verizon

MANAGED WAN

1. GENERAL

1.1 **Service Definition.** Managed Wide Area Network Service (Managed WAN) provides a range of service options enabling Customer to transfer all or part of its wide area network management to Verizon, including network design, CPE configuration, service installation, proactive monitoring, fault notification, reporting, device management, software support (subject to availability), as well as network support for both Verizon and third party transport.

- **General.** Managed WAN is supported on Customer Networks as determined and approved by Verizon. Networks approved by Verizon may include private networks, public networks, as well as wireline access, or cellular wireless access, or a combination thereof. Certain Networks may not be available for use with all Managed WAN Service options or features listed herein.
- **Platforms.** Except where explicitly stated otherwise, these terms apply to Optimized Service (denoted with a "+") and non-Optimized Service.

1.2 **Standard Features.** Managed WAN is offered at four service levels. The features and responsibilities are summarized in the table below. Management of SD WAN and Software Defined Secure Branch (collectively, Software Defined Networking or SDN) has features and responsibilities that are different from Managed WAN management, as shown below.

	Division of Responsibilities			
	Monitor and Notify	**Physical Management**	**Co Management**	**Full Management**
Customer	**Customer Manages:**	**Customer Manages:**	**Customer Manages:**	**Customer Manages:**
	• Strategic Direction • Fault Isolation • Fault Restoration-Logical • Fault Restoration-Physical • Maintenance-Break/Fix	• Strategic Direction • Fault Restoration-Logical • Change Management-Logical • Define Firewall Security/UTM Policy • Security Patching	• Strategic Direction • Define Firewall Security/UTM Policy • SDN Policy Management, if applicable	• Strategic Direction • Define Firewall Security/UTM Policy • SDN Policy Management, if applicable

	• Change Management-Logical • Change Management-Physical • Configuration Back-Up • Define Firewall Security / Unified Threat Management (UTM) Policy • Security Patching • SDN Policy Management, if applicable	• Configuration Back-Up (SDN only) • SDN Policy Management, if applicable		
Verizon	**Verizon Manages:**	**Verizon Manages:**	**Verizon Manages:**	**Verizon Manages:**
	• Monitoring • Fault Notification • Performance Reporting	• Monitoring • Fault Isolation • Fault Notification • Fault Restoration-Physical • Maintenance-Break/Fix • Configuration Back-Up (Excludes SDN) • Performance Reporting • Change Management-Physical	• Monitoring • Fault Isolation • Fault Notification • Fault Restoration-Logical • Fault Restoration-Physical • Maintenance-Break/Fix • Change Management-Logical • Change Management-Physical • Configuration Back-Up • Performance Reporting • Security Patching	• Monitoring • Fault Isolation • Fault Notification • Fault Restoration-Logical • Fault Restoration-Physical • Maintenance-Break/Fix • Change Management-Logical • Change Management-Physical • Configuration Back-Up • Performance Reporting • Security Patching • SDN Policy Management, if applicable

Change management of applicable software licenses that may be configured on Managed Devices does not include responsibility for tracking device-specific licenses where the device vendor permits re-use on new device acquisition.

1.2.1 **Monitor and Notify Service Level.** The most basic level of Managed WAN is Monitor and Notify, under which Verizon, provides the capabilities described below.

- **Monitoring.** Verizon proactively monitors all Managed Devices up to the local area network (LAN) interface of the Managed Device 24 hours a day, seven days a week.
- **Notification and Resolution.** Verizon will create a trouble ticket and send a notification to Customer's designated point of contact within 15 minutes of Verizon's determination of a Managed Device or transport failure. Following the creation of a trouble ticket, Verizon will a) if the trouble is due to a Verizon transport Service, troubleshoot the transport Service until the problem has been verified as fixed and the ticket will then be closed; or b) if the trouble is due to causes other than a Verizon transport Service, inform Customer of the fault and monitor the ticket.

- **Managed Services Customer Portals.** Verizon will provide a managed services portal on the Verizon Enterprise Center (VEC) (https://sso.verizonenterprise.com/amserver/sso/login.go?, or other website provided by Verizon from time to time). The VEC provides a consolidated view of Customer Network information 24 hours a day, seven days a week and real time access to project status, contact information, and information about Managed Devices. The Cloud-Controlled Routing (CCR) portal (Web Portal) is separate from the VEC, but is accessed via the VEC. Several portal permissions are generally available, however, currently, only one WEB Portal permission is available per VEC user.
- **Web Portal Administrative Access.** If Customer has Monitor and Notify CCR, Customer will have write administrative access to logically manage their Managed Devices.
- **Digital Connect API Gateway.** Verizon will provide access to the Digital Connect API gateway (https://digitalconnect.verizon.com) (API Gateway) so Customer can develop application program interfaces (API) to allow for eBonding to Verizon for services such as incident management or change management.

