verizon

MANAGED SECURITY SERVICES – POLICY MANAGEMENT +

1. GENERAL

1.1 **Service Definition.** Managed Security Services (MSS) - Policy Management+ (Policy Management) services for Serviced Devices that are certified on Verizon's MSS Product Feature Catalogue provides implementation of device initial Rule Sets and Policy Change Requests. The Serviced Devices may be located on the Customer's premises or may be located in a Verizon Virtual Network Service (VNS), Verizon Hosted Network Service (HNS) or third party cloud environment (such as Microsoft Azure and Amazon Web Services). Policy Management services are provided at three service levels: Retail, Corporate, and Enterprise. Policy Management is not sold as a standalone service and must be purchased with Health Monitoring and Device Management services.

1.2 **Service Implementation.** Verizon will assign a Project Manager to Customer who will schedule a kick off meeting to introduce the Verizon service delivery team, identify the Authorized Contacts for Customer, discuss the scope of the Policy Management service and its business impacts, and obtain any required information from Customer. Upon receipt from Customer of a completed Deployment Kit, Verizon will create a proposed project plan with high-level milestones and timelines. Verizon will only provision Policy Management service after Customer has approved the project plan.

1.3 **Service Features.** Policy Management services include Rule Set Management, Policy Change Management, Premises Based and Non-Premises Based device Policy back up and restoration services.

1.3.1 **Rule Set Management.** Verizon implements the initial device Rule Set developed by Customer that is approved by Verizon during the service provisioning phase. Customer may request changes to the Rule Set of a Serviced Device. Verizon evaluates, prepares, and implements changes to the Rule Set of a Serviced Device as described in the change management process. Customer can obtain a copy of the Rule Set via the Customer portal. The development, migration, and review of Rule Sets and/or Serviced Device Policies will be subject to a separate written work agreement and charged at the Applicable Rates.

1.3.2 **Policy Change Management.** Verizon manages Customer initiated Policy change requests (Change Request) which may be either Regular Change Request or Fast Track Change Requests.

1.3.2.1 **Change Requests.** Change Requests are submitted and tracked through the Customer portal by Authorized Contacts registered in the Service Context. Verizon assigns a unique Change Request number to each Change Request submitted and Customer must use this number in all communications about the Change Request. Change Requests are categorized as Regular Change, Fast Track and Urgent Change Requests. An optional Emergency Change Request feature is available at an additional charge. Verizon will send a confirmation request to the Authorized Contact who has submitted the Change Request, and to other Authorized Contacts registered in the Service Context if deemed necessary.

1.3.2.2 **Regular Change Request (RCR).** Verizon reviews and accepts a RCR within 24 hours after Customer submission. Verizon implements an accepted RCR in the next Maintenance Window as specified in the Service Context, provided that the minimum time between Verizon's acceptance of an RCR and the implementation is at least 48 hours. RCR is a planned change to the topology of the infrastructure or security Policy that:

- Changes to existing rules, or the creation of new rules and/or objects, in the Rule Set of the Serviced Device.
- Creation of new hosts in the Policy, and the host is part of a subnet that is already accessible and configured on the Serviced Device.
- Distribution of traffic between existing hosts.
- A change to the application software.
- Changes to operating system settings, except for changes to IP addresses.

1.3.2.3 **Fast Track Change Request (FCR).** Verizon reviews and accepts an FCR within ~~4~~ four hours and implements an accepted FCR within 36 hours after acceptance. A FCR consumes a number of Service Tickets. A FCR is a planned or unplanned change which:

- Changes existing rules or the creation of new rules and/or objects in the Rule Set.
- Creates new hosts in the Policy of the Serviced Device and the host is part of a subnet that is already accessible and configured on the Serviced Device.
- Allows or disallows network traffic between existing hosts.

