sales Order to Comcast for the Replacement Service within ninety (90) days after termination of the Existing Service and that Sales Order is accepted by Comcast; (d) Customer reimburses Comcast for any and all installation charges that were waived with respect to the Existing Service; and (e) Customer pays the actual costs incurred by Comcast in installing and provisioning the Replacement Service.

**7.2 Upgrades.** Customer may upgrade the speed or capacity of an Existing Service without incurring Termination Charges, provided that (a) the upgraded Service (the "Upgraded Service") must assume the remaining Service Term of the Existing Service, but in no event less than twelve (12) months; (b) the Upgraded Service must have the same points of termination on Comcast's network as the Existing Service; (c) Customer submits a Sales Order to Comcast for the Upgraded Service and that Sales Order is accepted by Comcast; (d) Customer pays Comcast's applicable nonrecurring charges for the upgrade; and (e) Customer agrees to pay the applicable

monthly recurring charges for the Upgraded Service commencing with the upgrade. Upgrades to Off-Net Services are subject to the applicable third party service provider rules and availability. Comcast has no obligation to upgrade Customer's Off-Net Service.

#### **ARTICLE 8. ADDITIONAL INFORMATION**

As necessary for the interconnection of the Service with services provided by third parties, Comcast may request (as applicable), and Customer will provide to Comcast, circuit facility assignment information, firm order commitment information, and design layout records necessary to enable Comcast to make the necessary cross-connection between the Service and Customer's other service provider(s). Comcast may charge Customer nonrecurring and monthly recurring cross-connect charges to make such connections.

#### **ARTICLE 9. TECHNICAL SPECIFICATIONS AND PERFORMANCE STANDARDS; SERVICE LEVEL AGREEMENT**

The technical specifications applicable to the Service are set forth in Schedule A-1 hereto ("**Technical Specifications**"). The service level agreement applicable to the Service is set forth in a **Schedule A-2** hereto and incorporated herein by reference.

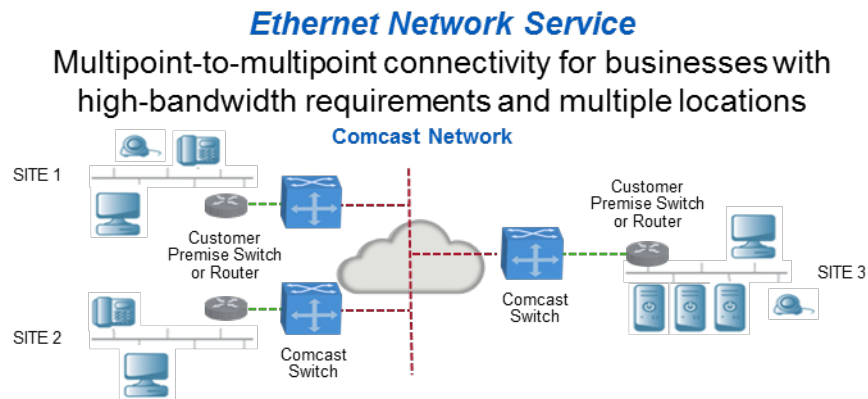
**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
ETHERNET TRANSPORT SERVICES**

**SCHEDULE A-1  
SERVICE DESCRIPTIONS, TECHNICAL SPECIFICATIONS AND PERFORMANCE STANDARDS  
COMCAST ETHERNET TRANSPORT SERVICES**

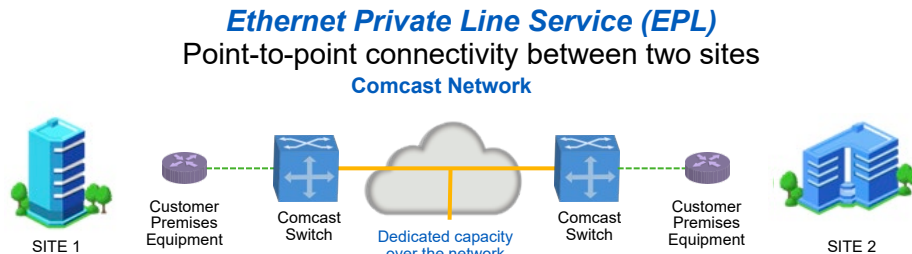
Comcast's Ethernet Transport Services will be provided in accordance with the service descriptions, technical specifications and performance standards set forth below:

**Service Descriptions**

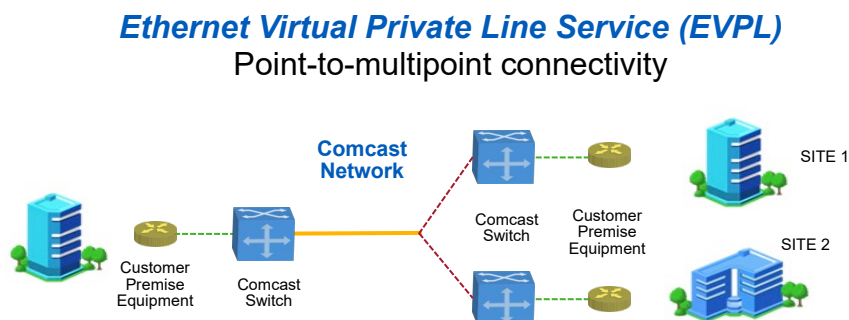
**Ethernet Network Service (ENS)** enables Customer to connect physically distributed locations across a Metropolitan Area Network (MAN) or Wide Area Network (WAN) as if they are on the same Local Area Network (LAN). The Service provides VLAN transparency enabling Customer to implement their own VLANs without any coordination with Comcast. ENS is a highly scalable service that enables customers to connect Customer Premises Equipment (CPE) using industry standard 100 Mbps, 1 Gbps or 10 Gbps Ethernet User-to-Network Interfaces (UNI) and is available with flexible bandwidth options from at 1 Mbps to 10 Gbps. Comcast ENS provides an Ethernet Virtual Connection (EVC) between Customer Service Locations that enables Customer to use any VLANs without coordination with Comcast. Comcast ENS offers three Classes of Service (CoS), as described below.



**Ethernet Private Line (EPL)** is a point-to-point transport service that provides secure, high-performance network connectivity between two Customer Service Locations. EPL is a highly scalable service that enables the Customer to connect their Customer Premises Equipment (CPE) using industry standard 100 Mbps, 1 Gbps or 10 Gbps Ethernet User-to-Network Interfaces (UNI) and is available with flexible bandwidth options from 1 Mbps to 10 Gbps. Comcast EPL provides an Ethernet Virtual Connection (EVC) between Customer Service Locations that enables the Customer to use any VLANs without coordination with Comcast. Comcast EPL offers three Classes of Service (CoS), as described below.



**Ethernet Virtual Private Line (EVPL)** service provides an Ethernet Virtual Connection (EVC) between two or more Customer Service Locations and supports the added flexibility to multiplex multiple services (EVCs) on a single UNI at the Customer's hub or aggregation site. The Service multiplexing capability is not available at sites served by the Comcast On-Net HFC. It is a highly scalable service that enables the Customer to connect their Customer Premises Equipment (CPE) using industry standard 100 Mbps, 1 Gbps or 10 Gbps Ethernet User-to-Network Interfaces (UNI) and is available with flexible bandwidth options from 1 Mbps to 10 Gbps. Comcast EVPL offers three Classes of Service (CoS), as described below.



## Multiple Access Options

Comcast Ethernet Transport Services are available with the following access options:

- On-Net Fiber Access – Connectivity to Customer Service Locations is enabled via Comcast On-Net fiber Infrastructure.
- On-Net Hybrid Fiber Coax (HFC) Access – Connectivity to Customer Service Locations is enabled via Comcast On-Net Hybrid Fiber Coax (HFC) infrastructure.
- Off-Net Access (both Fiber and Non-Fiber) – Connectivity to Customer Service Locations is enabled through a network-to-network interface (NNI) via third-party network provider.

## Ethernet Virtual Circuit (EVC) Area Types

Comcast Ethernet Transport Services are available both within and between certain major metropolitan areas throughout the United States. Each EVC is assigned an EVC Area Type based upon the proximity of respective A and Z locations.

- **Metro** – EVC enables connectivity between customer locations within a Comcast defined Metro.
- **Regional** – EVC enables connectivity between customer locations that are in different Comcast defined Metros, but within Comcast defined geographic Regions.
- **Continental** – EVC enables connectivity between customer locations that are in different Comcast defined geographic Regions.

## Ethernet Transport Technical Specifications

### 1. Ethernet User-to-Network Interface

Comcast Ethernet Transport Services provide bidirectional, full duplex transmission of Ethernet frames using a standard IEEE 802.3 Ethernet interface. Comcast implements ingress policies at CPE UNI interfaces to enforce subscribed bandwidth levels. Each ingress policing policy is created utilizing Committed Information Rate (CIR) and Committed Burst Size (CBS) components. The following table provides a list of available UNI physical interfaces and their available Committed Information Rate (CIR) bandwidth increments and Committed Burst Sizes (CBS).

UNI Speed	UNI Physical Interface	CIR Increments	CBS (bytes)
100 Mbps	100BaseT	10 Mbps	25,000
1 Gbps	1000Base T or 1000BaseSX	100 Mbps	250,000
10 Gbps	10GBase-SR or 10GBase-LR	1 Gbps	2,500,000
		10 Gbps	25,000,000

## 2. Class of Service (CoS) Options

Comcast Ethernet Transport Services are available with three different class of service (CoS) options that allow for differentiated service performance levels for different types of network traffic. This includes Basic (Low), Priority (Medium) and Premium (High). CoS is used to prioritize customer mission-critical traffic from lesser priority traffic in the network. The Customer must specify a CIR for each CoS to indicate how much bandwidth should be assigned to that CoS. The performance metrics associated with each CoS are described in the Ethernet Transport Service Level Agreement on Schedule A-2 of this PSA. As described in the following table, permissible CoS options vary by access type.

Access Type	CoS Options
On-Net Fiber	Basic, Priority & Premium
On-Net HFC	Basic & Priority
Off-Net Fiber	Basic, Priority & Premium
Off-Net Non-Fiber	Basic & Priority

## 3. CoS Identification and Marking

Customer traffic classification and forwarding is based upon Comcast CoS prioritization that must be specified in the Customer's Sales Order. It is the Customer's responsibility to shape traffic to ordered bandwidth. If the Customer only orders a single CoS solution, they are not required to mark their packets and all Customer packets will be forwarded based upon 802.1p value associated with the CoS level specified in the Sales order. All packets, tagged or untagged, will be mapped into the subscribed CoS. If Customer implements a multi-CoS solution or for EVPL ports with service multiplexing, the Customer must mark all packets using C-tag 802.1p CoS values as specified in the table below to ensure the Service will provide the intended CoS performance objectives. For multi-CoS solutions, untagged packets will be treated as if they are marked with a 0. Packets with other 802.1p values are mapped to the lowest subscribed CoS. For EVPL ports with service multiplexing, untagged packets will be discarded and C-tag VLAN ID values are used to map traffic to applicable EVC's. Based on Ethernet Frame 802.1p values, Customer's traffic is mapped to the Comcast forwarding classes traffic accordingly to the table below:

CoS Type	802.1p Marking
Basic (Low)	0-1
Priority (Medium)	2-3
Premium (High)	5

## 4. Mac Learning and Forwarding (ENS Service)

The ENS Service is capable of learning up to 2500 MAC addresses from all interfaces connecting to the Service. It is highly recommended that routing equipment be utilized to minimize the number of MAC addresses exposed directly to the Service in larger networks. Any addresses in excess of 2500 will not be learned and traffic directed to these addresses will be treated as "unknown unicast".

## 5. Traffic Management

Comcast's Network traffic-policing policies restrict traffic flows to the subscribed CIR for each service class. If the Customer-transmitted bandwidth rate for any CoS exceeds the subscribed committed information rate (CIR) and committed burst size (CBS), Comcast will discard the non-conformant packets. For packets marked with a non-conformant CoS marking, the Service will transmit them using the Basic CoS without altering the Customer's CoS markings. Traffic management policies associated with Off-Net Services will conform to the policies enforced by the third-party service provider.

## 6. Maximum Frame Size

Services delivered via Fiber support a Maximum Transmission Unit (MTU) frame size of 1600 bytes to support untagged, tagged and Q-in-Q traffic with 802.1q or 802.1ad encapsulation types. Services delivered via On-Net Fiber can, upon request, support a MTU up to 9100 bytes to support untagged, tagged and Q-in-Q frame sizes. Services delivered via Off-Net Fiber may, upon request, support a MTU up to 9100 bytes to support untagged, tagged and Q-in-Q frame sizes, but only, and solely, to the extent the applicable Off-Net provider can support such MTU frame size. Services delivered via HFC support a Maximum Transmission Unit (MTU) frame size of 1522 bytes. All frames that exceed specifications shall be dropped.

Transport Type	MTU Size
Fiber	1600-9100 bytes
HFC	1522 bytes

## 7. Customer Traffic Transparency

All fields within customers Ethernet frames (unicast, multicast and broadcast, except L2CP) from the first bit of payload are preserved and transparently transported over UNI to UNI connections, as long as they are mapped into the EVC.

## 8. Ethernet Service Frame Disposition

The Comcast Transport Services process different types of Ethernet frames differently. Frames may pass unconditionally through the Network or may be limited, as indicated in the table below, to ensure acceptable service performance. The following table illustrates Comcast's service frame disposition for each service frame type.

Service Frame Type	ENS Frame Delivery	EPL & EVPL Frame Delivery
Unicast	All frames delivered unconditionally	All frames delivered unconditionally
Multicast	All frames delivered conditionally	All frames delivered unconditionally
Broadcast	All frames delivered conditionally	All frames delivered unconditionally

### *ENS Services only:*

- Unicast Traffic. Unicast traffic must be bi-directional in order to facilitate mac-learning and avoid restriction.
- Multicast Traffic. By default, every ENS port is able to support up to 2 Mbps of multicast traffic. ENS customer who requires greater than 2 Mbps of multicast bandwidth must uniquely specify the bandwidth they require for each root site and associated Class of Service.
- Broadcast Traffic. Broadcast and unknown unicast traffic are restricted to 1.2mb or 300pps on ingress to the network.

### *EVPL Services only:*

- Customer is responsible for mapping multicast, broadcast and unknown unicast traffic to specific C-VLAN.

## **Monitoring, Technical Support and Maintenance**

1. **Network Monitoring.** Comcast monitors On-Net Services on a 24x7x365 basis.
2. **Technical Support.** Comcast provides a toll-free trouble reporting telephone number to the Comcast Enterprise Technical Support (ETS) center that operates on a 24x7x365 basis. Comcast provides technical support for service related inquiries. Technical support will not offer consulting or advice on issues relating to CPE or other equipment not provided by Comcast.
  - (a) **Escalation.** Reported troubles are escalated within the Comcast Business Services Network Operations Center (BNOC) to meet the response/restoration interval described below (Response and Restoration Standards). Service issues are escalated within the Comcast BNOC as follows: to a Supervisor at the end of the applicable time interval plus one (1) hour; to a Manager at the end of the applicable time interval plus two (2) hours, and to a Director at the end of the applicable time interval plus four (4) hours.
  - (b) **Maintenance.** Comcast's standard maintenance window for On-Net Services is Sunday to Saturday from 12:00am to 6:00am local time. Scheduled maintenance for On-Net Services is performed during the maintenance window and will be coordinated between Comcast and the Customer. Comcast provides a minimum forty eight (48) hour notice for non-service impacting maintenance. Comcast provides a minimum of seven (7) days' notice for On-Net Service impacting planned maintenance. Emergency maintenance is performed as needed without advance notice to Customer. Maintenance for Off-Net Services shall be performed in accordance with the applicable third party service provider rules. Therefore, maintenance for Off-Net Service may be performed without advance notice to Customer.
  - (c) Comcast provides certain Comcast Equipment for provisioning its Services and the delivery of the UNI, which will reside on the Customer-side of the Demarcation Point. Comcast will retain ownership and management responsibility for this Comcast Equipment. This Comcast Equipment must only be used for delivering Services. Customers are required to shape their egress traffic to the Committed Information Rate identified in the Sales Order. Comcast will be excused from paying SLA credits, as set forth in Schedule A-2, if the Service Interruption is the result of Customer's failure to shape their traffic to the contracted CIR or utilizing Comcast Equipment for non-Comcast provided services.
3. **Response and Restoration Standards.** Comcast has the following response and restoration objectives:

CATEGORY	OBJECTIVE	MEASUREMENT	REMEDIES
<i>Mean Time to Respond Telephonically to Call</i>	15 minutes	Averaged Over A Month	Escalation (see above)
<i>Mean Time to Restore On-Net Comcast Equipment</i>	4 hours	Averaged Over A Month	Escalation (see above)
<i>Mean Time to Restore Off-Net Equipment</i>	6 hours	Averaged Over A Month	Escalation (see above)
<i>Mean Time to Restore On-Net Services</i>	6 hours	Averaged Over A Month	Escalation (see above)
<i>Mean Time to Restore Off-Net Services</i>	9 hours	Averaged Over A Month	Escalation (see above)

Customer shall bear any expense incurred, e.g., dispatch/labor costs, where a Service Interruption is found to be the fault of Customer, its end users, agents, representatives or third-party suppliers.

## **Customer Responsibilities**

Comcast provides an Ethernet terminating device for provisioning its services and the delivery of the UNI. Comcast will retain ownership and management responsibility for this equipment. As a result, it must only be used for delivering Comcast Services. Customer is responsible for providing customer premises equipment (CPE) to connect to this device. To ensure proper performance, Customer is required to shape its egress traffic to the contracted CIR.

Customers have the following responsibilities related to the installation, support, and maintenance of the Service:

- Provide an operating environment with temperatures not below fifty-five (55) or above eighty-five (85) degrees Fahrenheit. Humidity shall not exceed ninety (90) percent at eighty-five (85) degrees Fahrenheit.
- Provide secure space sufficient for access to one (1) standard, freestanding, equipment cabinet at each of the Customer facilities, no further than fifty feet from the Customer router or switch interface.
- Provide outside cable entry conduit(s), entry cable ground point, and internal building conduit to allow Comcast the ability to rod/rope a fiber optic cable to the Demarcation Point.
- Locate and mark all private underground utilities (water, electric, etc.) along path of new underground placement not covered by utility companies.
- Provide a pull rope in any existing duct that Comcast is to use and ensure existing duct is serviceable for Comcast use.
- Obtain 'right-of-way' entry easement for Comcast facilities and equipment from property owners at each Customer location.
- The Customer is responsible for coring of the building's outside wall and internal walls. Upon request, Comcast can perform this activity on an 'as needed' basis for an additional one-time fee.
- Provide UPS AC power equipment, circuit sizing to be determined, if applicable.
- Emergency local generator backup service, if applicable.
- Provide access to the buildings and Demarcation Point at each Customer location to allow Comcast and its approved Contractors to install fiber for service installation. Provide access to each location for regular (8am - 5pm) and emergency (24 hour) service and maintenance of Comcast's equipment and facilities.
- Provide, install and maintain a device that is capable of interconnecting network traffic between the Service and the Customer's Local Area Network (LAN).
- Customer must provide a point of contact (POC) for installation, service activation and any maintenance activities.

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
ETHERNET TRANSPORT SERVICES**

**SCHEDULE A-2  
SERVICE LEVEL AGREEMENT**

Comcast's Ethernet Transport Services are backed by the following Service Level Agreement ("SLA"):

**A. Definitions:**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Ethernet Transport Services PSA or the General Terms and Conditions.

**Definitions**

**"Jitter"** means the short-term variations for a portion of successfully delivered service frames. Jitter may also be referred to as Frame Delay Variation.

**"Latency"** means the maximum delay for a portion of successfully delivered service frames. Latency may also be referred to as Frame Delay.

**"Market"** means the Comcast geographic region where the applicable Service Location is located, as identified on the Sales Order.

**"Packet Loss"** means the difference between the number of service frames transmitted at the ingress UNI and the total number of service frames received at the egress UNI. Packet Loss may also be referred to as Frame Loss.

**"Planned Service Interruption"** means any Service Interruption caused by planned work such as scheduled maintenance or planned enhancements or upgrades to the network.

**"Service Interruption"** means an interruption in transmission that renders the Service unusable due to a total loss of signal for the Service. The Service shall be "Available" in the absence of a Service Interruption.

**B. Ethernet Transport Service Level Agreements**

**1. Availability SLA**

Comcast's liability and Customer's sole remedy for Service Interruptions, and errors, omissions, interruptions, delays, outages, or defects in transmission or switching of any Services (individually or collectively, "**Liability**"), shall be limited to the amounts set forth in the Tables below with the stated percentages to be applied against the MRC associated with the impacted portion of the Service set forth in the Sales Order ("**Availability Credit**"). For the purposes of calculating credit for a Service Interruption, the "Length of Service Interruption" begins when the Customer reports such Service Interruption and a trouble ticket is opened, and concludes upon the closing of the same trouble ticket or, if sooner, the termination of the Service Interruption, less any time Comcast is awaiting additional information or premises testing from the Customer. The Length of Service Interruptions for separately occurring Service Interruptions will not be aggregated for purposes of determining Availability Credit allowances. To qualify, Customer must request the Availability Credit from Comcast within thirty (30) days of the beginning of the Service Interruption. Comcast shall not incur any Liability, including Availability Credit, for any failure of the Services caused by force majeure events, Planned Service Interruptions, Customer actions, omission or equipment, CPE, or any other items set forth in the "Exceptions to Credit Allowances" section below.

**TABLE 1: Availability SLA for Services provided over On-Net and Off-Net Fiber (99.99% Availability)**

<b>Length of Service Interruption:</b>	<b>Amount of Credit:</b>
Less than 4 minutes	None
At least 4 minutes but less than 4 hours	5% of Total MRC
At least 4 hours but less than 8 hours	10% of Total MRC
At least 8 hours but less than 12 hours	20% of Total MRC
At least 12 hours but less than 16 hours	30% of Total MRC
At least 16 hours but less than 24 hours	40% of Total MRC
At least 24 hours or greater	50% of Total MRC

**TABLE 3: Availability SLA for Services provided over On-Net HFC or Off-Net Non-Fiber Transport (99.9% Availability)**

<b>Length of Service Interruption:</b>	<b>Amount of Credit:</b>
Less than 40 minutes	None
At least 40 minutes but less than 4 hours	5% of Total MRC
At least 4 hours but less than 8 hours	10% of Total MRC
At least 8 hours but less than 12 hours	20% of Total MRC
At least 12 hours but less than 16 hours	30% of Total MRC
At least 16 hours but less than 24 hours	40% of Total MRC
At least 24 hours or greater	50% of Total MRC

SEPARATELY OCCURRING SERVICE INTERRUPTIONS ARE NOT AGGREGATED FOR THE PURPOSES OF DETERMINING CREDIT ALLOWANCES.

## **2. Performance Objectives SLA**

Comcast Ethernet Transport Services are available both within and between major metropolitan areas throughout the United States. The performance objectives associated with traffic flows between any two Customer Service Locations are dependent upon the locations of the respective sites, designated as Service Location A and Service Location Z on the applicable Sales Order.

### ***Access Types***

- 1. On-Net Access.** If On-Net Service Location A and On-Net Service Location Z reside within the same Market, Performance Tier 1 objectives will apply. If the On-Net Service Locations are in different Markets, a different Performance Tier will apply. The applicable Performance Tier will appear on/with the respective Sales Order.
- 2. Off-Net Access.** In addition to On-Net Access, Comcast enables Off-Net Access to Ethernet Transport Services via multiple third party providers. The Performance Tier for Off-Net Service is based upon the location of the Off-Net Service Location, the location of the Network to Network Interface (NNI) between Comcast and the third party provider and the performance commitment from the third party provider. The applicable Performance Tier will appear on the respective Sales Order.

### ***Performance Tiers and Performance Objectives***

Comcast collects continuous in-band performance measurements for its Ethernet Transport Services. The calculation of all Latency, Jitter and Packet Loss Performance Metrics for each calendar month for purposes of this Performance Objectives SLA are based upon the average of sample one-way measurements taken by Comcast during the applicable calendar month, excluding any period during which there is a Service Interruption. The below charts indicate the

Performance Standard that should be achieved for each of the Performance Metrics over each calendar month based on the applicable Performance Tier and Class of Service.

# 1. Performance Tier 1 (PT1) Agreements – Within Market

Performance Metric	Class of Service (CoS)		
	Basic	Priority	Premium
Latency (One-Way Network Delay)	45ms	23ms	12ms
Jitter (Network Delay Variation)	20ms	10ms	2ms
Packet Loss	<1%	<0.01%	<0.001%

# 2. Performance Tier 2 (PT2) Agreements

Performance Metric	Class of Service (CoS)		
	Basic	Priority	Premium
Latency (One-Way Network Delay)	80ms	45ms	23ms
Jitter (Network Delay Variation)	25ms	15ms	5ms
Packet Loss	<1%	<.02%	<.01%

# 3. Performance Tier 3 (PT3) Agreements

Performance Metric	Class of Service (CoS)		
	Basic	Priority	Premium
Latency (One-Way Network Delay)	100ms	80ms	45ms
Jitter (Network Delay Variation)	30ms	20ms	10ms
Packet Loss	<1%	<.04%	<.02%

# 4. Performance Tier 4 (PT4) Agreements

Performance Metric	Class of Service (CoS)		
	Basic	Priority	Premium
Latency (One-Way Network Delay)	120ms	100ms	80ms
Jitter (Network Delay Variation)	35ms	25ms	15ms
Packet Loss	<1%	<.05%	<.04%

# 5. Best Effort Performance Tier (BE)

No performance commitments will apply. Best Effort Performance Tier will appear on the associated Comcast Sales Order.

## Credit Allowance

Customer’s sole remedy for Comcast’s failure to achieve the applicable Performance Metric standards above over a given calendar month for the Service are the receipt of the following credit amounts with the stated percentages to be applied against the MRC associated with the impacted portion of the Service set forth in the Sales Order (“**Performance Objective Credits**”).

**TABLE 1: Credit Allowance for Latency Performance Metric**

		Performance Tier							
		PT1		PT2		PT3		PT4	
		Measurement (ms)	Credit	Measurement (ms)	Credit	Measurement (ms)	Credit	Measurement (ms)	Credit
Class of Service	Premium	0 -12	No Credit	0 - 23	No Credit	0 - 45	No Credit	0 to 80	No Credit
		12.01 - 23	10%	23.01 - 45	10%	45.01 - 80	10%	80.01 - 100	10%
		23.01 - 45	25%	45.01 - 80	25%	80.01 - 100	25%	100.01 - 120	25%
		>45	50%	>80.01	50%	>100	50%	>120	50%
	Priority	0 - 23	No Credit	0 - 45	No Credit	0 to 80	No Credit	0 to 100	No Credit
		23.01 - 45	10%	45.01 - 80	10%	80.01 - 100	10%	100.01 - 120	10%
		45.01 - 80	25%	80.01 - 100	25%	100.01 - 120	25%	120.01 - 150	25%
		>80.01	50%	>100	50%	>120	50%	>150	50%
	Basic	0 - 45	No Credit	0 to 80	No Credit	0 to 100	No Credit	0 to 120	No Credit
		45.01 - 80	10%	80.01 - 100	10%	100.01 - 120	10%	120.01 - 150	10%
		80.01 - 100	25%	100.01 - 120	25%	120.01 - 150	25%	150.01 - 180	25%
		>100	50%	>120	50%	>150	50%	>180	50%

TABLE 2: Credit Allowance for Jitter Performance Metric

		Performance Tier							
		PT1		PT2		PT3		PT4	
		Measurement (ms)	Credit	Measurement (ms)	Credit	Measurement (ms)	Credit	Measurement (ms)	Credit
Class of Service	Premium	0 - 2	No Credit	0 - 5	No Credit	0 - 10	No Credit	0 - 15	No Credit
		2.01 - 3	10%	5.01 - 10	10%	10.01 - 15	10%	15.01 - 20	10%
		3.01 - 5	25%	10.01 - 15	25%	15.01 - 20	25%	20.01 - 30	25%
		>5	50%	>15	50%	>20	50%	>30	50%
	Priority	0 - 10	No Credit	0 - 15	No Credit	0 - 20	No Credit	0 - 25	No Credit
		10.01 - 15	10%	15.01 - 20	10%	20.01 - 30	10%	25.01 - 40	10%
		15.01 - 20	25%	20.01 - 30	25%	30.01 - 50	25%	40.01 - 60	25%
		>20	50%	>30	50%	>50	50%	>60	50%
	Basic	0 - 20	No Credit	0 - 25	No Credit	0 - 30	No Credit	0 - 35	No Credit
		20.01 - 30	10%	25.01 - 40	10%	30.01 - 50	10%	35.01 - 60	10%
		30.01 - 50	25%	40.01 - 60	25%	50.01 - 80	25%	60.01 - 90.01	25%
		>50	50%	>60	50%	>80	50%	>90	50%

TABLE 3: Credit Allowance for Packet Loss Performance Metric

		Performance Tier							
		PT1		PT2		PT3		PT4	
		Measurement	Credit	Measurement	Credit	Measurement	Credit	Measurement	Credit
Class of Service	Premium	0% - 0.001%	No Credit	0% - 0.01%	No Credit	0% - 0.02%	No Credit	0% - 0.04%	No Credit
		0.001% - 2.00%	10%	0.01% - 2.00%	10%	0.02% - 2.00%	10%	0.04% - 2.00%	10%
		2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%
		>4.00%	50%	>4.00%	50%	>4.00%	50%	>4.00%	50%
	Priority	0% - 0.01%	No Credit	0% - 0.02%	No Credit	0% - 0.04%	No Credit	0% - 0.05%	No Credit
		0.01% - 2.00%	10%	0.02% - 2.00%	10%	0.04% - 2.00%	10%	0.05% - 2.00%	10%
		2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%
		>4.00%	50%	>4.00%	50%	>4.00%	50%	>4.00%	50%
	Basic	0% - 1.00%	No Credit	0% - 1.00%	No Credit	0% - 1%	No Credit	0% - 1%	No Credit
		1.01% - 2.00%	10%	1.01% - 2.00%	10%	1.01% - 2.00%	10%	1.01% - 2.00%	10%
		2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%
		>4.00%	50%	>4.00%	50%	>4.00%	50%	>4.00%	50%

Customer shall only be entitled to receive a Performance Objective Credit for one Performance Metric failure per affected portion of the Service per calendar month. For example, if the applicable metric for Jitter and Latency were missed for the same transport connection (Service Location A to Service Location Z) in a given calendar month, Customer will only be entitled to the Performance Objective Credit associated with either the Jitter or Latency failure for such portion of the Service. To qualify for a Performance Objective Credit, Customer must request the applicable Performance Objective Credit from Comcast within thirty (30) days of the end of the applicable calendar month in which the applicable Performance Metric standard was not achieved. Comcast shall not incur any liability, including Performance Objective Credit, for any failure of the Services caused by force majeure events, Planned Service Interruptions, Customer actions, omissions or equipment, CPE or any other items set forth in the "Exceptions to Credit Allowances" section below.