1.2.2 **Physical Management Service Level.** Customer can choose Physical Management which contains the capabilities of Monitor and Notify plus additional capabilities described below:

- **Design Services.** (Excludes SDN) Verizon will create a Customer design document (CDD) based on a written statement of requirements (SOR) agreed to by Customer. Verizon will activate, monitor, and manage the Customer Network as designed in the CDD.
- **Monitoring and Resolution.** Verizon provides physical fault detection, isolation, and monitoring services for Managed Devices, 24 hours per day, seven days per week. Verizon will resolve physical faults whether caused by Verizon, Customer or third party issues. Managed Device logical faults are Customer's responsibility. Customer will inform Verizon of physical faults once Customer has completed its logical troubleshooting.
- **CCR Network Image.** (Excludes SDN) If Customer has Physical Management CCR, a current image of Customer Network is stored on the Cloud Infrastructure. A roll-back to previous configurations is not supported.
- **Change Management Activities.** Verizon will perform the change management activities shown on the VEC as Standard Change Management at no charge. Optional Change Management activities will be performed at the rates shown below.

1.2.3 **Full Management Service Level.** Customer can choose Full Management, which contains the capabilities of Physical Management plus additional capabilities described below.

- **Monitoring and Resolution.** Verizon will resolve both logical and physical issues, with Customer's cooperation, either remotely or by dispatching a technician, whether caused by Verizon, Customer or a third party. The frequency of polling Managed Devices using Cellular Wireless Access is limited to conserve cellular network resources and to minimize management traffic on the cellular network.
- **Web Portal Administrative Access.** If Customer has Full Management CCR Customer will have read-only administrative access in the Web Portal.
- **SDN Policy Management.** If Customer has Full Management, Customer can make certain policy changes using the VEC for select SDN service features. Additional service features will be added to the VEC from time to time. Verizon, working with Customer, will set the initial policies during implementation. Additionally, Verizon will, from time to time, set policies that are not accessible to Customer. Customer may obtain a list of available policies by way of the VEC or by contacting Customer's account manager. Customer acknowledges and agrees that policy changes made by Customer may negatively impact application traffic, security, and UTM function performance.

1.2.4 **Co Management Service Level.** Customer can choose Co Management, which contains the capabilities of Full Management but allows Customer to manage certain capabilities as described below.

- **SDN Policy Management.** If Customer has Co Management, Customer can make certain policy changes using the VEC or API Gateway for additional select SDN service features. Additional service features will be added to the VEC and API Gateway from time to time. Verizon, working

with Customer, will set the initial policies during implementation. Additionally, Verizon will, from time to time, set policies that are not accessible to Customer. Customer may obtain a list of available policies by way of the VEC or API Gateway or by contacting Customer's account manager. Customer acknowledges and agrees that policy changes made by Customer may negatively impact application traffic, security, and UTM function performance.

1.2.5 **Implementation Options.** Managed WAN has two implementation options to bring devices under Verizon management: (a) Managed Implementation, which applies to Customer or Verizon provided devices and (b) Managed Take Over, which applies to existing, operating networks with Customer-provided devices. Managed Take Over may not be available for all Managed WAN services listed herein. Managed Implementation and Managed Take Over are both subject to an SOR to be agreed upon by the Parties.

1.2.6 **Managed Device Software Release Management**

1.2.6.1 **Installation.** Customer-requested installation of vendor software patches and updates will be installed as an Optional Change Management activity during a fixed update time period. Notwithstanding the forgoing, Verizon will install patches or updates that are related to security vulnerabilities as a Standard Change Management activity. Additionally for SDN, when a vendor no longer supports the Customer's installed software version, Verizon will install the relevant software update from the vendor as a Standard Change Management activity. Standard Change Management and Optional Change Management activities performed hereunder will be done in consultation with the Customer and at a time mutually agreed upon by the Parties. All warranties on software patches or updates, if available, will be provided directly by the vendor.

1.2.6.2 **Testing.** At Customer's request, Verizon will make commercially reasonable efforts to make available the resources of Verizon's Customer Test Center (CTC) for the purpose of testing Managed Device vendor software prior to the implementation of such software. Verizon's ability to control the implementation of any new Managed Device vendor software release may be limited by rules established by the Managed Device vendor software. CTC testing may be subject to additional fees and result in delay of the software deployment.

