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

ATTACHMENT IDENTIFIER: SD-WAN, Version 4.1

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 SD-WAN Service or Wireless Backup, as applicable.

"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.

"SD-WAN Service" means the Standard and/or Advanced SD-WAN Service, as applicable.

"Service(s)" for purposes of this PSA means the applicable SD-WAN Service(s). Wireless Backup shall be considered a "Service" for purposes of Articles 1-5 of this PSA.

"**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.

"**Wireless Backup**" means the 4G LTE Internet backup feature for the SD-WAN Service(s) as described in Schedule A-1.

ARTICLE 1. SERVICES

This attachment shall apply to the SD-WAN Services and, where applicable, Wireless Backup. 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, Wireless Backup or Cloud Connect). Charges for the Services shall begin to accrue on the Service Commencement Date.

ARTICLE 5. TERMINATION CHARGES; PORTABILITY

5.1 The charges set forth or referenced in each Sales Order have been extended to Customer in reliance on the Service Term.

5.2 Termination Charges.

A. Subject to Sections 5.2(C) and 5.2(D), in the event that a Service is terminated following Comcast's acceptance of the applicable Sales Order, but prior to the Service Commencement Date, Customer shall pay Termination Charges equal to one hundred and twenty percent (120%) of the costs and expenses incurred by Comcast in installing or preparing to install the Service.

B. Subject to Sections 5.2(C) and 5.2(D), in the event that a Service is terminated on or following the Service Commencement Date, but prior to the end of the applicable Service Term, Customer shall pay Termination Charges equal to a percentage of the monthly recurring Service charges remaining for the unexpired portion of the then-current Service Term, calculated as follows:

i 100% of the monthly recurring charges with respect to months 1-12 of the Service Term; plus
ii 80% of the monthly recurring charges with respect to months 13-24 of the Service Term; plus
iii 65% of the monthly recurring charges with respect to months 25 through the end of the Service Term.

Termination Charges shall be immediately due and payable upon cancellation or termination, and shall be in addition to any and all accrued and unpaid charges for the Service rendered by Comcast through the date of such cancellation or termination.

C. Exclusions. Termination Charges shall not apply to Service(s) terminated by Customer as a result of Comcast's material and uncured breach in accordance with the General Terms and Conditions.

D. Customer acknowledges and agrees that termination of the Comcast-provided Underlay Service, or termination of the associated SD-WAN Service in the case of Wireless Backup, shall constitute a termination of the Services and Customer shall pay Termination Charges with respect to the Services as provided herein; provided, that, if Customer terminated such Underlay Service (or associated SD-WAN Service in the case of Wireless Backup) as a result of Comcast's material and uncured breach in accordance with the General Terms and Conditions applicable hereto, then Customer will not be obliged to pay Termination Charges with respect to the Service.

5.3 Portability. Customer may terminate an existing Service (an "**Existing Service**") and turn up a replacement Service (*i.e.*, activate an equivalent 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.

ARTICLE 9. WIRELESS BACKUP

Customer acknowledges and agrees that, without limitation to any other provision in this Agreement, Wireless Backup is not intended to be a primary Underlay Service and may be used only to provide secondary connectivity for the Service(s). Wireless Backup may not be used at any location other than the Service Location for which Wireless Backup and the associated SD-WAN Service was ordered. Further, Customer shall not (a) move, unplug, rearrange, disconnect, remove, or transport the Comcast Equipment provided with Wireless Backup ("**Wireless Backup Equipment**"), (b) use the Wireless Backup Equipment with any device other than the Comcast Equipment provided with the associated SD-WAN Services, or (c) use the Wireless Backup Equipment in connection with any service(s) other than the specific SD-WAN Service for which Wireless Backup was ordered.

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 (Versa)**. 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 for the SD-WAN Service, 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 for the SD-WAN Service, 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).

v. The Advanced SD-WAN Service may be configured in a cloud environment. Cloud Connect is an optional configuration that enables the Advanced SD-WAN Service to be provisioned with one Service Location and a virtual site on the SD-WAN network. The virtual server enables a solution that is delivered and managed through the cloud. This configuration is not available with Wireless Backup.

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. Standard SD-WAN 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.

C. **SD-WAN Secure Service (Fortinet).** SD-WAN Secure Service is a wide area network ("WAN") solution built on a secure access service edge framework. The SD-WAN Secure Service provides organizations end-to-end WAN connectivity for Service Locations 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 Secure Service enables network abstraction and the separation of the control plane and data plane. The following features are also included with SD-WAN Secure Service:

i. SD-WAN Secure 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 Secure Service assists with the management, configuration, and orchestration of WANs.

iv. SD-WAN Secure 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 Secure Service monitors the CPE and circuits for "up/down" status, and alerts Customers based on configuration.
vi. 24x7x365 phone support.
vii. Access to the Portal, which provides analytics that show the performance and utilization of Customer's network applications and elements.
viii. Secure connectivity to Comcast's high-performance global network backbone.
ix. Built-in security functions, including Layer 4 Stateful Firewall, SSL VPN, and IPsec VPN.

D. **SD-WAN Secure OTT Service (Fortinet)**. The SD-WAN Secure OTT Service includes all features of the SD-WAN Secure Service, except for the secure connectivity to Comcast's high performance global network backbone. The Service may be configured as Standalone. Standalone is an optional configuration feature that enables the 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).

2. Service Requirements

In order to provide the Services to a 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, Internet connectivity services provided by a third-party service provider, or Wireless Backup (only as secondary connectivity to the primary Underlay Service(s)). The connectivity type may impact overall speed and performance. 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. In order to provide Wireless Backup to a Service Location, such Service Location must have at least one (1) primary Underlay Service and an SD-WAN Service.

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 and Features

A. **Local Internet Breakout.** Comcast can configure a local Internet breakout at each 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.

D. **Wireless Backup**. Wireless Backup is an optional pricing-impacting SD-WAN Service feature that provides cellular equipment and 4G LTE Internet to be used only as secondary connectivity to the primary Underlay Service(s) for the Services. The cellular router automatically switches over to an available wireless connection when the primary connection(s) is/are disrupted; provided that the timing and sequence of such switch over may depend on Customer's settings and configurations, to the extent available, and Comcast's settings and processes.

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:

SD-WAN SERVICE	
Category	**Objective**
Simple Configuration Change	24 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.

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 (including Wireless Backup, as applicable):

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 and the Wireless Backup Equipment. 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 or vCPE. 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.

L. Cloud Connect customers must set up their cloud environment and configure a cloud instance through an approved cloud providers platform prior to Comcast activation of the Service.

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. For clarity and avoidance of doubt, this Schedule A-2 does not apply to Wireless Backup.

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.

Service:	**Service Availability Objective:**	**Service Availability:**	**Amount of Credit:**
For Service Locations Not Configured as Standalone	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

		Equal to or greater than 99% but less than 99.9%	10% of MRC
		Less than 99%	20% of MRC
For Service Locations Configured as Standalone	99.995%	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; Wireless Backup or Wireless Backup Equipment; 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

PCI DSS v4.0 Requirements	Responsibility (Comcast / Customer / Shared)	Responsibility Summary
Requirement 1: Install and Maintain Network Security Controls		
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.		
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for security policies and operational procedures for managing their persons, processes, and technologies in scope.
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	Shared	Comcast is responsible for documenting roles and responsibilities for performing activities in Requirement 1 for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for documenting roles and responsibilities for performing activities in Requirement 1 for managing their persons, processes, and technologies in scope.
1.2 Network security controls (NSCs) are configured and maintained.		
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	Shared	Comcast is responsible for defining, implementing, and maintaining configuration standards for NSC rulesets for the uCPE firmware and their NSCs that could impact the security of the uCPE. Customer is responsible for defining, implementing, and maintaining configuration standards for NSC rulesets for the uCPE and their NSCs in scope.
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1. **Applicability Notes** Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.	Shared	Comcast is responsible for approving and managing network connection and configuration changes to uCPE firmware and their NSCs that could impact the security of the uCPE in accordance with their change control processes. Customer is responsible for approving and managing network connection and configuration changes to the uCPE and their NSCs in scope in accordance with their own change control processes.