1.3.2.4 **Urgent Change Request (UCR).** Verizon will review and accept a UCR within ~~2~~ two hours and will implement an accepted UCR within four~~4~~ hours after acceptance. Customer acknowledges that a UCR gives Verizon less time to review and mitigate security risks associated with the change request and implementation of UCR carries a higher degree of risk. Customer accepts such risks associated with a UCR when submitting a UCR. Customer will provide detailed data to allow Verizon to review the request within the SLA target of ≤ 2 hours, make available an Authorized Contact by telephone to further clarify the UCR, and provide written confirmation via Verizon email(s) of Customer UCR decisions made during phone calls with Verizon. An UCR consumes a number of Service Tickets. UCR is an unplanned change which:

- Modifies the existing rules or the creation of new rules and/or objects in the Rule Set of a Serviced Device.

- Specify the required configuration setting and its new value.

1.3.2.5 **Major Change Request.** A Major Change Request involves any of the following:

- Any policy change requiring more than ~~4~~ four hours (and less than ~~8~~ eight hours) end-to-end, including assessment, preparation and implementation phase.
- Any policy changes to be done by Verizon, that require a physical intervention on the device by the customer or through Verizon under a separate work order.
- Activating a previously unused function on a Serviced Device.
- Adding a new Site-to-Site VPN.
- Policy and MSS backend changes related to the move of equipment where the management IP Address or connectivity does not change.
- All change activities that have to be performed through the Microsoft Azure portal. Applies to Change Requests that require simultaneous configuration changes on the Azure Portal and on the device under management.

Service level agreements do not apply for implementation of Major Change Requests.

1.3.2.6 Emergency Change Requests (ECR). Emergency Change Request is an optional service, charged per device per month, and provides an additional urgency level for critical Change Requests. The Emergency Change Request service allows Customer to submit up to 5 ECRs per month per device. The target implementation period for Emergency Change Requests is ≤ 2 hours. The Emergency Change Request service can be ordered with any of the Service Levels provided in Section 1.4. Customer will submit an Emergency Change Request ticket through the Customer Portal and will be provided a reference number. Upon receipt of the ECR reference number (via the Customer Portal or email), Customer is required to contact the SOC by telephone to continue implementation of the ECR. If approved by Verizon, Verizon will implement the ECR within 2 hours after acceptance. Only one device or high-availability cluster can be specified per ECR. Customer will provide detailed data, including a script of the change to be implemented, to enable Verizon to implement the request within the implementation target of ≤ 2 hours. Customer will also make available an Authorized Contact who will be available by telephone to further clarify the ECR and provide written confirmation to Verizon via email(s) of decisions made during phone calls with Verizon. Customer acknowledges that an ECR provides Verizon less time to review and mitigate security risks associated with the Emergency Change Request and that implementation of an ECR carries a higher degree of risk. Customer accepts such risks associated with an ECR when submitting this level of request. Verizon will not be accountable for a failed ECR or for outages that result from an ECR. In case of an outage, Verizon will roll back an ECR without permission from Customer. An ECR cannot be reopened. If an ECR fails, a new ECR must be submitted. ECR is an unplanned change which:

- Modifies the existing rules or the creation of new rules and/or objects in the Rule Set; and,
- Specifies the required configuration setting and its new value.

Verizon reserves the right to convert any ECR to a Regular, Fast Track, Urgent, or Major Change Request with applicable service level agreements for those Change Request types.

~~1.3.2.6~~1.3.2.7 **Change Request Status.** The various status levels in the acceptance, implementation, and verification phase of the Change Request are described below:

Status Levels in the Acceptance Phase	**Change Request Conditions**
New	The Change Request has been received by Verizon.
Assigned	The Change Request has been assigned to a security team.