1.3 **Optional Features**

1.3.1 **Network Discovery.** Network Discovery is provided as part of the Managed Take Over implementation for certain management features. Otherwise, Customers may order Network Discovery for an additional Charge. If Customer orders Network Discovery, Verizon will electronically collect information on CPE connected to the Customer's network.

1.3.2 **Third Party Maintenance.** For Managed Devices under Physical, Full or Co Management service levels, Customer may elect to obtain CPE maintenance services from a third party other than Verizon. Customer shall provide Verizon a letter of authorization (LOA) to work directly with such third party on behalf of Customer.

1.3.3 **Third Party Transport Service.** With the Third Party Transport Service feature, if Customer has two or more managed Customer Sites, Verizon will monitor and manage covered third-party provided transport services and inform Customer of the existence of outages or problems with those third-party provided services.

1.3.4 **Management of Customer Premises Devices.** For management of Managed Devices on a Customer Site, Customer may select Router Management, SD WAN Management, Secure Hybrid Network, Software Defined Secure Branch, Virtual Host Management, Analog VoIP Gateway, Satellite Device Management, CCR, or Device Management. Router Management and CCR are available with all Managed WAN service levels. Secure Hybrid Network management is only available for the Secure Hybrid Network service. To effectively manage the Customer Network, all Customer

Sites with Cloud-Controlled management as part of Managed WAN or other Verizon Services (e.g., CCR, Cloud-Controlled Switching (CCS) or Cloud-Controlled Camera (CCC) for Managed LAN, and Cloud-Controlled Access Point (CCAP) for Managed WLAN) must be at the same service level. Satellite Device Management, SD WAN Management and Software Defined Secure Branch are available with Full Management, Co Management or Monitor and Notify. Virtual Host Management, Analog VoIP Gateway, Device Management, and Secure Hybrid Network are only available with Full Management.

1.3.5 **SD WAN Management + and Software Defined Secure Branch + (SDN).** Verizon proactively monitors all Verizon certified SDN Managed Devices up to the host controller for such Managed Devices, 24 hours a day, seven days a week.

- Verizon will provide programmable, rules-based WAN routing services, optional additional services, and centralized management. Available services and options are based on vendor license capabilities, regional availability, and Verizon support capabilities, and may include the options below. Customer may request a list of the services and options included in each vendor package by contacting Customer's account manager.
  - **Routing.** The routing function enables basic routing capabilities with support for common routing protocols.
  - **SD WAN Function.** This function maps Customer application traffic over the Customer Network in accordance with Customer defined policies that classify its traffic into application categories and define minimal requirements for loss, delay, and jitter per traffic or application group, such that application traffic can be routed over the preferred Customer Network paths as defined by Customer which can be updated by Customer either manually or automatically. Policies are customizable on an application-by-application basis. It also allows definition of parameters to prioritize handling of different types of application data through the quality of service (QoS) policy.
  - **Centralized enforcement of access control and network policies.** Any changes to the policy will be applied across the Customer Network automatically.
  - **Encrypted Control and Application Traffic.** The application traffic can be encrypted end to end for additional protection of the data as it traverses the Customer Network.
  - **Security.** Based on the vendor license and operating system and upon Customer's Order, Verizon will provide security functions that may include layer 4 firewall, next generation (layer 7) firewall, intrusion detection, intrusion prevention, anti-virus protection, malware protection, application control, antispam, content filtering features and zone-based firewall functionality. For select vendor licenses, Customer can change certain policy settings for select security and UTM functions for Managed Devices under Full or Co Management. Customer acknowledges and agrees that policy changes made by Customer may negatively impact application traffic, security, and UTM function performance.
  - **WAN Optimization.** Verizon will configure WAN optimization on each Managed Device as set forth in an order.
  - **Remote VPN Access.** Verizon will configure the Remote Access Server (RAS) Gateway to enable VPN tunneling and encryption between the RAS Gateway and a Remote Access Client on a remote user's endpoint device. This function enables Customer's users to remotely access the internet and corporate networks. Verizon manages the RAS Gateway but does not manage the Remote Access Client or the remote user's endpoint device.

1.3.6 **Device Management.** For select Managed Devices under Full or Physical Management, Verizon will manage such devices that terminate cellular wireless access service and are connected via Ethernet to a Router Management or SDN Managed Device that is under Full or Co Management.