1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks. **Applicability Notes** A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.	Shared	Comcast is responsible for maintaining a network diagram showing connections between the uCPE and their connecting backend system components. Customer is responsible for maintaining a network diagram that shows all connections between their CDE (including the uCPE where applicable) and other networks.
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment. **Applicability Notes** A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across systems and networks can be used to meet this requirement.	Customer	Comcast is not required to maintain a data-flow diagram as it does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. This requirement is the sole responsibility of the customer.
1.2.5 All services, protocols and ports allowed are identified, approved, and have a defined business need.	Shared	Comcast is responsible for identifying, approving, and justifying all services, protocols and ports allowed on the uCPE firmware and their NSCs that could impact the security of the uCPE. Customer is responsible for identifying, approving, and justifying all services, protocols and ports allowed on the uCPE and their NSCs in scope.
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Shared	Comcast is responsible for defining and implementing security features for all services, protocols and ports in use and considered to be insecure allowed on the uCPE firmware and their NSCs that could impact the security of the uCPE. Customer is responsible for defining and implementing security features for all services, protocols and ports in use and considered to be insecure allowed on the uCPE and their NSCs in scope.
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	Shared	Comcast is responsible for reviewing configurations on the uCPE firmware and their NSCs that could impact the security of the uCPE at least once every month. Customer is responsible for reviewing configurations on the uCPE and their NSCs in scope at least once every month.
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations. **Applicability Notes** Any file or setting used to configure or synchronize NSCs is considered to be a "configuration file." This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.	Shared	Comcast is responsible for securing configurations on the uCPE firmware and their NSCs that could impact the security of the uCPE. Customer is responsible for securing configurations on the uCPE and their NSCs in scope.
1.3 Network access to and from the cardholder data environment is restricted.		

1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary, • All other traffic is specifically denied.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore does not maintain a CDE in this context. This requirement is the sole responsibility of the customer.
1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore does not maintain a CDE in this context. This requirement is the sole responsibility of the customer.
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore does not maintain a CDE in this context. This requirement is the sole responsibility of the customer.
1.4 Network connections between trusted and untrusted networks are controlled.		
1.4.1 NSCs are implemented between trusted and untrusted networks.	Shared	Comcast is responsible for implementing NSCs between networks where system components that could impact the security of the uCPE are connected and untrusted networks. Customer is responsible for implementing NSCs between their trusted networks (including where the uCPE is connected) and untrusted networks.
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied. **Applicability Notes** The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols. This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC.	Shared	Comcast is responsible for restricting inbound traffic from untrusted networks to networks where system components that could impact the security of the uCPE are connected. Customer is responsible for restricting inbound traffic from untrusted networks to their trusted networks (including where the uCPE is connected).
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Shared	Comcast is responsible for implementing anti-spoofing measures to protect networks where system components that could impact the security of the uCPE are connected. Customer is responsible for implementing anti-spoofing measures to protect their trusted networks (including where the uCPE is connected).

1.4.4 System components that store cardholder data are not directly accessible from untrusted networks. **Applicability Notes** This requirement is not intended to apply to storage of account data in volatile memory but does apply where memory is being treated as persistent storage (for example, RAM disk). Account data can only be stored in volatile memory during the time necessary to support the associated business process (for example, until completion of the related payment card transaction).	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.	Shared	Comcast is responsible for limiting disclosure of internal IP addresses for networks where system components that could impact the security of the uCPE are connected. Customer is responsible for limiting the disclosure of internal IP addresses for their networks (including where the uCPE is connected).
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.		
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows. • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. **Applicability Notes** These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not active. This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore does not maintain a CDE in this context. This requirement is the sole responsibility of the customer.
Requirement 2: Apply Secure Configurations to All System Components		
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.		
2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for security policies and operational procedures for managing their persons, processes, and technologies in scope.

2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood. *New requirement - effective immediately*	Shared	Comcast is responsible for documenting roles and responsibilities for performing activities in Requirement 2 for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for documenting roles and responsibilities for performing activities in Requirement 2 for managing their persons, processes, and technologies in scope.
2.2 System components are configured and managed securely.		
2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	Shared	Comcast is responsible for developing, implementing, and maintaining configuration standards for the uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for developing, implementing, and maintaining configuration standards for the uCPE and their system components in scope.
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled. **Applicability Notes** This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults. This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.	Shared	Comcast is responsible for configuring the uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for configuring the uCPE and their system components in scope.
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, **OR** • Primary functions with differing security levels that exist on the same system component are isolated from each other, **OR** • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	Shared	Comcast is responsible for configuring the uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for configuring the uCPE and their system components in scope.
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Shared	Comcast is responsible for configuring the uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for configuring the uCPE and their system components in scope.

2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	Shared	Comcast is responsible for configuring the uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for configuring the uCPE and their system components in scope.
2.2.6 System security parameters are configured to prevent misuse.	Shared	Comcast is responsible for configuring the uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for configuring the uCPE and their system components in scope.
2.2.7 All non-console administrative access is encrypted using strong cryptography. **Applicability Notes** This includes administrative access via browser-based interfaces and application programming interfaces (APIs).	Shared	Comcast is responsible for encrypting non-console administrative access to the uCPE and the uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for encrypting non-console administrative access to their system components in scope.
2.3 Wireless environments are configured and managed securely.		
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults, • Any other security-related wireless vendor defaults. **Applicability Notes** This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults.	Customer	Comcast does not maintain a wireless environment in delivery of this product. Comcast therefore is not subject to wireless network requirements in this context. This requirement is the sole responsibility of the customer.
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.	Customer	Comcast does not maintain a wireless environment in delivery of this product. Comcast therefore is not subject to wireless network requirements in this context. This requirement is the sole responsibility of the customer.
Requirement 3: Protect Stored Account Data		
3.1 Processes and mechanisms for performing activities in Requirement 3 are defined and understood.		
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.

3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood. *New requirement - effective immediately*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.2 Storage of account data is kept to a minimum.		
3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable. **Applicability Notes** Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted. *The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.3 Sensitive authentication data is not stored after authorization.		
3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process **Applicability Notes** This requirement does not apply to issuers and companies that support issuing services (where SAD is needed for a legitimate issuing business need) and have a business justification to store the sensitive authentication data. Refer to Requirement 3.3.3 for additional requirements specifically for issuers. Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.