### **C. Exceptions and Terms applicable to all SLAs**

#### **1. Emergency Blocking**

The Parties agree that if either Party hereto, in its reasonable sole discretion, determines that an emergency action is necessary to protect its own network, the Party may, after engaging in reasonable and good faith efforts to notify the other Party of the need to block, block any transmission path over its network by the other Party where transmissions do not meet material standard industry requirements. The Parties further agree that none of their respective obligations to one another under the Agreement will be affected by any such blockage except that the Party affected by such blockage will be relieved of all obligations to make payments for charges relating to the circuit(s) which is so blocked and that no Party will have any obligation to the other Party for any claim, judgment or liability resulting from such blockage.

#### **2. Remedy Processes**

All claims and rights arising under this Service Level Agreement must be exercised by Customer in writing within the time period set forth in Sections B.1 and B.2, as applicable. The Customer must submit the following information to the Customer's Comcast account representative with any and all claims for credit allowances: (a) Organization name; (b) Customer account number; and (c) basis of credit allowance claim (including date and time, if applicable). Comcast will acknowledge and review all claims promptly and will inform the Customer by electronic mail or other correspondence whether a credit allowance will be issued or the claim rejected, with the reasons specified for the rejection.

#### **3. Exceptions to Credit Allowances**

Comcast's failure to meet the either of the SLAs set forth on this Schedule A-2 shall not qualify for the remedies set forth herein if such failure is related to, associated with, or caused by: Planned Service Interruptions or other scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment; any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers, any power, equipment or services provided by third parties; or an event of force majeure as defined in the Agreement.

#### **4. Other Limitations**

THE TOTAL CREDIT ALLOWANCES PER CALENDAR MONTH UNDER THIS SCHEDULE A-2 IS CAPPED AT 50% OF THAT MONTH'S MRC FOR THE IMPACTED PORTIONS OF SERVICE. In addition, the remedies set forth in this Service Level Agreement shall be Customer's sole and exclusive remedies for any Service Interruption, outage, unavailability, delay, or other degradation, or any Comcast failure to meet the service objectives.

#### **5. Notice of Outage for On-Net Services**

If Comcast identifies an outage with respect to an On-Net Service, Comcast will notify Customer of such outage, either via email or phone, within thirty (30) minutes of becoming aware of the same.

**/END OF INTERSTATE TRANSPORT PSA. TRUNK PSA BEGINS ON NEXT PAGE/**

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
TRUNK SERVICES**

The following additional terms and conditions are applicable to Sales Orders for Comcast's Trunk Services:

**DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

**"Estimated Availability Date"** means the target date for delivery of Service.

**"Interconnection Facilities"** means transmission capacity provided by Comcast, Customer or a third-party supplier to extend the Comcast Equipment from a Comcast terminal to any other location (e.g., a local loop provided by provided by a local exchange company or other communications company).

**"Services"** means Trunk Services.

**ARTICLE 1. SERVICES**

This attachment shall apply to Trunk Services. A further description of these Services is set forth in Schedule A-1 hereto which is incorporated herein by reference.

**ARTICLE 2. PROVIDER**

Service shall be provided by Comcast IP Phone, LLC or one of its applicable affiliates or subsidiaries.

**ARTICLE 3. CUSTOM INSTALLATION FEE**

Once Comcast accepts a Sales Order for Service, Comcast will invoice Customer for all Custom Installation Fee(s). Customer will pay the Custom Installation Fee(s) within thirty (30) days of the invoice date unless a payment schedule is specified in the applicable Service Order.

**ARTICLE 4. PROVISIONING INTERVAL**

Following its acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Service on or before the Estimated Availability Date; provided, however, that Comcast's failure to provision by said date shall not constitute a breach of the Agreement.

**ARTICLE 5. SERVICE COMMENCEMENT DATE**

The Service Commencement Date shall be defined as the date(s) on which Comcast first makes Service available for use by Customer. A single Service Order containing multiple Service Locations or Services may have multiple Service Commencement Dates. Comcast shall notify Customer that the Services are available for use on the Service Commencement Date. Any failure or refusal on the part of Customer to be ready to receive the Service on the Service Commencement Date shall not relieve Customer of its obligation to pay applicable Service charges.

**ARTICLE 6. PORTABILITY**

**6.1 Portability.** Customer may terminate an existing Service (an "Existing Service") and turn up a replacement Service (i.e., having different termination points on Comcast's network) (a "Replacement Service") without incurring Termination Charges with respect to the Existing Service, provided that (a) the Replacement Service must have a Service Term equal to the remaining Service Term of the Existing Service; (b) the Replacement Service must have monthly recurring charges equal to or

greater than the monthly recurring charges for the Existing Service; (c) Customer submits a Sales Order to Comcast for the Replacement Service within ninety (90) days after termination of the Existing Service and that order is accepted by Comcast; (d) Customer reimburses Comcast for any and all installation charges that were waived with respect to the Existing Service; and (e) Customer pays the actual costs incurred by Comcast in installing and provisioning the Replacement Service.

## **ARTICLE 7. SERVICE CREDITS**

**7.1 Credit Allowances.** Comcast will allow a pro-rata credit against future payment of the net monthly recurring charge (exclusive of nonrecurring charges, other one-time charges, per call charges, measured charges, regulatory fees and surcharges, taxes, and other governmental and quasi-governmental fees) for a Service Interruption, except as specified below or as may otherwise be legally required ("Credit"). "Service Interruption" shall mean a break in transmission that renders the Service unusable for transmission and reception. For the purposes of calculating a Credit allowance, the Service Interruption period begins when the Customer reports an interruption in the portion of the Service to Comcast, a trouble ticket is opened, and the Service is released to Comcast for testing and repair. The Service Interruption ends when the affected portion of the Service has been restored and Comcast has closed the trouble ticket. Service Interruption time does not include interruptions of less than thirty (30) minutes' duration. Credits will be as follows:

<u>Length of Service Interruption</u>	<u>Amount of Credit</u>
Less than 30 minutes	None
At least 30 minutes but less than 3 hours	1/8 of a day
At least 3 hours but less than 6 hours	1/4 of a day
At least 6 hours but less than 9 hours	2/5 of a day
At least 9 hours but less than 12 hours	1/2 of a day
At least 12 hours but less than 15 hours	4/5 of a day
At least 15 hours and up to and including 24 hours	1 full day

The total number of credit allowances per month shall not exceed the total monthly recurring charge for the affected Service. Credit allowances will not be made for less than \$1.00, unless required under applicable law. Service Interruptions will not be aggregated for purposes of determining credit allowances. To qualify, Customer must request the Credit from Comcast within 30 days of the interruption.

**7.2 Exceptions to Credit Allowances.** A Service Interruption shall not qualify for the Credits set forth herein if such Service Interruption is related to, associated with, or caused by: scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment; any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers; any power, equipment or services provided by third parties; or an event of force majeure as defined in this Agreement, unless otherwise provided under applicable law. The remedies set forth in this Article shall be Customer's sole and exclusive remedy for any Service Interruption in the Services, outage, unavailability, delay or other degradation in the Services or any Comcast failure to meet the objectives of the Services.

## **ARTICLE 8: USE POLICY**

**8.1 Additional Use Restrictions.** The Service may only be used at Service Location(s) where Service is installed by Comcast. Customer understands and acknowledges that if Customer attempts to install or use the Comcast Equipment or Service at another location, Service, including but not limited to 911/E911, may fail to function or may function improperly. It will be considered a material violation of the Agreement if Customer moves Service to another location without first notifying Comcast. Customer expressly agrees not to use the Service for auto-dialing, continuous or extensive call forwarding, telemarketing, fax broadcasting or fax blasting, or for any other use that results in excessive usage inconsistent with standard commercial calling patterns. If Comcast determines, in its sole discretion, that Customer's use of the Service is excessive or in violation of this Agreement, Comcast reserves the right, among other things, to terminate or modify the Service immediately and without notice.

## **ARTICLE 9: SERVICE LIMITATION**

**9.1 Service Disruption.** Customer acknowledges and understands that the Service will not be available for use under certain circumstances, including without limitation when the network or facilities are not operating or if normal electrical power to the MTA, ALA or ALG is interrupted and such equipment does not have a functioning backup. Customer also understands and acknowledges that the performance of the battery backup is not guaranteed. If the battery backup does not provide power, Services will not function until normal power is restored. Customer also understands that certain online features of the Service, where such features are available, will not be available under certain circumstances, including but not limited to the interruption of the Internet connection.

**9.2 Provision of Service.** Subject to the terms and conditions herein, the Services are intended for commercial use only.

#### **ARTICLE 10: LIMITATIONS OF 911/E911**

**10.1 Limitations.** Services includes a 911/ Enhanced 911 function ("911/E911") that may differ from the 911 or Enhanced 911 function furnished by other providers. As such, it may have certain limitations. CUSTOMER ACKNOWLEDGES AND ACCEPTS ANY LIMITATIONS OF 911/E911.

**10.2 Correct Address.** In order for Customer's 911/E911 calls to be properly directed to emergency services, Comcast must have Customer's correct Service Location address. If Customer moves the Service to a different Service Location without Comcast's approval, 911/E911 calls may be directed to the wrong emergency authority, may transmit the wrong Service Location address, and/or Service (including 911/E911) may fail altogether. Therefore, Customer must contact Comcast at least five (5) days before moving the Service to a new Service Location. All changes in Service Location require Comcast's prior approval.

**10.3 Service Interruptions.** Customer acknowledges and understands that the Service uses the electrical power in Customer's Service Location. If there is an electrical power outage, 911 calling may be interrupted if the battery backup in the associated MTA, ALA or ALG is not installed, fails, or is exhausted after several hours. Furthermore, calls, including calls to 911/E911, may not be completed if Customer exceeds its Service and equipment configuration calling capacity or if there is a problem with network facilities, including network congestion, network/equipment/power failure, or another technical problem.

**10.4 Suspension and Termination by Comcast.** Customer understands and acknowledges that the Service, including 911/E911, as well as all online features of the Service, where Comcast make these features available, will be disabled if Customer's account is suspended or terminated.

**10.5 LIMITATION OF LIABILITY AND INDEMNIFICATION.** CUSTOMER ACKNOWLEDGES AND AGREES THAT NEITHER COMCAST NOR ITS ASSOCIATED PARTIES WILL BE LIABLE FOR ANY SERVICE OUTAGE, INABILITY TO DIAL 911 USING THE SERVICES, AND/OR INABILITY TO ACCESS EMERGENCY SERVICE PERSONNEL. CUSTOMER AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS COMCAST AND ITS ASSOCIATED PARTIES FROM ANY AND ALL CLAIMS, LOSSES, DAMAGES, FINES, PENALTIES, COSTS, AND EXPENSES (INCLUDING BUT NOT LIMITED TO REASONABLE ATTORNEY FEES) BY, OR ON BEHALF OF, CUSTOMER OR ANY THIRD PARTY OR USER OF THE SERVICES RELATING TO THE FAILURE OR OUTAGE OF THE SERVICES, INCLUDING THOSE RELATED TO 911/E911.

**10.6 911 Notice for Trunk Services.** Customer expressly acknowledges and agrees that it has reviewed, understands, and agrees to the terms set forth below.

(a) **Customer action is essential to the protection of its employees and other users of the Services, as described below.** Multi-line telephone systems, such as PBX systems, ordinarily only transmit the same, generic location information for all 911 calls placed from any handset connected to the PBX or other system. For example, in the case of a business with telephone extensions in three buildings and multiple floors in each building, the E911 call taker would only see the same main telephone number and location that the customer has identified, regardless of which station was used to place the call. **If Customer does not take action as described below, fire, police and other emergency responders may be delayed or even prevented from timely reaching its location in response to a 911 call.**

(b) Comcast offers the opportunity for a Customer to designate up to 1000 different locations within its premises that would be separately identified to the E911 call taker, such as a specific floor, side of a building, room number, cubicle number, or other identifying information that could assist emergency responders to more quickly reach the appropriate location. To utilize this option, Customer must in the initial or a subsequent Service Order request the assignment of Emergency Location Information numbers and provide location information for each telephone number exactly as it should appear to the 911 call taker. For each requested telephone number, up to 1000, Customer will provide the specific location information (floor, room, and/or cubicle number). Customer is solely responsible for programming its telephone system to map each station to one of these numbers, and for updating the system as necessary to reflect moves or additions of stations within the premises.

(c) Many states now require businesses using multi-line telephone systems to program their systems to transmit specific location information for 911 calls. Customer acknowledges and understands that it, and not Comcast, bears sole responsibility to ensure that it identifies and complies with all such applicable laws, and any failure to do so is a breach of the Agreement. Customer represents, warrants and covenants that it will utilize the Comcast Emergency Location Information numbers described above at least to the extent required by law, and that Customer does not require the use of more than 1000 different location identifiers or other features not currently offered under this Agreement in order to comply with applicable laws. Customer also warrants that it does not currently have "Private Switch/Automatic Location Identification" service in connection with its existing telephone service from another provider at the location(s) for which it has ordered Services from Comcast.

(d) Comcast will post only the main billing telephone number in the 911 database or databases using Customer's billing address as the Registered Location, unless Customer requests the assignment of Emergency Location Information as set forth above. Customer must notify Comcast at least five (5) days prior to moving the Trunk Service to another location. Customer acknowledges that if they move prior to providing such notice and a 911 call is placed using the Services, or if Customer when using Emergency Location Information numbers does not timely update their telephone system to account for internal moves, adds and changes, the E911 call taker may see incorrect or incomplete location information and the caller may need to confirm their actual location information to the call taker.

(e) Some businesses elect to make test calls to 911 from multiple stations to verify that the 911 call taker receives the desired location information and is able to call back one or more of the telephone numbers that they receive to confirm it rings to the station from which the 911 call was placed. If Customer chooses to do so, it agrees to obtain prior approval from the relevant emergency communications center and assumes all responsibility for the placement of such calls.

## **10.7 Recommended Battery Back-Up is NOT Included**

Customer acknowledges and understands that the Services use the electrical power from the Service Location. Customer understands and acknowledges that they may lose access to and use of the Services, including 911/E911, if electrical power to the Integrated Access Device (IAD), PBX switch, and/or handsets is interrupted and such devices are not supported by a working battery backup. Customer also understands and acknowledges that Comcast does not provide a battery backup for such devices and Customer is urged to arrange for their own backup power supply to these devices. In the event of a power outage, the duration of Trunk Service during a power outage using the Comcast Equipment installed to provide Trunk Service will depend on Customer's backup power choice. If the IAD is disconnected or removed and/or a battery is not charged, Trunk Service, including access to 911, will not be available. Customer acknowledges and agrees that in the event of a power failure, Comcast bears no responsibility for such loss of service.

## **ARTICLE 11: EQUIPMENT REQUIREMENTS**

**11.1 MTA.** To use the Service, Customer will need a multimedia terminal adapter ("MTA"), application layer gateway ("ALG"), analog telephone adapter ("ATA") or other adapter device. Customer can lease an MTA from Comcast, in which case it will be Comcast Equipment. Or, in some areas, Comcast may permit Customer to use Service with an MTA that Customer has purchased, in which case the MTA will be Customer Equipment. Customer agrees to keep the MTA plugged into a working electrical power outlet at all times.

**11.2 Incompatible Equipment and Services.** Customer acknowledges and understands Service may not support or be compatible with:

- (f) Non-recommended configurations including but not limited to MTAs, ATAs or ALGs not currently certified by Comcast as compatible with Service;
- (b) Certain non-voice communications equipment, including certain makes or models of alarm and security systems, certain medical monitoring devices, certain fax machines, and certain “dial-up” modems;
- (c) Rotary-dial phone handsets, pulse-dial phone handsets, and models of other voice-related communications equipment such as certain private branch exchange (PBX) equipment, answering machines, and traditional Caller ID units;
- (d) Casual/dial around (10-10) calling; 976, 900, 700, or 500 number calling;
- (e) 311, 511, or other x11 calling (other than 411, 611, 711, and 911); and
- (f) Other call types not expressly set forth in Comcast’s product literature (e.g., outbound shore-to-ship calling).

Customer’s attempt to use any such systems in connection with the Services is solely at its own risk and Comcast shall not be liable for any damages whatsoever for any non-operation or damage to such services or devices.

**11.3 Customer Responsibility for Customer-Provided Equipment**

- (a) Customer is solely responsible for providing and maintaining working PBX equipment and handsets (Customer-Provided Equipment), notifying and training its users regarding proper use of the system in accordance with applicable, including regulatory, requirements, and for any programming to its telephone system that may be necessary to enable direct dialing of N11 numbers such as 911 or 711 and to enable calls to be connected to new area codes. Comcast will support N11 dialing service in areas where the service is made available by the local municipality. Customer also acknowledges and accepts that Comcast does not support seven-digit local calling even in areas of the country that still permit that option, and Customer will program its system as necessary to support ten-digit dialing for local calls.
- (b) Comcast shall not be responsible to the Customer if changes in any of the facilities, operations or procedures of Comcast utilized in the provision of Trunk Service render any Customer-Provided Equipment or other equipment provided by a Customer obsolete or require modification or alteration of such equipment or system or otherwise affect its use or performance.
- (c) Customer must arrange its Customer-Provided Equipment to provide for the interception of assigned but unused station numbers. A call intercepted by the attendant will be considered to be completed and subject to a charge for the call.

**ARTICLE 12: ADDITIONAL LIMITATIONS ON COMCAST’S LIABILITY FOR VOICE SERVICE**

**12.1 Limitations on Comcast’s Liability for Directories and Directory Assistance for Service Customers.** THESE LIMITATIONS SHALL APPLY WHERE COMCAST MAKES AVAILABLE AN OPTION TO LIST CUSTOMER’S NAME, ADDRESS, AND/OR TELEPHONE NUMBER IN A PUBLISHED DIRECTORY OR DIRECTORY ASSISTANCE DATABASE, AND ONE OR MORE OF THE FOLLOWING CONDITIONS OCCURS: (i) CUSTOMER REQUESTS THAT CUSTOMER’S NAME, ADDRESS AND/OR PHONE NUMBER BE OMITTED FROM A DIRECTORY OR DIRECTORY ASSISTANCE DATABASE, BUT THAT INFORMATION IS INCLUDED IN EITHER OR BOTH; (ii) CUSTOMER REQUESTS THAT CUSTOMER’S NAME, ADDRESS AND/OR PHONE NUMBER BE INCLUDED IN A DIRECTORY OR DIRECTORY ASSISTANCE DATABASE, BUT THAT INFORMATION IS OMITTED FROM EITHER OR BOTH; OR (iii) THE PUBLISHED OR LISTED INFORMATION FOR CUSTOMER’S ACCOUNT CONTAINS MATERIAL ERRORS OR OMISSIONS. IF ANY OF THESE CONDITIONS PERTAIN, THEN THE AGGREGATE LIABILITY OF COMCAST AND ITS ASSOCIATED PARTIES SHALL NOT EXCEED THE MONTHLY CHARGES, IF ANY, WHICH CUSTOMER HAS ACTUALLY PAID TO COMCAST TO LIST, PUBLISH, NOT LIST, OR NOT PUBLISH THE INFORMATION FOR THE AFFECTED PERIOD. CUSTOMER SHALL HOLD HARMLESS COMCAST AND ITS

ASSOCIATED PARTIES AGAINST ANY AND ALL CLAIMS FOR DAMAGES CAUSED OR CLAIMED TO HAVE BEEN CAUSED, DIRECTLY OR INDIRECTLY, BY THE ERRORS AND OMISSIONS REFERENCED ABOVE. FURTHERMORE, IF COMCAST MAKES AVAILABLE DIRECTORY ADVERTISING SERVICES, NEITHER COMCAST NOR ANY OF ITS ASSOCIATED PARTIES WILL BE LIABLE FOR ANY ACTS, ERRORS, OR OMISSIONS RELATED TO SUCH DIRECTORY ADVERTISING.

12.2 **CUSTOMER INFORMATION.** Comcast and its suppliers reserve the right both during the term of the Agreement and upon its termination to delete Customer's voicemail, call detail, data, files, or other information that is stored on Comcast's or its suppliers' servers or systems, in accordance with our storage policies. Customer understands and acknowledges that Comcast shall have no liability whatsoever as a result of the loss or removal of any such voicemail, call detail, data, files, or other information.

### **ARTICLE 13: SERVICE CHARGES**

(a) **Prices.** The Service is subject to the trunk service pricing identified in the applicable Service Order, and subject to the pricing lists and fees found at <http://www.comcast.com/corporate/about/phonetermsofservice/comcastdigitalvoice/cdvbusiness.html>.

(b) **Billing Increments.** Unless otherwise stated in a Service Order, domestic long distance calls, and in-bound domestic calls to toll-free numbers associated with the Services will be billed on basis of six (6) second increments with a minimum call duration of six (6) seconds. All other calls will be billed in accordance with the increments identified in the pricing lists and fees found at <http://www.comcast.com/corporate/about/phonetermsofservice/comcastdigitalvoice/cdvbusiness.html>. For purposes of this section, "domestic long distance" means non-local calls to the fifty (50) United States, Washington, D.C., Puerto Rico, US Virgin Islands, Guam, Saipan, N. Mariana Islands and American Samoa.

(c) **Pooled Minutes.** Each channel purchased in connection with Trunk Service includes a monthly allotment of 200 minutes of domestic long distance. These minutes shall be pooled at the Service Location level within an account. Any usage in excess of the earned amount shall be considered overage and be rated at the then current rate. Unused minutes expire at the end of the billing period and are not carried forward or otherwise creditable to Customer's account.

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
TRUNK SERVICES**

**SCHEDULE A-1**

**SERVICE DESCRIPTIONS AND TECHNICAL SPECIFICATIONS**

Trunk Service is a switched voice trunk service with ISDN / PRI connectivity from a customer's Private Branch Exchange (PBX) to the Comcast network. The Service is delivered by Comcast Equipment installed at the Customer Location. The Comcast Equipment provides a PRI interface with the customer's Private Branch Exchange, and connects to the Comcast DOCSIS or Fiber fed facilities (determined by Comcast). The Service supports the following standard variants of ISDN: NI-2, ATT 4ESS, ATT 5ESS, NT DMS-100, NT DMS-250. As with other Comcast voice services, Trunk Services are supported by Comcast's own network, and like other voice traffic is provided the highest Quality of Service (QoS) with respect to traffic prioritization and bandwidth allocation.

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
TRUNK SERVICES**

**SCHEDULE A-2**

**SERVICE LEVEL AGREEMENT**

**Trunk Services, Version 1.2**

Comcast's Trunk Services is backed by the following Service Level Agreement ("SLA"):

**Definitions**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Trunk Services PSA or the General Terms and Conditions.

**"Degraded Service"** – A trouble ticket classification where calls can be made but may be suffering from limited or intermittent problems such as sound quality impairment

**"Monthly Recurring Charge (MRC)"** – The monthly recurring charges for Service.

**Service Level Agreement (SLA)**

Company's liability for any Total Service Interruption of its Trunk Services (individually or collectively, "Liability"), shall be limited to the amounts set forth in the below Table 1. The term "Liability" refers to an interruption in transmission that renders the Service unusable due to a total loss of signal for the service ("Total Service Interruption"). For the purposes of calculating credit for any such Liability, the Liability period begins when the Customer reports an interruption in the portion of the Service to Company, provided that the Liability is reported by Customer during the duration of the Liability, and, a trouble ticket is opened; the Liability shall be deemed resolved upon closing of the same trouble ticket or the termination of the interruption, if sooner, less any time Comcast is awaiting additional information or premises testing from the Customer. Multiple events will require multiple trouble tickets to be opened. Service that fails to materially conform to the stated technical specifications and performance standards but is not a considered a total loss of Service shall be considered a Degraded Service, and will be entitled to Credits as identified in Article 7.1 of the Trunk Service PSA.

**TABLE 1**

For all Total Service Interruptions within any thirty (30) day period

<b>Aggregate length of Total Service Interruptions during a 30 day period:</b>	<b>Amount of Credit</b>
Less than 4 hours	None
At least 4 hours but less than 5 hours	1/30 of the MRC*
For each additional whole hour thereafter.	Additional 1/30 of the MRC*

\*Based on a 30 day month

THE TOTAL CREDIT ALLOWANCE PER MONTH IS CAPPED AT 100% of THAT MONTH'S MRC FOR THE INTERRUPTED CIRCUIT/SERVICE.

Customer shall bear any expense incurred, e.g., dispatch/labor costs, where a Service Interruption is found to be the fault of Customer, its end users, agents, representatives or third-party suppliers.

### **Emergency Blocking**

The parties agree that if either party hereto, in its reasonable sole discretion, determines that an emergency action is necessary to protect its own network, the party may, after engaging in reasonable and good faith efforts to notify the other party of the need to block, block any transmission path over its network by the other party where transmissions do not meet material standard industry requirements. The parties further agree that none of their respective obligations to one another under the Agreement will be affected by any such blockage except that the party affected by such blockage will be relieved of all obligations to make payments for charges relating to the circuit(s) which is so blocked and that no party will have any obligation to the other party for any claim, judgment or liability resulting from such blockage.

### **Remedy Processes**

All claims and rights arising under this Service Level Agreement must be exercised by Customer in writing within thirty (30) days of the event that gave rise to the claim or right. The Customer must submit the following information to the Customer's Comcast account representative with any and all claims for credit allowances: (a) Organization name; (b) Customer account number; (c) Trouble Ticket number(s) opened by the customer, and (d) basis of credit allowance claim (including date and time, if applicable). Comcast will acknowledge and review all claims promptly and will inform the Customer by electronic mail or other correspondence whether a credit allowance will be issued or the claim rejected, with the reasons specified for the rejection.

### **Exceptions to Credit Allowances**

A Total Service Interruption shall not qualify for the remedies set forth herein if such Total Service Interruption is related to, associated with, or caused by: scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment; any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers, any power, equipment or services provided by third parties; or an event of Force Majeure as defined in the Agreement. Further a Total Service Interruption shall not qualify for remedies set forth herein if Comcast has provided a reasonable temporary work around which the Customer has or has not accepted.

### **Other Limitations**

The remedies set forth in this Service Level Agreement shall be Customer's sole and exclusive remedies for any Service Interruption, outage, unavailability, delay, or other degradation, or any Comcast failure to meet the service objectives.

**/END OF TRUNK PSA. BUSINESS INTERNET PSA BEGINS ON NEXT PAGE/**

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
CABLE MODEM INTERNET SERVICES**

The following additional terms and conditions are applicable to Sales Orders for Comcast's Cable Modem Internet Service:

**DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

**"Estimated Availability Date"** means the target date for delivery of Service.

**"Interconnection Facilities"** means transmission capacity provided by Comcast, Customer or a third-party supplier to extend the Comcast Equipment from a Comcast terminal to any other location (e.g., a local loop provided by a local exchange company or other communications company).

**"Off-Net"** means geographical locations that are outside of Comcast's service area and/or geographical locations that are within Comcast's service area generally, but are not readily accessible by Comcast Network facilities. All Off-Net Services are provided by third-party service providers.

**"On-Net"** means geographical locations where Comcast currently provides Services through its Comcast Network. On-Net Services may be provisioned over a fiber optic network, or via a hybrid fiber coax network ("HFC Network"), as available through Comcast.

**"Service"** means Cable Modem Internet Service offered under the Agreement.

**ARTICLE 1. SERVICES**

This attachment shall apply to Cable Modem Internet Service offered under the Agreement.

**ARTICLE 2. PROVIDER**

On-Net Service shall be provided by the operating company subsidiary of Comcast Corporation that owns and/or operates the cable television system in the applicable service area.

On-Net Service provided over the HFC Network and Off-Net Services are available in a limited number of markets. For information on service availability, contact your Program Manager

All Off-Net Services are provided by third-party service providers, and managed by Comcast

**ARTICLE 3. CUSTOM INSTALLATION FEES**

Once Comcast accepts a Sales Order for Service, Comcast will invoice Customer for any and all Custom Installation Fee(s) unless otherwise specified in the SOW/Sales Order. Customer will pay the Customer Installation Fee(s) within thirty (30) days of the invoice date unless a payment schedule is specified in the applicable SOW/Sales Order.

**ARTICLE 4. PROVISIONING INTERVAL**

Following its acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Service on or before the Estimated Availability Date; provided, however, that Comcast's failure to provision by said date shall not constitute a breach of the Agreement.

**ARTICLE 5. SERVICE COMMENCEMENT DATE**

The Service Commencement Date for On-Net Services shall be the date Comcast completes installation and connection of

the necessary facilities and equipment to provide the Service at a Service Location. Comcast shall inform Customer when Service is available for all Off Net locations ("Service Commencement Date"). Charges for Service shall begin to accrue as of the Service Commencement Date.

#### **ARTICLE 6. PROVISION OF SERVICE/USE**

Subject to the terms and conditions herein, Internet Services are intended for commercial use only. Customer is prohibited from reselling the Services.

#### **ARTICLE 7: SERVICE CREDITS**

**7.1 Credit Allowances.** Comcast will allow a pro-rata credit against future payment of the net monthly recurring charge (exclusive of nonrecurring charges, other one-time charges, per call charges, measured charges, regulatory fees and surcharges, taxes, and other governmental and quasi-governmental fees) for a Service Interruption, except as specified below or as may otherwise be legally required ("Credit"). "Service Interruption" shall mean a break in transmission that renders the Service unusable for transmission and reception. For the purposes of calculating a Credit allowance, the Service Interruption period begins when the Customer reports an interruption in the portion of the Service to Comcast, a trouble ticket is opened, and the Service is released to Comcast for testing and repair. The Service Interruption ends when the affected portion of the Service has been restored and Comcast has closed the trouble ticket. Service Interruption time does not include interruptions of less than thirty (30) minutes' duration. Credits will be as follows:

<u>Length of Service Interruption</u>	<u>Amount of Credit</u>
At least 4 hours and up to and including 24 hours	1 full day

The total number of credit allowances per month shall not exceed the total monthly recurring charge for the affected Service. Credit allowances will not be made for less than \$1.00, unless required under applicable law. To qualify, Customer must request the Credit from Comcast within 30 days of the Service Interruption.