1.3.7 **Managed Device Enhanced Features.** For select Managed Devices under Full Management, Verizon can provide configuration, implementation, administration, monitoring, support, reporting (if applicable), and installation of available vendor-provided and/or hardware patch/upgrades for the following features as selected by Customer.

- **Firewall.** With Firewall, Verizon will manage Customer-selectable zones (e.g. external or untrusted, internal or trusted, DMZ), firewall policies, and firewall rule sets between all zones.
- **Content Filtering.** With Content Filtering, Verizon will configure the feature to interface with Customer's Websense server based on information provided by Customer. Customer can use that server, and/or a backup list of up to 25 URL filters, to control web-based content accessed by end users.
- **Switching (For LAN Module on a Managed Device).** With LAN Module Switching, Verizon provides additional LAN ports on the Managed Device. Verizon monitors the LAN module generally, but not individual ports.
- **Encryption.** With Encryption, in countries where it is available, Verizon will encrypt Customer application traffic between Managed Devices on the Verizon Private IP Network. Customer will provide at least two additional Managed Devices with the Encryption feature to act as key servers. If circumstances arise that cause the Encryption feature to fail and prevent communication to and from that Managed Device, Customer will notify Verizon.
- **WAN Acceleration.** With WAN Acceleration, Verizon will optimize application traffic using compression, caching protocol optimization where other Sites on the Customer Network have compatible application optimization CPE.
- **Wireless LAN Controller Management.** With Wireless LAN Controller Management, Verizon will configure the Managed Device to provide Wireless LAN controller management capabilities for Customer Sites with compatible access point CPE.
- **Lightweight Access Point Management.** With Access Point Management, Verizon will configure the Managed Device with embedded Access Point functionality such that it will interoperate with Verizon Managed Wireless LAN service.
- **VPN IPSec Tunneling.** With VPN IPSec Tunneling, available on certain Managed Devices, Verizon enables the tunneling and encryption of Customer application traffic between two Managed Devices. Enabling this feature on a remote Managed Device is dependent on the same feature being enabled on a separate Customer Managed Device, typically located at the Customer hub site.
- **Wireless LAN Access Point.** With Wireless LAN Access Point, available on certain Managed Devices that have Access Point functionality, Verizon will configure the Managed Device as a Wireless access point so long as at least one other site or Managed Device in the Customer Network has a compatible Wireless LAN Controller.
- **Virtual Blade Management.** With Virtual Blade Management, Verizon makes available management of the blade on certain Managed Devices that support additional hardware used to host Virtual Machines (VMs) running Virtual Network Services (which above-described combination may also be referred to as Virtual Network Functions). To the extent Virtual Network Services are required, they are to be purchased separately.
- **Managed VoIP Services including Voice Gateway, Analog VoIP Gateway, and Multi-Service IP-to-IP Gateway**. With Managed VoIP Services, Verizon will manage VoIP CPE Elements (not VoIP Service devices such as phones) at the same management level as the related Managed Devices. Certain Customer roles and responsibilities for the underlying VoIP Service may be impacted by Managed VoIP Services. Verizon will work with Customer to address such impacts.
- **Virtual Host Management.** Virtual Host Management supports a universal CPE device deployed to the Customer Site. This hardware device is used to host virtual machines running virtual network services (which may also be referred to as Virtual Network Functions) which include Security and WAN Services. Customer acknowledges that Virtual Host Management covers the universal CPE device only, and does not cover any Virtual Network Functions hosted on that universal CPE. For Virtual Network Functions hosted on the universal CPE, Customer must purchase Virtual Network Services separately.
- **Cloud Security Services.** For select Managed Devices, Verizon will configure and manage the connection from the Managed Device to an external cloud-based security service. Approved security services may be provided by Verizon or a third party.
- **Embedded WiFi.** For select Managed Devices, Verizon will configure and manage WiFi service; WiFi services are standalone and not compatible or interoperable with Managed Wireless LAN service.

- **Vendor Reporting.** For select Managed Devices, Verizon will configure the controllers and network to allow Customer access to specific SDN vendor reporting tools as necessary. No vendor reporting data shall be used for service level monitoring purposes, and Customer acknowledges that Verizon has no responsibility for the accuracy or availability of vendor reporting tools.
- **WAN Back Up.** With WAN Back up, Verizon configures a Managed Device to support a second access circuit (separately provided by Verizon or a third party) in the event the primary network connection fails. For select Managed Devices, an embedded LTE modem is available for use to provide an access path for wireless WAN Back up applications. For SDN services, the wireless back up path is set up as a path of last resort.