3.3.1.1 The full contents of any track are not retained upon completion of the authorization process. **Applicability Notes** In the normal course of business, the following data elements from the track may need to be retained: • Cardholder name. • Primary account number (PAN). • Expiration date. • Service code. To minimize risk, store securely only these data elements as needed for business.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.3.1.2 The card verification code is not retained upon completion of the authorization process. **Applicability Notes** The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.3.1.3 The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process. **Applicability Notes** PIN blocks are encrypted during the natural course of transaction processes, but even if an entity encrypts the PIN block again, it is still not allowed to be stored after the completion of the authorization process.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography. Applicability Notes Whether SAD is permitted to be stored prior to authorization is determined by the organizations that manage compliance programs (for example, payment brands and acquirers). Contact the organizations of interest for any additional criteria. This requirement applies to all storage of SAD, even if no PAN is present in the environment. Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of authorization. This requirement does not apply to issuers and companies that support issuing services where there is a legitimate issuing business justification to store SAD). Refer to Requirement 3.3.3 for requirements specifically for issuers. This requirement does not replace how PIN blocks are required to be managed, nor does it mean that a properly encrypted PIN block needs to be encrypted again. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.

3.3.3 ***Additional requirement for issuers and companies that support issuing services and store sensitive authentication data:*** Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. **Applicability Notes** This requirement applies only to issuers and companies that support issuing services and store sensitive authentication data. Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data. PCI DSS requirements are intended for all entities that store, process, or transmit account data, including issuers. The only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. Any such data must be stored securely and in accordance with all PCI DSS and specific payment brand requirements. (continued on next page) *The bullet above (for encrypting stored SAD with strong cryptography) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.3.3 and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.4 Access to displays of full PAN and ability to copy account data is restricted.		
3.4.1 PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN. **Applicability Notes** This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment brand requirements for point-of-sale (POS) receipts. This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.5.1 for protection of PAN when stored, processed, or transmitted.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. **Applicability Notes** Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.5 PAN is secured wherever it is stored.		

3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). • Index tokens. • Strong cryptography with associated key-management processes and procedures. • Where hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place to ensure that the different versions cannot be correlated to reconstruct the original PAN. **Applicability Notes** 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. This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1), are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7. **Applicability Notes** This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN. *This requirement is considered a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.

3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows : • On removable electronic media **OR** • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1. Note: Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements. **Applicability Notes** While disk encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices. Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies. Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows:, • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely. **Applicability Notes** Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.6 Cryptographic keys used to protect stored account data are secured.		

3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms. **Applicability Notes** This requirement applies to keys used to encrypt stored account data and to key-encrypting keys used to protect data-encrypting keys. The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.6.1.1 ***Additional requirement for service providers only:*** A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. In cloud HSM implementations, responsibility for the cryptographic architecture according to this Requirement will be shared between the cloud provider and the cloud customer. *The bullet above (for including, in the cryptographic architecture, that the use of the same cryptographic keys in production and test is prevented) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.6.1.1 and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.

3.6.1.2 Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: • 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. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method. **Applicability Notes** It is not required that public keys be stored in one of these forms. Cryptographic keys stored as part of a key management system (KMS) that employs SCDs are acceptable. A cryptographic key that is split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within an SCD, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.6.1.4 Cryptographic keys are stored in the fewest possible locations.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.		
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.

3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations. **Applicability Notes** If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key).	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control. **Applicability Notes** This control is applicable for manual key-management operations or where key management is not controlled by the encryption product. A cryptographic key that is simply split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.

3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
3.7.9 ***Additional requirement for service providers only:*** Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission		
4.1 Processes and mechanisms for performing activities in Requirement 4 are defined and documented.		
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented • Kept up to date • In use • Known to all affected parties	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data transmission requirements in this context. This requirement is the sole responsibility of the customer.
4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood. *New requirement - effective immediately*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data transmission requirements in this context. This requirement is the sole responsibility of the customer.
4.2 PAN is protected with strong cryptography during transmission.		

4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until its effective date; refer to applicability notes below for details.* • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use. **Applicability Notes** There could be occurrences where an entity receives cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of receiving sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or implement measures to prevent the channel from being used for cardholder data. A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organization, the certificate's author is confirmed, and the certificate is verified—for example, via hash or signature—and has not expired. Note that self-signed certificates where the Distinguished Name (DN) field in the "issued by" and "issued to" field is the same are not acceptable. *The bullet above (for confirming that certificates used to safeguard PAN during transmission over open, public networks are valid and are not expired or revoked) is a best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data transmission requirements in this context. This requirement is the sole responsibility of the customer.
4.2.1.1 An inventory of the entity's trusted keys and certificates is maintained. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data transmission requirements in this context. This requirement is the sole responsibility of the customer.
4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data transmission requirements in this context. This requirement is the sole responsibility of the customer.

4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies. **Applicability Notes** This requirement also applies if a customer, or other third-party, requests that PAN is sent to them via end-user messaging technologies. There could be occurrences where an entity receives unsolicited cardholder data via an insecure communication channel that was not intended for transmissions of sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or delete the cardholder data and implement measures to prevent the channel from being used for cardholder data.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data transmission requirements in this context. This requirement is the sole responsibility of the customer.
Requirement 5: Protect All Systems and Networks from Malicious Software		
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.		
5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented • Kept up to date • In use • Known to all affected parties	Shared	Comcast is responsible for security policies and operational procedures for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for security policies and operational procedures for managing their persons, processes, and technologies in scope.
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood. *New requirement - effective immediately*	Shared	Comcast is responsible for documenting roles and responsibilities for performing activities in Requirement 5 for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for documenting roles and responsibilities for performing activities in Requirement 5 for managing their persons, processes, and technologies in scope.
5.2 Malicious software (malware) is prevented, or detected and addressed.		
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	Shared	Comcast is responsible for deploying an anti-malware solution to their system components that could impact the security of the uCPE. Customer is responsible for deploying an anti-malware solution to their system components in scope.
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	Shared	Comcast is responsible for deploying an anti-malware solution to their system components that could impact the security of the uCPE. Customer is responsible for deploying an anti-malware solution to their system components in scope.

5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection. **Applicability Notes** System components covered by this requirement are those for which there is no anti-malware solution deployed per Requirement 5.2.1.	Shared	Comcast is responsible for evaluating whether or not their system components that could impact the security of the uCPE are at risk for malware. Customer is responsible for evaluating whether or not their system components in scope are at risk for malware.
5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for completing a targeted risk analysis to identify the frequency for performing evaluations to determining if the system components that could impact the security of the uCPE are at risk for malware. Customer is responsible for completing a targeted risk analysis to identify the frequency for performing evaluations to determine if their system components in scope are at risk for malware.
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.		
5.3.1 The anti-malware solution(s) is kept current via automatic updates.	Shared	Comcast is responsible for configuring the anti-malware solution deployed to their system components that could impact the security of the uCPE. Customer is responsible for configuring the anti-malware solution deployed to their system components in scope.
5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans **OR** • Performs continuous behavioral analysis of systems or processes.	Shared	Comcast is responsible for configuring the anti-malware solution deployed to their system components that could impact the security of the uCPE. Customer is responsible for configuring the anti-malware solution deployed to their system components in scope.
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1**.** **Applicability Notes** This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for configuring the anti-malware solution deployed to their system components that could impact the security of the uCPE. Customer is responsible for configuring the anti-malware solution deployed to their system components in scope.