**7.2 Exceptions to Credit Allowances.** Except as otherwise provided in the General Terms and Conditions, a Service Interruption shall not qualify for the Credits set forth herein if such Service Interruption is related to, associated with, or caused by: scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment; any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers; any power, equipment or services provided by third parties; or an event of force majeure as defined in this Agreement, unless otherwise provided under applicable law. The remedies set forth in this Article 9 shall be Customer's sole and exclusive remedy for any Service Interruption in the Services, outage, unavailability, delay or other degradation in the Services or any Comcast failure to meet the objectives of the Services.

#### **ARTICLE 8: ADDITIONAL TERMS APPLICABLE TO PRIVATE WI-FI AND PUBLIC WI-FI (INCLUDING WI-FI HOTSPOT SERVICES) SERVICES**

If Customer submits a Sales Order(s) for Private Wi-Fi ("Private Wi-Fi Services") and Public Wi-Fi (including Hot Spot Service, "Public Wi-Fi Services") services (collectively "Wi-Fi Services") the following terms shall also apply:

**11.1 Limitation.** Subject to service availability, Customer may order Wi-Fi Services to provide Internet connectivity to certain areas of the Service Location as further described below. Wi-Fi Services are not intended for use within residential dwellings or for multi-tenant use (i.e. common areas within a mall or office building). In order to order and retain Wi-Fi Service with Comcast, Customer must have Internet Service at the applicable Service Location. Comcast shall have no liability for loss of Wi-Fi Services which results from Customer's failing to maintain Internet Service at the Service Location.

- (a) Private Wi-Fi Services are offered together with Public Wi-Fi Services, and may not be ordered separately.
- (b) Public Wi-Fi Services may be order with or without Private Wi-Fi Services.

**11.2 Term and Termination.** Wi-Fi Services are offered on a month to month basis. Customer shall have the right to terminate Wi-Fi Services, at any time, for any reason, upon thirty (30) days prior written notice to Comcast, subject to payment of all outstanding amounts due for the Wi-Fi Services, if any, and the return of any and all Comcast Equipment. Termination of Wi-Fi Services is not subject to Termination Charges. Wi-Fi Services will terminate simultaneously with Customer's Internet Services.

**11.3 Supplemental Terms.** Comcast agrees to provide Wi-Fi Services pursuant to the General Terms and Conditions and the supplemental Wi-Fi Terms and Conditions located at <http://business.comcast.com/wifi/hotspot-terms> ("Wi-Fi Terms and Conditions"). Comcast may at its sole option change or modify the Wi-Fi Terms and Conditions, and any related policies from time to time ("Revisions") by posting such Revisions to the Comcast website at the above URL. The Revisions are effective upon posting.

**[END OF BUSINESS INTERNET PSA. ETHERNET INTRASTATE PSA BEGINS ON NEXT  
PAGE]**

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
ETHERNET INTRASTATE TRANSPORT SERVICES**

**ATTACHMENT IDENTIFIER: Ethernet Transport, Version 1.9**

The following additional terms and conditions are applicable to Sales Orders for Comcast's Ethernet Transport Services:

**DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

**"Estimated Availability Date"** means the target date for delivery of Service.

**"HFC Network"** means a hybrid fiber coax network.

**"Interconnection Facilities"** means transmission capacity provided by Comcast, Customer or a third-party supplier to extend the Comcast Equipment from a Comcast terminal to any other location (e.g., a local loop provided by a local exchange company or other communications company).

**"Off-Net"** means geographical locations that are outside of Comcast's service area and/or geographical locations that are within Comcast's service area generally but are not readily accessible by Comcast Network facilities. All Off-Net Services are provided by third-party service providers. Off-Net Services provisioned over a fiber optic network are referred to as **"Off-Net Fiber."**

**"On-Net"** means geographical locations where Comcast currently provides Services through its Comcast Network. On-Net Services may be provisioned over a fiber optic network (**"On-Net Fiber"**), or via an HFC Network (**"On-Net HFC"**), as available through Comcast.

**"Service(s)"** means Ethernet Transport Services.

**ARTICLE 1. SERVICES**

This attachment shall apply to Ethernet Transport Services. A further description of these Services is set forth in **Schedule A-1** hereto which is incorporated herein by reference.

**ARTICLE 2. PROVIDER**

On-Net Service provided over Fiber shall be provided by Comcast Business Communications, LLC.

On-Net Service provided over the HFC Network and Off-Net Services are available in a number of Comcast markets. For information on service availability, call 866-429-0152.

**ARTICLE 3. REGULATORY APPROVAL; TRAFFIC MIX**

Customer represents that its use of Service hereunder will be jurisdictionally intrastate. If Customer's use of the Service now or at any time in the future is jurisdictionally interstate, Customer shall immediately notify Comcast of the same in writing. Further, Comcast reserves the right, in its reasonable sole discretion, to reclassify Customer's use of Service as jurisdictionally interstate or intrastate, as appropriate Customer agrees to indemnify and hold Comcast harmless from any claims by third parties resulting from or arising out of Customer's failure to properly represent or certify the jurisdictional nature of its use of the Service(s).

**ARTICLE 4. CUSTOM INSTALLATION FEE**

Once Comcast accepts a Sales Order for Service, Comcast will invoice Customer for all Custom Installation Fee(s). Customer will pay the Custom Installation Fee(s) within thirty (30) days of the invoice date unless a payment schedule is specified in the applicable Sales Order.

**ARTICLE 5. PROVISIONING INTERVAL**

Following its acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Service on or before the Estimated Availability Date; provided, however, that Comcast's failure to provision by said date shall not constitute a breach of the Agreement.

**ARTICLE 6. SERVICE COMMENCEMENT DATE**

Comcast shall inform Customer when Service is available and performing in accordance with the "Technical Specifications" set forth in Schedule A-1 hereto (**"Availability Notification"**). Charges for Service shall begin to accrue as of the Service Commencement Date. The Service Commencement Date shall be earliest of: (A) the date on which Customer confirms receipt of and concurrence with the Availability Notification; (B) five (5) business days following the date of the Availability Notification, if Customer fails to notify Comcast that the Service does not comply materially with the Technical Specifications (defined in Article 9) or (C) the date on which Customer first uses the Service. In the event that a Service Term has not been expressly set forth in a Sales Order, the

Service Term for such Sales Order shall be twelve (12) months.

#### **ARTICLE 7. PORTABILITY; UPGRADES**

**7.1 Portability.** Customer may terminate an existing On-Net Service (an “Existing Service”) and turn up a replacement On-Net Service (i.e., activate Service with termination points on Comcast’s network that are different than those of the Existing Service) (a “Replacement Service”) without incurring Termination Charges with respect to the Existing Service, provided that (a) the Replacement Service must have a Service Term equal to or greater than the remaining Service Term of the Existing Service but in no event less than twelve (12) months; (b) the Replacement Service must have monthly recurring charges equal to or greater than the monthly recurring charges for the Existing Service; (c) Customer submits a Sales Order to Comcast for the Replacement Service within ninety (90) days after termination of the Existing Service and that Sales Order is accepted by Comcast; (d) Customer reimburses Comcast for any and all installation charges that were waived with respect to the Existing Service; and (e) Customer pays the actual costs incurred by Comcast in installing and provisioning the Replacement Service.

**7.2 Upgrades.** Customer may upgrade the speed or capacity of an Existing Service without incurring Termination Charges, provided that (a) the upgraded Service (the “Upgraded Service”) must assume the remaining Service Term of the Existing Service, but in no event less than twelve (12) months; (b) the Upgraded Service must have the same points of termination on Comcast’s network as the Existing Service; (c) Customer submits a Sales Order to Comcast for the Upgraded

Service and that Sales Order is accepted by Comcast; (d) Customer pays Comcast’s applicable nonrecurring charges for the upgrade; and (e) Customer agrees to pay the applicable monthly recurring charges for the Upgraded Service commencing with the upgrade. Upgrades to Off-Net Services are subject to the applicable third party service provider rules and availability. Comcast has no obligation to upgrade Customer’s Off-Net Service.

#### **ARTICLE 8. ADDITIONAL INFORMATION**

As necessary for the interconnection of the Service with services provided by third parties, Comcast may request (as applicable), and Customer will provide to Comcast, circuit facility assignment information, firm order commitment information, and design layout records necessary to enable Comcast to make the necessary cross-connection between the Service and Customer’s other service provider(s). Comcast may charge Customer nonrecurring and monthly recurring cross-connect charges to make such connections.

#### **ARTICLE 9. TECHNICAL SPECIFICATIONS AND PERFORMANCE STANDARDS; SERVICE LEVEL AGREEMENT**

The technical specifications applicable to the Service are set forth in Schedule A-1 hereto (“**Technical Specifications**”). The service level agreement applicable to the Service is set forth in a **Schedule A-2** hereto and incorporated herein by reference.

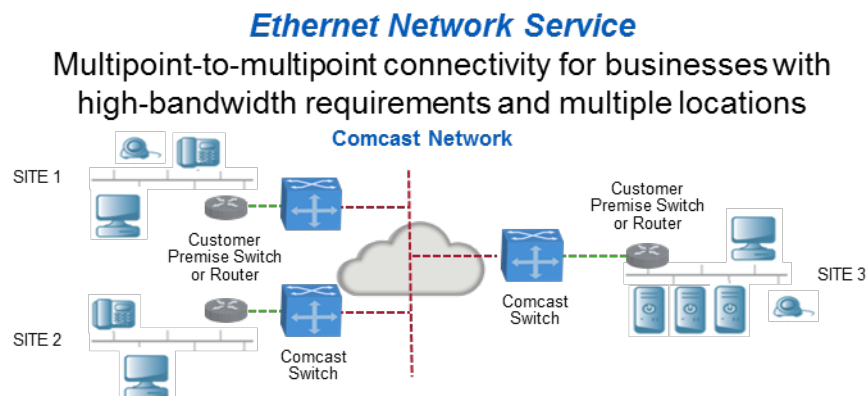
**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
ETHERNET INTRASTATE TRANSPORT SERVICES**

**SCHEDULE A-1  
SERVICE DESCRIPTIONS, TECHNICAL SPECIFICATIONS AND PERFORMANCE STANDARDS  
COMCAST ETHERNET TRANSPORT SERVICES**

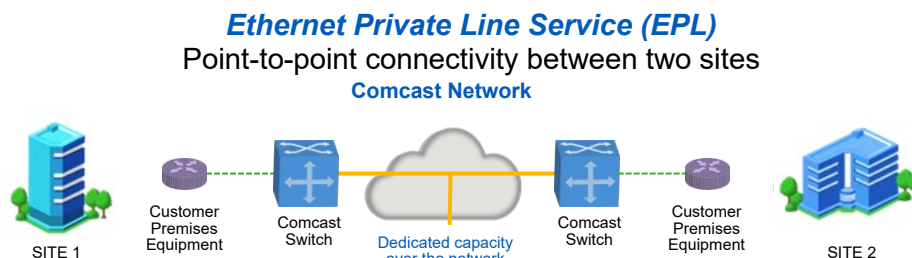
Comcast's Ethernet Transport Services will be provided in accordance with the service descriptions, technical specifications and performance standards set forth below:

**Service Descriptions**

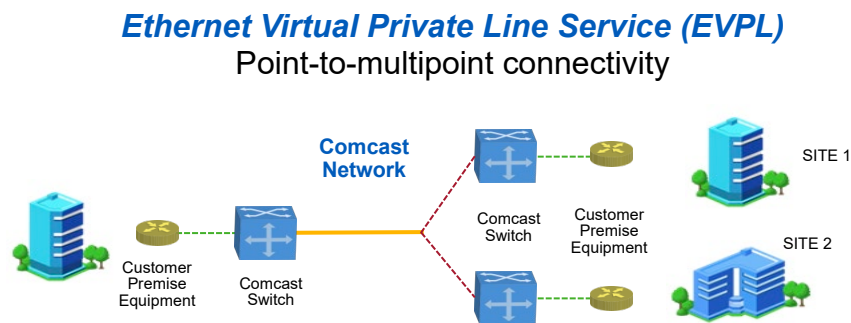
**Ethernet Network Service (ENS)** enables Customer to connect physically distributed locations across a Metropolitan Area Network (MAN) or Wide Area Network (WAN) as if they are on the same Local Area Network (LAN). The Service provides VLAN transparency enabling Customer to implement their own VLANs without any coordination with Comcast. ENS is a highly scalable service that enables customers to connect Customer Premises Equipment (CPE) using industry standard 100 Mbps, 1 Gbps or 10 Gbps Ethernet User-to-Network Interfaces (UNI) and is available with flexible bandwidth options from at 1 Mbps to 10 Gbps. Comcast ENS provides an Ethernet Virtual Connection (EVC) between Customer Service Locations that enables Customer to use any VLANs without coordination with Comcast. Comcast ENS offers three Classes of Service (CoS), as described below.



**Ethernet Private Line (EPL)** is a point-to-point transport service that provides secure, high-performance network connectivity between two Customer Service Locations. EPL is a highly scalable service that enables the Customer to connect their Customer Premises Equipment (CPE) using industry standard 100 Mbps, 1 Gbps or 10 Gbps Ethernet User-to-Network Interfaces (UNI) and is available with flexible bandwidth options from 1 Mbps to 10 Gbps. Comcast EPL provides an Ethernet Virtual Connection (EVC) between Customer Service Locations that enables the Customer to use any VLANs without coordination with Comcast. Comcast EPL offers three Classes of Service (CoS), as described below.



**Ethernet Virtual Private Line (EVPL)** service provides an Ethernet Virtual Connection (EVC) between two or more Customer Service Locations and supports the added flexibility to multiplex multiple services (EVCs) on a single UNI at the Customer's hub or aggregation site. The Service multiplexing capability is not available at sites served by the Comcast On-Net HFC. It is a highly scalable service that enables the Customer to connect their Customer Premises Equipment (CPE) using industry standard 100 Mbps, 1 Gbps or 10 Gbps Ethernet User-to-Network Interfaces (UNI) and is available with flexible bandwidth options from 1 Mbps to 10 Gbps. Comcast EVPL offers three Classes of Service (CoS), as described below.



## Multiple Access Options

Comcast Ethernet Transport Services are available with the following access options:

- On-Net Fiber Access – Connectivity to Customer Service Locations is enabled via Comcast On-Net fiber Infrastructure.
- On-Net Hybrid Fiber Coax (HFC) Access – Connectivity to Customer Service Locations is enabled via Comcast On-Net Hybrid Fiber Coax (HFC) infrastructure.
- Off-Net Access (both Fiber and Non-Fiber) – Connectivity to Customer Service Locations is enabled through a network-to-network interface (NNI) via third-party network provider.

## Ethernet Virtual Circuit (EVC) Area Types

Comcast Ethernet Transport Services are available both within and between certain major metropolitan areas throughout the United States. Each EVC is assigned an EVC Area Type based upon the proximity of respective A and Z locations.

- **Metro** – EVC enables connectivity between customer locations within a Comcast defined Metro.
- **Regional** – EVC enables connectivity between customer locations that are in different Comcast defined Metros, but within Comcast defined geographic Regions.
- **Continental** – EVC enables connectivity between customer locations that are in different Comcast defined geographic Regions.

## Ethernet Transport Technical Specifications

### 1. Ethernet User-to-Network Interface

Comcast Ethernet Transport Services provide bidirectional, full duplex transmission of Ethernet frames using a standard IEEE 802.3 Ethernet interface. Comcast implements ingress policies at CPE UNI interfaces to enforce subscribed bandwidth levels. Each ingress policing policy is created utilizing Committed Information Rate (CIR) and Committed Burst Size (CBS) components. The following table provides a list of available UNI physical interfaces and their available Committed Information Rate (CIR) bandwidth increments and Committed Burst Sizes (CBS).

UNI Speed	UNI Physical Interface	CIR Increments	CBS (bytes)
100 Mbps	100BaseT	10 Mbps	25,000
1 Gbps	1000Base T or 1000BaseSX	100 Mbps	250,000
10 Gbps	10GBase-SR or 10GBase-LR	1 Gbps	2,500,000
		10 Gbps	25,000,000

## 2. Class of Service (CoS) Options

Comcast Ethernet Transport Services are available with three different class of service (CoS) options that allow for differentiated service performance levels for different types of network traffic. This includes Basic (Low), Priority (Medium) and Premium (High). CoS is used to prioritize customer mission-critical traffic from lesser priority traffic in the network. The Customer must specify a CIR for each CoS to indicate how much bandwidth should be assigned to that CoS. The performance metrics associated with each CoS are described in the Ethernet Transport Service Level Agreement on Schedule A-2 of this PSA. As described in the following table, permissible CoS options vary by access type.

Access Type	CoS Options
On-Net Fiber	Basic, Priority & Premium
On-Net HFC	Basic & Priority
Off-Net Fiber	Basic, Priority & Premium
Off-Net Non-Fiber	Basic & Priority

## 3. CoS Identification and Marking

Customer traffic classification and forwarding is based upon Comcast CoS prioritization that must be specified in the Customer's Sales Order. It is the Customer's responsibility to shape traffic to ordered bandwidth. If the Customer only orders a single CoS solution, they are not required to mark their packets and all Customer packets will be forwarded based upon 802.1p value associated with the CoS level specified in the Sales order. All packets, tagged or untagged, will be mapped into the subscribed CoS. If Customer implements a multi-CoS solution or for EVPL ports with service multiplexing, the Customer must mark all packets using C-tag 802.1p CoS values as specified in the table below to ensure the Service will provide the intended CoS performance objectives. For multi-CoS solutions, untagged packets will be treated as if they are marked with a 0. Packets with other 802.1p values are mapped to the lowest subscribed CoS. For EVPL ports with service multiplexing, untagged packets will be discarded and C-tag VLAN ID values are used to map traffic to applicable EVC's. Based on Ethernet Frame 802.1p values, Customer's traffic is mapped to the Comcast forwarding classes traffic accordingly to the table below:

CoS Type	802.1p Marking
Basic (Low)	0-1

Priority (Medium)	2-3
Premium (High)	5

#### 4. Mac Learning and Forwarding (*ENS Service*)

The ENS Service is capable of learning up to 2500 MAC addresses from all interfaces connecting to the Service. It is highly recommended that routing equipment be utilized to minimize the number of MAC addresses exposed directly to the Service in larger networks. Any addresses in excess of 2500 will not be learned and traffic directed to these addresses will be treated as “unknown unicast”.

#### 5. Traffic Management

Comcast’s Network traffic-policing policies restrict traffic flows to the subscribed CIR for each service class. If the Customer-transmitted bandwidth rate for any CoS exceeds the subscribed committed information rate (CIR) and committed burst size (CBS), Comcast will discard the non-conformant packets. For packets marked with a non-conformant CoS marking, the Service will transmit them using the Basic CoS without altering the Customer’s CoS markings. Traffic management policies associated with Off-Net Services will conform to the policies enforced by the third-party service provider.

#### 6. Maximum Frame Size

Services delivered via Fiber support a Maximum Transmission Unit (MTU) frame size of 1600 bytes to support untagged, tagged and Q-in-Q traffic with 802.1q or 802.1ad encapsulation types. Services delivered via On-Net Fiber can, upon request, support a MTU up to 9100 bytes to support untagged, tagged and Q-in-Q frame sizes. Services delivered via Off-Net Fiber may, upon request, support a MTU up to 9100 bytes to support untagged, tagged and Q-in-Q frame sizes, but only, and solely, to the extent the applicable Off-Net provider can support such MTU frame size. Services delivered via HFC support a Maximum Transmission Unit (MTU) frame size of 1522 bytes. All frames that exceed specifications shall be dropped.

Transport Type	MTU Size
Fiber	1600-9100 bytes
HFC	1522 bytes

#### 7. Customer Traffic Transparency

All fields within customers Ethernet frames (unicast, multicast and broadcast, except L2CP) from the first bit of payload are preserved and transparently transported over UNI to UNI connections, as long as they are mapped into the EVC.

#### 8. Ethernet Service Frame Disposition

The Comcast Transport Services process different types of Ethernet frames differently. Frames may pass unconditionally through the Network or may be limited, as indicated in the table below, to ensure acceptable service performance. The following table illustrates Comcast’s service frame disposition for each service frame type.

Service Frame Type	ENS Frame Delivery	EPL & EVPL Frame Delivery
Unicast	All frames delivered unconditionally	All frames delivered unconditionally

Multicast	All frames delivered conditionally	All frames delivered unconditionally
Broadcast	All frames delivered conditionally	All frames delivered unconditionally

***ENS Services only:***

- **Unicast Traffic.** Unicast traffic must be bi-directional in order to facilitate mac-learning and avoid restriction.
- **Multicast Traffic.** By default, every ENS port is able to support up to 2 Mbps of multicast traffic. ENS customer who requires greater than 2 Mbps of multicast bandwidth must uniquely specify the bandwidth they require for each root site and associated Class of Service.
- **Broadcast Traffic.** Broadcast and unknown unicast traffic are restricted to 1.2mb or 300pps on ingress to the network.

***EVPL Services only:***

- Customer is responsible for mapping multicast, broadcast and unknown unicast traffic to specific C-VLAN.

**Monitoring, Technical Support and Maintenance**

1. **Network Monitoring.** Comcast monitors On-Net Services on a 24x7x365 basis.
2. **Technical Support.** Comcast provides a toll-free trouble reporting telephone number to the Comcast Enterprise Technical Support (ETS) center that operates on a 24x7x365 basis. Comcast provides technical support for service related inquiries. Technical support will not offer consulting or advice on issues relating to CPE or other equipment not provided by Comcast.
  - (d) **Escalation.** Reported troubles are escalated within the Comcast Business Services Network Operations Center (BNOC) to meet the response/restoration interval described below (Response and Restoration Standards). Service issues are escalated within the Comcast BNOC as follows: to a Supervisor at the end of the applicable time interval plus one (1) hour; to a Manager at the end of the applicable time interval plus two (2) hours, and to a Director at the end of the applicable time interval plus four (4) hours.
  - (e) **Maintenance.** Comcast's standard maintenance window for On-Net Services is Sunday to Saturday from 12:00am to 6:00am local time. Scheduled maintenance for On-Net Services is performed during the maintenance window and will be coordinated between Comcast and the Customer. Comcast provides a minimum forty-eight (48) hour notice for non-service impacting maintenance. Comcast provides a minimum of seven (7) days' notice for On-Net Service impacting planned maintenance. Emergency maintenance is performed as needed without advance notice to Customer. Maintenance for Off-Net Services shall be performed in accordance with the applicable third party service provider rules. Therefore, maintenance for Off-Net Service may be performed without advance notice to Customer.
  - (f) Comcast provides certain Comcast Equipment for provisioning its Services and the delivery of the UNI, which will reside on the Customer-side of the Demarcation Point. Comcast will retain ownership and management responsibility for this Comcast Equipment. This Comcast Equipment must only be used for delivering Services. Customers are required to shape their egress traffic to the Committed Information Rate identified in the Sales Order. Comcast will be excused from paying SLA credits, as set forth in Schedule A-2, if the Service Interruption is the result of Customer's failure to shape their traffic to the contracted CIR or utilizing Comcast Equipment for non-Comcast provided services.
3. **Response and Restoration Standards.** Comcast has the following response and restoration objectives:

CATEGORY	OBJECTIVE	MEASUREMENT	REMEDIES
<i>Mean Time to Respond Telephonically to Call</i>	15 minutes	Averaged Over A Month	Escalation (see above)

<i>Mean Time to Restore On-Net Comcast Equipment</i>	4 hours	Averaged Over A Month	Escalation (see above)
<i>Mean Time to Restore Off-Net Equipment</i>	4 hours	Averaged Over A Month	Escalation (see above)
<i>Mean Time to Restore On-Net Services</i>	6 hours	Averaged Over A Month	Escalation (see above)
<i>Mean Time to Restore Off-Net Services</i>	6 hours	Averaged Over A Month	Escalation (see above)

Customer shall bear any expense incurred, e.g., dispatch/labor costs, where a Service Interruption is found to be the fault of Customer, its end users, agents, representatives or third-party suppliers.

### **Customer Responsibilities**

Comcast provides an Ethernet terminating device for provisioning its services and the delivery of the UNI. Comcast will retain ownership and management responsibility for this equipment. As a result, it must only be used for delivering Comcast Services. Customer is responsible for providing customer premises equipment (CPE) to connect to this device. To ensure proper performance, Customer is required to shape its egress traffic to the contracted CIR.

Customers have the following responsibilities related to the installation, support, and maintenance of the Service:

- Provide an operating environment with temperatures not below fifty-five (55) or above eighty-five (85) degrees Fahrenheit. Humidity shall not exceed ninety (90) percent at eighty-five (85) degrees Fahrenheit.
- Provide secure space sufficient for access to one (1) standard, freestanding, equipment cabinet at each of the Customer facilities, no further than fifty feet from the Customer router or switch interface.
- Provide outside cable entry conduit(s), entry cable ground point, and internal building conduit to allow Comcast the ability to rod/rope a fiber optic cable to the Demarcation Point.
- Locate and mark all private underground utilities (water, electric, etc.) along path of new underground placement not covered by utility companies.
- Provide a pull rope in any existing duct that Comcast is to use and ensure existing duct is serviceable for Comcast use.
- Obtain 'right-of-way' entry easement for Comcast facilities and equipment from property owners at each Customer location.
- The Customer is responsible for coring of the building's outside wall and internal walls. Upon request, Comcast can perform this activity on an 'as needed' basis for an additional one-time fee.
- Provide UPS AC power equipment, circuit sizing to be determined, if applicable.
- Emergency local generator backup service, if applicable.
- Provide access to the buildings and Demarcation Point at each Customer location to allow Comcast and its approved Contractors to install fiber for service installation. Provide access to each location for regular (8am - 5pm) and emergency (24 hour) service and maintenance of Comcast's equipment and facilities.
- Provide, install and maintain a device that is capable of interconnecting network traffic between the Service and the Customer's Local Area Network (LAN).
- Customer must provide a point of contact (POC) for installation, service activation and any maintenance activities.

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
ETHERNET INTRASTATE TRANSPORT SERVICES**

**SCHEDULE A-2  
SERVICE LEVEL AGREEMENT**

Comcast's Ethernet Transport Services are backed by the following Service Level Agreement ("SLA"):

**A. Definitions:**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Ethernet Transport Services PSA or the General Terms and Conditions.

**Definitions**

**"Jitter"** means the short-term variations for a portion of successfully delivered service frames. Jitter may also be referred to as Frame Delay Variation.

**"Latency"** means the maximum delay for a portion of successfully delivered service frames. Latency may also be referred to as Frame Delay.

**"Market"** means the Comcast geographic region where the applicable Service Location is located, as identified on the Sales Order.

**"Packet Loss"** means the difference between the number of service frames transmitted at the ingress UNI and the total number of service frames received at the egress UNI. Packet Loss may also be referred to as Frame Loss.

**"Planned Service Interruption"** means any Service Interruption caused by planned work such as scheduled maintenance or planned enhancements or upgrades to the network.

**"Service Interruption"** means an interruption in transmission that renders the Service unusable due to a total loss of signal for the Service. The Service shall be "Available" in the absence of a Service Interruption.

**B. Ethernet Transport Service Level Agreements**

**1. Availability SLA**

Comcast's liability and Customer's sole remedy for Service Interruptions, and errors, omissions, interruptions, delays, outages, or defects in transmission or switching of any Services (individually or collectively, "**Liability**"), shall be limited to the amounts set forth in the Tables below with the stated percentages to be applied against the MRC associated with the impacted portion of the Service set forth in the Sales Order ("**Availability Credit**"). For the purposes of calculating credit for a Service Interruption, the "Length of Service Interruption" begins when the Customer reports such Service Interruption and a trouble ticket is opened, and concludes upon the closing of the same trouble ticket or, if sooner, the termination of the Service Interruption, less any time Comcast is awaiting additional information or premises testing from the Customer. The Length of Service Interruptions for separately occurring Service Interruptions will not be aggregated for purposes of determining Availability Credit allowances. To qualify, Customer must request the Availability Credit from Comcast within thirty (30) days of the beginning of the Service Interruption. Comcast shall not incur any Liability, including Availability Credit, for any failure of the Services caused by force majeure events, Planned Service Interruptions, Customer actions, omission or equipment, CPE, or any other items set forth in the "Exceptions to Credit Allowances" section below.

**TABLE 1: Availability SLA for Services provided over On-Net or Off-Net Fiber (99.99% Availability)**

<b>Length of Service Interruption:</b>	<b>Amount of Credit:</b>
Less than 4 minutes	None
At least 4 minutes but less than 4 hours	5% of Total MRC
At least 4 hours but less than 8 hours	10% of Total MRC
At least 8 hours but less than 12 hours	20% of Total MRC
At least 12 hours but less than 16 hours	30% of Total MRC
At least 16 hours but less than 24 hours	40% of Total MRC
At least 24 hours or greater	50% of Total MRC

**TABLE 2: Availability SLA for Services provided over On-Net HFC or Off-Net Non-Fiber Transport (99.9% Availability)**

<b>Length of Service Interruption:</b>	<b>Amount of Credit:</b>
Less than 40 minutes	None
At least 40 minutes but less than 4 hours	5% of Total MRC
At least 4 hours but less than 8 hours	10% of Total MRC
At least 8 hours but less than 12 hours	20% of Total MRC
At least 12 hours but less than 16 hours	30% of Total MRC
At least 16 hours but less than 24 hours	40% of Total MRC
At least 24 hours or greater	50% of Total MRC

SEPARATELY OCCURRING SERVICE INTERRUPTIONS ARE NOT AGGREGATED FOR THE PURPOSES OF DETERMINING CREDIT ALLOWANCES.

## **2. Performance Objectives SLA**

Comcast Ethernet Transport Services are available both within and between major metropolitan areas throughout the United States. The performance objectives associated with traffic flows between any two Customer Service Locations are dependent upon the locations of the respective sites, designated as Service Location A and Service Location Z on the applicable Sales Order.