Reopened	The Change Request has been reopened for further action or feedback. This may be due to an internal Customer or failed change.
Work in Progress	The Change Request is being managed by a Security Engineer.
Hold	The Change Request is under review and the SLA is paused.
Status Levels in the Implementation Phase	**Change Request Conditions**
Hold - Accepted	The Change Request has been reviewed and accepted for implementation. The implementation SLA is in effect.
Hold - Internal	The Change Request has been put on hold by Verizon and the implementation SLA is in effect.
Hold – Under Review or Pending Peer Review	The Change Request is pending an action from Verizon. The implementation SLA is in effect.
Hold – Customer Request or Awaiting Customer Feedback	The Change Request is on hold by request of Customer or it is on hold pending an action by Customer which is preventing the implementation of the Change Request. The implementation SLA is not in effect.
Hold – Internal Vendor	The Change Request is pending an action by a Verizon vendor and implementation of the Change Request is pending. The implementation SLA is in effect.
Hold – Customer's Vendor	The Change Request is pending an action by Customer's vendor, which is preventing implementation of the Change Request. The implementation SLA is not in effect, as Verizon is awaiting action from Customer's vendor.
Hold – Scheduled Work	The Change Request has been scheduled for a specific date and time to activate the Change Request. The implementation SLA is in effect.
Status Levels in the Verification Phase	**Change Request Conditions**
Resolved - Discarded	The Change Request has been discarded. The implementation SLA is stopped.
Resolved - Implemented	The Change Request has been implemented. The implementation SLA is stopped.
Closed	The Change Request has been implemented and Customer has verified the implementation. No further action is required.

1.3.3 Premises Based Device Policy Back-up and Restoration

1.3.3.1 **Device Back-up.** Verizon uses an automated process to perform a back-up of the Premises Based Devices after each configuration change or Rule Set change. The back-up tools may vary depending on the device type and manufacturer. Verizon keeps at least ~~1~~ one back-up of the previous configuration version. These back-ups are securely stored in the Security Management Center (SMC) and may also be used to return to the previous version if the Policy changes do not have the expected result.

1.3.3.2 **Device Restoration.** Verizon will restore the configuration of the Premises Based Device from its own most recent back-up copies, except windows server. Verizon will work remotely with Customer to test the operational availability of the Premises Based Device and the connection to the SMC. Customer is responsible for installing the correct operating system version and patch level on the restored Premises Based Devices if it is deployed on a Windows Operating server platform. In case of a replacement of a Premises Based Device, Customer will also provide physical installation of the replacement device and configure an external IP address on that device.

1.3.4 Non-Premises Based Device Policy Back-up and Restoration

1.3.4.1 **Verizon VNS/HNS Device.** Verizon will take on-demand backups before major changes, such as Policy Change Requests, once approved by Customer as the backup procedure will result in a VM downtime. Verizon will be able to restore the complete VM to one of these backups in case of a complete failure. If Customer does not provide approval for Verizon to take such backup, Verizon will re-configure the VM using software backups.

1.3.4.2 **Third Party Cloud - Microsoft Azure.** Customer is responsible to take regular/on-demand backups before major changes, e.g. Policy Change Requests. Verizon will be able to restore the complete VM to one of these backups in case of a complete failure. If Customer does not take regular/on-demand backups, Verizon will re-configure the VM using software backups.

1.3.4.3 **Third Party Cloud – Amazon Web Services.** Customer will make available a snapshot of its VMs and update such snapshot before and after each major change or firmware upgrade. Customer will restore the snapshot on request of the MSS SOC in case of a major issue. If Customer snapshot is also non-functional, Customer will create the virtual instance from scratch, configure basic networking, and provide MSS SOC with management access. After getting management access, the MSS SOC will restore the latest configuration backup.

1.3.5 **Customer Portal.** Authorized Contacts have 24x7 access, exclusive of Maintenance Windows, to a Customer Portal. Customer is able to see reporting for Policy Management in the Customer Portal.

1.3.6 **Request for Information.** Customer can submit a Request for Information (RFI) on Serviced Devices or RFIs can be raised through the Customer Portal. Each RFI creates an RFI incident ticket and will receive a unique reference number that must be used in all further communications on the RFI. Request for Information incident tickets can be raised by the Customer for support requests not already covered by other ticket types

1.3.7 **Security Services Advisor (SSA).** Customer is assigned an SSA who serves as the Customer's primary point of contact for security service management needs related to Policy Management and acts as a trusted security advisor to the Customer. The SSA provides updates on service observations and trends as well as recommendations to the Customer on improving their overall security posture.