5.3.3 For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. **Applicability Notes** This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment**.**	Shared	Comcast is responsible for configuring the anti-malware solution deployed to their system components that could impact the security of the uCPE. Customer is responsible for configuring the anti-malware solution deployed to their system components in scope.
5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	Shared	Comcast is responsible for configuring the anti-malware solution deployed to their system components that could impact the security of the uCPE. Customer is responsible for configuring the anti-malware solution deployed to their system components in scope.
5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period. **Applicability Notes** Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware 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 during which anti-malware protection is not active.	Shared	Comcast is responsible for configuring the anti-malware solution deployed to their system components that could impact the security of the uCPE. Customer is responsible for configuring the anti-malware solution deployed to their system components in scope.
5.4 Anti-phishing mechanisms protect users against phishing attacks.		
5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. **Applicability Notes** This requirement applies to the automated mechanism. It is not intended that the systems and services providing such automated mechanisms (such as email servers) are brought into scope for PCI DSS. The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for deploying processes and automated mechanisms to detect and protect their personnel with access to system components that could impact the security of the uCPE against phishing attacks. Customer is responsible for deploying processes and automated mechanisms to detect and protect their personnel in scope against phishing attacks.
Requirement 6: Develop and Maintain Secure Systems and Software		
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.		

6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for security policies and operational procedures for managing their persons, processes, and technologies in scope.
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood. *New requirement - effective immediately*	Shared	Comcast is responsible for documenting roles and responsibilities for performing activities in Requirement 6 for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for documenting roles and responsibilities for performing activities in Requirement 6 for managing their persons, processes, and technologies in scope.
6.2 Bespoke and custom software is developed securely.		
6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle. **Applicability Notes** This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.	Shared	Comcast is responsible for securely developing bespoke and customer software that could impact the security of the uCPE. Customer is responsible for securely developing bespoke and custom software in scope.
6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. **Applicability Notes:** This requirement for code reviews applies to all bespoke and custom software (both internal and public facing), as part of the system development lifecycle. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.4. Code reviews may be performed using either manual or automated processes, or a combination of both.	Shared	Comcast is responsible for training their personnel that develop bespoke and customer software that could impact the security of the uCPE. Customer is responsible for training their personnel that develop bespoke and custom software in scope.
6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.	Shared	Comcast is responsible for reviewing their bespoke and customer software that could impact the security of the uCPE. Customer is responsible for their bespoke and custom software in scope.

6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: • Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. • Reviewed and approved by management prior to release. **Applicability Notes** Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel. An individual that has been formally granted accountability for release control and who is neither the original code author nor the code reviewer fulfills the criteria of being management.	Shared	Comcast is responsible for reviewing their bespoke and customer software that could impact the security of the uCPE. Customer is responsible for their bespoke and custom software in scope.
6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities for bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. **Applicability Notes** This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.	Shared	Comcast is responsible for defining software engineering techniques in use by their personnel that develop bespoke and customer software that could impact the security of the uCPE. Customer is responsible for defining software engineering techniques in use by their personnel that develop bespoke and custom software in scope.
6.3 Security vulnerabilities are identified and addressed.		

6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings, at a minimum, identify all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. **Applicability Notes** This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.	Shared	Comcast is responsible for identifying and managing security vulnerabilities in uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for identifying and managing security vulnerability in their system components in scope.
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for maintaining an inventory of their bespoke and customer software that could impact the security of the uCPE. Customer is responsible for maintaining an inventory of their bespoke and custom software in scope.
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	Shared	Comcast is responsible for installing patches to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for installing patches to their system components in scope.
6.4 Public-facing web applications are protected against attacks.		

6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: • At least once every 12 months and after significant changes. • By an entity that specializes in application security. • Including, at a minimum, all common software attacks in Requirement 6.2.4. • All vulnerabilities are ranked in accordance with requirement 6.3.1. • All vulnerabilities are corrected. • The application is re-evaluated after the corrections **OR** • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: • Installed in front of public-facing web applications to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated. **Applicability Notes** This assessment is not the same as the vulnerability scans performed for Requirement 11.3.1 and 11.3.2. This requirement will be superseded by Requirement 6.4.2 after 31 March 2025 when Requirement 6.4.2 becomes effective.	Shared	Comcast is responsible for protecting their public-facing web applications that could impact the security of the uCPE. Customer is responsible for protecting their public-facing web applications in scope.
6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated. Applicability Notes This new requirement will replace Requirement 6.4.1 once its effective date is reached. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for protecting their public-facing web applications that could impact the security of the uCPE. Customer is responsible for protecting their public-facing web applications in scope.
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary. **Applicability Notes** This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to payment page requirements in this context. This requirement is the sole responsibility of the customer.
6.5 Changes to all system components are managed securely.		

6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.	Shared	Comcast is responsible for securely managing changes to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for securely managing changes to their system components in scope.
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable. **Applicability Notes** These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmation activity per Requirement 12.5.2.	Shared	Comcast is responsible for confirming that all applicable PCI DSS requirements are in place after significant changes to uCPE firmware or their system components that could impact the security of the uCPE. Customer is responsible confirming that all applicable PCI DSS requirements are in place after significant changes to their system components in scope.
6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.	Shared	Comcast is responsible for separating environments where their uCPE firmware or their system components that could impact the security of the uCPE are deployed. Customer is responsible for separating environments where their system components in scope.
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed. **Applicability Notes** In environments with limited personnel where individuals perform multiple roles or functions, this same goal can be achieved with additional procedural controls that provide accountability. For example, a developer may also be an administrator that uses an administrator-level account with elevated privileges in the development environment and, for their developer role, they use a separate account with user-level access to the production environment.	Shared	Comcast is responsible for separating roles and functions for their uCPE firmware or their system components that could impact the security of the uCPE are deployed. Customer is responsible for separating roles and functions for their system components in scope.
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data change management requirements in this context. This requirement is the sole responsibility of the customer.

6.5.6 Test data and test accounts are removed from system components before the system goes into production.	Shared	Comcast is responsible for removing test data and test accounts from uCPE firmware and their system components that could impact the security of the uCPE before going into production. Customer is responsible for removing test data and test accounts from the uCPE and their system components in scope before going into production.
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know		
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.		
7.1.1 All security policies and operational procedures that are identified in Requirement 7 are: • Documented, • Kept up to date • In use • Known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for security policies and operational procedures for managing their persons, processes, and technologies in scope.
7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood. *New requirement - effective immediately*	Shared	Comcast is responsible for documenting roles and responsibilities for performing activities in Requirement 7 for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for documenting roles and responsibilities for performing activities in Requirement 7 for managing their persons, processes, and technologies in scope.
7. 2 Access to system components and data is appropriately defined and assigned.		
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	Shared	Comcast is responsible for defining an access control model for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for defining an access control model for access to the uCPE and their system components in scope.
7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	Shared	Comcast is responsible for appropriately assigning access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for appropriately assigning access to the uCPE and their system components in scope.

7.2.3 Required privileges are approved by authorized personnel.	Shared	Comcast is responsible for approving access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for approving access to the uCPE and their system components in scope.
7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate. **Applicability Notes** This requirement applies to all user accounts and related access privileges, including those used by personnel and third parties/vendors, and accounts used to access third-party cloud services. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for reviewing access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for reviewing access to the uCPE and their system components in scope.
7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for assigning and managing application and system account access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for assigning and managing application and system account access to the uCPE and their system components in scope.
7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/ system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for reviewing application and system account access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for assigning and managing application and system account access to the uCPE and their system components in scope.
7.2.6 All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD. **Applicability Notes** This requirement applies to controls for user access to query repositories of stored cardholder data. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.