### ***Access Types***

1. **On-Net Access.** If On-Net Service Location A and On-Net Service Location Z reside within the same Market, Performance Tier 1 objectives will apply. If the On-Net Service Locations are in different Markets, a different Performance Tier will apply. The applicable Performance Tier will appear on/with the respective Sales Order.
2. **Off-Net Access.** In addition to On-Net Access, Comcast enables Off-Net Access to Ethernet Transport Services via multiple third party providers. The Performance Tier for Off-Net Service is based upon the location of the Off-Net Service Location, the location of the Network to Network Interface (NNI) between Comcast and the third party provider and the performance commitment from the third party provider. The applicable Performance Tier will appear on the respective Sales Order.

### ***Performance Tiers and Performance Objectives***

Comcast collects continuous in-band performance measurements for its Ethernet Transport Services. The calculation of all Latency, Jitter and Packet Loss Performance Metrics for each calendar month for purposes of this Performance Objectives SLA are based upon the average of sample one-way measurements taken by Comcast during the applicable calendar month, excluding any period during which there is a Service Interruption. The below charts indicate the Performance Standard that should be achieved for each of the Performance Metrics over each calendar month based on the applicable Performance Tier and Class of Service.

## 1. Performance Tier 1 (PT1) Agreements – Within Market

Performance Metric	Class of Service (CoS)		
	Basic	Priority	Premium
Latency (One-Way Network Delay)	45ms	23ms	12ms
Jitter (Network Delay Variation)	20ms	10ms	2ms
Packet Loss	<1%	<0.01%	<0.001%

## 2. Performance Tier 2 (PT2) Agreements

Performance Metric	Class of Service (CoS)		
	Basic	Priority	Premium
Latency (One-Way Network Delay)	80ms	45ms	23ms
Jitter (Network Delay Variation)	25ms	15ms	5ms
Packet Loss	<1%	<.02%	<.01%

## 3. Performance Tier 3 (PT3) Agreements

Performance Metric	Class of Service (CoS)		
	Basic	Priority	Premium
Latency (One-Way Network Delay)	100ms	80ms	45ms
Jitter (Network Delay Variation)	30ms	20ms	10ms
Packet Loss	<1%	<.04%	<.02%

## 4. Performance Tier 4 (PT4) Agreements

Performance Metric	Class of Service (CoS)		
	Basic	Priority	Premium
Latency (One-Way Network Delay)	120ms	100ms	80ms
Jitter (Network Delay Variation)	35ms	25ms	15ms
Packet Loss	<1%	<.05%	<.04%

## 5. Best Effort Performance Tier (BE)

No performance commitments will apply. Best Effort Performance Tier will appear on the associated Comcast Sales Order.

### *Credit Allowance*

Customer's sole remedy for Comcast's failure to achieve the applicable Performance Metric standards above over a given calendar month for the Service are the receipt of the following credit amounts with the stated percentages to be applied against the MRC associated with the impacted portion of the Service set forth in the Sales Order ("Performance Objective Credits").

**TABLE 1: Credit Allowance for Latency Performance Metric**

Performance Tier			
PT1	PT2	PT3	PT4

		Measurement (ms)	Credit	Measurement (ms)	Credit	Measurement (ms)	Credit	Measurement (ms)	Credit
Class of Service	Premium	0 - 12	No Credit	0 - 23	No Credit	0 - 45	No Credit	0 to 80	No Credit
		12.01 - 23	10%	23.01 - 45	10%	45.01 - 80	10%	80.01 - 100	10%
		23.01 - 45	25%	45.01 - 80	25%	80.01 - 100	25%	100.01 - 120	25%
		>45	50%	>80.01	50%	>100	50%	>120	50%
	Priority	0 - 23	No Credit	0 - 45	No Credit	0 to 80	No Credit	0 to 100	No Credit
		23.01 - 45	10%	45.01 - 80	10%	80.01 - 100	10%	100.01 - 120	10%
		45.01 - 80	25%	80.01 - 100	25%	100.01 - 120	25%	120.01 - 150	25%
		>80.01	50%	>100	50%	>120	50%	>150	50%
	Basic	0 - 45	No Credit	0 to 80	No Credit	0 to 100	No Credit	0 to 120	No Credit
		45.01 - 80	10%	80.01 - 100	10%	100.01 - 120	10%	120.01 - 150	10%
		80.01 - 100	25%	100.01 - 120	25%	120.01 - 150	25%	150.01 - 180	25%
		>100	50%	>120	50%	>150	50%	>180	50%

**TABLE 2: Credit Allowance for Jitter Performance Metric**

		Performance Tier							
		PT1		PT2		PT3		PT4	
		Measurement (ms)	Credit	Measurement (ms)	Credit	Measurement (ms)	Credit	Measurement (ms)	Credit
Class of Service	Premium	0 - 2	No Credit	0 - 5	No Credit	0 - 10	No Credit	0 - 15	No Credit
		2.01 - 3	10%	5.01 - 10	10%	10.01 - 15	10%	15.01 - 20	10%
		3.01 - 5	25%	10.01 - 15	25%	15.01 - 20	25%	20.01 - 30	25%
		>5	50%	>15	50%	>20	50%	>30	50%
	Priority	0 - 10	No Credit	0 - 15	No Credit	0 - 20	No Credit	0 - 25	No Credit
		10.01 - 15	10%	15.01 - 20	10%	20.01 - 30	10%	25.01 - 40	10%
		15.01 - 20	25%	20.01 - 30	25%	30.01 - 50	25%	40.01 - 60	25%
		>20	50%	>30	50%	>50	50%	>60	50%
	Basic	0 - 20	No Credit	0 - 25	No Credit	0 - 30	No Credit	0 - 35	No Credit
		20.01 - 30	10%	25.01 - 40	10%	30.01 - 50	10%	35.01 - 60	10%
		30.01 - 50	25%	40.01 - 60	25%	50.01 - 80	25%	60.01 - 90.01	25%
		>50	50%	>60	50%	>80	50%	>90	50%

**TABLE 3: Credit Allowance for Packet Loss Performance Metric**

		Performance Tier							
		PT1		PT2		PT3		PT4	
		Measurement	Credit	Measurement	Credit	Measurement	Credit	Measurement	Credit
Class of Service	Premium	0% - 0.001%	No Credit	0% - 0.01%	No Credit	0% - 0.02%	No Credit	0% - 0.04%	No Credit
		0.001% - 2.00%	10%	0.01% - 2.00%	10%	0.02% - 2.00%	10%	0.04% - 2.00%	10%
		2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%
		>4.00%	50%	>4.00%	50%	>4.00%	50%	>4.00%	50%
	Priority	0% - 0.01%	No Credit	0% - 0.02%	No Credit	0% - 0.04%	No Credit	0% - 0.05%	No Credit
		0.01% - 2.00%	10%	0.02% - 2.00%	10%	0.04% - 2.00%	10%	0.05% - 2.00%	10%
		2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%
		>4.00%	50%	>4.00%	50%	>4.00%	50%	>4.00%	50%
	Basic	0% - 1.00%	No Credit	0% - 1.00%	No Credit	0% - 1%	No Credit	0% - 1%	No Credit
		1.01% - 2.00%	10%	1.01% - 2.00%	10%	1.01% - 2.00%	10%	1.01% - 2.00%	10%
		2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%	2.01% - 4.00%	25%
		>4.00%	50%	>4.00%	50%	>4.00%	50%	>4.00%	50%

Customer shall only be entitled to receive a Performance Objective Credit for one Performance Metric failure per affected portion of the Service per calendar month. For example, if the applicable metric for Jitter and Latency were missed for the same transport connection (Service Location A to Service Location Z) in a given calendar month, Customer will only be entitled to the Performance Objective Credit associated with either the Jitter or Latency failure for such portion of the Service. To qualify for a Performance Objective Credit, Customer must request the applicable Performance Objective

Credit from Comcast within thirty (30) days of the end of the applicable calendar month in which the applicable Performance Metric standard was not achieved. Comcast shall not incur any liability, including Performance Objective Credit, for any failure of the Services caused by force majeure events, Planned Service Interruptions, Customer actions, omissions or equipment, CPE or any other items set forth in the "Exceptions to Credit Allowances" section below.

### **C. Exceptions and Terms applicable to all SLAs**

#### **1. Emergency Blocking**

The Parties agree that if either Party hereto, in its reasonable sole discretion, determines that an emergency action is necessary to protect its own network, the Party may, after engaging in reasonable and good faith efforts to notify the other Party of the need to block, block any transmission path over its network by the other Party where transmissions do not meet material standard industry requirements. The Parties further agree that none of their respective obligations to one another under the Agreement will be affected by any such blockage except that the Party affected by such blockage will be relieved of all obligations to make payments for charges relating to the circuit(s) which is so blocked and that no Party will have any obligation to the other Party for any claim, judgment or liability resulting from such blockage.

#### **2. Remedy Processes**

All claims and rights arising under this Service Level Agreement must be exercised by Customer in writing within the time period set forth in Sections B.1 and B.2, as applicable. The Customer must submit the following information to the Customer's Comcast account representative with any and all claims for credit allowances: (a) Organization name; (b) Customer account number; and (c) basis of credit allowance claim (including date and time, if applicable). Comcast will acknowledge and review all claims promptly and will inform the Customer by electronic mail or other correspondence whether a credit allowance will be issued or the claim rejected, with the reasons specified for the rejection.

#### **3. Exceptions to Credit Allowances**

Comcast's failure to meet the either of the SLAs set forth on this Schedule A-2 shall not qualify for the remedies set forth herein if such failure is related to, associated with, or caused by: Planned Service Interruptions or other scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment; any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers, any power, equipment or services provided by third parties; or an event of force majeure as defined in the Agreement.

#### **4. Other Limitations**

THE TOTAL CREDIT ALLOWANCES PER CALENDAR MONTH UNDER THIS SCHEDULE A-2 IS CAPPED AT 50% OF THAT MONTH'S MRC FOR THE IMPACTED PORTIONS OF SERVICE. In addition, the remedies set forth in this Service Level Agreement shall be Customer's sole and exclusive remedies for any Service Interruption, outage, unavailability, delay, or other degradation, or any Comcast failure to meet the service objectives.

#### **5. Notice of Outage for On-Net Services**

If Comcast identifies an outage with respect to an On-Net Service, Comcast will notify Customer of such outage, either via email or phone, within thirty (30) minutes of becoming aware of the same.

**/END OF ETHERNET INTRASTATE PSA. SD WAN PSA BEGINS ON NEXT PAGE/**

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
STANDARD AND ADVANCED SOFTWARE-DEFINED WIDE AREA NETWORKING**

The following additional terms and conditions are applicable to Sales Orders for Comcast's Standard and Advanced SD-WAN Services:

**DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

**"Advanced SD-WAN Service"** includes the Standard SD-WAN Service plus the additional features described in Section 1.A. of Schedule A-1.

**"Architectural Confirmation Document"** or **"ACD"** means a document that contains the initial configuration for the SD-WAN Services, as agreed to by Customer and Comcast.

**"Comcast System"** means applications, websites, computing assets, systems, databases, devices, products, or services owned or operated by or for Comcast.

**"Customer Expectations Document"** means a document created by Comcast that identifies Comcast's and Customer's responsibilities and obligations with respect to the delivery and support of the Services.

**"Customer System"** means any of Customer's or Customer's subcontractor's(s') applications, websites, computing assets, systems, databases, devices, products, or services that process Comcast data.

**"Estimated Availability Date"** means the target Service Commencement Date for the Service.

**"Information Security Standards"** means the standards prescribed for use by the National Institute of Standards and Technology, aligned with the International Organization for Standardization/International Electrotechnical Commission 27000 series of standards.

**"SD-WAN"** means Software-defined Wide Area Network.

**"Service(s)"** for purposes of this PSA means the Standard and/or Advanced SD-WAN Services, as applicable.

**"Standalone"** means an optional configuration feature of the Advanced SD-WAN Service as described in Section 1.A. of Schedule A-1.

**"Standard SD-WAN Service"** means the Standard SD-WAN Service as described in Section 1.B. of Schedule A-1.

**"Underlay Service"** means the connectivity over which the Service operates.

**ARTICLE 1. SERVICES**

This attachment shall apply to Standard and Advanced SD-WAN Services. A further description of these Services is set forth in Schedule A-1 hereto, which is incorporated herein by reference.

**ARTICLE 2. PROVIDER**

The Services shall be provided by Comcast Business Communications, LLC or its applicable subsidiaries or Affiliates ("**Comcast**").

**ARTICLE 3. SERVICE PROVISIONING INTERVAL**

Following Customer's acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Service on or about the Estimated Availability Date; provided, however, that Comcast's failure to provision Service by said date shall not constitute a breach of the Agreement.

**ARTICLE 4. SERVICE COMMENCEMENT DATE**

The Service Commencement Date shall be the date Comcast informs Customer that the Service is available and performing at a minimum of two (2) Service Locations (or one (1) Service Location, in the case of Standalone). Charges for the Services shall begin to accrue on the Service Commencement Date.

**ARTICLE 5. PORTABILITY**

**5.1 Portability.** Customer may terminate an existing Service (an **"Existing Service"**) and turn up a replacement Service (*i.e.*, activate Service at a different Service Location) (a **"Replacement Service"**) without incurring Termination Charges with respect to the Existing Service, provided that: (a) the Replacement Service must have a Service Term equal to or greater than the remaining Service Term of the Existing Service, but in no event less than twelve (12) months; (b) the Replacement Service must have monthly recurring charges equal to or greater than the monthly recurring charges for the Existing Service; (c) Customer submits a Sales Order to

Comcast for the Replacement Service within ninety (90) days after termination of the Existing Service and that Sales Order is accepted by Comcast; (d) Customer reimburses Comcast for any and all installation charges that were waived with respect to the Existing Service; and (e) Customer pays the actual costs incurred by Comcast in installing and provisioning the Replacement Service.

#### **ARTICLE 6. SD-WAN CUSTOMER PORTAL**

Comcast provides Customer with access to a password-protected web portal for the purpose of accessing information regarding Customer's Service. The portal also provides a view of certain network-related data, subject to the availability of the Service.

#### **ARTICLE 7. TECHNICAL SPECIFICATIONS; SERVICE LEVEL AGREEMENT**

The technical specifications applicable to the Services are set forth in Schedule A-1 hereto. The service level agreement applicable to the Services is set forth in Schedule A-2 hereto. Comcast strives to achieve all service levels from the start of the SOW. However, Comcast is contractually relieved of the service level agreement set forth in Schedule A-2 and any service level requirements specified in SOWs for the first ninety (90) days immediately following the Service Commencement Date at any Service Location. Any remedies, including service level credits, set forth in Schedule A-2 and, where applicable, in any SOW shall be the Customer's sole and exclusive remedy for any failure to meet the specified service levels.

#### **ARTICLE 8. PAYMENT CARD INDUSTRY COMPLIANCE**

Subject to the terms outlined herein and below, the Services provided under this PSA are compliant with the current Payment Card Industry Data Security Standard ("PCI DSS") as set forth by the PCI Security Standards Council®. The Attestation of Compliance ("AOC") is limited to Comcast applications, software, infrastructure, network, and IT support of the SD-WAN with unified security (Versa Unified Threat Management) and Universal Customer Premises Equipment ("uCPE") provided by Comcast. All other Comcast Equipment and Customer-Provided Equipment are outside the scope of the AOC.

The obligations of each Party are outlined in the Responsibility Matrix set forth in Appendix A-3 to this PSA. Any variance to the Responsibility Matrix shall be identified in the ACD. Any Customer failure to meet an obligation set forth in the Responsibility Matrix, and/or any change to the Services may result in the Services no longer being deemed compliant with PCI DSS.

For clarity, PCI DSS compliance is ultimately the responsibility of the Customer. Comcast does not store, process, or transmit cardholder data on behalf of Customer or its end users in delivery of the Services, nor does Comcast have access to Customer's or its end users' cardholder data, the protection of which is the sole responsibility of Customer. Customer is responsible for security issues resulting from Customer change requests that deviate from Comcast's compliant configuration and all changes should be reviewed and documented through the Customer's internal change order process for PCI purposes and the configuration should be validated by the Customer's auditor for Customer to ensure PCI DSS compliance. Comcast cannot provide PCI DSS compliance-related guidance or advice on any Customer-requested changes to the Services as Customer is responsible for its own network operation and internal processes.

**COMCAST ENTERPRISE SERVICES**  
**PRODUCT-SPECIFIC ATTACHMENT SOFTWARE DEFINED WIDE AREA NETWORKING**

**SCHEDULE A-1**  
**SERVICE DESCRIPTIONS AND TECHNICAL SPECIFICATIONS**

The Services will be provided in accordance with the service descriptions and technical specifications set forth below:

**1. Service Descriptions**

- A. **Advanced SD-WAN Service.** Advanced SD-WAN Service includes the Standard SD-WAN Service features described in Section 1.B. as well as the following additional features:
- i. Comcast will create a custom configuration for Customer's Service based on the Customer-approved ACD.
  - ii. Following the Service Commencement Date, Comcast will provide Customer with a Service Location birth certificate which will include service details and test results; and during the first thirty (30) days after the Service Commencement Date, Comcast will provide Customer with a curation period during which Comcast will perform network tuning to Customer's SD-WAN Service.
  - iii. The Advanced SD-WAN Service configuration response objectives set forth in Section 5.E.i. below.
  - iv. The Advanced SD-WAN Service may be configured as Standalone. Standalone is an optional configuration feature that enables the Advanced SD-WAN Service to be provisioned, with or without the need for Service Location-to-Service Location or IPsec Tunnels to Third Party Peer topologies (as described in Section 4(C) below).
- B. **Standard SD-WAN Service.** Standard SD-WAN Service is available only to Customers that have an active subscription to the Standard SD-WAN Service under a Sales Order entered into prior to September 26, 2022, this Service provides a secure connection, both point-to-point and point-to-multi-point, creating an encrypted overlay network to Customer's Underlay Service, regardless of whether such Underlay Service is provided by Comcast or a third party. SD-WAN Service enables network abstraction and the separation of the control plane and data plane. The following features are also included with SD-WAN Service:
- i. SD-WAN Service is agnostic as to WAN transport technologies.
  - ii. Automatic and dynamic routing and load balancing of application traffic across multiple WAN connections based on business and application policies set by Customer.
  - iii. SD-WAN Service assists with the management, configuration, and orchestration of WANs.
  - iv. SD-WAN Service provides secure VPNs and has the ability to integrate additional network services and offload Internet-destined traffic closer to the edge of the network.
  - v. SD-WAN Service monitors the uCPE and circuits for "up/down" status, and alerts Customers based on configuration.
  - vi. 24x7 phone support.
  - vii. Access to the Portal (defined below), which provides analytics that show the performance and utilization of the Customer's network applications and elements.

**2. Service Requirements**

In order to provide the Services to a Customer Service Location, such Service Location must have Internet connectivity. The connectivity may be pre-existing or ordered in conjunction with the Services. Comcast supports the Services over Comcast EDI Service, Comcast Business Internet Service, or Internet connectivity services provided by a third-party service provider. If the underlying connectivity is terminated at a Service Location or unavailable for any reason at any time, the Services at said Service Location will be inoperable.

### 3. SD-WAN Services Technical Specifications

- A. **Underlay connectivity.** This Service leverages the public Internet (Comcast on-net Layer 3 internet access services over fiber and DOCSIS, Comcast provided off-net Layer 3 internet access, or third-party-provided internet access, or LTE provided by Comcast or a third party).
- B. **Hybrid WAN connectivity.** This Service will work over any industry standard third-party Layer 3 IP technology (e.g., IP VPN and MPLS) which can serve as additional underlay to the public Internet.
- C. **SD-WAN Overlay.** This Service uses Underlay Service access to establish IPSec VPN tunnels using AES-256 or AES-128 encryption between Comcast provided uCPEs as well as to provide control plane access from the uCPE to the SD-WAN controller. The SD-WAN software steers application traffic real time based on business policy rules provided by the Customer.
- D. **SD-WAN uCPE.** Comcast will provide robust and flexible uCPEs. Such uCPEs are “x86” hardware that are service-agnostic and can host Comcast-provided applications.
- E. **SD-WAN Firewall.** Comcast will provide a Layer 3/Layer 4 Stateful Firewall as part of this Service.
- F. **Dynamic WAN utilization; Traffic Steering.** For Service Location-to-Service Location traffic, the Service automatically selects the best available WAN connection based on a combination of traffic flows and application policies that have been defined by Comcast and the Customer in the ACD. For Standalone, the Customer may prioritize certain applications and/or application groups to be re-routed in the event the primary route is unavailable, and to opt-in to LTE back-up on a per-application or per-application group basis; however, certain features of Dynamic WAN utilization are not available for Standalone.
- G. **Service Orchestration.** Provisioning and configuration of connectivity, routing policies, security, and application aware traffic steering is provided through a centralized, geo-redundant orchestration plane that is logically segregated per Customer. Connectivity to the orchestration layer occurs through encrypted tunnels across the public Internet.
- H. **Digital Experience.** Service visibility, control, and reporting is provided via the Comcast Business Digital Experience web portal (“Portal”).

### 4. Optional SD-WAN Service Configurations

- A. **Local Internet Breakout.** Comcast can configure a local Internet breakout at each Customer Service Location with the purpose of routing traffic directly to the Internet as needed. Local Internet breakout is not a connectivity service and is solely a route configuration inside the uCPE to allow local hosts to bypass the VPN tunnel and access the internet using the local underlay directly.
- B. **High Availability.** High Availability is an optional price-impacting SD-WAN Service feature that enhances resiliency by eliminating the single point of failure at the hardware (uCPE) level. Two (2) uCPEs are placed at the Service Location, both connected to the network and functioning in Active/Active mode.
- C. **IPSec Tunnels to Third Party Peers.** An optional SD-WAN Service feature that allows Customer to establish IPSec tunnels between Customer Systems and up to three (3) third-party peers’ networks, applications, software-as-a-service solutions, or other business-to-business services not provided by Comcast (“**Third-Party System(s)**”), provided such Third-Party System supports policy-based VPN. Use of Third-Party Systems is subject to Customer’s agreement with the relevant provider and not the Agreement. Further to the limitations of liability set forth in Section 5.1(C) of the General Terms and Conditions, Comcast does not control, and has no liability for, how Third-Party Systems or their providers use Customer’s data or for any claim related to connecting Customer Systems to a Third-Party System via the Services, even where Comcast supports Customer in configuring IPSec tunnel(s). It is entirely within Comcast’s discretion as to whether Comcast will provide support for IPSec tunnel configuration.

### 5. Service Delivery and Service Management

- A. **Kick-off call:** Comcast will sponsor a kick-off call with the Customer to explain the Service delivery process and Comcast and Customer will review the Customer Expectations Document.
- B. **Technical interview:** Comcast will engage Customer in one or more interviews related to Customer's network design initiatives. Comcast will document the technical information discovered through the interview process in an Architectural Confirmation Document and the Customer will review and confirm that the ACD is correct.
- C. **Managed Install, Test, and Turn-up:** When Comcast installs the SD-WAN equipment, the configuration created for the Customer will be loaded onto the SD-WAN equipment and Comcast will test the Service.
- D. **Network Monitoring and Management:** On and after the Service Commencement Date, Comcast will monitor the SD-WAN Service 24/7/365 and pull alarms from the equipment related to the availability of the Services. Comcast will send an alert to the Customer for specific, Service-impacting alarms. After receiving such an alarm, Comcast will open an internal ticket and begin to troubleshoot the issue.
- E. **On-Going Solution Support:**
- i. **Configuration Changes.** Comcast will support Customer-requested configuration changes, in accordance with Comcast's then current configuration change policy (the "**Configuration Change Policy**"). Upon request, Comcast shall provide Customer with its then current Configuration Change Policy. Any moves, additions, changes, or deletions to the Services shall be requested over the phone. This includes any changes to the Service configuration as initially outlined in the ACD. Comcast endeavors to meet the following configuration change response objectives:

STANDARD SD-WAN SERVICE	
Category	Objective
Simple Configuration Change	4 hours
Complex Configuration Change	48 hours

ADVANCED SD-WAN SERVICE	
Category	Objective
Simple Configuration Change	30 minutes
Complex Configuration Change	12 hours

"**Simple Configuration Change**" means changes such as firewall updates, traffic steering policies, quality of service changes, adding and removing IP addresses, and NAT and PAT changes.

"**Complex Configuration Change**" means changes such as WAN/LAN reconfiguration, DHCP scope changes, DNS changes, and changes to routing policies.

- ii. **Software Updates and Security Patches.** If a Comcast vendor develops software updates and/or security patches for such vendor's equipment which Comcast uses to provide the Services, Comcast will upload such software updates and/or security patches to the applicable equipment to the extent Comcast determines, in its sole discretion, that such software updates and/or security patches are necessary. Updates or patches that are viewed as critical may require immediate action with a maintenance window. For the avoidance of doubt, Comcast shall have no obligation to develop software updates or security patches and its only obligation under this paragraph is to install updates and security patches developed by its applicable vendors to the extent Comcast determines, in its sole discretion, that such software updates and/or security patches are necessary.
- iii. **Technical Support.** Comcast provides Customers a toll-free trouble reporting telephone number to reach the Enterprise Customer Care (ECC) that operates on a 24x7x365 basis. Comcast provides technical support for Service-related inquiries. Technical support will not offer consulting or advice on issues relating to non-Comcast Equipment.

- iv. Escalation. Reported troubles are escalated within the Comcast Advanced Solutions Operations (AS Ops) to meet the standard restoration interval described in the Service Availability Objectives. For Service Interruptions (as defined in Schedule A-2), troubles are escalated within the Comcast AS Ops as follows: Supervisor at the end of the standard interval plus one (1) hour; to the Manager at the end of the standard interval plus two (2) hours, and to the Director at the end of the standard interval, plus four (4) hours.
- v. Maintenance. Comcast's standard maintenance window is Sunday to Saturday from 12:00 a.m. to 6:00 a.m. local time. Scheduled maintenance is performed during the maintenance window and will be coordinated between Comcast and the Customer. Comcast provides a minimum of forty-eight (48) hours' notice for non-service impacting scheduled maintenance. Comcast provides a minimum of seven (7) days' notice for service impacting planned maintenance. Emergency maintenance is performed as needed.

## **6. Security Monitoring and Mitigation.**

For the Services, Comcast monitors the equipment. **COMCAST DOES NOT PROVIDE MONITORING OF SECURITY EVENTS, ANY SECURITY EVENT MITIGATION, OR ADVICE REGARDING SECURITY ISSUES OR THREATS.** Upon request by Customer, Comcast will modify the configuration of the Services in accordance with specifications provided by Customer to attempt to mitigate security events and security threats identified by Customer. Comcast's sole obligation is to implement the configuration settings requested by Customer. This Service is provided on a commercially reasonable efforts basis only and Comcast makes no guarantees with respect to the detection or blocking of viruses/worm/malware or any other types of attacks and is not responsible for any such malicious data that may be transmitted over the provided network.

## **7. Customer Responsibilities**

**In addition to the responsibilities and obligations identified in the Customer Expectations Document, Customer shall have the following responsibilities related to the installation, support, and maintenance of the Service:**

- A. Provide an operating environment with temperatures not below fifty-five (55) or above eighty-five (85) degrees Fahrenheit. Humidity shall not exceed ninety (90) percent at eighty-five (85) degrees Fahrenheit.
- B. Provide secure space sufficient for access to one (1) standard, freestanding equipment cabinet at each of the Customer facilities, no farther than fifty feet from the Customer router or switch interface.
- C. Provide power including UPS AC power equipment, circuit sizing to be determined, if applicable.
- D. Provide emergency local generator backup service, if applicable.
- E. Provide access to the buildings and point of demarcation at each Customer Service Location to allow Comcast and its approved contractors to install uCPE. Provide access to each location for regular (8 a.m. - 5 p.m.) and emergency (24 hour) service and maintenance of Comcast's equipment and facilities.
- F. If interfacing with a third-party IP service: provide, install and maintain a device that is capable of routing network traffic between the Service and the Customer's Wide Area Network (WAN).
- G. Customer must provide a point of contact (POC) for installation, service activation, notices for Service Interruptions, and any maintenance activities.
- H. Customer must approve the final Architecture Configuration Document (ACD) prior to installation of the Services.
- I. Customer must ensure that any Customer-provided or existing Underlay Service is installed and operational prior to installation of the Services.
- J. The demarcation point of the SD-WAN Service is the ActiveCore uCPE. Customer shall have sole responsibility for installing, configuring, providing and maintaining all customer LAN equipment.

- K. With respect to IP SEC Tunnels to Third-Party Peers:
- Customer must provide all third-party technical information required for establishing IP Sec tunnel connectivity.
  - Customer must establish and maintain all required accounts and infrastructure with the applicable third-party peer prior to any technical discussions with the ActiveCore Engineer or Solutions Architect.
  - If Customer receives any infringement notices related to its use of Third-Party System(s), it must promptly: (a) stop using the related item with the Service; and (b) notify Comcast.

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
SD-WAN SERVICES**

**SCHEDULE A-2  
SERVICE LEVEL AGREEMENTS AND OBJECTIVES**

The Services are backed by the following Service Availability Objectives:

**1. Definitions**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the SD-WAN Services PSA or the General Terms and Conditions.

**“Available”** means the Service at a Service Location is available to transmit and receive data, as measured by Comcast’s systems. The Service is considered “Available” whether data is passing through the primary connection or through a backup connection at a given Service Location.

**“Planned Service Interruption”** means any Service Interruption caused by planned work such as scheduled maintenance or planned enhancements or upgrades to the network.

**“Service Interruption”** means, subject to the exclusions set forth in Section 6 (Exceptions to Credit Allowance), the Service is completely Unavailable outside of Planned Service Interruption(s).

**“Service Availability”** means a percentage of time in a calendar month during which the Service is Available. The Service Availability percentage for a given calendar month is calculated as follows:  $(A/M) * 100$ , where A is the total number of minutes the Service was Available during such calendar month and M is the total number of minutes in such calendar month.

**“Service Availability Objective(s)”** means the intended Service Availability for a calendar month, as set forth in Section 2 below.

**“Unavailable”** means the Service is not Available (*i.e.*, the Service is completely unable to transmit or receive any data, as measured by Comcast’s systems).