1.3.7.1 **SSA Scope.** SSA service management activities are limited to the defined scope of Managed Security Service products and the standard hours of operations for the region in which the SSA is assigned. The SSA scope includes the following activities, in partnership with the Customer:

- Participate in the Verizon-hosted Customer kick-off meeting and provide up to a two-hour "train-the-trainer" remote training session on the Customer Portal to authorized Customer contacts. Customer Portal training will be delivered once annually.
- Remotely host a one-hour, quarterly service and analysis review (QSR) meeting to include a review of the following standard deliverables:
  - SSA will deliver the standard QSR
  - Highlights and trends from the previous quarter
  - Review bug submissions
  - Review feature requests
- Notify Customer of any applicable updates/enhancements to the service and/or Customer Portal.
- Facilitate Customer contact and communication with other Verizon service teams, such as the Security Operations Center (SOC), in support of Managed Security Service issue resolution (e.g. SLA breach) and service improvement.
- Field customer questions regarding service observations, trends, and relevant advisories.

1.3.7.2 **Dedicated SSA.** A dedicated SSA and can be contracted at an additional charge to perform additional services beyond the SSA scope.

1.3.8 **Managed Security Services Policy Management Consultation.** The Policy Management Consultation service is an optional feature which provides clients with advisory assistance on security policy and change management processes including policy design, policy change request risk assessments, and policy lifecycle support for devices that are part of the managed service. The service is remotely delivered based on a set number of Business Hours per week as detailed in the Agreement.

1.3.8.1 **Policy Design.** Verizon works with Customer to design policy recommendations based on industry best practice and Customer Environment.

1.3.8.2 **Policy Change Request Risk Assessment.** Customer may request changes to the Rule Set associated with a SaaS Policy Management service instance. At the Customer's request, Verizon will conduct an in depth analysis of the requested change to identify potential risks and security problems that could result from the implementation of the policy change.

1.3.8.3 **Policy Lifecycle Support.** Verizon can assist in remediation of security/configuration and/or performance issues identified in the policy review. The schedule and frequency of the reviews will vary based upon the scope and scale of the engagement as mutually agreed with Customer.

1.4 **Service Levels.** Policy Management is provided in three service levels: Retail, Corporate and Enterprise Environments.

1.4.1 **Retail Environment.** The Retail Environment service level provides the following features:

- A maximum of ~~3~~ three Rule Sets
- Only Regular Change Requests (No Fast Track or Urgent Change Requests)
- Emergency Change Requests optional feature (additional charge)

1.4.2 **Corporate Environment.** The Corporate Environment service level provides the following features:

- Maximum ~~5~~ five Rule Sets
- Regular Change Requests
- Fast Track Change Requests (no Urgent Change Requests)
- Emergency Change Requests optional feature (additional charge)

1.4.3 **Enterprise Environment.** The Enterprise Environment service level provides the following features

- Unlimited rule sets
- Regular Change Requests
- Fast Track Change Requests
- Urgent change Requests
- Emergency Change Requests optional feature (additional charge)

2. **SUPPLEMENTAL TERMS**

2.1 **Excluded Serviced Device.** Policy Management are not available for any Serviced Device that: (i) has been subjected to unusual physical or electrical stress, misuse, negligence or accident; (ii) has been modified, merged, relocated, repaired, serviced or otherwise attended to by a Party other than Verizon or without Verizon's prior written consent; (iii) runs a version of operating system and/or application software that is not supported by Verizon, or that is no longer supported or maintained by the relevant manufacturer or licensor; or (iv) has not been properly registered and/or for which required permits or approvals are no longer maintained.