7.3 Logical access to system components and data is managed via an access control system(s).		
7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	Shared	Comcast is responsible for deploying an access control system for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for deploying an access control system for access to their system components in scope.
7.3.2 The access control system(s) is configured to enforce privileges assigned to individuals, applications, and systems based on job classification and function.	Shared	Comcast is responsible for configuring an access control system for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for configuring an access control system for access to their system components in scope.
7.3.3 The access control system(s) is set to "deny all" by default.	Shared	Comcast is responsible for configuring an access control system for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for configuring an access control system for access to their system components in scope.
Requirement 8: Identify Users and Authenticate Access to System Components		
8.1 Processes and mechanisms to perform activities in Requirement 8 are defined and understood.		
8.1.1 All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for security policies and operational procedures for managing their persons, processes, and technologies in scope.
8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood. *New requirement - effective immediately*	Shared	Comcast is responsible for documenting roles and responsibilities for performing activities in Requirement 8 for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for documenting roles and responsibilities for performing activities in Requirement 8 for managing their persons, processes, and technologies in scope.
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.		

8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed. **Applicability Notes** This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).	Shared	Comcast is responsible for assigning unique IDs for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for assigning unique IDs for access to the uCPE and their system components in scope.
8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user. **Applicability Notes** This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).	Shared	Comcast is responsible for managing group, shared, or generic for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for assigning unique IDs for access to the uCPE and their system components in scope.
8.2.3 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises use unique authentication factors for each customer premises. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. This requirement is not intended to apply to service providers accessing their own shared services environments, where multiple customer environments are hosted. If service provider employees use shared authentication factors to remotely access customer premises, these factors must be unique per customer and managed in accordance with Requirement 8.2.2.	Shared	Comcast is responsible for managing access to uCPE firmware. If customer serves in Service Provider role, they are responsible for managing access to their downstream customer's premises.
8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval. **Applicability Notes** This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers and third-party vendors.	Shared	Comcast is responsible for managing identifiers for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for managing identifiers for access to the uCPE and their system components in scope.
8.2.5 Access for terminated users is immediately revoked	Shared	Comcast is responsible for terminating access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for terminating access to the uCPE and their system components in scope.

8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.	Shared	Comcast is responsible for removing or disabling access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for removing or disabling access to the uCPE and their system components in scope.
8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.	Shared	Comcast is responsible for third-party access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for third-party access to the uCPE and their system components in scope.
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session. **Applicability Notes** This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.	Shared	Comcast is responsible for session timeouts for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for session timeouts for access to the uCPE and their system components in scope.
8.3 Strong authentication for users and administrators is established and managed.		
8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element. **Applicability Notes** This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements. A digital certificate is a valid option for "something you have" if it is unique for a particular user.	Shared	Comcast is responsible for authentication factors for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for authentication factors for access to their system components in scope.
8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	Shared	Comcast is responsible for using strong cryptography for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for strong cryptography for access to their system components in scope.

8.3.3 User identity is verified before modifying any authentication factor.	Shared	Comcast is responsible for managing authentication factors for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for managing authentication factors for access to the uCPE and their system components in scope.
8.3.4 Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. **Applicability Notes** This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).	Shared	Comcast is responsible for managing authentication attempts for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for managing authentication attempts for access to the uCPE and their system components in scope.
8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	Shared	Comcast is responsible for managing password policies for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for password policies for access to the uCPE and their system components in scope.
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters. **Applicability Notes** This requirement is not intended to apply to: • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). • Application or system accounts, which are governed by requirements in section 8.6. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.	Shared	Comcast is responsible for managing password policies for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for password policies for access to the uCPE and their system components in scope.
8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used. **Applicability Notes** This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).	Shared	Comcast is responsible for managing password policies for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for password policies for access to the uCPE and their system components in scope.

8.3.8 Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	Shared	Comcast is responsible for documenting authentication policies and procedures for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for documenting authentication policies and procedures for access to the uCPE and their system components in scope.
8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, **OR** • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. **Applicability Notes** This requirement applies to in-scope system components that are not in the CDE because these components are not subject to MFA requirements. This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not apply to service providers' customer accounts but does apply to accounts for service provider personnel.	Shared	Comcast is responsible for managing password policies for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for password policies for access to the uCPE and their system components in scope.
8.3.10 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically. • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. This requirement does not apply to accounts of consumer users accessing their own payment card information. This requirement for service providers will be superseded by Requirement 8.3.10.1 once 8.3.10.1 becomes effective.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data access requirements in this context. This requirement is the sole responsibility of the customer, if they serve in the Service Provider role.

8.3.10.1 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, **OR** • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. This requirement does not apply to accounts of consumer users accessing their own payment card information. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* Until this requirement is effective on 31 March 2025, service providers may meet either Requirement 8.3.10 or 8.3.10.1.	Customer	Comcast does not support customer user accounts in delivery of this product. Comcast therefore is not subject to customer user access requirements in this context. This requirement is the sole responsibility of the customer, if they serve in the Service Provider role.
8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	Shared	Comcast is responsible for managing authentication factors for access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for managing authentication factors for access to the uCPE and their system components in scope.
8.4 Multi-factor authentication (MFA) systems are configured to prevent misuse.		
8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access. **Applicability Notes** The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection—that is, via logical access occurring over a network interface rather than via a direct, physical connection. MFA is considered a best practice for non-console administrative access to in-scope system components that are not part of the CDE.	Shared	Comcast is responsible for implementing MFA for non-console access to the uCPE and uCPE firmware and to their system components that could be used to administer the uCPE. Customer is responsible for implementing MFA for non-console access to the uCPE and for access to components within their CDE.

8.4.2 MFA is implemented for all access into the CDE. **Applicability Notes** This requirement does not apply to: • Application or system accounts performing automated functions. • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting via non-console administrative access from the entity's network into the CDE. (continued on next page) The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function. MFA for remote access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.	Shared	Comcast is responsible for implementing MFA for non-console access to the uCPE and uCPE firmware and to their system components that could be used to administer the uCPE. Customer is responsible for implementing MFA for non-console access to the uCPE and for access to components within their CDE.
8.4.3 MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors. **Applicability Notes** The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE. If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity's networks. The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.	Shared	Comcast is responsible for implementing MFA for remote access from outside networks to networks that could access or impact the security of the uCPE. Customer is responsible for implementing MFA for remote access from outside networks to networks that could access or impact the security of their CDE.

8.5 Multi-factor authentication is implemented to secure access to the CDE.		
8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for implementing MFA for remote access from outside networks to networks that could access or impact the security of the uCPE. Customer is responsible for implementing MFA for remote access from outside networks to networks that could access or impact the security of their CDE.
8.6 Use of application and system accounts and associated authentication factors are strictly managed.		
8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for managing application and system account access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for managing application and system account access to the uCPE and their system components in scope.
8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. Note: stored passwords/ passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2. **Applicability Notes** Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for managing password policies for application and system account access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for managing password policies for application and system account access to the uCPE and their system components in scope.
8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for managing password policies for application and system account access to uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for managing password policies for application and system account access to the uCPE and their system components in scope.

Requirement 9: Restrict Physical Access to Cardholder Data		
9.1 Processes and mechanisms for performing activities in Requirement 9 are defined and understood.		
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood. *New requirement - effective immediately*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.2 Physical access controls manage entry into the cardholder data environment.		
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.

9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.3 Physical access to the cardholder data environment for personnel and visitors is authorized and managed.		
9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.3.4 A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.		

9.4.1 All media with cardholder data is physically secured.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.4.1.1 Offline media backups with cardholder data are stored in a secure location.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). **Applicability Notes** Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have "manager" as part of their title.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.4.5 Inventory logs of all electronic media with cardholder data are maintained.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.