1.3.8 **WAN Analysis**

1.3.8.1 **Non-Optimized Service.** If Customer receives non-Optimized Managed WAN, the terms and conditions for WAN Analysis are located at the following URL:
For U.S. Services:
www.verizon.com/business/service_guide/reg/cp_war_plus_wan_analysis_reporting.pdf.
For non-U.S. Services:
https://www.verizon.com/business/service_guide/reg/cp_war_plus_wan_analysis_reporting_2020JUN15.pdf.

1.3.8.2 **Optimized Service.** For Managed WAN +, WAN Analysis includes support for SDN reports for Verizon-supported vendors. WAN Analysis is not included for certain vendor software license levels under Software Defined Secure Branch that do not include SDN functions.

1.3.8.3 WAN Analysis is not available for Managed Devices that utilize Cellular Wireless Access as the primary or active network connection.

1.3.9 **Network Analysis Service (NA)**. (For Customer Networks with 20 or more Managed Devices with an Agreement governed by U.S. law). With NA, Verizon will provide monthly network analysis reporting, including interactive monthly calls to review that reporting, starting 60-90 days after installation.

1.3.10 **Network Engineering Service (NE).** (For larger Customer Networks, i.e., those with 20 or more Managed Devices under Full Management). With NE, Verizon provides engineering planning, design and change-management support services.

1.3.11 **Managed WAN Support for Private IP (PIP) Dynamic Network Manager.** PIP Dynamic Network Manager is available in either fully automated or semi-automated mode for Managed Devices under Full Management. For Full Management, Verizon is responsible for updating both Provider Edge (PE) and Customer Edge (CE) Managed Devices. Verizon will make changes only to PE Managed Devices for Physical and Monitor and Notify management levels; Customer is responsible for any changes to the CE Managed Devices.

1.3.12 **CCR Reporting.** This feature enables Customer to access comprehensive daily and ad hoc reporting via the Web Portal – which may aid Customer in accessing the health and performance of Managed Devices under CCR.

1.3.13 **Guest Access.** Verizon offers two Guest Access options available per Lightweight Access Point or Wi-Fi-enabled Managed Device under CCR: (a) Cisco Meraki, with additional information available at the Web Portal; and (b) Purple Wi-Fi, with additional information available at https://purpleportal.net/ or other URL provided by Verizon from time to time (the Guest Access Portal). These Guest Access options provide the following functionality:

- **Mobile Location Analytics (MLA).** This feature enables Customer to choose to (a) capture information broadcast by the wireless devices of guests and end users (collectively referred to as

MLA Data); and (b) use MLA Data for the protection of the Customer Network and marketing purposes.

- **Content Filtering (Purple Wi-Fi-only).** Customer can block inappropriate content by requesting either a specific category of websites to be blocked or the specific websites. Customer also has the option to limit traffic via bandwidth controls.

1.4 Customer Responsibilities

1.4.1 **Customer Sites with Cellular Wireless Access.** Customer is responsible for ensuring cellular wireless signal parameters meet Verizon management standards where the Managed Device is installed. Wireless signals are affected by a number of factors, including other radio transmissions, weather conditions, topographical features, in building construction, large structures or other objects between the Managed Device and the nearest cell. Relocation of the Managed Device may also affect the signal parameters or strength. Customers may either perform a site assessment to assess cellular wireless performance or feasibility or, for an additional cost, order a site survey from Verizon. Customer's assessment or Verizon's site survey must determine:

- In-building cabling of where the Managed Device is going to be installed from demarcation point to Customer Managed Device termination point.
- Cellular signal parameters at each Managed Device location and termination point, to determine the need for antenna extenders or signal boosters.

If Customer requires onsite assistance from Verizon, Verizon reserves the right to charge a Dispatch Charge, as listed below, for each additional visit.

1.4.2 **In Band Access.** At all times, Customer must:

- Not add, move or remove devices, licenses or administrators to or from the Web Portal, in order to ensure that devices, licenses and administrators are those provisioned by Verizon, and shall not modify the administrators that are used for the provisioning and fault monitoring interface with Verizon's systems. At all times, Verizon must have write administrative access to Managed Devices for provisioning and management through the Web Portal.
- For Managed WAN Physical, Customer will also provide Verizon read access to the Managed Device configuration, and will maintain any software licenses associated with Managed Devices. Customer will provide Verizon the Simple Network Management Protocol (SNMP) read/write community string to any Managed Device whose configuration it wants Verizon to automatically backup.