2.2 **Connectivity and Connectivity Equipment.** Verizon requires a secure routable path between Customer's managed devices and the Verizon SMC to enable direct connection to Customer's Serviced Devices. The applicable and necessary connectivity equipment is determined prior to the quoting and engagement process to ensure that connectivity architecture is adequate to support Policy Management services. Verizon can support several options for a secure routable path including:

- Internal devices with Verizon Private IP can connect via Multi-Protocol Label Switching (MPLS) or Virtual Private Network (VPN).
- Devices with a public IP can be monitored over internet if traffic is allowed by the firewall.
- Connection Kits (for Out-Of- Band connectivity).

2.2.1 **Connection Kits.** Connection Kits enable Out-Of-Band access to Serviced Devices. Customer must either: (i) provide such Connection Kits subject to Verizon specifications, or (ii) purchase Connection Kits from Verizon or another provider. If the Connection Kit is Customer provided or purchased through Verizon, Customer must install and connect the Connection Kit to the internet and configure an IP address for internet connectivity. Once Customer completes physical installation and internet connectivity, Verizon will remotely harden and configure the Connection Kit for Out-Of- Band access.

2.2.1.1 **Out-Of-Band Connectivity – Opt-Out.** Customer may choose to opt-out of the use of a Connection Kit and Out-Of-Band access to Serviced Devices. If Customer chooses to opt-out, Customer is subject to the following terms:

- Customer is solely responsible to restore standard remote access to the Serviced Devices; and,
- Verizon disclaims all Warranties for the Service, including any warranties in Section 2.5.1; and,
- Verizon does not provide any SLAs for the Service, including any SLAs in Section 3.0.

2.2.2 **Management Stations.** A management station may be required to capture and manage the Logs or Security Events from specific Serviced Devices. Verizon may provision Customer- or Verizon-owned management stations hosted in Verizon's SMC for certain types and categories of Serviced Devices. Customer is responsible for all necessary management licenses and/or related software/hardware. The requirement for and deployment location of a management station is determined prior to the quoting and engagement process to ensure the architecture is adequate to support Device Management services.

2.2.3 **Connectivity for Azure Microsoft Cloud.** Customer will keep full control of the Azure portal and will provide Verizon with restricted access to the Azure Portal for the Verizon managed devices. Verizon will support only those activities that are available via the Azure portal functions for Start/Stop/restart the virtual instance, create and restore snapshot, view the virtual serial console output, and monitor the secure virtual private network (VPN) to the SMC. A secure network connection to the Verizon SMC is required; Private IP (MPLS) customers can use SCI connection using Azure Express Route or a Direct IPSEC VPN terminated on Azure VPN Gateway. Verizon requires additional Azure resources (Virtual Network Gateways, Public IP addresses,) to manage virtual instances. The costs related to these services are at charge of the customer. A dedicated management station will be deployed in the SMC to manage the virtual instance(s). Verizon will have limited access to the Azure portal and customer is required to provide a technical contact person to communicate with and provide assistance if the SOC cannot access the serviced device. The customer is responsible to engage the Microsoft Azure service desk in case of technical issues with the underlying Azure platform.

2.2.4 **Connectivity for Amazon Web Services:** A read-only console is available for troubleshooting services. Customer will make a serial output available if required by Verizon. A secure network connection to the Verizon SMC is required; Private IP (MPLS) customers can use SCI connection using AWS Direct Connect or a Direct IPSEC VPN terminated on AWS virtual private Gateway. Customer is responsible for setup and configuration of the management connectivity at Amazon AWS. Customer is required to provide a contact person to assist with troubleshooting to take corrective action if management activity is

down or unstable. A dedicated management station will be deployed in the SMC to manage the virtual instance(s). Verizon will have no access to the AWS portal and customer is required to provide a technical contact person to communicate with and provide assistance if the SOC cannot access the serviced device. The customer is responsible to engage the AWS service desk in case of technical issues with the underlying AWS platform.