**2. SD-WAN Service Level Agreement (SLA)**

The Credit allowance available to Customer for failure to meet Service Availability Objectives shall be limited to the amounts set forth in the table below (**“Credits”**). For the purposes of calculating Credits for any such failure to meet a Service Availability Objective, (A) the Service Interruption on which such failure is based begins upon Comcast’s creation of a trouble ticket for the earlier of: (i) an automatic Service Interruption alarm (as described in Section 5.D. of Schedule A-1), or (ii) Customer’s report to Comcast of an interruption in the Service, provided that the interruption is reported by Customer during the duration of the interruption; and (B) the Service Interruption shall be deemed resolved upon closing of the same trouble ticket or, if sooner, the termination of the interruption, less any time Comcast is awaiting additional information or premises testing from the Customer. In no event shall the total amount of Credit issued to Customer’s account on a per-month basis exceed fifty percent (50%) of the total monthly recurring charge (**“MRC”**) associated with the impacted portion of the Service set forth in the Sales Order. Failures to meet Service Availability Objectives will not be aggregated for purposes of determining Credit allowances. To qualify, Customer must request the Credit from Comcast within thirty (30) days of the Service Interruption that resulted in failure to meet the Service Availability Objective. Customer will not be entitled to any additional credits for Service Interruptions or failures to meet the Service Availability Objective.

<b>Service:</b>	<b>Service Availability Objective:</b>	<b>Service Availability:</b>	<b>Amount of Credit:</b>
<b>For Service Locations Not Configured as Standalone</b>	99.99%	Equal to or greater than 99.99%	None
		Equal to or greater than 99.9% but less than 99.99%	5% of MRC

<b>For Service Locations Configured as Standalone</b>	99.995%	Equal to or greater than 99% but less than 99.9%	10% of MRC
		Less than 99%	20% of MRC
		Equal to or greater than 99.995%	None
		Equal to or greater than 99.9% but less than 99.995%	5% of MRC
		Equal to or greater than 99% but less than 99.9%	10% of MRC
		Less than 99%	20% of MRC

THE TOTAL CREDIT ALLOWANCE PER MONTH IS CAPPED AT FIFTY PERCENT (50%) OF THAT MONTH'S MRC FOR THE IMPACTED PORTIONS OF THE SERVICE. SEPARATELY OCCURRING SERVICE INTERRUPTIONS AND RESULTING FAILURES TO MEET SERVICE AVAILABILITY OBJECTIVES ARE NOT AGGREGATED FOR THE PURPOSES OF DETERMINING CREDIT ALLOWANCES.

### 3. Additional Service Availability Objectives

Comcast provides Service Availability Objectives for the Service, including mean time to respond, and mean time to restore. These service objectives are measured, on a calendar month basis, from the Comcast point of demarcation. Service availability is also affected by the choice of Underlay Service.

- A. **Mean Time to Respond.** The Mean Time to Respond objective is the average time required for Comcast to begin troubleshooting a Service Interruption. The Mean Time to Respond objective is fifteen (15) minutes from the earlier of Comcast's receipt of a fault notification or from the time a trouble ticket is opened with Comcast.
- B. **Mean Time to Restore.** The Mean Time to Restore objective is the average time required to restore Service after a Service Interruption to an operational condition as defined by the technical specifications in Section 1 of this Schedule. The Mean Time to Restore objective is as follows:
  - i. for Service Locations within the Comcast franchise footprint: Comcast will endeavor to restore the Service, including any required repair or replacement of uCPE, within four (4) hours of the time a customer reported trouble ticket is opened with Comcast.
  - ii. for Service Locations outside the Comcast franchise footprint: Comcast will endeavor to restore the Service, including any required repair or replacement of uCPE, the next Business Day after the day on which a customer reported trouble ticket is opened with Comcast; provided the trouble ticket is opened before 1:00 p.m. EST on a Business Day. For trouble tickets opened on Saturday, Sunday, a holiday, or after 1:00 p.m. EST on a Business Day, Comcast will endeavor to restore the Service the second Business Day thereafter. "Business Days" are Monday through Friday, excluding federal holidays.

### 4. Emergency Blocking

The parties agree that if either party hereto, in its reasonable sole discretion, determines that an emergency action is necessary to protect its own network, the party may, after engaging in reasonable and good faith efforts to notify the other party of the need to block, block any transmission path over its network by the other party where transmissions do not meet material standard industry requirements. The parties further agree that none of their respective obligations to one another under the Agreement will be affected by any such blockage except that the party affected by such blockage will be relieved of all obligations to make payments for charges relating to the circuit(s) which is so blocked and that no party will have any obligation to the other party for any claim, judgment, or liability resulting from such blockage.

### 5. Remedy Processes

All claims and rights arising under this Service Level Agreement must be exercised by Customer in writing within thirty (30) days of the event that gave rise to the claim or right. The Customer must submit the following information to the Customer's Comcast account representative with any and all claims for Credit allowances: (a) organization name; (b) Customer account number; and (c) basis of

Credit allowance claim (including date and time, if applicable). Comcast will acknowledge and review all claims promptly and will inform the Customer by electronic mail or other correspondence whether a Credit allowance will be issued or the claim rejected, with the reasons specified for the rejection.

#### **6. Exceptions to Credit Allowances**

Comcast shall not be liable for any Service Interruption, and a Service Interruption shall not qualify for the remedies set forth herein, if such Service Interruption is related to, associated with, or caused by: force majeure events, Planned Service Interruptions, Customer actions or inactions; Customer-Provided Equipment or power; or any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers, any power, equipment or services provided by third parties.

#### **7. Eligibility for Credit Allowances**

In order to be eligible for Credits, each Service Location must have at least two primary WAN interfaces from at least two Underlay Service providers.

#### **8. Other Limitations**

The remedies set forth in this Service Level Agreement shall be Customer's sole and exclusive remedies for any Service Interruption, outage, unavailability, delay, or other degradation, or any Comcast failure to meet the Service Availability Objectives.

**SCHEDULE A-3  
RESPONSIBILITY MATRIX**

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
<b>1</b>	<b><i>Requirement 1: Install and maintain a firewall configuration to protect cardholder data</i></b>			
<b>1.1</b>	<b>1.1</b> Establish and implement firewall and router configuration standards that include the following:		Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
<b>1.1.1</b>		<b>1.1.1</b> A formal process for approving and testing all network connections and changes to the firewall and router configurations	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
<b>1.1.2</b>		<b>1.1.2</b> Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
<b>1.1.3</b>		<b>1.1.3</b> Current diagram that shows all cardholder data flows across systems and networks	Customer	Though configuration standards are a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
<b>1.1.4</b>		<b>1.1.4</b> Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
<b>1.1.5</b>		<b>1.1.5</b> Description of groups, roles, and responsibilities for management of network components	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
<b>1.1.6</b>		<b>1.1.6</b> Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
<b>1.1.7</b>		<b>1.1.7</b> Requirement to review firewall and router rule sets at least every six months	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
1.2	<p><b>1.2</b> Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.</p> <p><b>Note:</b> An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.</p>	Shared	<p>Comcast is responsible for building configurations that restrict connections between untrusted networks and its backend system components.</p> <p>Customer is responsible for building configurations that restrict connections between untrusted networks and the uCPE and its CDE.</p>
1.2.1	<p><b>1.2.1</b> Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.</p>	Shared	<p>Comcast is responsible for building configurations that restrict connections between untrusted networks and its backend system components.</p> <p>Customer is responsible for building configurations that restrict connections between untrusted networks and the uCPE and its CDE.</p>
1.2.2	<p><b>1.2.2</b> Secure and synchronize router configuration files.</p>	Shared	<p>Comcast is responsible for building configurations that restrict connections between untrusted networks and its backend system components.</p> <p>Customer is responsible for building configurations that restrict connections between untrusted networks and the uCPE and its CDE.</p>
1.2.3	<p><b>1.2.3</b> Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.</p>	Shared	<p>Comcast is responsible for building configurations that restrict connections between untrusted networks and its backend system components.</p> <p>Customer is responsible for building configurations that restrict connections between untrusted networks and the uCPE and its CDE.</p>
1.3	<p><b>1.3</b> Prohibit direct public access between the Internet and any system component in the cardholder data environment.</p>	Shared	<p>Comcast is responsible for prohibiting direct public access between the Internet and its backend system components.</p> <p>Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.</p>
1.3.1	<p><b>1.3.1</b> Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.</p>	Shared	<p>Comcast is responsible for prohibiting direct public access between the Internet and its backend system components.</p> <p>Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.</p>
1.3.2	<p><b>1.3.2</b> Limit inbound Internet traffic to IP addresses within the DMZ.</p>	Shared	<p>Comcast is responsible for prohibiting direct public access between the Internet and its backend system components.</p> <p>Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.</p>
1.3.3	<p><b>1.3.3</b> Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)</p>	Shared	<p>Comcast is responsible for prohibiting direct public access between the Internet and its backend system components.</p> <p>Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.</p>
1.3.4	<p><b>1.3.4</b> Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.</p>	Shared	<p>Comcast is responsible for prohibiting direct public access between the Internet and its backend system components.</p> <p>Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.</p>

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
1.3.5	1.3.5 Permit only “established” connections into the network.	Shared	Comcast is responsible for prohibiting direct public access between the Internet and its backend system components. Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.
1.3.6	1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	Customer	Though prohibiting direct public access from the Internet is a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
1.3.7	1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. <b>Note:</b> Methods to obscure IP addressing may include, but are not limited to: · Network Address Translation (NAT) · Placing servers containing cardholder data behind proxy servers/firewalls, · Removal or filtering of route advertisements for private networks that employ registered addressing, · Internal use of RFC1918 address space instead of registered addresses.	Shared	Comcast is responsible for prohibiting direct public access between the Internet and its backend system components. Customer is responsible for prohibiting direct public access between the Internet and the uCPE and its CDE.
1.4	1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: · Specific configuration settings are defined. · Personal firewall (or equivalent functionality) is actively running. · Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	Shared	Comcast is responsible for installing personal firewall software or equivalent functionality on any portable computing devices that connects to the Internet when outside the network, and which are also used to access the uCPE and backend system components. Customer is responsible for installing personal firewall software or equivalent functionality on any portable computing devices that connect to the Internet when outside the network, and which are also used to access the uCPE and its CDE.
1.5	1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing the uCPE and backend system components. Customer is responsible for security policies and operational procedures for managing components in its CDE and components that connect to the uCPE.
2	<b>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters</b>		
2.1	2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts <b>before</b> installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, <i>point-of-sale</i> (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	Shared	Comcast is responsible for changing vendor-supplied defaults and removing or disabling unnecessary default accounts on the uCPE and backend system components. Customer is responsible for changing vendor-supplied defaults and removing or disabling unnecessary default accounts on components in its CDE and on components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
2.1.1	<b>2.1.1</b> For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Customer	Though changing and/or removing defaults is a shared responsibility, Comcast does not deploy a wireless environment as part of the SD-WAN product, so this requirement is the sole responsibility of the customer.
2.2	<b>2.2</b> Develop configuration standards for all system components. Assume that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: <ul style="list-style-type: none"> <li>· Center for Internet Security (CIS)</li> <li>· International Organization for Standardization (ISO)</li> <li>· SysAdmin Audit Network Security (SANS) Institute</li> <li>· National Institute of Standards Technology (NIST).</li> </ul>	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components.  Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.1	<b>2.2.1</b> Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) <b>Note:</b> Where virtualization technologies are in use, implement only one primary function per virtual system component.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components.  Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.2	<b>2.2.2</b> Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components.  Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.3	<b>2.2.3</b> Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. <b>Note:</b> Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components.  Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.4	<b>2.2.4</b> Configure system security parameters to prevent misuse.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components.

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
				Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.2.5		2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Shared	Comcast is responsible for configuration standards for the uCPE and backend system components. Customer is responsible for configuration standards for the components in its CDE and components that connect to the uCPE.
2.3		2.3 Encrypt all non-console administrative access using strong cryptography.	Shared	Comcast is responsible for encrypting all non-console administrative access to the uCPE and backend system components. Customer is responsible for encrypting all non-console administrative access to components in its CDE and components that connect to the uCPE.
2.4		2.4 Maintain an inventory of system components that are in scope for PCI DSS.	Shared	Comcast is responsible for maintaining an inventory of the uCPEs and backend system components. Customer is responsible for maintaining an inventory of components in its CDE and components that connect to the uCPE.
2.5		2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing the uCPE and backend system components. Customer is responsible for security policies and operational procedures for managing components in its CDE and components that connect to the uCPE.
2.6		2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.	N/A	
3	<b>Requirement 3: Protect stored cardholder data</b>			
3.1		3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	<ul style="list-style-type: none"> <li>Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements</li> <li>Specific retention requirements for cardholder data</li> <li>Processes for secure deletion of data when no longer needed</li> <li>A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.</li> </ul>		
<b>3.2</b>	<p><b>3.2</b> Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.</p> <p><i>It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:</i></p> <ul style="list-style-type: none"> <li>There is a business justification and</li> <li>The data is stored securely.</li> </ul> <p>Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:</p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
<b>3.2.1</b>	<p><b>3.2.1</b> Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</p> <p><b>Note:</b> <i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</i></p> <ul style="list-style-type: none"> <li>The cardholder's name</li> <li>Primary account number (PAN)</li> <li>Expiration date</li> <li>Service code</li> </ul> <p><i>To minimize risk, store only these data elements as needed for business.</i></p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
<b>3.2.2</b>	<p><b>3.2.2</b> Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card- not-present transactions after authorization.</p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
<b>3.2.3</b>	<p><b>3.2.3</b> Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.</p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
<b>3.3</b>	<p><b>3.3</b> Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a</p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	<p>legitimate business need can see more than the first six/last four digits of the PAN.</p> <p><b>Note:</b> This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.</p>		
3.4	<p><b>3.4</b> Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:</p> <ul style="list-style-type: none"> <li>· One-way hashes based on strong cryptography, (hash must be of the entire PAN)</li> <li>· Truncation (hashing cannot be used to replace the truncated segment of PAN)</li> <li>· Index tokens and pads (pads must be securely stored)</li> <li>· Strong cryptography with associated key-management processes and procedures.</li> </ul> <p><b>Note:</b> <i>It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.</i></p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.4.1	<p><b>3.4.1</b> If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.</p> <p><b>Note:</b> This requirement applies in addition to all other PCI DSS encryption and key-management requirements.</p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.5	<p><b>3.5</b> Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:</p> <p><b>Note:</b> <i>This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys— such key-encrypting keys must be at least as strong as the data-encrypting key.</i></p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
3.5.1	<b>3.5.1</b> Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: <ul style="list-style-type: none"> <li>· Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date</li> <li>· Description of the key usage for each key</li> <li>· Inventory of any HSMs and other SCDs used for key management</li> </ul> <b>Note:</b>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.5.2	<b>3.5.2</b> Restrict access to cryptographic keys to the fewest number of custodians necessary.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.5.3	<b>3.5.3</b> Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: <ul style="list-style-type: none"> <li>· Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key</li> <li>· Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device)</li> <li>· As at least two full-length key components or key shares, in accordance with an industry-accepted method</li> </ul> <b>Note:</b> <i>It is not required that public keys be stored in one of these forms.</i>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.5.4	<b>3.5.4</b> Store cryptographic keys in the fewest possible locations.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6	<b>3.6</b> Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: <b>Note:</b> <i>Numerous industry standards for key management are available from various resources including NIST, which can be found at <a href="http://csrc.nist.gov">http://csrc.nist.gov</a>.</i>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.1	<b>3.6.1</b> Generation of strong cryptographic keys	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.2	<b>3.6.2</b> Secure cryptographic key distribution	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.3	<b>3.6.3</b> Secure cryptographic key storage	Customer	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
			Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.4	<b>3.6.4</b> Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.5	<b>3.6.5</b> Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. <i>Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.</i>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.6	<b>3.6.6</b> If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. <i>Note: Examples of manual key- management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.</i>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.7	<b>3.6.7</b> Prevention of unauthorized substitution of cryptographic keys.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.6.8	<b>3.6.8</b> Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
3.7	<b>3.7</b> Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
4	<b>Requirement 4: Encrypt transmission of cardholder data across open, public networks</b>		
4.1	<b>4.1</b> Use strong cryptography and security protocols to safeguard sensitive cardholder data during	Customer	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	<p>transmission over open, public networks, including the following:</p> <ul style="list-style-type: none"> <li>· Only trusted keys and certificates are accepted.</li> <li>· The protocol in use only supports secure versions or configurations.</li> <li>· The encryption strength is appropriate for the encryption methodology in use.</li> </ul> <p><b>Note:</b> Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include but are not limited to:</p> <ul style="list-style-type: none"> <li>· The Internet</li> <li>· Wireless technologies, including 802.11 and Bluetooth</li> <li>· Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)</li> <li>· General Packet Radio Service (GPRS)</li> <li>· Satellite communications</li> </ul>		Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
4.1.1	4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
4.2	4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
4.3	4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
5	<b>Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs</b>		
5.1	5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Shared	<p>Comcast is responsible for deploying anti-virus software on backend system components that are commonly affected by malicious software.</p> <p>Customer is responsible for deploying anti-virus software on components in its CDE and on components that connect to the uCPE.</p>
5.1.1	5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Shared	<p>Comcast is responsible for deploying anti-virus software on backend system components that are commonly affected by malicious software.</p> <p>Customer is responsible for deploying anti-virus software on components in its CDE and on components that connect to the uCPE.</p>

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
5.1.2	5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Shared	Comcast is responsible for deploying anti-virus software on backend system components that are commonly affected by malicious software. Customer is responsible for deploying anti-virus software on components in its CDE and on components that connect to the uCPE.
5.2	5.2 Ensure that all anti-virus mechanisms are maintained as follows: · Are kept current, · Perform periodic scans · Generate audit logs which are retained per PCI DSS Requirement 10.7.	Shared	Comcast is responsible for maintaining anti-virus software on backend system components that are commonly affected by malicious software. Customer is responsible for maintaining anti-virus software on components in its CDE and on components that connect to the the uCPE.
5.3	5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. <b>Note:</b> <i>Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.</i>	Shared	Comcast is responsible for maintaining anti-virus software on backend system components that are commonly affected by malicious software. Customer is responsible for maintaining anti-virus software on components in its CDE and those that connect to the the uCPE.
5.4	5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for protecting backend system components. Customer is responsible for security policies and operational procedures for protecting components in its CDE and components that connect to the uCPE.
6	<b>Requirement 6: Develop and maintain secure systems and applications</b>		
6.1	6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for	Shared	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	<p>security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.</p> <p><b>Note:</b> Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk- assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.</p>		<p>Comcast is responsible for establishing a process to identify security vulnerabilities affecting the uCPE and backend system components.</p> <p>Customer is responsible for establishing a process to identify security vulnerabilities affecting components in its CDE and components that connect to the uCPE.</p>
6.2	<p><b>6.2</b> Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release.</p> <p><b>Note:</b> Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</p>	Shared	<p>Comcast is responsible for installing applicable vendor-supplied security patches on the uCPE and backend system components.</p> <p>Customer is responsible for installing patches on components in its CDE and on components that connect to the uCPE.</p>
6.3	<p><b>6.3</b> Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:</p> <ul style="list-style-type: none"> <li>· In accordance with PCI DSS (for example, secure authentication and logging)</li> <li>· Based on industry standards and/or best practices.</li> <li>· Incorporating information security throughout the software-development life cycle</li> </ul> <p><b>Note:</b> this applies to all software developed internally as well as bespoke or custom software developed by a third party.</p>	Shared	<p>Comcast is responsible for developing secure software for those applications deployed to the uCPE and backend system components based on industry standards and/or best practices.</p> <p>Customer is responsible for developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.</p>
6.3.1	<p><b>6.3.1</b> Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.</p>	Shared	<p>Comcast is responsible for developing secure software for those applications deployed to the uCPE and backend system components based on industry standards and/or best practices.</p> <p>Customer is responsible for developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.</p>
6.3.2	<p><b>6.3.2</b> Review custom code prior to release to production or customers in order to identify</p>	Shared	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	<p>any potential coding vulnerability (using either manual or automated processes) to include at least the following:</p> <ul style="list-style-type: none"> <li>· Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.</li> <li>· Code reviews ensure code is developed according to secure coding guidelines</li> <li>· Appropriate corrections are implemented prior to release.</li> <li>· Code-review results are reviewed and approved by management prior to release.</li> </ul> <p><i>Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.</i></p> <p><i>Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.</i></p>		<p>Comcast is responsible for developing secure software for those applications deployed to the uCPE and backend system components based on industry standards and/or best practices.</p> <p>Customer is responsible for developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.</p>
6.4	<p><b>6.4</b> Follow change control processes and procedures for all changes to system components. The processes must include the following:</p>	Shared	<p>Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.</p> <p>Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.</p>
6.4.1	<p><b>6.4.1</b> Separate development/test environments from production environments, and enforce the separation with access controls.</p>	Shared	<p>Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.</p> <p>Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.</p>
6.4.2	<p><b>6.4.2</b> Separation of duties between development/test and production environments</p>	Shared	<p>Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.</p> <p>Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.</p>
6.4.3	<p><b>6.4.3</b> Production data (live PANs) are not used for testing or development</p>	Shared	

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
				Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.  Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.4		6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.  Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5		6.4.5 Change control procedures for the implementation of security patches and software modifications must include the following:	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.  Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5.1		6.4.5.1 Documentation of impact.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.  Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5.2		6.4.5.2 Documented change approval by authorized parties.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.  Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5.3		6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.  Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
6.4.5.4		6.4.5.4 Back-out procedures.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.  Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
		<b>6.4.6</b> Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	Shared	Comcast is responsible for following control processes and procedures for changes to the uCPE operating system and backend system components.  Customer is responsible for following control processes and procedures for changes to the uCPE it makes via the Activecore Portal, to components in its CDE, and to components connected to the uCPE.
<b>6.5</b>	<b>6.5</b> Address common coding vulnerabilities in software-development processes as follows: · Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. · Develop applications based on secure coding guidelines. <b>Note:</b> The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.		Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components.  Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
<b>6.5.1</b>		<b>6.5.1</b> Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components.  Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
<b>6.5.2</b>		<b>6.5.2</b> Buffer overflows	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components.  Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
<b>6.5.3</b>		<b>6.5.3</b> Insecure cryptographic storage	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components.  Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
<b>6.5.4</b>		<b>6.5.4</b> Insecure communications	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components.  Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
6.5.5		6.5.5 Improper error handling	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.6		6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
		<b>Note:</b> Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):		
6.5.7		6.5.7 Cross-site scripting (XSS)	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.8		6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.9		6.5.9 Cross-site request forgery (CSRF)	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.
6.5.10		6.5.10 Broken authentication and session management	Shared	Comcast is responsible for training developers and developing software securely for those applications deployed to the uCPE and backend system components. Customer is responsible for training developers and developing software securely for those applications deployed to components in its CDE and to components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
6.6	<p><b>6.6</b> For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:</p> <ul style="list-style-type: none"> <li>· Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes</li> </ul> <p><b>Note:</b> <i>This assessment is not the same as the vulnerability scans performed for Requirement 11.2.</i></p> <ul style="list-style-type: none"> <li>· Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.</li> </ul>	Shared	<p>Comcast is responsible for addressing new threats and vulnerabilities applicable to public-facing web applications hosted on backend system components.</p> <p>Customer is responsible for addressing new threats and vulnerabilities applicable to public-facing web applications hosted in its CDE.</p>
6.7	<p><b>6.7</b> Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.</p>	Shared	<p>Comcast is responsible for security policies and operational procedures for developing and maintaining secure systems and applications deployed to the uCPE and backend system components.</p> <p>Customer is responsible for security policies and operational procedures for developing and maintaining secure systems and applications deployed to components in its CDE and to components that connect to the uCPE.</p>
7	<b>Requirement 7: Restrict access to cardholder data by business need to know</b>		
7.1	<p><b>7.1</b> Limit access to system components and cardholder data to only those individuals whose job requires such access.</p>	Shared	<p>Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.</p>
7.1.1	<p><b>7.1.1</b> Define access needs for each role, including:</p> <ul style="list-style-type: none"> <li>· System components and data resources that each role needs to access for their job function</li> <li>· Level of privilege required (for example, user, administrator, etc.) for accessing resources.</li> </ul>	Shared	<p>Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.</p>
7.1.2	<p><b>7.1.2</b> Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.</p>	Shared	<p>Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.</p>
7.1.3	<p><b>7.1.3</b> Assign access based on individual personnel's job classification and function.</p>	Shared	<p>Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.</p>

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
7.1.4		7.1.4 Require documented approval by authorized parties specifying required privileges.	Shared	Comcast is responsible for limiting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for limiting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.2		7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	Shared	Comcast is responsible for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.2.1		7.2.1 Coverage of all system components	Shared	Comcast is responsible for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.2.2		7.2.2 Assignment of privileges to individuals based on job classification and function.	Shared	Comcast is responsible for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.2.3		7.2.3 Default "deny-all" setting.	Shared	Comcast is responsible for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
7.3		7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for restricting access to the uCPE (via underlying operating system) and backend system components. Customer is responsible for security policies and operational procedures for restricting access to the uCPE (via Activecore Portal), to components in its CDE, and to components that connect to the uCPE.
8	<b>Requirement 8: Identify and authenticate access to system components</b>			
8.1		8.1 Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components as follows:	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.1		8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
8.1.2		<b>8.1.2</b> Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.3		<b>8.1.3</b> Immediately revoke access for any terminated users.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.4		<b>8.1.4</b> Remove/disable inactive user accounts at least every 90 days.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.5		<b>8.1.5</b> Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: · Enabled only during the time period needed and disabled when not in use. · Monitored when in use.	Customer	Comcast does not allow third parties to access in-scope systems. All access, if needed, is done through screen shares and is monitored at all times. For third-party access to customer systems which connect to the uCPE, this requirement is the sole responsibility of the customer.
8.1.6		<b>8.1.6</b> Limit repeated access attempts by locking out the user ID after not more than six attempts.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.7		<b>8.1.7</b> Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.1.8		<b>8.1.8</b> If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
8.2	<p><b>8.2</b> In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> <li>· Something you know, such as a password or passphrase</li> <li>· Something you have, such as a token device or smart card</li> <li>· Something you are, such as a biometric.</li> </ul>	Shared	<p>Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.</p>
8.2.1	<p><b>8.2.1</b> Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.</p>	Shared	<p>Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.</p>
8.2.2	<p><b>8.2.2</b> Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.</p>	Shared	<p>Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.</p>
8.2.3	<p><b>8.2.3</b> Passwords/phrases must meet the following:</p> <ul style="list-style-type: none"> <li>· Require a minimum length of at least seven characters.</li> <li>· Contain both numeric and alphabetic characters.</li> </ul> <p>Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.</p>	Shared	<p>Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.</p>
8.2.4	<p><b>8.2.4</b> Change user passwords/passphrases at least every 90 days.</p>	Shared	<p>Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.</p>
8.2.5	<p><b>8.2.5</b> Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.</p>	Shared	<p>Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components.</p> <p>Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.</p>

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
8.2.6		8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	Shared	Comcast is responsible for policies and procedures for user identification management of users on the uCPE (via underlying operating system) and backend system components. Customer is responsible for policies and procedures for user identification management of users on the components in its CDE, and on components that connect to the uCPE.
8.3		8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. <b>Note:</b> Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	Shared	Comcast is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to the uCPE and backend system components. Customer is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to components in its CDE and to components that connect to the uCPE.
8.3.1		8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Shared	Comcast is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to the uCPE and backend system components. Customer is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to components in its CDE and to components that connect to the uCPE.
8.3.2		8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	Shared	Comcast is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to the uCPE and backend system components. Customer is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to components in its CDE and to components that connect to the uCPE.
8.4		8.4 Document and communicate authentication procedures and policies to all users including: <ul style="list-style-type: none"> <li>Guidance on selecting strong authentication credentials</li> <li>Guidance for how users should protect their authentication credentials</li> <li>Instructions not to reuse previously used passwords</li> <li>Instructions to change passwords if there is any suspicion the password could be compromised.</li> </ul>	Shared	Comcast is responsible for documenting and communication authentication procedures and policies to users on the uCPE (via underlying operating systems) and backend system components. Customer is responsible for securing all individual non-console administrative access and all remote access using multi-factor authentication to components in its CDE and to components that connect to the uCPE.
8.5		8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: <ul style="list-style-type: none"> <li>Generic user IDs are disabled or removed.</li> <li>Shared user IDs do not exist for system administration and other critical functions.</li> <li>Shared and generic user IDs are not used to administer any system components.</li> </ul>	Shared	Comcast is responsible for not using group, shared, or generic IDs, passwords, or other authentication methods for the uCPE (via underlying operating systems) and backend system components. Customer is responsible for not using group, shared, or generic IDs, passwords, or other authentication methods for components in its CDE and for components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
8.5.1	<p><b>8.5.1 Additional requirement for service providers:</b> Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.</p> <p><b>Note:</b> This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.</p>	Comcast	
8.6	<p><b>8.6</b> Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:</p> <ul style="list-style-type: none"> <li>· Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.</li> <li>· Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.</li> </ul>	Shared	<p>Comcast is responsible for authentication methods for the uCPE and backend system components.</p> <p>Customer is responsible for authentication methods for components in its CDE and for components that connect to the uCPE.</p>
8.7	<p><b>8.7</b> All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:</p> <ul style="list-style-type: none"> <li>· All user access to, user queries of, and user actions on databases are through programmatic methods.</li> <li>· Only database administrators have the ability to directly access or query databases.</li> <li>· Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).</li> </ul>	Customer	<p>Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.</p>
8.8	<p><b>8.8</b> Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.</p>	Shared	<p>Comcast is responsible for security policies and operational procedures for identification and authentication for the uCPE and backend system components.</p> <p>Customer is responsible for security policies and operational procedures for identification and authentication for components in its CDE, and for components that connect to the uCPE.</p>
9	<b>Requirement 9: Restrict physical access to cardholder data</b>		
9.1	<p><b>9.1</b> Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.</p>	Customer	<p>Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.</p>
9.1.1	<p><b>9.1.1</b> Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at</p>	Customer	<p>Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.</p>

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	<p>least three months, unless otherwise restricted by law.</p> <p><b>Note:</b> "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.</p>		
9.1.2	<p><b>9.1.2</b> Implement physical and/or logical controls to restrict access to publicly accessible network jacks.</p> <p><i>For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.</i></p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.1.3	<p><b>9.1.3</b> Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.</p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.2	<p><b>9.2</b> Develop procedures to easily distinguish between onsite personnel and visitors, to include:</p> <ul style="list-style-type: none"> <li>Identifying new onsite personnel or visitors (for example, assigning badges)</li> <li>Changes to access requirements</li> <li>Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).</li> </ul>	Shared	<p>Comcast is responsible for procedures for distinguishing between onsite personnel and visitors on its property.</p> <p>Customer is responsible for procedures for distinguishing between onsite personnel and visitors on its property.</p>
9.3	<p><b>9.3</b> Control physical access for onsite personnel to the sensitive areas as follows:</p> <ul style="list-style-type: none"> <li>Access must be authorized and based on individual job function.</li> <li>Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.</li> </ul>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.4	<p><b>9.4</b> Implement procedures to identify and authorize visitors.</p> <p>Procedures should include the following:</p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.4.1	<p><b>9.4.1</b> Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.</p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.4.2	<p><b>9.4.2</b> Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.</p>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
9.4.3	9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.4.4	9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.5	9.5 Physically secure all media.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.5.1	9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.6	9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.6.1	9.6.1 Classify media so the sensitivity of the data can be determined.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.6.2	9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.6.3	9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.7	9.7 Maintain strict control over the storage and accessibility of media.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.7.1	9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.8	9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.8.1	9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
9.8.2	<b>9.8.2</b> Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.9	<b>9.9</b> Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. <i><b>Note:</b> These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.</i>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.9.1	<b>9.9.1</b> Maintain an up-to-date list of devices. The list should include the following: <ul style="list-style-type: none"> <li>· Make, model of device</li> <li>· Location of device (for example, the address of the site or facility where the device is located)</li> <li>· Device serial number or other method of unique identification.</li> </ul>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.9.2	<b>9.9.2</b> Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). <i><b>Note:</b> Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.</i>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
9.9.3	<b>9.9.3</b> Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: <ul style="list-style-type: none"> <li>· Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.</li> <li>· Do not install, replace, or return devices without verification.</li> <li>· Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).</li> <li>· Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).</li> </ul>	Customer	Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
9.10	<b>9.10</b> Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for restricting physical access to systems at Comcast owned locations. Customer is responsible for security policies and operational procedures for restricting physical access to systems at its locations.
10	<b>Requirement 10: Track and monitor all access to network resources and cardholder data</b>		
10.1	<b>10.1</b> Implement audit trails to link all access to system components to each individual user.	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2	<b>10.2</b> Implement automated audit trails for all system components to reconstruct the following events:	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.1	<b>10.2.1</b> All individual user accesses to cardholder data	Customer	Though implementing audit trails is a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
10.2.2	<b>10.2.2</b> All actions taken by any individual with root or administrative privileges	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.3	<b>10.2.3</b> Access to all audit trails	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.4	<b>10.2.3</b> Access to all audit trails	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.5	<b>10.2.5</b> Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.6	<b>10.2.6</b> Initialization, stopping, or pausing of the audit logs	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.2.7	<b>10.2.7</b> Creation and deletion of system- level objects	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
10.3	10.3 Record at least the following audit trail entries for all system components for each event:			Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.1		10.3.1 User identification	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.2		10.3.2 Type of event	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.3		10.3.3 Date and time	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.4		10.3.4 Success or failure indication	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.5		10.3.5 Origination of event	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.3.6		10.3.6 Identity or name of affected data, system component, or resource.	Shared	Comcast is responsible for implementing audit trails to link all access to the uCPE and backend system components. Customer is responsible for implementing audit trails to link all access to its CDE and to components connected to the uCPE.
10.4	10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. <i>Note: One example of time synchronization technology is Network Time Protocol (NTP).</i>		Shared	Comcast is responsible for using time-synchronization technology to synchornize clocks on the uCPE and backend system components. Customer is responsible for using time-synchronization technology to synchornize clocks on components in its CDE and on components connected to the uCPE.
10.4.1		10.4.1 Critical systems have the correct and consistent time.	Shared	Comcast is responsible for using time-synchronization technology to synchornize clocks on the uCPE and backend system components. Customer is responsible for using time-synchronization technology to synchornize clocks on components in its CDE and on components connected to the uCPE.
10.4.2		10.4.2 Time data is protected.	Shared	Comcast is responsible for using time-synchronization technology to synchornize clocks on the uCPE and backend system components. Customer is responsible for using time-synchronization technology to synchornize clocks on components in its CDE and on components connected to the uCPE.