1.4.3 **Out of Band (OOB) Access.** Where available, OOB Access is a Managed WAN service option that can be selected by Customer for Managed WAN with the Physical Management, Co Management or Full Management service level. Unless otherwise agreed, Customer will provide OOB Access to each Managed Device over a separate PSTN line (Analog OOB) or cellular wireless connection (Wireless OOB) through direct console access connections that are used to provide OOB Access to the Managed Devices. Console access works without an actual configuration on the Managed Device. Inline management requires a configured Managed Device. OOB Access is not required for the Monitor and Notify service level or for Managed Devices under CCR. Where Verizon provides OOB Access, Customer will not interfere with it, or use it for any purpose other than enabling OOB management by Verizon. Unless otherwise agreed to by Verizon, disconnecting the OOB Service voids any SLAs provided by Verizon.

For Customer Sites with two or more circuits, Customer may utilize the Alternate Circuit or Backup Wireless options, where the backup access is used in lieu of either Analog OOB or Wireless OOB for inline management access to the Managed Devices, either connecting into two separate Managed Devices or into a single Managed Device.

Verizon also offers the No OOB option to Customers that do not have any OOB Access or backup access that can be used for management access.

1.4.4 **Physical Verification of Managed Devices.** Upon Verizon's request, Customer will reboot the Managed Devices, provide the LED light statuses of the third party provider Network Terminating Unit where applicable, verify equipment power, verify if all cables are securely connected, and insert a loopback plug.

1.4.5 **Customer Initiated Site Maintenance.** Customer will notify Verizon using a Customer Maintenance Change Management Request via the VEC of any maintenance (powering down the site/managed device/third party provider Network Terminating Unit, resetting equipment, re-cabling, physical equipment move) that may affect the operating status of the Managed Devices.

1.4.6 **Customer Equipment.** Managed Take Over or Managed Implementation may show Customer Equipment needs upgrading before it can be managed. Verizon will manage such Customer Equipment after the upgrade is complete. Customer is responsible to refresh the Customer Equipment as required, including upgrades for Managed Device Enhanced Features, end-of-life conditions, and the like.

1.4.7 **Managed VoIP Services.** Customer will do the following for Managed VoIP Services:

- **Configuration Requests.** Confirm configuration of its active Managed VoIP Services is consistent with its preferences.
- **PSTN Lines.** Arrange for the purchase and installation of any PSTN lines for its Verizon or third party VoIP Service design.
- **Feature Changes.** Make feature changes at the user or administrator level (e.g., setting up call forwarding for a phone or establishing an auto-attendant) through the VEC.
- **IP Phone and IP PBX Changes.** Make IP phone and IP PBX configuration changes (unless Customer is subscribed to Verizon Managed IP PBX Service).
- **Server Support.** Implement and maintain a server (e.g., for Cisco, a TFTP (trivial file transfer protocol) server) for IP phone configuration support.

1.4.8 **Guest Access Notice.** Customers utilizing the MLA feature must display a notice, in a conspicuous location proximate to the area where the MLA data is collected, that at a minimum: (a) identifies Customer as the Data Controller (as defined in applicable law); (b) describes the type of personal data collected; (c) describes the purpose(s) for which guests' and end users' personal data is processed; (d) provides a summary of Customer's privacy practices and/or a link to its privacy policy; (e) describes any third parties to which Customer will disclose the personal data of guests and end users and the countries to which such personal data may be transferred; (f) explains how guests and end users can contact the privacy officer or other person who is accountable for the Customer's privacy practices and how to access and/or correct their personal data; (g) explains how such guests and end users can opt out from the collection and processing of their personal data; and (h) notifies guests and end users that their decision not to opt out constitutes consent to the collection, processing, transfer and use of their personal data. Where the guest or end user is located outside of the United States, the opt out requirement in subsections (g) and (h) above will not apply and instead the notice must: (i) include an opt-in click box or other mechanism that guests and end users must check or accept prior to gaining access to the MLA feature; and (ii) notify guests and end users that their decision to opt-in constitutes express consent to the collection, processing, transfer and use of their personal data in accordance with the terms described in (a) through (f) herein.

1.4.9 **SDN Remote VPN Access.** Customer is responsible for the following aspects of SDN Remote VPN Access:

- **Remote Access Client.** Customer is responsible to download, setup and manage the Remote Access Client and all aspects of the end user's endpoint device including security management.
- **Active Directory.** Customer is responsible to enable and manage all aspects of the active directory, policy administration, user authentication, and associated two factor authentication. Customers must notify Verizon of active directory service disruptions.