9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction. **Applicability Notes** These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed. **Applicability Notes** These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.		
9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices. **Applicability Notes** These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped). This requirement is not intended to apply to manual PAN key-entry components such as computer keyboards. This requirement is recommended, but not required, for manual PAN key-entry components such as computer keyboards. This requirement does not apply to commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.

9.5.1.1 An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data physical access requirements in this context. This requirement is the sole responsibility of the customer.
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data		
10.1 Processes and mechanisms for performing activities in Requirement 10 are defined and documented.		
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for security policies and operational procedures for managing their persons, processes, and technologies in scope.
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood. *New requirement - effective immediately*	Shared	Comcast is responsible for documenting roles and responsibilities for performing activities in Requirement 10 for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for documenting roles and responsibilities for performing activities in Requirement 10 for managing their persons, processes, and technologies in scope.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.		
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	Shared	Comcast is responsible for configuring and implementing logging on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring and implementing logging on their system components in scope.
10.2.1.1 Audit logs capture all individual user access to cardholder data.	Shared	Comcast is responsible for configuring and implementing logging on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring and implementing logging on their system components in scope.
10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	Shared	Comcast is responsible for configuring and implementing logging on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring and implementing logging on their system components in scope.
10.2.1.3 Audit logs capture all access to audit logs.	Shared	Comcast is responsible for configuring and implementing logging on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring and implementing logging on their system components in scope.
10.2.1.4 Audit logs capture all invalid logical access attempts.	Shared	Comcast is responsible for configuring and implementing logging on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring and implementing logging on their system components in scope.
10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	Shared	Comcast is responsible for configuring and implementing logging on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring and implementing logging on their system components in scope.

10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.	Shared	Comcast is responsible for configuring and implementing logging on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring and implementing logging on their system components in scope.
10.2.1.7 Audit logs capture all creation and deletion of system-level objects.	Shared	Comcast is responsible for configuring and implementing logging on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring and implementing logging on their system components in scope.
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	Shared	Comcast is responsible for configuring and implementing logging on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring and implementing logging on their system components in scope.
10.3 Audit logs are protected from destruction and unauthorized modifications.		
10.3.1 Read access to audit logs files is limited to those with a job-related need.	Shared	Comcast is responsible for limiting read access to logs from the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for limiting read access to logs from their system components in scope.
10.3.2 Audit log files are protected to prevent modifications by individuals.	Shared	Comcast is responsible for protecting logs from the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for protecting logs from their system components in scope.
10.3.3 Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	Shared	Comcast is responsible for backing up logs from the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for backing up logs from their system components in scope.
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	Shared	Comcast is responsible for deploying change-detection mechanism on logs from the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for deploying change-detection mechanisms on logs from their system components in scope.
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.		

10.4.1 The following audit logs are reviewed at least once 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, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).	Shared	Comcast is responsible for reviewing logs from the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for reviewing logs from their system components in scope.
10.4.1.1 Automated mechanisms are used to perform audit log reviews. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for using automated mechanisms to review logs from the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for using automated mechanisms to review logs from their system components in scope.
10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically. **Applicability Notes** This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1.	Shared	Comcast is responsible for reviewing logs from the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for reviewing logs from their system components in scope.
10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for completing a targeted risk analysis to identify the frequency for reviewing logs not already defined for 10.4.1. Customer is responsible for completing a targeted risk analysis to identify the frequency for reviewing logs not already defined for 10.4.1.
10.4.3 Exceptions and anomalies identified during the review process are addressed.	Shared	Comcast is responsible for addressing exceptions and anomalies identified when reviewing logs from the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for addressing exceptions and anomalies identified when reviewing logs from their system components in scope.
10.5 Audit log history is retained and available for analysis.		
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	Shared	Comcast is responsible for retaining logs from the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for retaining logs from their system components in scope.
10.6 Time-synchronization mechanisms support consistent time settings across all systems.		

10.6.1 System clocks and time are synchronized using time-synchronization technology. **Applicability Notes** Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3.	Shared	Comcast is responsible for synchronizing system clocks on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for synchronizing system clocks on their system components in scope.
10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).	Shared	Comcast is responsible for configuring time settings on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring time settings on their system components in scope.
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.	Shared	Comcast is responsible for configuring time settings on the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for configuring time settings on their system components in scope.
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.		
10.7.1 ***Additional requirement for service providers only:*** Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls • IDS/IPS • FIM • Anti-malware solutions • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. This requirement will be superseded by Requirement 10.7.2 as of 31 March 2025.	Shared	Comcast is responsible for detecting, alerting on, and addressing failures of critical security control systems that protect the uCPE and their system components that could impact the security of the uCPE. If customer serves in Service Provider role, they are responsible for detecting, alerting on, and addressing failures of critical security control systems that protect their system components in scope.

10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used). **Applicability Notes** This requirement applies to all entities, including service providers, and will supersede Requirement 10.7.1 as of 31 March 2025. It includes two additional critical security control systems not in Requirement 10.7.1. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for detecting, alerting on, and addressing failures of critical security control systems that protect the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for detecting, alerting on, and addressing failures of critical security control systems that protect their system components in scope.
10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure, and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider, until the 31 March 2025, after which this requirement will apply to all entities. *This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a best practice for all other entities until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for responding to failures of critical security control systems that protect the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for responding to failures of critical security control systems that protect their system components in scope.
Requirement 11: Test Security of Systems and Networks Regularly		
11.1 Processes and mechanisms for performing activities in Requirement 11 are defined and understood.		
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Shared	Comcast is responsible for security policies and operational procedures for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for security policies and operational procedures for managing their persons, processes, and technologies in scope.

11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood. *New requirement - effective immediately*	Shared	Comcast is responsible for documenting roles and responsibilities for performing activities in Requirement 11 for managing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for documenting roles and responsibilities for performing activities in Requirement 11 for managing their persons, processes, and technologies in scope.
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.		
11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts. **Applicability Notes** The requirement applies even when a policy exists that prohibits the use of wireless technology since attackers do not read and follow company policy. Methods used to meet this requirement must be sufficient to detect and identify both authorized and unauthorized devices, including unauthorized devices attached to devices that themselves are authorized.	Shared	Comcast is responsible for testing for the presence of unauthorized wireless access points within spaces that house system components that could impact the security of the uCPE; however, as Comcast does not use wireless networks in the delivery of this product, Comcast is not subject to any wireless network management requirements in this context. Customer is responsible for managing authorized and unauthorized wireless access points within spaces that house their system components in scope.
11.2 2 An inventory of authorized wireless access points is maintained, including a documented business justification.	Customer	Comcast does not use wireless networks in the delivery of this product. Comcast therefore is not subject to wireless access point management requirements in this context. This requirement is the sole responsibility of the customer.
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.		
11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists. **Applicability Notes** It is not required to use a QSA or ASV to conduct internal vulnerability scans. Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a network administrator should not be responsible for scanning the network), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.	Shared	Comcast is responsible for performing internal vulnerability scans of their system components that could impact the security of the uCPE. Customer is responsible for performing internal vulnerability scans of the uCPE and their system components in scope.