Req.	PCI DSS v3.2.1 Requirements		Responsibility (Comcast / Customer / Shared)	Responsibility Summary
10.4.3		10.4.3 Time settings are received from industry-accepted time sources.	Shared	Comcast is responsible for using time-synchronization technology to synchronize clocks on the uCPE and backend system components. Customer is responsible for using time-synchronization technology to synchronize clocks on components in its CDE and on components connected to the uCPE.
10.5	10.5 Secure audit trails so they cannot be altered.		Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.1		10.5.1 Limit viewing of audit trails to those with a job-related need.	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.2		10.5.2 Protect audit trail files from unauthorized modifications.	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.3		10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.4		10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.5.5		10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Shared	Comcast is responsible for securing audit trails for the uCPE and backend system components. Customer is responsible for securing audit trails for components in its CDE and for components connected to the uCPE.
10.6	10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. <i>Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.</i>		Shared	Comcast is responsible for reviewing logs and security events for the uCPE and backend system components. Customer is responsible for reviewing logs and security events for components in its CDE and for components connected to the uCPE.
10.6.1		10.6.1 Review the following at least daily: · All security events · Logs of all system components that store, process, or transmit CHD and/or SAD · Logs of all critical system components · Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	Shared	Comcast is responsible for reviewing logs and security events for the uCPE and backend system components. Customer is responsible for reviewing logs and security events for components in its CDE and for components connected to the uCPE.
10.6.2		10.6.2 Review logs of all other system components periodically based on the	Shared	Comcast is responsible for reviewing logs and security events for the uCPE and backend system components.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	organization's policies and risk management strategy, as determined by the organization's annual risk assessment.		Customer is responsible for reviewing logs and security events for components in its CDE and for components connected to the uCPE.
10.6.3	<b>10.6.3</b> Follow up exceptions and anomalies identified during the review process.	Shared	Comcast is responsible for reviewing logs and security events for the uCPE and backend system components. Customer is responsible for reviewing logs and security events for components in its CDE and for components connected to the uCPE.
10.7	<b>10.7</b> Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Shared	Comcast is responsible for retaining audit trails of the uCPE and backend system components. Customer is responsible for retaining audit trails of components in its CDE and of components connected to the uCPE.
10.8	<b>10.8 Additional requirement for service providers only:</b> Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: <ul style="list-style-type: none"> <li>· Firewalls</li> <li>· IDS/IPS</li> <li>· FIM</li> <li>· Anti-virus</li> <li>· Physical access controls</li> <li>· Logical access controls</li> <li>· Audit logging mechanisms</li> <li>· Segmentation controls (if used)</li> </ul>	Comcast	
10.8.1	<b>10.8.1</b> Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: <ul style="list-style-type: none"> <li>· Restoring security functions</li> <li>· Identifying and documenting the duration (date and time start to end) of the security failure</li> <li>· Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause</li> <li>· Identifying and addressing any security issues that arose during the failure</li> <li>· Performing a risk assessment to determine whether further actions are required as a result of the security failure</li> <li>· Implementing controls to prevent cause of failure from reoccurring</li> <li>· Resuming monitoring of security controls</li> </ul>	Comcast	

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
10.9	<b>10.9</b> Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for monitoring the uCPE and backend system components. Customer is responsible for security policies and operational procedures for monitoring components in its CDE, components connected to the uCPE, and cardholder data.
<b>11</b>	<b>Requirement 11: Regularly test security systems and processes.</b>		
11.1	<b>11.1</b> Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. <b>Note:</b> <i>Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.</i>	Shared	Comcast is responsible for implementing processes to test for the presence of wireless access points at Comcast owned locations. Customer is responsible for implementing processes to test for the presence of wireless access points at its locations.
11.1.1	<b>11.1.1</b> Maintain an inventory of authorized wireless access points including a documented business justification.	Customer	Though implementing processes to test for the presence of wireless access points is a shared responsibility, Comcast does not use wireless access points to support the product, so this requirement is the sole responsibility of the customer.
11.1.2	<b>11.1.2</b> Implement incident response procedures in the event unauthorized wireless access points are detected.	Shared	Comcast is responsible for implementing processes to test for the presence of wireless access points at Comcast owned locations. Customer is responsible for implementing processes to test for the presence of wireless access points at its locations.
11.2	<b>11.2</b> Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). <b>Note:</b> <i>Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.</i>	Shared	Comcast is responsible for running internal and external network vulnerability scans targeting backend system components. Customer is responsible for running internal and external network vulnerability scans targeting components in its CDE and targeting the uCPE and connecting components.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
11.2.1	<p><b>11.2.1</b> Perform quarterly internal vulnerability scans and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.</p>	Shared	<p>Comcast is responsible for running internal and external network vulnerability scans targetting backend system components.</p> <p>Customer is responsible for running internal and external network vulnerability scans targetting components in its CDE and targetting the uCPE and connecting components.</p>
11.2.2	<p><b>11.2.2</b> Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.</p> <p><b>Note:</b> <i>Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.</i></p>	Shared	<p>Comcast is responsible for running internal and external network vulnerability scans targetting backend system components.</p> <p>Customer is responsible for running internal and external network vulnerability scans targetting components in its CDE and targetting the uCPE and connecting components.</p>
11.2.3	<p><b>11.2.3</b> Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.</p>	Shared	<p>Comcast is responsible for running internal and external network vulnerability scans targetting backend system components.</p> <p>Customer is responsible for running internal and external network vulnerability scans targetting components in its CDE and targetting the uCPE and connecting components.</p>
11.3	<p><b>11.3</b> Implement a methodology for penetration testing that includes the following:</p> <ul style="list-style-type: none"> <li>· Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)</li> <li>· Includes coverage for the entire CDE perimeter and critical systems</li> <li>· Includes testing from both inside and outside the network</li> <li>· Includes testing to validate any segmentation and scope-reduction controls</li> <li>· Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5</li> <li>· Defines network-layer penetration tests to include components that support network functions as well as operating systems</li> <li>· Includes review and consideration of threats and vulnerabilities experienced in the last 12 months</li> <li>· Specifies retention of penetration testing results and remediation activities results.</li> </ul>	Shared	<p>Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components.</p> <p>Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.</p>
11.3.1	<p><b>11.3.1</b> Perform <i>external</i> penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).</p>	Shared	<p>Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components.</p> <p>Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.</p>

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
11.3.2	<b>11.3.2</b> Perform <i>internal</i> penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Shared	Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components.  Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.
11.3.3	<b>11.3.3</b> Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	Shared	Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components.  Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.
11.3.4	<b>11.3.4</b> If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Shared	Comcast is responsible for implementing a methodology for and conducting penetration tests targetting backend system components.  Customer is responsible for implementing a methodology for and conducting penetration tests targetting components in its CDE and targetting the uCPE and connecting components.
	<b>11.3.4.1</b> Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	Comcast	
11.4	<b>11.4</b> Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	Customer	Customer is responsible for using intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into components in its CDE and into components that connect to the the uCPE.
11.5	<b>11.5</b> Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. <i>Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre- configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).</i>	Shared	Comcast is responsible for deploying a change-detection mechanism for the uCPE and backend system components.  Customer is responsible for deploying a change-detection mechanism for components in its CDE and for components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
11.5.1	11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	Shared	Comcast is responsible for deploying a change-detection mechanism for the uCPE and backend system components. Customer is responsible for deploying a change-detection mechanism for components in its CDE and for components that connect to the uCPE.
11.6	11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for security monitoring and testing the uCPE and backend system components. Customer is responsible for security policies and operational procedures for security monitoring and testing components in its CDE and components connected to the uCPE.
12	<b>Requirement 12: Maintain a policy that addresses information security for all personnel.</b>		
12.1	12.1 Establish, publish, maintain, and disseminate a security policy.	Shared	Comcast is responsible for establishing, publishing, maintaining, and disseminating a security policy that regards all the requirements for which it is responsible per this matrix. Customer is responsible for establishing, publishing, maintaining, and disseminating a security policy that regards all the requirements for which it is responsible per this matrix.
12.1.1	12.1.1 Review the security policy at least annually and update the policy when the environment changes.	Shared	Comcast is responsible for establishing, publishing, maintaining, and disseminating a security policy that regards all the requirements for which it is responsible per this matrix. Customer is responsible for establishing, publishing, maintaining, and disseminating a security policy that regards all the requirements for which it is responsible per this matrix.
12.2	12.2 Implement a risk-assessment process that: · Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), · Identifies critical assets, threats, and vulnerabilities, and · Results in a formal risk assessment. <i>Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.</i>	Shared	Comcast is responsible for implementing a risk-assessment process that is performed at least annually and upon significant changes to the uCPE and backend system component environment which identifies critical assets, threats, and vulnerabilities.. Customer is responsible for implementing a risk-assessment process that is performed at least annually and upon significant changes to components in its PCI in-scope environment which identifies critical assets, threats, and vulnerabilities relevant to those components.
12.3	12.3 Develop usage policies for critical technologies and define proper use of these technologies. <b>Note:</b> <i>Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.</i> Ensure these usage policies require the following:	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.1	12.3.1 Explicit approval by authorized parties	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
12.3.2	12.3.2 Authentication for use of the technology	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.3	12.3.3 A list of all such devices and personnel with access	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.4	12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.5	12.3.5 Acceptable uses of the technology	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.6	12.3.6 Acceptable network locations for the technologies	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.7	12.3.7 List of company-approved products	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.8	12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.9	12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	Shared	Comcast is responsible for developing usage policies for its critical technologies. Customer is responsible for developing usage policies for its critical technologies.
12.3.10	12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	Customer	Though developing usage policies is a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
12.4	12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	Shared	Comcast is responsible for defining information security responsibilities for all personnel in its security policies and procedures. Customer is responsible for defining information security responsibilities for all personnel in its security policies and procedures.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
	<b>12.4.1</b> Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: · Overall accountability for maintaining PCI DSS compliance · Defining a charter for a PCI DSS compliance program and communication to executive management	Comcast	
<b>12.5</b>	<b>12.5</b> Assign to an individual or team the following information security management responsibilities:	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
<b>12.5.1</b>	<b>12.5.1</b> Establish, document, and distribute security policies and procedures.	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
<b>12.5.2</b>	<b>12.5.2</b> Monitor and analyze security alerts and information, and distribute to appropriate personnel.	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
<b>12.5.3</b>	<b>12.5.3</b> Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
<b>12.5.4</b>	<b>12.5.4</b> Administer user accounts, including additions, deletions, and modifications.	Shared	Comcast is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix. Customer is responsible for assigning an individual or a team for managing information security responsibilities that regard all the requirements for which it is responsible per this matrix.
<b>12.5.5</b>	<b>12.5.5</b> Monitor and control all access to data.	Customer	Though assigning an individual or a team for managing information security responsibilities is a shared responsibility, Comcast does not store, process, or transmit CHD as part of this service offering. This requirement is the sole responsibility of the customer.
<b>12.6</b>	<b>12.6</b> Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	Shared	Comcast is responsible for implementing a formal security awareness program to inform its personnel. Customer is responsible for implementing a formal security awareness program to inform its personnel.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
12.6.1	<p><b>12.6.1</b> Educate personnel upon hire and at least annually.</p> <p><i>Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.</i></p>	Shared	<p>Comcast is responsible for implementing a formal security awareness program to inform its personnel.</p> <p>Customer is responsible for implementing a formal security awareness program to inform its personnel.</p>
12.6.2	<p><b>12.6.2</b> Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.</p>	Shared	<p>Comcast is responsible for implementing a formal security awareness program to inform its personnel.</p> <p>Customer is responsible for implementing a formal security awareness program to inform its personnel.</p>
12.7	<p><b>12.7</b> Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)</p> <p><i>Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</i></p>	Shared	<p>Comcast is responsible for screening its potential personnel prior to hire.</p> <p>Customer is responsible for screening its potential personnel prior to hire.</p>
12.8	<p><b>12.8</b> Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:</p>	Shared	<p>Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers.</p> <p>Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.</p>
12.8.1	<p><b>12.8.1</b> Maintain a list of service providers including a description of the service provided.</p>	Shared	<p>Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers.</p> <p>Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.</p>
12.8.2	<p><b>12.8.2</b> Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.</p> <p><i>Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.</i></p>	Shared	<p>Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers.</p> <p>Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.</p>
12.8.3	<p><b>12.8.3</b> Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.</p>	Shared	<p>Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers.</p> <p>Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.</p>

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
12.8.4	<b>12.8.4</b> Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Shared	Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers. Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.
12.8.5	<b>12.8.5</b> Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	Shared	Comcast is responsible for maintaining and implementing policies and procedures to manage its services providers. Customer is responsible for maintaining and implementing policies and procedures to manage its services providers.
12.9	<b>12.9 Additional requirement for service providers only:</b> Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	Comcast	
12.10	<b>12.10</b> Implement an incident response plan. Be prepared to respond immediately to a system breach.	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.1	<b>12.10.1</b> Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: <ul style="list-style-type: none"> <li>· Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum</li> <li>· Specific incident response procedures</li> <li>· Business recovery and continuity procedures</li> <li>· Data backup processes</li> <li>· Analysis of legal requirements for reporting compromises</li> <li>· Coverage and responses of all critical system components</li> <li>· Reference or inclusion of incident response procedures from the payment brands.</li> </ul>	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.2	<b>12.10.2</b> Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually..	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.

Req.	PCI DSS v3.2.1 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
12.10.3	12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.4	12.10.4 Provide appropriate training to staff with security breach response responsibilities.	Shared	Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.5	12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion- prevention, firewalls, and file-integrity monitoring systems.	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.10.6	12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Shared	Comcast is responsible for implementing an incident response plan for preparation for responding to a breach to the uCPE and backend system components. Customer is responsible for implementing an incident response plan for preparation for responding to a breach to components in its CDE and to components that connect to the uCPE.
12.11	12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: <ul style="list-style-type: none"> <li>· Daily log reviews</li> <li>· Firewall rule-set reviews</li> <li>· Applying configuration standards to new systems</li> <li>· Responding to security alerts</li> <li>· Change management processes</li> </ul>	Comcast	
12.11.1	12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: <ul style="list-style-type: none"> <li>· Documenting results of the reviews</li> <li>· Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program</li> </ul>	Comcast	

**[END OF SD-WAN PSA. DDoS PSA BEGINS ON NEXT PAGE]**

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
DDoS MITIGATION SERVICE**

The following additional terms and conditions are applicable to Sales Orders for Comcast's DDoS Mitigation Service:

**DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

**"Estimated Availability Date"** means the target date for delivery of Service.

**"On-Net"** means a Comcast-provided internet circuit that carries internet service to a Service Location and which uses an internet backbone provided by Comcast.

**"Service(s)"** means the Comcast DDoS Mitigation Services as described in **Schedule A-1**.

**ARTICLE 1. SERVICES**

This attachment shall apply to the Services. A further description of the Services is set forth in Schedule A-1 hereto which is incorporated herein by reference.

**ARTICLE 2. PROVIDER**

Service shall be provided by Comcast Business Communications, LLC.

**ARTICLE 3. SERVICE COMMENCEMENT DATE**

Comcast shall inform Customer when the Service is available and performing in accordance with the "Technical Specifications" set forth in Schedule A-1 hereto (**"Availability Notification"**). Charges for Services shall begin to accrue as of the Service Commencement Date. The Service Commencement Date shall be earliest of: (A) the date on which Customer confirms receipt of and concurrence with the Availability Notification; (B) five (5) business days following the date of the Availability Notification, if Customer fails to notify Comcast that the Service does not comply materially with the Technical Specifications (defined in Article 6); or (C) the date on which Customer first uses the Service. In the event that a Service Term has not been expressly set forth in a Sales Order, the Service Term for such Sales Order shall be twelve (12) months.

**ARTICLE 4. SERVICE REQUIREMENTS**

**4.1** Notwithstanding anything to the contrary contained herein (including, but not limited to, Articles 5.3 and 5.4), in order to provide the Service at a Service Location: (i) the Service Location must have Comcast Ethernet Dedicated Internet Service provided on a "Type I" or "Type II" basis (**"Underlay EDI Service"**), which must be ordered from Comcast and may be pre-existing or ordered in conjunction with the Service; and (ii) the applicable Underlay EDI Service (i.e., the applicable EDI circuit) must have bandwidth capacity to support the Services as determined by Comcast (the **"Bandwidth Requirement"**).

**4.2** The Service is provided on a per circuit basis. For the purposes of an example only, if Customer has two EDI circuits (whether at a single Service Location or at two separate Service Locations) and desires to have the Service with respect to both circuits, it will be required to order the Service with respect to each circuit and each ordered Service will constitute a separate Service for the purposes of the Agreement.

**4.3** Customer acknowledges and agrees that charges may begin to accrue with respect to Underlay EDI Service and the Service at different times. For the avoidance of doubt, charges will begin to accrue with respect to the Underlay EDI Service in accordance with the PSA applicable thereto.

**ARTICLE 5. PORTABILITY; BANDWIDTH UPGRADES**

**5.1 Portability.** Customer may terminate an existing Service (an **"Existing Service"**) and turn up a replacement Service (i.e., activate Service with termination points on Comcast's network that are different than those of the Existing Service) (a **"Replacement Service"**) without incurring Termination Charges with respect to the Existing Service, provided that: (a) the Replacement Service has bandwidth equal to or greater than the bandwidth of the Existing Service; and (b) Customer submits a Sales Order to Comcast for the Replacement Service within ninety (90) days after termination of the Existing Service and that Sales Order is accepted by Comcast.

**5.2 Bandwidth Upgrades.** Customer may upgrade bandwidth of an Existing Service without incurring Termination Charges, provided that: (a) the upgraded Service (the **"Upgraded Service"**) must assume the remaining Service Term of the Existing Service, but in no event less than twelve (12) months; (b) the Upgraded Service is provided to the same Service Location as the

Existing Service; (c) Customer submits a Sales Order to Comcast for the Upgraded Service and that Sales Order is accepted by Comcast; and (d) Customer agrees to pay the applicable monthly recurring charges for the Upgraded Service commencing with the upgrade.

#### **ARTICLE 6. TECHNICAL SPECIFICATIONS; SERVICE LEVEL AGREEMENT**

The technical specifications applicable to the Service are set forth in Schedule A-1 hereto (“**Technical Specifications**”). The service level agreement applicable to the Service is set forth in a Schedule A-2 hereto and incorporated herein by reference.

#### **ARTICLE 7. CUSTOMER PORTAL**

Comcast provides the Customer with a password-protected web portal (“**Portal**”), which Customer will be required to access to operate and view information regarding the Service. Customer may have the option to use the Portal to enter changes to the Customer’s Service settings and configurations, subject to the availability of self-service settings and configurations, as determined by Comcast in its sole discretion.

**COMCAST ENTERPRISE SERVICES**  
**PRODUCT-SPECIFIC ATTACHMENT**  
**DDoS MITIGATION SERVICES**

**SCHEDULE A-1**  
**SERVICE DESCRIPTIONS AND TECHNICAL SPECIFICATIONS**

The Services will be provided in accordance with the service descriptions and technical specifications set forth below.

**I. Service Descriptions**

The Service is a managed security service that includes threat mitigation functionality to respond to certain types of distributed denial of service (“**DDoS**”) attacks, including volumetric and flood attacks. The Service is available to Customer on an unlimited subscription basis or an emergency basis, and is available to Legacy Customers (as defined in Section (I)(4)(A) below) as an incident-based subscription, all as described in more detail below. All versions of the Service require Customer to have Comcast provided EDI Underlay Service at the applicable Service Location which meets the Bandwidth Requirement. The Unlimited Subscription Service (as defined below) is also available to Customers on an Off-Net (as defined in Section 2 below) basis subject to the conditions herein, including those set forth in Section 2.

**1. Unlimited Subscription DDoS Mitigation Service (“Unlimited Subscription Service”)**

- A. The Unlimited Subscription Service is a subscription-based Service offering that provides Customer with proactive network detection of DDoS attack traffic, alert notifications, mitigation of attacks, and online reporting. Upon receipt of complete and accurate Customer contact and network information, Comcast will configure Customer’s site(s), related IP addresses, and countermeasure options. Following Comcast’s completion of such configuration, Comcast shall make three (3) attempts to schedule a call during which Customer will conduct an acceptance test to confirm that the Unlimited Subscription Service is configured in accordance with Customer’s preferences after activation and to verify the operation of the Unlimited Subscription Service (“**Customer Confirmation of Unlimited Subscription Service**”). If Comcast’s attempts to schedule a call are unsuccessful, Comcast shall automatically activate the Unlimited Subscription Service unless and until Customer contacts Comcast and requests that Comcast deactivate the Unlimited Subscription Service. Customer acknowledges and agrees that without Customer Confirmation of Unlimited Subscription Service, Comcast may (i) be unable to prevent DDoS attack traffic from reaching the Service Location and (ii) block legitimate traffic from reaching the Service Location.
- B. Comcast monitors the Customer network traffic and will automatically detect DDoS attack traffic at the closest Comcast network edge router using filtering rules. If Comcast detects high severity DDoS attack traffic, as defined by Comcast, (a “**High Severity Attack**”) after applying such filtering rules, Comcast will send an alert to Customer notifying them that the Service detected a DDoS attack.
- C. During DDoS attack mitigation, Comcast will leverage Border Gateway Protocol (BGP) to route any traffic that is not filtered at the network edge router to a Comcast scrubbing center that filters malicious traffic and routes legitimate traffic back to Customer’s network. After mitigation terminates, Comcast delivers all traffic to Customer’s network via normal routes.
- D. Customer has a choice of “On-Demand” or “Automatic” mitigation options, which are described below, under the Unlimited Subscription Service. Automatic mitigation is the default option and will apply unless Customer selects the On-Demand option. Such mitigation options are selected and applied on a per circuit basis.
  - a. On-Demand. Customer must authorize Comcast to initiate mitigation through the Portal or by contacting the Comcast Security Assurance Team at 877-215-5529. Once Customer authorizes Comcast to initiate mitigation for a particular circuit, such circuit converts to an Automatic circuit only during the Mitigation Incident (as defined herein) such that High Severity Attacks are mitigated automatically without Customer intervention. Upon expiration of the Mitigation Incident, the circuit reverts to On-Demand. Time to mitigate (the “**Mitigation Interval**”) is the elapsed time from when the Customer authorizes Comcast to enable mitigation until Comcast initiates mitigation of any attack traffic. Mitigation of a particular attack ceases when Comcast no longer detects such attack traffic. With respect to On-Demand, a “**Mitigation Incident**” is defined as one (1) twelve-hour (12) hour window in which Comcast provides

Customer with DDoS mitigation assistance as set forth above regardless of whether Comcast provides such assistance for the full twelve (12) hours or less than twelve (12) hours. Customer acknowledges and agrees that Comcast will discontinue mitigation efforts upon the expiration of each Mitigation Incident unless instructed by Customer to continue mitigation efforts, which Customers may do through the Portal or by contacting the Comcast Security Assurance Team at 877-215-5529.

- b. Automatic. The Automatic mitigation option mitigates High Severity Attacks automatically without Customer intervention following the detection of attack traffic that exceeds pre-set thresholds. The Mitigation Interval is the elapsed time from when Comcast detects a High Severity attack to when Comcast initiates mitigation of attack traffic. Mitigation ceases when attack traffic is no longer detected.

## 2. Off-Net DDoS Mitigation Service (“Off-Net Service”)

- A. The Off-Net Service is a subscription-based service that provides Customer with proactive network detection of DDoS attack traffic, alert notifications, mitigation of attacks, and online reporting for non-Comcast circuits. For purposes of this Agreement, “Off-Net” means one or more multihomed internet circuits that carry internet service to the same Service Location as the Unlimited Subscription Service, and which use an internet back bone provided by a third-party service provider that is not Comcast. Upon receipt of complete and accurate Customer contact and network information, Comcast will configure Customer’s site(s), related IP addresses, and countermeasure options. Following Comcast’s completion of such configuration, Comcast shall make three (3) attempts to schedule a call during which Customer will conduct an acceptance test to confirm that the Off-Net Service is configured in accordance with Customer’s preferences after activation and to verify the operation of the Off-Net Service (“**Customer Confirmation of Off-Net Service**”). If Comcast’s attempts to schedule a call are unsuccessful, Comcast shall automatically activate the Off-Net Service unless Customer contacts Comcast and requests that Comcast deactivate the Off-Net Service. Customer acknowledges and agrees that without Customer Confirmation of Off-Net Service, Comcast may (i) be unable to prevent DDoS attack traffic from reaching the Service Location and (ii) block legitimate traffic from reaching the Service Location.
- B. Customers subscribing to the Off-Net Service must also have an Unlimited Subscription Service at the same Service Location. The Off-Net Service requires a Comcast EDI Underlay Service at the same Service Location that meets the Bandwidth Requirement.
- C. The Off-Net Service requires a router at the Service Location configured to Comcast specifications.
- D. The Off-Net Service will be configured based on the Automatic mitigation option described in Section 1(D) above. The On-Demand mitigation option is not available for the Off-Net Service.
- E. Customer acknowledges and agrees that credit allowances as described in Schedule A-2 shall not be applicable to the Off-Net Service.

## 3. Emergency DDoS Mitigation Service (“Emergency Service”)

- A. The Emergency Service is available only on an On-Net basis and is available for Service Locations for which Customer does not have an Unlimited Subscription Service.
- B. Upon notification of suspicious traffic from Customer, Comcast will analyze traffic for anomaly detection and patterns to determine whether the business is under a DDoS attack. In performing this analysis, Comcast will gather the appropriate network information (e.g., routable IP addresses). When authorized by Customer via the execution of a Sales Order, which will include relevant fees, Comcast will monitor Customer’s incoming Internet traffic to detect and filter malicious traffic matching specific DDoS attack vectors and route legitimate traffic to Customer’s network.
- C. For Customers receiving the Emergency Service, applicable charges shall apply with respect to each Mitigation Incident. With respect to Emergency Services, a “**Mitigation Incident**” is defined as one (1) seventy-two (72) hour window in which Comcast provides Customer with DDoS mitigation assistance as set forth above regardless of whether Comcast provides such assistance for the full seventy-two (72) hours or less than seventy-two (72) hours. Customer acknowledges and agrees that Comcast will discontinue mitigation efforts upon the expiration of each Mitigation Incident unless instructed by Customer to continue

mitigation efforts, which Customers may do through the Portal or by contacting the Comcast Security Assurance Team at 877-215-5529. Each seventy-two (72) hour period in which Comcast provides mitigation assistance shall constitute a separate Mitigation Incident subject to additional charges; provided, however, that if Customer purchases an Unlimited Subscription Service for the applicable Service Location prior to the expiration of the Mitigation Incident, then Customer will not be charged for additional Mitigation Incidents. For illustrative purposes only, if Comcast provides mitigation assistance (i) for seventy-two (72) or fewer hours, there will have been one (1) Mitigation Incident, (ii) for one hundred (100) hours, there will have been two (2) Mitigation Incidents and (iii) for one hundred fifty (150) hours, there will have been three (3) Mitigation Incidents.