- **Remote Access Server.** Customer must assign a fully qualified domain name to the RAS Gateway and provide all digital certificates (root, intermediate or otherwise), server certificates, and associated private keys. Verizon will install certificates and certificate renewals provided by Customer, as required. Customer must inform Verizon of certificate-related issues and provide renewal certificates at least 90 days prior to the expiration of the certificate.

2. SUPPLEMENTAL TERMS

2.1 **Restriction on Encryption Functionality in India.** Due to differing license requirements attaching to different Services in India, with respect to: (a) Internet Dedicated Services, Customer may use encryption up to 40 bit key length in RSA algorithm. If Customer requires encryption higher than this limit, then Customer must obtain approval from the relevant telecom authority. Customer will not employ bulk encryption equipment in connection with Verizon Facilities in India; and (b) Broadband Services, the use of encryption shall be governed by the government policy/rules made under the Information Technology Act, 2000.

2.2 **Turkey Use Prohibition.** Connections to and use of the Public Internet, World Wide Web, and Social Media by a user in Turkey requires the exclusive use of the service of a locally licensed internet service provider (such as Verizon) in a manner that is compliant with all applicable laws and with any licenses, codes of practice, instructions, or guidelines issued by regulatory authorities. Customer must immediately notify Verizon of any known contravention of the foregoing. Any violation of this express prohibition may result in immediate suspension of the relevant Services by Verizon until, in Verizon's sole judgement, the violation has been cured. Customer is responsible for any fines, penalties, losses, damages, costs or expenses incurred by Verizon due to Customer's violation of this prohibition.

2.3 **Network Discovery.** Customer will provide Verizon with accurate information about proper scope of the Network Discovery, represents that it has all necessary authority to have Verizon undertake the Network Discovery requested under these terms, and will indemnify Verizon and its employees, affiliates and agents against any liability if it does not. Verizon reserves the right to stop or withhold from performing Network Discovery, at its sole discretion. Customer's sole remedy for any failure, inadequacy or other problem of Network Discovery is to request that Verizon re-perform it.

2.4 **NE and NA Services Disclaimer.** Customer will make its own independent decision whether to consider or implement any Verizon recommendation, referral or introduction in connection with NE and/or NA.

2.5 **VEC, API Gateway, or Web Portal User Names and Passwords.** Customer must immediately notify Verizon upon learning of any unauthorized use of Customer's login credentials. Customer is responsible for all activities and Charges incurred through the use of the compromised login credentials.

2.6 **VoIP Restrictions.** Customer acknowledges that a number of jurisdictions impose restrictions and/or licensing or registration conditions on VoIP transmission over the network. Customer shall comply with such regulations, as applicable.

2.7 **CPE or Managed Device for End-Use in Burma, China, Russia and Venezuela.** Without limiting the foregoing or its obligations to comply with applicable export law, Customer specifically represents that the CPE or Managed Device and related software used in conjunction with any services provided hereunder, including equipment or software that is virtualized or cloud based, will not be used by a military or military-intelligence end-user or for a military, military-intelligence, or any other prohibited end-use, as defined by the U.S. Export Administration Regulations, in Burma, China (including Hong Kong), Russia or Venezuela.

2.8 **Phased Installation.** Customer can order or subsequently request Phased Installation, by which Verizon will install and activate Managed WAN features in phases, including on a rolling basis by circuit.

Each onsite visit by a technician to implement Phased Installation will result in a Dispatch Charge, as listed below.

3. **SERVICE LEVEL AGREEMENT (SLA).** The SLA for Managed WAN may be found by clicking on the following: www.verizon.com/business/service_guide/reg/cp_mwan_sla.pdf.

4. **FINANCIAL TERMS**

4.1 **Optimized Service.** Customer will pay the Charges for Managed WAN + specified in the Agreement, including those below and at the following URL: www.verizon.com/business/service_guide/reg/applicable_charges_toc.htm. Charges below are in U.S. dollars and will be billed in the invoice currency for the associated Service. Monthly recurring Charges (MRC) and non-recurring Charges (NRC) are based on management level and size of Managed Device.

4.1.1 **Administrative Charges.** The following administrative charges are applicable to Managed WAN:

Administrative Charge	Charge Instance	NRC
Dispatch Charge	Dispatch/Re-dispatch	$300.00
Expedite Fee	Per Device, Upon Customer Request	$1,100.00
After Hours: Installation	Per Site	$600.00

4.1.2 **Managed Devices.** The Managed Device sizes apply to the rates shown in the Agreement.