11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed. **Applicability Notes** The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requirement 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for managing internal vulnerability scans of their system components that could impact the security of the uCPE. Customer is responsible for managing internal vulnerability scans of the uCPE and their system components in scope.
11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • Sufficient privileges are used, for those systems that accept credentials for scanning. • If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2. **Applicability Notes** The authenticated scanning tools can be either host-based or network-based. "Sufficient" privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities. This requirement does not apply to system components that cannot accept credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, and containers. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for performing internal vulnerability scans of their system components that could impact the security of the uCPE. Customer is responsible for performing internal vulnerability scans of the uCPE and their system components in scope.
11.3.1.3 Internal vulnerability scans are performed after any significant change as follows: • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1 are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). **Applicability Notes** Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed after significant changes.	Shared	Comcast is responsible for performing internal vulnerability scans of their system components that could impact the security of the uCPE. Customer is responsible for performing internal vulnerability scans of the uCPE and their system components in scope.

11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan. **Applicability Notes** For initial PCI DSS compliance, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). (continued on next page) However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred. ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer. Refer to the *ASV Program Guide* published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.	Shared	Comcast is responsible for performing external vulnerability scans of their system components that could impact the security of the uCPE using an ASV. Customer is responsible for performing external vulnerability scans of the uCPE and their system components in scope using an ASV.
11.3.2.1 External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	Shared	Comcast is responsible for performing external vulnerability scans of their system components that could impact the security of the uCPE using an ASV. Customer is responsible for performing external vulnerability scans of the uCPE and their system components in scope using an ASV.
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.		

11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months. **Applicability Notes** Testing from inside the network (or "internal penetration testing") means testing from both inside the CDE and into the CDE from trusted and untrusted internal networks. Testing from outside the network (or "external" penetration testing" means testing the exposed external perimeter of trusted networks, and critical systems connected to or accessible to public network infrastructures.	Shared	Comcast is responsible for defining, documenting, and implementing a penetration test methodology for their system components that could impact the security of the uCPE. Customer is responsible is responsible for defining, documenting, and implementing a penetration test methodology for the uCPE and their system components in scope.
11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).	Shared	Comcast is responsible for performing internal penetration testing of their system components that could impact the security of the uCPE. Customer is responsible for performing internal penetration testing of the uCPE and their system components in scope.
11.4.3 External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV).	Shared	Comcast is responsible for performing external penetration testing of their system components that could impact the security of the uCPE. Customer is responsible for performing external penetration testing of the uCPE and their system components in scope.
11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Require ment 6.3.1. • Penetration testing is repeated to verify the corrections.	Shared	Comcast is responsible for correcting vulnerabilities found during penetration testing of their system components that could impact the security of the uCPE. Customer is responsible for correcting vulnerabilities found during penetration testing of the uCPE and their system components in scope.

11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to segmentation requirements in this context. This requirement is the sole responsibility of the customer.
11.4.6 ***Additional requirement for service providers only:*** If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV). **Applicability Notes** This requirement applies only when the entity being assessed is a service provider.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to segmentation requirements in this context. This requirement is the sole responsibility of the customer, if they serve in the Service Provider role.

11.4.7 ***Additional requirement for third-party hosted/cloud service providers only:*** Third-party hosted/cloud service providers support to their customers for external penetration testing per Requirement 11.4.3 and 11.4.4. **Applicability Notes** To meet this requirement, third-party hosted/cloud service providers may either: • Provide evidence to its customers to show that penetration testing has been performed according to Requirements 11.4.3 and 11.4.4 on the customers' subscribed infrastructure, or • Provide prompt access to each of their customers, so customers can perform their own penetration testing. Evidence provided to customers can include redacted penetration testing results but needs to include sufficient information to prove that all elements of Requirements 11.4.3 and 11.4.4 have been met on the customer's behalf. This requirement applies only when the entity being assessed is a service provider managing third-party hosted/cloud environments. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does provide third-party hosting or cloud service in delivery of this product. Comcast therefore is not subject to third-party hosted / cloud service provider requirements in this context. This requirement is the sole responsibility of the customer, if they serve in the Third-Party Hosted / Cloud Service Provider role.
11.5 Network intrusions and unexpected file changes are detected and responded to.		
11.5.1 Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to IDS/IPS requirements in this context. This requirement is the sole responsibility of the customer.
11.5.1.1 ***Additional requirement for service providers only:*** Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to IDS/IPS requirements in this context. This requirement is the sole responsibility of the customer, they serve in the Service Provider role.
11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files • To perform critical file comparisons at least once weekly. **Applicability Notes** 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).	Shared	Comcast is responsible for deploying a change-detection mechanism on the uCPE firmware and their system components that could impact the security of the uCPE. Customer is responsible for deploying a change-detection mechanism on their system components in scope.
11.6 Unauthorized changes on payment pages are detected and responded to.		

11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: - At least once every seven days **OR** - Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). **Applicability Notes** The intention of this requirement is not that an entity installs software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described under Examples in the PCI DSS Guidance to prevent and detect unexpected script activities. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to payment page requirements in this context. This requirement is the sole responsibility of the customer.
Requirement 12: Support information security with organizational policies and programs		
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.		
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	Shared	Comcast is responsible for establishing, publishing, maintaining, and disseminating an information security policy governing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for establishing, publishing, maintaining, and disseminating an information security policy governing their persons, processes, and technologies in scope.
12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.	Shared	Comcast is responsible for reviewing and updating their information security policy governing their system components, people, and processes that could impact the security of the uCPE annually. Customer is responsible for reviewing and updating their information security policy governing their persons, processes, and technologies in scope annually.

12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware and acknowledge their information security responsibilities.	Shared	Comcast is responsible for defining roles and responsibilities in their information security policy governing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for defining roles and responsibilities in their information security policy governing their persons, processes, and technologies in scope.
12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.	Shared	Comcast is responsible for defining responsibilities in their information security policy governing their system components, people, and processes that could impact the security of the uCPE. Customer is responsible for defining responsibilities in their information security policy governing their persons, processes, and technologies in scope.
12.2 Acceptable use policies for end-user technologies are defined and implemented.		
12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software. **Applicability Notes** Examples of end-user technologies for which acceptable use policies are expected, include but are not limited to, remote access and wireless technologies, laptops, tablets, mobile phones, and removable electronic media, email usage, and Internet usage.	Shared	Comcast is responsible for documenting acceptable use policies for end-user technologies that could impact the security of the uCPE. Customer is responsible for documenting acceptable use policies for their technologies in scope.
12.3 Targeted risks to the cardholder data environment are formally identified, evaluated, and managed.		
12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for completing a targeted risk analysis for requirements that provide flexibility for how frequently they are performed for controls that could impact the security of the uCPE. Customer is responsible for completing a targeted risk analysis for requirements that provide flexibility for how frequently they are performed for their controls in scope.

12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix B: Guidance and Instructions for Using Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months. *New requirement - effective immediately* **Applicability Notes** This only applies to entities using a Customized Approach.	Shared	Comcast is responsible for completing a targeted risk analysis for requirements they meet using the customized approach. Customer is responsible for completing a targeted risk analysis for requirements they meet using the customized approach.
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities. **Applicability Notes** The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for documenting and reviewing cryptographic cipher suites and protocols in use on the uCPE and their system components that could impact the security of the uCPE at least once every 12 months. Customer is responsible for documenting and reviewing cryptographic cipher suites and protocols in use on their system components in scope at least once every 12 months.
12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for reviewing hardware and software technologies on the uCPE and their system components that could impact the security of the uCPE at least once every 12 months. Customer is responsible for reviewing hardware and software technologies for their technologies in scope.
12.4 PCI DSS compliance is managed.		