#### **4. Incident-Based Subscription DDoS Mitigation Service (“Incident-Based Subscription Service”)**

- A. Incident-Based Subscription Services are available only to Customers that currently have an active subscription to the Incident-Based Subscription Service (each such Customer, a “**Legacy Customer**”). The following terms will apply only to Legacy Customers.
- B. The Incident-Based Subscription Service is a subscription-based Service offering that provides Legacy Customers with proactive network detection of DDoS attack traffic, alert notifications, and mitigation of attacks. Upon receipt of complete and accurate Legacy Customer contact and network information, Comcast will configure Legacy Customer’s site(s), related IP addresses, and countermeasure options. Following Comcast’s completion of such configuration, the parties will conduct an on-boarding call during which Legacy Customer will conduct an acceptance test to confirm that the Incident-Based Subscription Service is configured in accordance with Legacy Customer’s preferences after activation and to verify the operation of Incident-Based Service.
- C. Comcast monitors the Legacy Customer network traffic and will automatically drop or rate limit Layer 3 and Layer 4 traffic at the closest network edge router using filtering rules. If Comcast detects High Severity Attack traffic after applying such filtering rules, an alert will be sent to the Legacy Customer notifying Legacy Customer that mitigation is required. Legacy Customer must authorize Comcast by phone or as otherwise determined by Comcast to initiate mitigation (i.e., On-Demand) and the Mitigation Interval shall be the elapsed time from when the Legacy Customer authorizes Comcast to enable mitigation until Comcast initiates mitigation of any attack traffic. Comcast will continue its mitigation efforts with respect to a particular attack until the earlier of the time such attack traffic is no longer detected or Comcast is instructed by Customer to terminate mitigation. During the mitigation, Comcast will leverage BGP to route any traffic that is not filtered to Comcast scrubbing centers where malicious traffic will be filtered and legitimate traffic will be routed back to Legacy Customer’s network. After mitigation ends, Comcast will deliver all traffic to Legacy Customer’s network via normal routes.
- D. For those Legacy Customers receiving the Incident-Based Subscription Service, additional charges (in addition to the monthly recurring charges (MRC)) shall apply with respect to each Mitigation Incident. With respect to the Incident-Based Subscription Service, a “**Mitigation Incident**” is defined as one (1) twelve-hour (12) hour window in which Comcast provides Legacy Customer with DDoS mitigation assistance as set forth above regardless of whether Comcast provides such assistance for the full twelve (12) hours or less than twelve (12) hours. Legacy Customer acknowledges and agrees that Comcast will discontinue mitigation efforts upon the expiration of each Mitigation Incident unless instructed by Legacy Customer to continue mitigation efforts, which Legacy Customers may do by contacting the Comcast Security Assurance Team at 877-215-5529 or as otherwise instructed by Comcast. Each twelve (12) hour period in which Comcast provides mitigation assistance shall constitute a separate Mitigation Incident subject to additional charges. For illustrative purposes only, if Comcast provides mitigation assistance (i) for twelve (12) or fewer hours, there will have been one (1) Mitigation Incident, (ii) for fifteen (15) hours, there will have been two (2) Mitigation Incidents and (iii) for twenty-five (25) hours, there will have been three (3) Mitigation Incidents.

**II. Service Management.** Certain settings and configurations are applied and managed on a per circuit basis, not at the Service Location level. Customer shall be responsible for setting up and maintaining an account within the Portal, including setting up a primary user and secondary users with appropriate privileges, such as administrator or read-only.

**III. Disclaimer.** Customer acknowledges the following additional terms for the Services:

- A. When Customer Internet traffic is traversing Comcast mitigation platform, Comcast makes no guarantees that only DDoS attack traffic will be prevented from reaching the Service Location nor that only legitimate traffic will be allowed to reach Customer.

- B. Comcast mitigation constitutes only one component of Customer's overall security program and is not a comprehensive security solution; instead, the DDoS Mitigation Service is intended to mitigate the impacts of certain types of DDoS attacks that are already underway.
- C. Comcast makes no warranty, express or implied, that: (i) all DDoS attacks will be detected (for Customers receiving a Subscription Service (as defined in Schedule A-2)); (ii) the mitigation efforts implemented by Comcast in response to such DDoS attacks will be successful in mitigating the overall impact of the incident; or (iii) or that Comcast detection, alerting, and/or mitigation (a) will be uninterrupted or error-free or (b) will not inadvertently block non-malicious traffic. Customer also understands that there may be volumetric-based attacks that exceed the amount of traffic volume that Comcast can successfully divert.
- D. Comcast's ability to provide the DDoS Mitigation Services is contingent on (i) Customer providing accurate and timely information to Comcast, including the provision of IP addresses and a list of trusted applications and sites (ii) Customer provided equipment and software (including Customer-Provided Equipment) being compatible with the Service as determined by Comcast in its sole discretion (*e.g.*, Comcast will not be able to provide a 3GB DDoS Mitigation Service if Customer has a 1GB Firewall).

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
DDoS MITIGATION SERVICES**

**SCHEDULE A-2  
SERVICE LEVEL AGREEMENT**

Except for the Off-Net Service, the Services are backed by the following Service Level Agreement (“SLA”):

**A. Definitions**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the DDoS Mitigation Services PSA or the General Terms and Conditions.

“**Subscription Service**” means, as applicable, the Unlimited Subscription Service or Incident-Based Subscription Service.

**B. DDoS Mitigation Services - Service Level Agreement**

Service	Mitigation Option	Mitigation Interval	Remedy
Emergency Service	N/A	Less than or equal to 60 minutes	No Credit
		Greater than 60 minutes	Account Credit = one (1) day of Daily Mitigation fee
Unlimited Subscription Service	On-Demand	Less than or equal to 15 minutes from Customer authorization*	No Credit
		Greater than 15 minutes from Customer authorization*	Account Credit = 1/30 of MRC
	Automatic	Less than or equal to 5 minutes from discovery of attack traffic**	No Credit
		Greater than 5 minutes from discovery of attack traffic**	Account Credit = 1/30 of MRC
Incident-Based Subscription Service	On-Demand	Less than or equal to 15 minutes from Customer authorization*	No Credit
		Greater than 15 minutes from Customer authorization*	Account Credit = 1/30 of MRC

\*Comcast will notify Customer of any High Severity DDoS Attacks targeting their protected IP addresses. To commence On-Demand mitigation, Customer must authorize incident mitigation through the Portal or by contacting the Comcast Security Assurance Team at 877-215-5529. Upon Customer’s authorization for incident mitigation, the “**Mitigation Interval**” will commence.

\*\*Upon Comcast’s detection of a high severity Internet traffic incident, the Mitigation Interval will commence.

Customer shall be entitled to up to one credit per day and, for any billing month, Credits may not exceed fifty percent (50%) of the total monthly recurring charge (“**MRC**”), or in the case of Emergency Service total daily mitigation fees charged in the applicable month, of the applicable Subscription Service.

In order to receive a Credit for Comcast’s failure to meet the SLA detailed above, Customer must open a trouble ticket with Comcast. Customer must request a credit within thirty (30) days following the completion of the Mitigation Interval.

**C. Exceptions and Terms applicable to all SLAs**

**1. Emergency Blocking**

The parties agree that if either party hereto, in its reasonable and sole discretion, determines that an emergency action is necessary to protect its own network, the Party may, after engaging in reasonable and good faith efforts to notify the other party of the need to block, block any transmission path over its network by the other party where transmissions do not meet material standard industry

requirements. The parties further agree that none of their respective obligations to one another under the Agreement will be affected by any such blockage except that the party affected by such blockage will be relieved of all obligations to make payments for charges relating to the circuit(s) which is so blocked and that no party will have any obligation to the other party for any claim, judgment or liability resulting from such blockage.

## **2. Remedy Processes**

All claims and rights arising under this Service Level Agreement must be exercised by Customer in writing within thirty (30) days of the conclusion of the applicable Mitigation Interval. The Customer must submit the following information to the Customer's Comcast account representative with any and all claims for credit allowances: (a) Organization name; (b) Customer account number; and (c) basis of credit allowance claim (including date and time, if applicable). Comcast will acknowledge and review all claims promptly and will inform the Customer by electronic mail or other correspondence whether a credit allowance will be issued, or the claim rejected, with the reasons specified for the rejection.

## **3. Exceptions to Credit Allowances**

Comcast failure to meet the service objectives or the Mitigation Intervals shall not qualify for the remedies set forth herein if such failures related to, associated with, or caused by: scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment (including Customer-Provided Equipment); any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers, any power, equipment or services provided by third parties; or an event of force majeure as defined in the Agreement.

## **4. Other Limitations**

The remedies set forth in this Service Level Agreement shall be Customer's sole and exclusive remedies for any service interruption, liability, outage, unavailability, delay, or other degradation, or any Comcast failure to meet the service objectives and Mitigation Intervals.

**/END OF DDoS PSA. VIDEO PSA BEGINS ON NEXT PAGE/**

**COMCAST ENTERPRISE SERVICES  
PRODUCT SPECIFIC ATTACHMENT  
BUSINESS VIDEO SERVICE**

**ATTACHMENT IDENTIFIER: Business Video**

The following additional terms and conditions are applicable to Comcast's Business Video Services ordered under an Enterprise Services Master Service Agreement ("Agreement"):

**DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Enterprise Services General Terms and Conditions ("General Terms and Conditions").

**"Estimated Availability Date"** means the target date for delivery of Service.

**"Service"** means Comcast Business private view commercial cable television services ("Private View Video"), public view commercial cable television services ("Public View Video") and Hospitality cable television services ("Hospitality Video"), (Private View Video, Public View Video and Hospitality Video, collectively "Business Video Service(s)"). Subject to service availability, Customer may order Business Video Service for use at Service Locations within Comcast's service areas.

**ARTICLE 1. SERVICES**

This attachment shall apply to Business Video Service offered under the Agreement.

**ARTICLE 2. PROVIDER**

Business Video Service shall be provided by the operating company subsidiary of Comcast Corporation that owns and/or operates the cable television system in the applicable service area.

**ARTICLE 3. CUSTOM INSTALLATION FEE**

Once Comcast accepts a Sales Order for Business Video Service, Comcast will invoice Customer for any and all Custom Installation Fee(s) unless otherwise specified on the Sales Order. Customer will pay the Custom Installation Fee(s) within thirty (30) days of the invoice date unless a payment schedule is specified in the applicable Sales Order.

**ARTICLE 4. PROVISIONING INTERVAL**

Following its acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date(s) applicable to the ordered Business Video Service(s). Comcast shall use commercially reasonable efforts to provision the Business Video Service(s) on or before the Estimated Availability Date(s); provided, however, that Comcast's failure to provision by said date shall not constitute a breach of the Agreement.

**ARTICLE 5. SERVICE COMMENCEMENT DATE**

The Service Commencement Date shall be the date(s) Comcast completes installation and connection of the necessary facilities and equipment to provide the Business Video Service at a Service Location. Comcast will consider the Service installation completed if Comcast has delivered Service, regardless of whether Customer refuses or fails to be ready to receive the Service.

A single Sales Order containing multiple Service Locations may have multiple Service Commencement Dates. Any failure or refusal on the part of Customer to be ready to receive the Business Video Service on the Service Commencement Date shall not relieve Customer of its obligation to pay applicable service charges and may be treated as a termination for cause by Customer as provided under Article 5 of the General Terms and Conditions of the Agreement.

**ARTICLE 6. RESERVED**

**ARTICLE 7. USE**

Subject to the terms and conditions herein, Business Video Services are intended for commercial use only. Customer is prohibited from reselling Business Video Services.

**ARTICLE 8. SERVICE CREDITS**

**8.1 Credit Allowances.** Comcast will allow a pro-rata credit against future payment of the net monthly recurring charge (exclusive of nonrecurring charges, other one-time charges, per call charges, measured charges, regulatory fees and surcharges, taxes, and other governmental and quasi-governmental fees) for a Service Interruption, except as specified below or as may otherwise be legally required ("Credit"). "Service Interruption" shall mean a break in transmission that renders the Business Video Service unusable for transmission and reception. For the purposes of calculating a Credit allowance, the Service Interruption period begins when the Customer reports an interruption in the portion of the Business Video Service to Comcast and a trouble ticket is opened. The Service Interruption ends when the affected portion of the Business Video Service has been restored and Comcast has closed the trouble ticket. Service Interruption time does not include interruptions of less than thirty (30) minutes' duration. Credits will be as follows:

<u>Length of Service Interruption</u>	<u>Amount of Credit</u>
At least 4 hours and up to and including 24 hours	1 full day

The total number of credit allowances per month shall not exceed the total monthly recurring charge for the affected Business Video Service. Credit allowances will not be made for less than \$1.00, unless required under applicable law. To qualify, Customer must request the Credit from Comcast within 30 days of the Service Interruption.

**8.2 Exceptions to Credit Allowances.** Except as otherwise provided in the General Terms and Conditions, a Service Interruption shall not qualify for the Credits set forth herein if the Service Interruption is related to, associated with, or caused by: scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment; any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers; any power, equipment or services provided by third parties; or an event of force majeure as defined in this Agreement, unless otherwise provided under applicable law. The remedies set forth in this Article 8 shall be Customer's sole and exclusive remedy for any Service Interruption in the Business Video Services, outage, unavailability, delay or other degradation in the Business Video Service or any Comcast failure to meet the objectives of the Business Video Service.

**ARTICLE 9: LIMITATION OF SERVICE**

**9.1 Redistribution Limitation.** Customer hereby acknowledges and agrees that Comcast does not have the absolute right to distribute pay-per-view video programming (including programming such as sporting events) and certain premium video services to commercial establishments. Therefore, Customer agrees that it shall not exhibit nor assist in the exhibition of any such programming unless explicitly authorized to do so, in advance and in writing, by Comcast and the applicable program or event distributor. In requesting such explicit authorization, Customer agrees to identify itself as a commercial establishment. Customer shall not, and shall not authorize or permit any other person to, and shall take all reasonable measures to prevent (e.g. encryption) (i) copy, record, dub, duplicate, alter or make or manufacture any recordings or other reproductions of Business Video Service (or any part thereof); (ii) transmit Business Video Service (or any part thereof) by any television or radio broadcast or by any other means or use Business Video Service (or any part thereof) outside of the Service Locations(s). Customer acknowledges that such duplication or reproduction may subject Customer to criminal penalties under applicable copyright and/or trademark laws. Customer agrees to not move any Comcast Equipment from another

location to any Service Location, or from any Service Location to any other location. Customer further agrees not to undertake any activity related to the unauthorized reception of the Business Video Service at any Service Locations.

**9.2 Additional Licenses.** Customer shall not, and shall not authorize or permit any other person to (i) charge a cover charge or admission fee to the Service Location(s) at the time Business Video Service (or any part thereof) is being or is to be performed therein; (ii) permit dancing, skating or other similar forms of entertainment or physical activity in conjunction with the performance of Business Video Service (or any part thereof) unless Customer has obtained all necessary licenses and authorizations from the applicable copyright owners (Customer acknowledges and agrees that it shall be solely responsible for the payment of any charges or fees in connection therewith); or (iii) insert any commercial announcements into Business Video Service, or interrupt any performance of Business Video Service for the making of any commercial announcements, except that public address commercial announcements may be made concerning goods or services sold or offered to the public at the Service Location provided that no compensation (whether in money or in any other form) is paid by any person or entity, directly or indirectly, for such announcements unless pursuant to a separate written agreement which permits store-casting or ad-casting. Customer acknowledges and understands Customer may be responsible for additional music licensing or copyright fees for music contained in any or all of the Services, including, but not limited to Business Video Service.

**9.3 Provision of Service.** Customer acknowledges and agrees that Comcast has the right at any time to preempt specific Business Video Service programs, without prior notice to Customer, and to determine what substitute programming, if any, shall be made available. Comcast may in its discretion make additions, deletions or modifications to its Business Video Service channel line-ups without liability to Customer or anyone claiming through Customer. Comcast shall not be liable for failure to deliver any Business Video Service programming, which is caused, by the failure of the programmer to deliver or make such programming available to Comcast or any other reason beyond the reasonable control of Comcast.

(a) **Private View Video.** Private View Video, including without limitation HD DVR service, is for private commercial viewing venues only, and is not for use in public viewing areas such as bars, restaurants, fitness centers or at residential addresses.

(b) **Public View Video.** Public View Video is for use in commercial, public viewing areas such as bars and restaurants. In the event Comcast makes a material change to the Public View Video channel lineup, Customer will have thirty (30) days from the date of the material channel lineup change to cancel Public View Video Service without further liability beyond the termination date. Should Customer fail to cancel within this timeframe, Customer will be deemed to have accepted the modified Public View Video channel lineup. Comcast shall not be liable for failure to deliver any programming, which is caused, by the failure of the programmer to deliver or make such programming available to Comcast or any other reason beyond the reasonable control of Comcast.

(c) **Hospitality Video.** Hospitality Video is for hospitality in-room guest use at the Service Location(s) (each a "Customer Guest") only and is not for use, and should not be made available to any Customer Guest, in private commercial viewing venues, public viewing areas or at residential addresses. Comcast shall provide Hospitality Video Service to a demarcation point at the Service Location. Customer shall be responsible for any and all facilities, equipment and/or devices required to use Hospitality Video on the Customer-side of the demarcation point, and depending on the configuration of the Customer-side Service Location infrastructure, certain components of the Hospitality Video may be unavailable. Notwithstanding Customer's use of facilities, equipment and/or devices on

the Customer-side of the demarcation point, Customer shall comply with all obligations and restrictions regarding Business Video Service and Hospitality Video contained in this Agreement. Notwithstanding anything to the contrary contained herein, Customer may offer Hospitality Video at the Service Location(s) to its hospitality guests.

**9.4 Additional Sets.** Customer agrees not to add additional sets or disturb, alter or remove any portion of the Comcast Equipment. Any unauthorized connection or other tampering with Business Video Service or Comcast Equipment shall be cause for disconnection of the applicable Business Video Service, legal action and Comcast shall be entitled to recover damages, including, but not limited to, the value of any Business Video Service illegally obtained plus reasonable collection costs including reasonable attorney's fees.

**9.5 Installation of Advanced Comcast Equipment.** In the event Comcast agrees to install certain advanced Comcast Equipment (i.e. Q2Q devices), Customer acknowledges that Business Video Service will be delivered to the demarcation point at the Service Location(s). Customer shall be responsible for any and all facilities, equipment and/or devices required to use Business Video Service on the Customer-side of the demarcation point, and depending on the configuration of the Customer-side Service Location infrastructure, certain components of the Business Video Service may be unavailable. Notwithstanding Customer's use of facilities, equipment and/or devices on the Customer-side of the demarcation point, Customer shall comply with all obligations and restrictions regarding Business Video Service contained in the Agreement.

#### **ARTICLE 10: BUSINESS VIDEO SERVICE INDEMNIFICATION**

In addition to the indemnification obligations contained elsewhere in the Agreement, Customers using Business Video Service agree to indemnify and hold Comcast harmless from any and all demands, claims, suits, costs of defense, reasonable attorney's fees, witness fees and other expenses for claims relating to or resulting from the unauthorized distribution and/or exhibition of the Business Video Service, including without limitation, pay-per-view video programming and premium video services.

#### **ARTICLE 11: STATE-SPECIFIC PROVISIONS APPLICABLE TO BUSINESS VIDEO SERVICE**

**11.1 Disruption of Service.** Notwithstanding the terms of the Agreement, the following service interruption credits will apply to qualifying Customers:

(a) **Connecticut Customers.** In the event of an interruption of Business Video Service of more than twenty-four (24) consecutive hours and of which Comcast has received actual notice, a credit will be issued towards Customer's Business Video Service monthly service charge for the length of time such Business Video Service was interrupted.

(b) **New York Customers.** In the event of an interruption of Business Video Service for at least four (4) hours between 6:00pm and 12:00am, except for emergency notice events, a credit equal to one day will be issued towards Customer's Business Video Service monthly service charge. If Customer's Business Video Service is interrupted for less than four (4) hours or outside of the hours of 6:00pm and 12:00am, please call 1-860-827-2622 to request a credit.

(c) **Vermont Customers.** In the event of an interruption of Business Video Service for more than twenty-four consecutive hours and of which Comcast has received actual notice, a credit will be issued towards Customer's Business Video Service monthly service charge for the total period of the interruption in an amount proportionate to Customer's regular monthly service charge. If Comcast has not been made aware of the interruption, Customer must call 1-860-827-2622 to request a credit.

**11.2 Regulatory Contact Information.** Customer may contact the Comcast corporate offices at One Comcast Center, 1701 JFK Blvd., Philadelphia, PA 19103 with concerns and complaints.

(a) **Connecticut Customers.** If Comcast is unable to resolve Customer's problem, Customer may contact the Connecticut Department of Utility Control at 1-800-382-4586 (toll free within Connecticut) or 1-860-827-2622 (outside Connecticut) or TDD 1-860-827-2837.

(b) **Maine and New Hampshire Customers.** The Office of the Attorney General Consumer Protection and Antitrust Bureau has the authority to enforce Consumer Protection laws and provide assistance in the mediation of consumer complaints. Customers should file written complaints concerning any alleged misrepresentations and unfair and deceptive practices of a cable company to:

Maine – Office of the Attorney General, Department of Consumer Fraud and Antitrust, State House Station #6, Augusta, ME 04333.

New Hampshire – Office of the Attorney General, Department of Consumer Fraud and Antitrust, 25 Capital Street, Concord, NH 03301.

(c) **Maryland Customers.**

(i) **Montgomery County, MD Customers.** Under its franchise with Montgomery County, Comcast has the following rebate policy: In the event of a Business Video Service interruption (loss of picture or sound of one or more channels to any customer) Comcast shall repair the interruption as soon as possible. This obligation is satisfied if Comcast offers Customer the next available repair appointment within the 24-hour period following the interruption, or at Customer's request, to a mutually convenient later time for the repair call, and successfully repairs the interruption during the agreed upon appointment. If the Business Video Service interruption is not repaired at the time of the scheduled appointment, Customer will receive a credit equal to 10% of for the Business Video Service monthly recurring charge for each 24-hour period, or segment thereof that the Business Video Service interruption continues beyond the scheduled repair call. Customers may contact Comcast at (301) 424-4400.

(ii) **Prince Georges County, MD Customers.** In the event of a Business Video Service interruption (loss of picture or sound of one or more channel to any customer) lasting between two (2) and six (6) hours, Customer shall be entitled upon request, to a pro-rata credit for such Business Video Service interruption. In the event of a Business Video Service interruption lasting between six (6) and twenty-four (24) consecutive hours, Customer shall be entitled to a pro-rata credit equal to one day of Customer's monthly Business Video Service charge.

(d) **Massachusetts Customers.** If Comcast is unable to resolve Customer's problem, Customer may contact its local franchise authority: the Consumer Division of the Department of Telecommunications and Energy toll free at 1-800-392-6066 or write to the DTE at One South Station, Boston, MA 02110.

(e) **New York Customers.** If Comcast is unable to resolve Customer's problem, Customer may their local government or call the New York State Public Service Commission (PSC) at 1-800-342-3377, or write to: Customer Service Representative, New York State Public Service Commission, Office of Customer Service, Three Empire State Plaza, Albany, NY 12223-1350.

(f) **Vermont Customers.** The Vermont Department of Public Service can provide assistance in the resolution of consumer complaints. Customers should file complaints with the Customer Hotline at 1-800-622-4496.

**11.3 Billing Questions.** Notwithstanding the terms of the Agreement, the following billing question provisions will apply to qualifying Customers:

(a) **Sacramento, CA Customers.** If there are any billing errors or other requests for credit, Customer must inform Comcast within sixty (60) days of the time Customer receives the disputed bill, unless applicable law provides for a longer period which cannot be waived or otherwise modified. Comcast will investigate and respond to all billing complaints within five (5) business days of the receipt of the

complaint. In some cases, an investigation might require a search of historical records that could take up to fourteen (14) business days. If Customer believes a payment was made which was not credited to Customer's account, a copy of a cancelled check or money order may be required and the disputed amount will be set aside for up to fourteen (14) days while Customer gather that documentation.

**11.4 Access to Customer's Premises, Credit for Missed Appointments.** Notwithstanding the terms of the Agreement, the following credit for missed appointment provisions will apply to qualifying Customers:

(a) **West Bay and San Francisco, CA Customers.** If Comcast fails to keep a scheduled Business Video Service appointment, Comcast will credit Customer's account with either free installation or a service call free of charge if the appointment was for an installation or service call for which a fee was to be charged, or a minimum credit of \$20.

(b) **Sacramento, CA Customers.** If Comcast fails to keep a scheduled Business Video Service appointment, Comcast will credit Customer's account with one (1) month of limited commercial basic up to a maximum credit equal to one month of the standard commercial cable price.

**11.5 Remedies for Late Payment/Non-Payment.** Notwithstanding the terms of the Agreement, the following late payment/nonpayment fees will apply to qualifying Customers:

(a) **Maryland Customers.** If Customer fails to make any required payment for Business Video Service by the payment due date or pays less than the full amount due for such Business Video Service, Comcast may bill fees, charges and assessments related to late payments or non-payments.

(1) EACH MARYLAND CUSTOMER WILL BE ASSESSED A LATE FEE OF \$5.00 PER MONTH FOR EACH BUSINESS VIDEO SERVICE ACCOUNT THAT HAS NOT BEEN PAID IN FULL AFTER 45 DAYS FROM THE DATE THE INVOICE WAS SENT.

(2) **Montgomery County, MD Customers Only.** CUSTOMER WILL BE ASSESSED A LATE FEE OF \$4.00 PER MONTH FOR EACH BUSINESS VIDEO SERVICE ACCOUNT THAT HAS NOT BEEN PAID IN FULL AFTER 45 DAYS FROM THE DATE THE INVOICE WAS SENT.

**11.6 Provisions specific to Prince Georges County, MD Business Video Service Customers.** Notwithstanding the terms of the Agreement, the following provisions will apply to qualifying Customers

(a) **Deposits.** If Comcast disconnects Customer's Business Video Service or is otherwise required under applicable law to a refund of any deposit, Comcast shall within thirty (30) days or Customer's next billing cycle, whichever is earlier, return a sum equal to the deposit(s) Customer paid (without interest unless otherwise required by law) minus any amounts due on Customer's account (including without limitation, any amounts owed for Business Video Service or for any Comcast Equipment that is damaged, altered, or not returned).

(b) **Termination of Business Video Service by Customer.** All applicable fees and charges will accrue until the termination of the Agreement or the date Customer requests the Business Video Service be disconnected, whichever is earlier.

## **ARTICLE 12: CHARGES**

Comcast may modify the charges for Business Video Service subject to thirty (30) days prior notice to Customer. Customer will have thirty (30) days from receipt of such notice to cancel the affected Business Video Service

without further liability beyond the termination date. Should Customer fail to cancel within this timeframe, Customer will be deemed to have accepted the modified Business Video Service pricing.

### **ARTICLE 13: BUSINESS VIDEO SERVICE STREAMING**

To the extent Comcast provides Customer with the ability to stream the Business Video Services, Customer acknowledges and agrees that (i) such streaming functionality may only be used by Customer's employees at the applicable Service Location(s) on Approved Devices, (ii) Customer may register up to four hundred (400) Approved Devices; provided, that, the Business Video Services may be streamed on no more than five (5) such devices at any given time, (iii) the streamed video shall be used solely for private viewing purposes and shall not be displayed for public viewing (either in whole or in part), including, but not limited to, in any common areas and/or conference rooms and (iv) Customer shall not, and shall cause its employees not to, (A) stream, display or transmit the Business Video Services outside of the applicable Service Location(s) or (B) distribute the Business Video Services from the Customer-side of the demarcation point via a virtual private network. The following are "Approved Devices" (unless Comcast notifies Customer otherwise): (I) a PC or Apple laptop or desktop computer and (II) a tablet and/or smart phone with an iOS or Android operating system.

### **ARTICLE 14: ADDITIONAL TERMS APPLICABLE TO HOSPITALITY VIDEO**

#### **14.1 Resetting of X1 TV Boxes**

(a) Customer acknowledges that unless the X1 TV Boxes used by a Customer Guest are reset to their X1 default settings, certain activity of, information provided by, and/or content accessed by, such Customer Guest in connection with its use of the Hospitality Video Service may be viewable and/or accessible by subsequent Customer Guests that are provided with access to such X1 TV Boxes. Customer shall be solely responsible for resetting any X1 TV Boxes used by a Customer Guest to their X1 default settings and Comcast shall have no obligation to reset any such X1 TV Boxes.

(b) If the Hospitality Video Services provided to Customer pursuant to this Agreement enables a Customer Guest to access certain content upon the provision of personal information (e.g., Netflix, YouTube, etc.), including, but not limited to, by way of providing login information such as a username and/or passwords, then upon, or as soon as reasonably possible after, check-out by a Customer Guest, any X1 TV Box to which such Customer Guest had access shall be reset by Customer to its X1 default settings; provided, that, Customer shall, in all events, reset any such X1 TV Box prior to the time that another Customer Guest is provided with access thereto.