4.1.3 **One-Time Management Charges.** Optional Change Management (OCM) provides additional remote change management support for Managed WAN for the NRC shown below. Customer can order specific OCM activities through the VEC. The Standard Change Management (SCM) activities shown in the VEC are included in the MRC of Managed WAN, however upon notice Verizon may limit the number of SCM changes in a month.

Managed WAN OCM Charges		
Change	**Change Instance (Charged per device unless noted)**	**NRC**
After Hours: Changes	Per request per Site	$600.00
Implementation (Modify Existing)[1,3]	Change per Managed Device	$50.00
Design (Single Feature/Protocol)[2]	Change per Managed Device	$250.00
Design Plus (Multiple Feature/Protocol)[2]	Change per Managed Device	$400.00
Engineering – 1 Hour[4]	Per request and block of hours, 1 hour block	$300.00
Engineering – 5 Hours[4]	Per request and block of hours, 5 hour block	$1,375.00
Engineering – 10 Hours[4]	Per request and block of hours, 10 hour block	$2,500.00
Engineering – 20 Hours[4]	Per request and block of hours, 20 hour block	$4,500.00
Engineering – 40 Hours[4]	Per request and block of hours, 40 hour block	$8,000.00

1. Implementation is used to modify existing features or protocols including the following: dynamic host configuration protocol (DHCP), IP network address translation, network routed protocol, MNSO IP address/subnet mask change, permanent virtual circuit (PVC) Change, routing protocol changes, switch VLAN, dynamic port/CAR, and VPN Tunnel.
2. Design and Design Plus is used for requests to evaluate or add single (Design) or multiple (Design Plus) new or changed features, protocols or applications/policies in the Customer Network, including the following: add DHCP, quality of service (QoS), network address translation (NAT) router configuration, traffic filter design, traffic shaping/queuing, and SDN policies.
3. Customer may create a new design at one Site by selecting Design/Design Plus to add the new feature(s) or protocol(s) and then replicate the design across other Sites by selecting Implementation for the remaining Sites.
4. Customer may select Engineering Hours and request additional Engineering OCM hours from time to time as needed. Verizon will track the number of hours spent per OCM request against the hours selected and will report remaining hours to Customer upon request.

4.1.4 **IP Addresses.** Verizon may use secondary IP addressing if Customer is using unregistered IP address space. If secondary IP addressing is not available, Customer must pay reasonable costs for

a dedicated management domain or an IP proxy hardware solution. Additionally, Verizon may use border gateway protocol (BGP) routing used to access and monitor the Customer Network.

4.2 **Non-Optimized Service.** Customer will pay the Charges for Managed WAN specified in the Agreement, including those at the following URL: http://www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm. In addition, online pricing for Managed WAN provided by a Verizon entity organized in the U.S. www.verizon.com/business/service_guide/reg/cp_managed_wan_services.htm.

5. **DEFINITIONS.** The following definitions apply to Managed WAN, in addition to those identified in the Master Terms and the administrative Charge definitions at the following URL: www.verizon.com/business/service_guide/reg/definitions_toc_2017DEC01.htm.

Term	Definition
Alternate Circuit	A secondary WAN connection that is used, without an OOB device or modem, to verify the availability of the primary WAN connection to a Managed Device.
Backup Wireless	Type of out of band access which connects a wireless service and wireless modem to a Managed Device for management purposes.
Cellular Wireless Access	Cellular wireless access service delivered in the U.S. which is sold and provided by Cellco Partnership, LLC, d/b/a as Verizon Wireless.
Cloud-Controlled Routing (CCR)	Cloud Infrastructure-controlled appliances at a Customer Site.
Cloud Infrastructure	The Cloud Infrastructure consists of all cloud-hosted elements that are used to provision and manage the architectural aspects of the system comprised of the CCR and related equipment; such aspects to include security policies, and quality of service. Internet access services, non-CCR equipment at the Customer Site, including other Managed Devices, are not part of the Cloud Infrastructure.
Customer Network	A collection of Managed Devices and the network they are connected to.
Dispatch	A Customer service request that results in Verizon going on to, or attempting to go on to, a Customer Site.
Expedite	An Order that is processed, at the request of the Customer, with the objective of installing or changing the Service in a time period shorter than the Verizon's standard installation time period for that Service, whether or not the installation or change is completed in that time period.
Managed Device	Items of CPE that have been designated as supported by Managed WAN.
Managed Implementation	A Managed WAN implementation option which applies to Customer and Verizon provided devices, to bring devices under Verizon management.
Managed Take Over	A Managed WAN implementation option which applies to existing, operating networks with Customer-provided devices, to bring devices under Verizon management.