12.4.1 ***Additional requirement for service providers only:*** Responsibility is established by executive management 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. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure. Responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization.	Shared	Comcast is responsible for establishing a PCI DSS compliance program governing their system components, people, and processes that could impact the security of the uCPE. If customer serves in Service Provider role, they are responsible for establishing a PCI DSS compliance program governing their persons, processes, and technologies in scope.
12.4.2 ***Additional requirement for service providers only:*** Reviews are performed at least once every three months to confirm personnel are performing their tasks in accordance with all security policies and all operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider.	Shared	Comcast is responsible for reviewing that security policies and operational procedures are operating effectively that governing their system components, people, and processes that could impact the security of the uCPE at least once every three months. If customer serves in Service Provider role, they are responsible for reviewing that security policies and operational procedures are operating effectively that governing their persons, processes, and technologies in scope at least once every three months.
12.4.2.1 Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include: • Results of the reviews. • Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider.	Shared	Comcast is responsible for reviewing that security policies and operational procedures are operating effectively that governing their system components, people, and processes that could impact the security of the uCPE at least once every three months. If customer serves in Service Provider role, they are responsible for reviewing that security policies and operational procedures are operating effectively that governing their persons, processes, and technologies in scope at least once every three months.
12.5 PCI DSS scope is documented and validated.		
12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	Shared	Comcast is responsible for maintaining an inventory of their system components that could impact the security of the uCPE. Customer is responsible for maintaining an inventory of their system components in scope.

12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. *New requirement - effective immediately* **Applicability Notes** This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the annual assessment.	Shared	Comcast is responsible for documenting scope, which includes their system components that could impact the security of the uCPE at least once every 12 months. Customer is responsible for documenting their scope at least once every 12 months.
12.5.2.1 ***Additional requirement for service providers only:*** PCI DSS scope is documented and confirmed by the entity at least once every six months and after significant changes. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment*.	Shared	Comcast is responsible for documenting scope, which includes their system components that could impact the security of the uCPE at least once every 6 months. If customer serves in Service Provider role, they are responsible for documenting their scope at least once every 6 months.
12.5.3 ***Additional requirement for service providers only:*** Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for reviewing their scope, which includes their system components that could impact the security of the uCPE upon significant changes to organizational structure. If customer serves in Service Provider role, they are responsible for reviewing their scope upon significant changes to organizational structure.
12.6 Security awareness education is an ongoing activity		

12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures and their role in protecting the cardholder data.	Shared	Comcast is responsible for implementing a formal security awareness program for their personnel that could impact the security of the uCPE. Customer is responsible for implementing a formal security awareness program for their personnel in scope.
12.6.2 The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for reviewing the security awareness program for their personnel that could impact the security of the uCPE at least once every 12 months. Customer is responsible for reviewing the security awareness program for their personnel in scope at least once every 12 months.
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	Shared	Comcast is responsible for delivering security awareness training for their personnel that could impact the security of the uCPE. Customer is responsible for delivering security awareness training for their personnel in scope.
12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks. • Social engineering. **Applicability Notes** See Requirement 5.4.1 for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for delivering security awareness training for their personnel that could impact the security of the uCPE. Customer is responsible for delivering security awareness training for their personnel in scope.
12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for delivering security awareness training for their personnel that could impact the security of the uCPE. Customer is responsible for delivering security awareness training for their personnel in scope.
12.7 Personnel are screened to reduce risks from insider threats.		
12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources. **Applicability Notes** For those potential personnel to be hired for 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.	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to personnel screening requirements in this context. This requirement is the sole responsibility of the customer.
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.		

12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided. **Applicability Notes** The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.	Shared	Comcast is responsible for maintaining a list of all third-party service providers that could impact the security of the uCPE. Customer is responsible for maintaining a list of all third-party service providers in scope.
12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgements from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE. **Applicability Notes** The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement. Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) or a declaration on a company's website) is not the same as a written agreement specified in this requirement.	Shared	Comcast is responsible for maintaining written agreements with all third-party service providers that could impact the security of the uCPE. Customer is responsible for maintaining written agreements with all third-party service providers in scope.
12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	Shared	Comcast is responsible for implementing an established process for engaging all third-party service providers that could impact the security of the uCPE. Customer is responsible for implementing an established process for engaging all third-party service providers in scope.
12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months. **Applicability Notes** Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.	Shared	Comcast is responsible for implementing an established program for monitoring PCI DSS compliance status of all third-party service providers that could impact the security of the uCPE at least once every 12 months. Customer is responsible for implementing an established program for monitoring PCI DSS compliance status for all third-party service providers in scope at least once every 12 months.
12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	Shared	Comcast is responsible for maintaining information about PCI DSS requirement responsibilities with third-party service providers that could impact the security of the uCPE. Customer is responsible for maintaining information about PCI DSS requirement responsibilities with all third-party service providers in scope.
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.		

12.9.1 ***Additional requirement for service providers only:*** TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP 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 CDE. **Applicability Notes** This requirement applies only when the entity being assessed is a service provider. The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement.	Shared	Comcast is responsible for acknowledging in writing that they are responsible for security to the extent that they could impact the security of the uCPE. If customer serves in the Service Provider role, they are responsible for acknowledging in writing that they are responsible for the security of account data the TPSP 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 CDE.
12.9.2 Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5). *New requirement - effective immediately* **Applicability Notes** This requirement applies only when the entity being assessed is a service provider.	Shared	Comcast is responsible for supporting their customers' requests for information to meet Requirements 12.8.4 and 12.8.5. If customer serves in the Service Provider role, they are responsible for supporting their customers' requests for information to meet Requirements 12.8.4 and 12.8.5.
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.		
12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	Shared	Comcast is responsible for establishing an incident response plan ready to be activated in the event of a security incident on the uCPE or their system components that could impact the security of the uCPE. Customer is responsible for establishing an incident response plan ready to be activated in the event of a security incident on their system components in scope.
12.10.2 At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	Shared	Comcast is responsible for reviewing, updating, and testing their incident response plan at least once every 12 months. Customer is responsible for reviewing, updating, and testing their incident response plan at least once every 12 months.

12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	Shared	Comcast is responsible for designating personnel to respond to security incidents on the uCPE or their system components that could impact the security of the uCPE. Customer is responsible for designating personnel to respond to security incidents on their system components in scope.
12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.	Shared	Comcast is responsible for training personnel who respond to security incidents on the uCPE or their system components that could impact the security of the uCPE. Customer is responsible for training personnel who to respond to security incidents on their system components in scope.
12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis which is performed according to all elements specified in Requirement 12.3.1. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for performing a targeted risk analysis to define the frequency for providing training to the personnel who respond to security incidents on the uCPE or their system components that could impact the security of the uCPE. Customer is responsible for performing a targeted risk analysis to define the frequency for providing training to personnel who to respond to security incidents on their system components in scope.
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Detection of unauthorized wireless access points. **Applicability Notes** *The bullet above (for monitoring and responding to alerts from a change- and tamper-detection mechanism for payment pages) is a best practice until 31 March 2025, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.*	Shared	Comcast is responsible for monitoring and responding to alerts from security monitoring systems that protect the uCPE and their system components that could impact the security of the uCPE. Customer is responsible for monitoring and responding to alerts from security monitoring systems that protect their system components in scope.
12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	Shared	Comcast is responsible for modifying and evolving their incident response plan according to lessons learned Customer is responsible for modifying and evolving their incident response plan according to lessons learned.

12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	Customer	Comcast does not store, process, or transmit account data for or on behalf of its customers in delivery of this product. Comcast therefore is not subject to account data storage requirements in this context. This requirement is the sole responsibility of the customer.