(c) CUSTOMER ACKNOWLEDGES AND AGREES THAT NEITHER COMCAST NOR ITS ASSOCIATED PARTIES WILL BE LIABLE FOR ANY FAILURE TO RESET ANY X1 TV BOX. CUSTOMER AGREES TO DEFEND, INDEMNIFY, AND HOLD HARMLESS COMCAST AND ITS ASSOCIATED PARTIES FROM ANY AND ALL CLAIMS, LOSSES, DAMAGES, FINES, PENALTIES, COSTS, AND EXPENSES (INCLUDING, BUT NOT LIMITED TO, REASONABLE ATTORNEY FEES) THAT COMCAST AND/OR ITS ASSOCIATED PARTIES MAY INCUR, INCLUDING ANY SUCH LOSSES, DAMAGES, FINES, PENALTIES, COST AND/OR EXPENSES COMCAST AND/OR ITS ASSOCIATED PARTIES MAY INCUR IN AN ACTION BROUGHT BY OR ON BEHALF OF A THIRD PARTY (INCLUDING, BUT NOT LIMITED TO, ANY CUSTOMER GUEST), ARISING OUT OF, OR RELATING TO, (I) THE RESETTING OF, OR THE FAILURE TO RESET, ANY X1 TV BOX USED BY, OR MADE AVAILABLE TO, A CUSTOMER GUEST AND/OR (II) CUSTOMER'S BREACH OF ARTICLE 14.1(B).

## 14.2 Netflix Services

(a) This Article 14.2 applies to the extent Customer's Hospitality Video Service includes access to the Netflix Services. "Netflix Services" means the Netflix subscription service which will be accessible via the use of an application available on the Comcast Equipment used to deliver the Hospitality Video Service.

(b) Customer shall (i) place one remote control with a dedicated Netflix button, to be provided by Comcast, per set-top box or other Comcast Equipment through which the Netflix Services are available in each guest room in which the Hospitality Video Service is installed, including swapping out non-branded remote controls with remote controls featuring a dedicated Netflix button, and (ii) remove any Comcast remote controls from such guest rooms that do not have a dedicated Netflix button.

(c) In connection with the Hospitality Video Service, Comcast will provide a Property Management System (PMS) Integration application which will automatically clear viewing history and application account information on the in-room set-top boxes used by Customer Guests when such Customer Guests check-out ("Automatic Reset Function"). Customer acknowledges and agrees that in order for Comcast to provide the Automatic Reset Function, (i) Customer's PMS must be capable of, and be enabled to, send and receive the necessary data values which will allow Comcast to reset guest set-top boxes upon check-out and (ii) Customer will be required to provide a PMS interface (which may have to be obtained from Customer's PMS provider) which will allow Comcast to receive and send data to the Customer PMS in connection with performing the Automatic Reset Function (the "Customer PMS Requirements"). If Customer does not satisfy the Customer PMS Requirements, then, notwithstanding anything to the contrary contained in this Article 14.2, Comcast shall have no obligation to provide the Netflix Services or the Automatic Reset Function in connection with the Hospitality Video Services.

If at any time the Automatic Reset Function is not functioning (i.e., viewing history and application account information is not being cleared from the set-top boxes upon guest check-in/check-out), Comcast may notify Customer of the same. Upon receipt of such notice and until Comcast notifies Customer that the Automatic Reset Function is functioning, Customer shall be responsible for resetting the guest room set-top boxes in accordance with Article 14.1(b) and shall be liable to Comcast in accordance with Article 14.1(c) for any failure to do so.

(d) Customer acknowledges and agrees it is expressly prohibited from:

- (i) providing free Netflix subscriptions or house accounts to Customer Guests;
- (ii) displaying the Netflix Service in any public or common areas;
- (iii) charging Customer Guests an additional fee or other charge for the use of the Netflix Service; provided the foregoing does not prohibit Customer from billing and collecting standard room charges;
- (iv) using any Netflix trademarks, service marks or other Netflix intellectual property, or any marketing materials related to Netflix without Netflix's express written consent, except to the extent such are incorporated in the Netflix Services;
- (v) collecting data, in any manner whatsoever, about Customer Guest's usage related to the Netflix Services; or

(vi) disclosing or making available any usage data specific to the Netflix Services provided to Customer to any third party or the public generally.

(e) CUSTOMER ACKNOWLEDGES AND AGREES THAT NEITHER COMCAST NOR ITS ASSOCIATED PARTIES WILL BE LIABLE FOR ANY ISSUES RELATED TO THE NETFLIX SERVICE. CUSTOMER AGREES TO DEFEND, INDEMNIFY, AND HOLD HARMLESS COMCAST AND ITS ASSOCIATED PARTIES FROM ANY AND ALL CLAIMS, LOSSES, DAMAGES, FINES, PENALTIES, COSTS, AND EXPENSES (INCLUDING, BUT NOT LIMITED TO, REASONABLE ATTORNEY FEES) THAT COMCAST AND/OR ITS ASSOCIATED PARTIES MAY INCUR, INCLUDING ANY SUCH LOSSES, DAMAGES, FINES, PENALTIES, COST AND/OR EXPENSES COMCAST AND/OR ITS ASSOCIATED PARTIES MAY INCUR IN AN ACTION BROUGHT BY OR ON BEHALF OF A THIRD PARTY (INCLUDING, BUT NOT LIMITED TO, ANY CUSTOMER GUEST), ARISING OUT OF, OR RELATING TO, (I) CUSTOMER'S USE OF THE NETFLIX SERVICE AND/OR (II) CUSTOMER'S BREACH OF THIS ARTICLE 14.2.

**/END OF VIDEO PSA. WAVE INTRASTATE PSA BEGINS ON NEXT PAGE/**

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
INTRASTATE WAVELENGTH SERVICES**

The following additional terms and conditions are applicable to Sales Orders for Comcast Business Intrastate Wavelength Services. A further description of the Service is set forth in Schedule A-1 hereto.

**ARTICLE 1. DEFINITIONS**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

“**Estimated Availability Date**” means the target date for delivery of Service.

“**Services**” means Intrastate Wavelength Services.

**ARTICLE 2. SERVICES AND SERVICE AVAILABILITY**

This attachment shall apply to the Services, as defined herein. A further description of these Services is set forth in Schedule A-1 hereto which is incorporated herein by reference.

**ARTICLE 3. PROVIDER**

Service shall be provided by Comcast Business Communications, LLC or its applicable affiliates and subsidiaries.

Comcast may provide Customer with Service and fiber maps during the Term of the Agreement to further describe Service availability. Such maps are hereby deemed Comcast Confidential Information (as defined in the Agreement).

**ARTICLE 4. REGULATORY APPROVAL; TRAFFIC MIX**

Comcast’s pricing for Service may be subject to FCC,

public service commission or other regulatory approval. Further, Customer represents that its use of Service hereunder will be exclusively for the transmission of communications traffic that is classified as jurisdictionally intrastate under FCC rules and regulations. Customer specifically represents that ten percent (10%) or less of the traffic transmitted via the Service will be interstate. (For this purpose, Customer’s representation relates to the traffic carried over the Service rather than the locations of the physical endpoints of the facility over which the Service is delivered.) If at any time during the term of the Agreement or any Service Term, more than ten percent (10%) of the traffic transmitted via the Service is interstate, Customer shall immediately notify Comcast of the same in writing. Further, Comcast reserves the right, in its reasonable sole discretion, to reclassify Customer’s use of Service as jurisdictionally interstate or intrastate, as appropriate.

**ARTICLE 5. CUSTOM INSTALLATION FEES AND OTHER FEES**

Once Comcast accepts a Sales Order for Service, Comcast will invoice Customer for all Custom Installation Fee(s). Customer will pay the Custom Installation Fee(s) within thirty (30) calendar days of the invoice date unless a payment schedule is specified in the applicable Sales Order.

**ARTICLE 6. PROVISIONING INTERVAL**

Following its acceptance of a Sales Order, Comcast shall notify Customer of the Estimated Availability Date applicable to that Sales Order. Comcast shall use commercially reasonable efforts to provision the Service on or about the Estimated Availability Date; provided,

however, that Comcast's failure to provision the Service by the Estimated Availability Date shall not constitute a breach of the Agreement.

## **ARTICLE 7. SERVICE COMMENCEMENT DATE**

Comcast shall inform Customer when the Service is available and performing at the Service Location in accordance with the "Technical Specifications" set forth in Schedule A-1 hereto ("**Availability Notification**"). Charges for Service shall begin to accrue as of the Service Commencement Date. The Service Commencement Date shall be the earliest of: (A) the date on which Customer confirms receipt of and concurrence with the Availability Notification; (B) five (5) business days following the date of the Availability Notification, if Customer fails to notify Comcast that the Service does not comply materially with the Technical Specifications (as defined below); or (C) the date on which Customer first uses the Service. To the extent that a Service Term has not been expressly set forth in a Sales Order, the Service Term for such Sales Order shall be twelve (12) months.

## **ARTICLE 8. PORTABILITY; UPGRADES**

**8.1**     **RESERVED.**

**8.2**     **RESERVED.**

**8.3**     **RESERVED.**

**8.4**     **Portability.** Customer may terminate an existing Service (an "**Existing Service**") and turn up a replacement Service (*i.e.*, activate Service with termination points on Comcast's network that are different than those of the Existing Service) (a "**Replacement Service**") without incurring Termination Charges with respect to the Existing Service, provided that (a) the Replacement Service must have a Service Term equal to or greater than the remaining Service Term of the Existing Service but in no event less than twelve (12) months; (b) the Replacement Service must have monthly recurring charges equal to or greater than the monthly recurring charges for the Existing Service; (c) Customer submits a Sales Order to Comcast for the Replacement Service within ninety (90) days after

termination of the Existing Service and that Sales Order is accepted by Comcast; (d) Customer reimburses Comcast for any and all installation charges that were waived with respect to the Existing Service; and (e) Customer pays the actual costs incurred by Comcast in installing and provisioning the Replacement Service.

**8.5**     **Upgrades.** Customer may upgrade the speed of an Existing Service or convert an Unprotected Circuit to a Protected Circuit (as defined and further described in Schedule A-1 herein) (in each case, an "**Upgraded Service**") without incurring Termination Charges, provided that (A) the Upgraded Service must assume the remaining Service Term of the Existing Service, but in no event less than twelve (12) months; (B) the Upgraded Service must have the same points of termination on Comcast's Network as the Existing Service; (C) Customer submits a Sales Order to Comcast for the Upgraded Service and that Sales Order is accepted by Comcast; (D) Customer pays Comcast's applicable nonrecurring charges for the Upgraded Service; and (E) Customer agrees to pay the applicable monthly recurring charges for the Upgraded Service commencing with the Service Commencement Date for such Upgraded Service.

## **ARTICLE 9. ADDITIONAL INFORMATION**

As necessary for the interconnection of the Service with services provided by third parties, Comcast may request (as applicable), and Customer will provide to Comcast, circuit facility assignment information, firm order commitment information, and design layout records necessary to enable Comcast to make the necessary cross-connection between the Service and Customer's other service provider(s). Comcast may charge Customer nonrecurring and monthly recurring cross-connect charges to make such connections.

## **ARTICLE 10. TECHNICAL SPECIFICATIONS; SERVICE LEVEL AGREEMENT**

The technical specifications applicable to the Service are set forth in Schedule A-1 hereto ("**Technical Specifications**"). The service level agreement applicable to the Service is set forth in Schedule A-2 hereto and incorporated herein by reference.

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
INTRASTATE WAVELENGTH SERVICES**

**SCHEDULE A-1  
SERVICE DESCRIPTIONS AND TECHNICAL SPECIFICATIONS**

**Intrastate Wavelength Version 1.0**

Comcast's Intrastate Wavelength Services will be provided in accordance with the service descriptions and technical specifications set forth below:

**1. Service Descriptions.**

The Service is a private, dedicated, point-to-point transport service that provides secure, high-performance network connectivity between two (2) Service Locations to send and receive data by utilizing Dense Wavelength Division Multiplexing (DWDM) technology over Comcast lit fiber-optic lines. The Service can be delivered as either an Unprotected Circuit or a Protected Circuit, each as defined below.

**A. Unprotected.** An “**Unprotected Circuit**” is a point-to-point linear circuit utilizing one (1) static physical fiber path (“**Fiber Path**”) terminating on single Comcast-owned Network Terminating Equipment (“**NTE**”) at each circuit endpoint. NTE constitutes Comcast Equipment. Protection Switching (as defined below) is not provided at the NTE or within the transport network, even if Customer has more than one Unprotected Circuit. 10G and 100G circuits are available as Unprotected Circuits.

**B. Protected.** A “**Protected Circuit**” is a point-to-point linear circuit utilizing two (2) diverse Comcast Fiber Paths that both terminate on the same NTE at each circuit endpoint, but diverge along the circuit at the nearest point of divergence from each circuit endpoint and are routed to diverse Comcast headends. Each circuit utilizes a dedicated port on the NTE for the Customer handoff. One of the two (2) diverse Fiber Paths is designated by Comcast as the primary Fiber Path and the other Fiber Path is designated by Comcast as the secondary Fiber Path. In the event the primary Fiber Path is unavailable, Comcast re-routes traffic from the primary Fiber Path to the secondary Fiber Path (“**Protection Switching**”). Only one (1) Fiber Path is active at a given time. Only 10G circuits are available as Protected Circuits.

**2. Technical Specifications for Services.**

The Services are bi-directional, point-to-point optical Services capable of transporting high bandwidths (*e.g.*, 10G and 100G) using Ethernet or Optical Transport Network (OTN) protocols. Each Service constitutes an entire wavelength or “Lambda” channel of a DWDM.

**Customer Interface.** Table 1 shows the Customer interfaces supported, by protocol, for the Service.

<b>Protocol</b>	<b>Interface(s)</b>
Ethernet – 10G LAN PHY	10GBase-LR
Ethernet – 10G WAN PHY	10GBase-LW

Ethernet – 100G	100GBASE-LR4
OTN – 10G	OTU2, OTU2e
OTN – 100G	OTU4

**Table 1: Wavelength Services Protocols and Customer Interfaces**

### 3. Service Monitoring, Technical Support and Maintenance.

**A. Network Monitoring.** Comcast monitors Services on a 24x7x365 basis.

**B. Technical Support.** Comcast provides a toll-free trouble reporting telephone number to the Comcast Business Services Network Operations Center that operates on a 24x7x365 basis. Comcast provides technical support for Service-related inquiries. Comcast Business Services Network Operations Center will not offer consulting or advice on issues relating to non-Comcast Equipment.

**C. Escalation.** Reported troubles are escalated within the Comcast Business Services Network Operations Center to meet the response/restoration objectives described below (Response and Restoration Standards). Service issues are escalated within the Comcast Business Services Network Operations Center as follows: to a Supervisor at the end of the applicable objective time interval plus one (1) hour; to a Manager at the end of the applicable objective time interval plus two (2) hours; and to a Director at the end of the applicable objective time interval plus four (4) hours.

**D. Maintenance.** Comcast's standard maintenance window for Services is Sunday to Saturday from 12:00am to 6:00am local time. Scheduled maintenance for Services is performed during the maintenance window and will be coordinated between Comcast and the Customer. Comcast provides a minimum three (3) business days' notice for maintenance expected to impact service for  $\leq 50$ ms. Comcast provides a minimum of seven (7) business days' notice for maintenance expected to impact service for  $> 50$ ms. Emergency maintenance is performed as needed without advance notice to Customer.

**E. Comcast Equipment.** Comcast provides certain Comcast Equipment, which will reside at the Service Location, for provisioning its Services. Comcast will retain ownership and management responsibility for this Comcast Equipment. This Comcast Equipment must only be used for receipt of Services.

4. **Restoration Standards.** Comcast has the following response and restoration objectives:

CATEGORY	OBJECTIVE	MEASUREMENT	REMEDIES
<i>Mean Time to Restore Comcast Equipment</i>	4 hours	Averaged Over A Month	Escalation (see above)
<i>Mean Time to Restore Services</i>	6 hours	Averaged Over A Month	Escalation (see above)

Customer shall bear any expense incurred, e.g., dispatch/labor costs, where a Service Interruption (as defined in Schedule A-2) is found to be the fault of Customer, its end users, agents, representatives or third-party suppliers.

### 5. Customer Responsibilities.

Customer shall have the following responsibilities related to the installation, support, and maintenance of the Service:

- Connecting to the Demarcation Point.
- Responsibility for all equipment and service beyond the Demarcation Point and/or interconnection between Comcast Equipment and the wiring at the Demarcation Point.
- Procuring and maintaining equipment which is technically compatible with the Service and the Network.
- Providing an operating environment with temperatures not below fifty-five (55) or above eighty-five (85) degrees Fahrenheit. Humidity shall not exceed ninety (90) percent at eighty-five (85) degrees Fahrenheit.
- Providing secure space sufficient for access to one (1) standard, freestanding, equipment cabinet at each of the Customer facilities, no further than fifty feet from the Customer router or switch interface.
- Providing outside cable entry conduit(s), entry cable ground point, and internal building conduit to allow Comcast the ability to rod/rope a fiber optic cable to the Demarcation Point.
- Locating and marking all private underground utilities (water, electric, etc.) along path of new underground placement not covered by utility companies.
- Providing a pull rope in any existing duct that Comcast is to use and ensure existing duct is serviceable for Comcast use.
- Obtaining “right-of-way” entry easement for Comcast facilities and equipment from property owners at each Customer location.
- Coring of the Service Location’s outside wall and internal walls. Upon request, Comcast can perform this activity on an “as needed” basis for an additional one-time fee.
- Providing UPS AC power (back-up battery power) equipment, circuit sizing to be determined, if applicable.
- Emergency local generator backup service, if applicable.
- Providing access to the buildings and Demarcation Point at each Service Location to allow Comcast and its approved contractors to install the Service and for regular (8am - 5pm) and emergency (24 hour) service and maintenance of Comcast’s equipment and facilities.
- Providing, installing and maintaining a device that is capable of interconnecting network traffic between the Service and the Customer’s Local Area Network (“LAN”).
- Providing a point of contact (“POC”) for installation, service activation and any maintenance activities.

**COMCAST ENTERPRISE SERVICES  
PRODUCT-SPECIFIC ATTACHMENT  
INTRASTATE WAVELENGTH SERVICES**

**SCHEDULE A-2  
SERVICE LEVEL AGREEMENT**

**Intrastate Wavelength, Version 1.0**

The Service(s) are backed by the following Service Level Agreement (“SLA”):

**1. Definitions.**

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the Intrastate Wavelength Services PSA or the General Terms and Conditions.

**“Planned Service Interruption”** means any Service Interruption caused by planned work such as scheduled maintenance or planned enhancements or upgrades to the network.

**“Service Interruption”** means an interruption in transmission that renders the Service unusable due to a total loss of signal for the Service. The Service shall be **“Available”** in the absence of a Service Interruption.

**2. Intrastate Wavelength Service Level Agreements.**

**A. Availability SLA**

Comcast’s liability and Customer’s sole remedy for Service Interruptions, and errors, omissions, interruptions, delays, outages, or defects in transmission or switching of any Services (individually or collectively, **“Liability”**), shall be limited to the amounts set forth in the Tables in this Section 2(A) below (**“Availability Credit”**). For the purposes of calculating credit for a Service Interruption, the **“Length of Service Interruption”** begins when the Customer reports such Service Interruption and a trouble ticket is opened, and concludes upon the closing of the same trouble ticket or, if sooner, the termination of the Service Interruption, less any time Comcast is awaiting additional information or premises testing from the Customer. In no event shall the total amount of Availability Credit issued to Customer’s account on a per-month basis exceed 50% of the total monthly recurring charge (**“MRC”**) associated with the impacted portion of the Service set forth in the Sales Order. The Length of Service Interruptions for separately occurring Service Interruptions will not be aggregated for purposes of determining Availability Credit allowances. For purposes of calculating the Service credit percentage in the below tables, only the MRC of the impacted wavelength circuit shall apply. To qualify, Customer must request the Availability Credit from Comcast within thirty (30) days of the beginning of the Service Interruption. Comcast shall not incur any Liability, including Availability Credit, for any failure of the Services caused by force majeure events, Planned Service Interruptions, Customer actions, omission or equipment (including all Customer-Provided Equipment), or any other items set forth in the “Exceptions to Credit Allowances” section below.

**TABLE 1: Availability SLA for Unprotected Circuits**

<b>Availability</b>	<b>Length of Service Interruption</b>	<b>Service Credit</b> (Based on MRC of only the impacted wavelength circuit)
$\geq 99.44\%$	Less than 4 hours	No Credit
$\geq 98.89\%$ and $< 99.44\%$	At least 4 hours but less than 8 hours	10% of the MRC
$\geq 98.33\%$ and $< 98.89\%$	At least 8 hours but less than 12 hours	25% of the MRC
$< 98.33\%$	At least 12 hours or greater	50% of the MRC

**TABLE 2: Availability SLA for Protected Circuits\***

<b>Availability</b>	<b>Length of Service Interruption</b>	<b>Service Credit</b> (Based on MRC of only the impacted wavelength circuit)
$\geq 99.99\%$	Less than 4 minutes 19 seconds	No Credit
$\geq 99.86\%$ and $< 99.99\%$	At least 4 minutes 20 seconds but less than 1 hour	10% of the MRC
$\geq 98.61\%$ and $< 99.85\%$	At least 1 hour but less than 10 hours	25% of the MRC
$< 98.61\%$	At least 10 hours or greater	50% of the MRC

\*Availability Credits for Protected Circuits are available only to the extent both Fiber Paths for such Protected Circuit simultaneously sustain a Service Interruption. For clarity and avoidance of doubt, if either Fiber Path for a Protected Circuit is Available, the entire Protected Circuit shall be considered Available for purposes of calculating Availability.

SEPARATELY OCCURRING SERVICE INTERRUPTIONS ARE NOT AGGREGATED FOR THE PURPOSES OF DETERMINING CREDIT ALLOWANCES.

## **B. Exceptions and Terms applicable to all SLAs**

### **1. Remedy Processes**

All claims and rights arising under this SLA must be exercised by Customer in writing within the time period set forth in Section 2(A). The Customer must submit the following information to the Customer's Comcast account representative with any and all claims for credit allowances: (a) Organization name; (b) Customer account number;

and (c) basis of credit allowance claim (including date and time, if applicable). Comcast will acknowledge and review all claims promptly and will inform the Customer by electronic mail or other correspondence whether a credit allowance will be issued or the claim rejected, with the reasons specified for the rejection.

## **2. Exceptions to Credit Allowances**

Comcast's failure to meet either of the SLAs set forth on this Schedule A-2 shall not qualify for the remedies set forth herein if such failure is related to, associated with, or caused by: Planned Service Interruptions or other scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment (including Customer-Provided Equipment); any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers, any power, equipment or services provided by third parties; or an event of force majeure as defined in the Agreement.

## **3. Other Limitations**

THE TOTAL CREDIT ALLOWANCES PER CALENDAR MONTH UNDER THIS SCHEDULE A-2 IS CAPPED AT 50% OF THAT MONTH'S MRC FOR THE IMPACTED PORTIONS OF SERVICE. In addition, the remedies set forth in this Service Level Agreement shall be Customer's sole and exclusive remedies for any Service Interruption, outage, unavailability, delay, or other degradation, or any Comcast failure to meet the service objectives.

## Contract Generated Date: \_\_\_\_\_

Division: \_\_\_\_\_



COMCAST ENTERPRISE SERVICES SALES ORDER FORM

ETHERNET SERVICES AND PRICING

Account Name:

MSA ID#:

Date:

SO ID#:

Short  
Description  
of  
Service:

Service Term (Months):

Solution Charges

Line	Request	Action	Service(s)	Description	Service Location A*	Service Location Z*	Comcast Metro	Performance Tier**	Tax Jurisdiction	Monthly	One-Time
* Services Location Details attached							Total			Service Charges:	
**Performance Tier Matrix Attached (For On-Net to On-Net or On-Net to Off-Net)										Equipment Fees:	

### SERVICE LOCATION DETAIL INFORMATION



COMCAST BUSINESS SALES ORDER

Company Name: \_\_\_\_\_ Order #: \_\_\_\_\_

<b>Service Location:</b>	<b>Billing Location:</b>
Address 1	Address 1
Address 2	Address 2
City	City
State	State
Zip	Zip
Primary Contact Name	Billing Contact Name
Primary Contact Phone	Billing Contact Phone
Primary Contact Email	Billing Contact Email
	Tax Exempt <b>Yes</b>

**Service Term:** 36 Months

Equipment(s) and Service(s)	Qty	Monthly Service Charge <sup>1</sup>	Non-Recurring Charge <sup>2</sup>
<b>Business Internet</b>			
Business Internet 100	1	\$ -	
<b>WiFi Pro</b>			
WiFi Pro Service	1	\$ -	
Equipment - WiFi Pro	1	\$ -	
<b>Business Voice</b>			
Mobility Lines	1	\$ -	
Equipment - Modem	1	\$ -	
<b>Business Video</b>			
TV Standard	1	\$ -	
<b>Installation Fees</b>			
Standard Installation Fee	1		\$ -
<b>Total Charges<sup>3</sup></b>		\$ -	\$ -

	<b>Monthly Service Charge<sup>1</sup></b>	<b>Non-Recurring Charge<sup>2</sup></b>
<b>Total Charge for Service Order</b>	\$ -	\$ -

<sup>1</sup>Charges identified in the Service Order Agreement are exclusive of maintenance and repair charges, and applicable federal, state, and local surcharges and recoupments (however designated).

<sup>2</sup> Non-Recurring Charges in the Service Order Agreement reflect activation and installation fees for this order. this exludes any custom installation fees.

<sup>3</sup> Additional Service(s) and Charge listed above are incremental to current Service(s) and Charge.

**General Special Instructions**

Notwithstanding any other information or statement anywhere on this Sales Order, it is governed by the State of Vermont Contract # [ASSIGNED CONTRACT NUMBER].

AGREEMENT

1. This Comcast Enterprise Services Sales Order Form ("Sales Order") shall be effective upon acceptance by Comcast. This Sales Order is made a part of the Comcast Enterprise Services Master Services Agreement, entered between Comcast and the undersigned. Unless otherwise indicated herein, capitalized words shall have the same meaning as in the Agreement.
2. Each Comcast Business Service ("Service") carries a 30 day money back guarantee. If within the first thirty days following Service activation Customer is not completely satisfied, Customer may cancel Service and Comcast will issue a refund for Service charges actually paid by Customer, custom installation, voice usage charges, and optional service fees excluded. In order to be eligible for the refund, Customer must cancel Service within thirty days of activation and return any Comcast-provided equipment in good working order. In no event shall the refund exceed \$500.00. If you use the service in the first 30 days, you will be refunded your subscription fees, but charged the applicable one-time fee.
3. To complete a Voice order, Customer must execute a Comcast Letter or Authorization ("LOA") and submit it to Comcast, or Comcast's third party order entry integrator, as directed by Comcast.
4. New telephone numbers are subject to change prior to the install. Customers should not print their new number on stationery or cards until after the install is complete.
5. Modifications: All modifications to the Agreement, if any, must be captured in a written Amendment, executed by an authorized Comcast Senior Vice President and the Customer. All other attempts to modify the Agreement shall be void and non-binding on Comcast. Customer by signing below, agrees and accepts the Terms and Conditions of this Agreement.
6. IF CUSTOMER IS SUBSCRIBING TO COMCAST'S BUSINESS DIGITAL VOICE SERVICE, CUSTOMER, BY SIGNING BELOW, ACKNOWLEDGES RECEIPT AND UNDERSTANDING OF THE FOLLOWING 911 NOTICE:

911 Notice

Comcast business digital voice service ("Voice Service") may have the 911 limitations specified below:

- In order for 911 calls to be properly directed to emergency services using the Voice Service, Comcast must have the correct service address for the telephone number used by Customer. If the Voice Service or any Voice Service device is moved to a different location without Customer providing an updated service address, 911 calls may be directed to the wrong emergency authority, may transmit the wrong address, and/or the Voice Service (including 911) may fail altogether. Customer's use of a telephone number not associated with its geographic location may also increase these risks.
- The Voice Service uses electrical power in the Customer's premises. If there is an electrical power outage, 911 calling may be interrupted if a battery back-up is not installed in the voice modem or if a battery back-up fails or is exhausted.
- Calls using the Voice Service, including calls to 911, may not be completed if there is a problem with network facilities, including network congestion, network, equipment, and/or power failure, a broadband connection failure, or another technical problem.
- Customer should call Comcast at 1-888-824-8104 if it has any questions or needs to update a service address in the 911 system. Delays in updating the service address may also impact 911.

**BY SIGNING BELOW, CUSTOMER ACKNOWLEDGES THAT IT HAS READ AND UNDERSTANDS THE FOREGOING 911 NOTICE AND THE 911 LIMITATIONS OF THE VOICE SERVICE.**

CUSTOMER SIGNATURE
By signing below, Customer agrees and accepts the Terms and Conditions of this Agreement. General Terms and Conditions can be found at <a href="http://business.comcast.com/terms-conditions/index.aspx">http://business.comcast.com/terms-conditions/index.aspx</a>
Signature
Name
Title
Date

FOR COMCAST USE ONLY	
Sales Representative	
Sales Representative Code	
Sales Manager Name	
Sales Manager Approval	
Division	
SmartOffice License Number	
Agreement Generation Date:	6/12/2020



COMCAST BUSINESS SERVICE PROVISIONING DETAILS

Company Name:

Order #:

BUSINESS INTERNET CONFIGURATION DETAILS

Transfer Existing Comcast.net Email

No

Equipment Selection

Business Wireless Gateway

Number of Static IPs\*

Business Web Hosting

No

BUSINESS VIDEO CONFIGURATION DETAILS

Outlet Details	Location	Outlet Type
Outlet 1 - Primary		
Outlet 2 - Additional		
Outlet 3 - Additional		
Outlet 4 - Additional		
Outlet 5 - Additional		
Outlet 6 - Additional		
Outlet 7 - Additional		
Outlet 8 - Additional		

Additional Comments

Total Occupancy

OUTLETS 9 & UP	QUANTITY
TV Box + Remote (STB)	0
TV Adapter (DTA)	0

BUSINESS VOICE CONFIGURATION DETAILS

Directory Listing Details	
Directory Listing (Published, Non-Published, Unlisted)	Published
Directory Listing Phone Number	
Directory Listing Display Name	
DA/DL Header Text Information	
DA/DL Header Code Information	
Standard Industry Code	

Additional Voice Details	
Caller ID (Yes/No)	No
Caller ID Display Name (max 15 char.)	
International Dialing (Yes/No)	No
Call Blocking (Yes/No)	No
Auto Attendant (Yes/No)	No
Enterprise Extension Dialing?	No

Hunt Group Configuration Details	
Hunt Group Features Requested (Yes/No)	No
Hunt Group 1 Confituration Type	
Hunt Group 2 Confituration Type	