2.2.5 **Connectivity for HNS/VNS.** Verizon provides Policy Management services as an overlay to VNS/HNS service offering. The Customer will manage the Verizon Enterprise Portal (VEC) functionality. Customer will also have access to availability monitoring service of the underlying platform (uCPE) as delivered by VNS. In case of any problems with the underlying VNS platform, Customer will be responsible to start/stop/restart the virtual instances and devices in VNS according to the VNS service settings and SLA's. Verizon Policy Management will only provide service on the virtual instance and will not manage or interact through the VEC portal. Security devices deployed as virtual machine do not require a physical console access. However, a secure connection is always required from the SMC to uCPE via IPSEC or MPLS and MPLS from SMC to HNS. Verizon VNS does not provide the equivalent of a virtual console access through its portal. Access to the console of a security device instance is provided as follows:

- uCPE (whitebox): Ericsson Service Management Portal (SMP)
- uCPE (greybox): Juniper Device Manager (JDM)
- VCP/HNS: Ericsson Service Management Portal (SMP)

2.2.5.1 **Verizon Enterprise Portal (VEC).** MSS will not be able to access the VEC to manage the VNS infrastructure. All activities that require VEC access will remain the responsibility of the Customer. A dedicated management station will be deployed in the SMC to manage the virtual instance(s). Customer has to provide a technical contact person to communicate with and provide assistance if the SOC cannot access the Serviced Device through the SMC.

2.3 **End of Life Devices.** An end-of-life (EOL) device is defined as a device where either (i) the hardware has reached end-of-life per a manufacturer announcement, or (ii) the software version is no longer supported by the vendor or Verizon. Verizon may manage end-of-life devices for a maximum duration of ~~6~~ sisx months after the end-of-life determination and when the customer has a transition plan in place to replace or upgrade the device to a Verizon supported hardware or software version, or to phase out the EOL device within that timeframe. When no corrective steps are taken within ~~6~~ six months after the initial notification Verizon reserves the right to terminate the management service for the affected device. After EOL determination and communication of EOL, the following restrictions apply for EOL devices: (a) management of the EOL device is provided on an 'as is' and best effort basis, and (b) Customer understands and accepts full liability on the increased security risk and exposure. SLAs do not apply on devices in EOL status.

2.3.1 **Hardware Replacements and Software Upgrades/Migrations.** Hardware replacements and software upgrades/migrations for end-of-life software may be planned and carried out by Verizon, if agreed under a separate written work agreement, at the Applicable Rates. If Customer wants to change the vendor of a Serviced Device or upgrade to a model of a Serviced Device provided by the same vendor, Verizon will charge a configuration fee to perform the operational changes.

2.4 **Customer Responsibilities**

2.4.1 **Customer Deliverables for Implementation.** Customer will complete a Verizon Deployment Kit within 15 Business Days of the kick off meeting. Verizon may terminate Customer's Service Order for Policy Management if the Deployment Kit is not received in a timely manner and/or the Customer is not communicating a good-faith effort to complete the Deployment Kit. Customer will timely approve the project plan, or provide necessary information to implement the project plan. Verizon may terminate the Customer's Service Order if delays in project plan approval or necessary information causes any activity

on the critical path of the project plan to be delayed by more than 25 Business Days. Upon termination of any such Service Order(s), Verizon reserves the right to charge Customer for any expenses incurred by Verizon (including labor fees) up through the date of termination based on such project plan delay.

2.4.2 **Subordinate Devices and Maintenance Contract.** Unless otherwise provided herein, Customer is responsible for monitoring/management activities for Subordinate Devices. Customer shall (i) at its own expense, procure and maintain with each vendor adequate maintenance contracts and all licenses necessary for the Serviced Devices to enable Verizon to properly perform Policy Management (ii) comply with Policy Management prerequisites and operational procedures as set forth in the applicable terms; (iii) promptly inform Verizon of any changes effectuated in the Customer Environment; and, (iv) any changes to the nomination and/or authorization level of the individuals Customer has authorized to oversee, monitor or evaluate the provision of Policy Management services.

2.4.3 **Interoperability.** Customer acknowledges that modifications or changes to the Serviced Devices (such as future releases to the Serviced Device's operating software) or to the Customer Environment may cause interoperability problems or malfunctions in a Serviced Device and/or the Customer Environment. Customer acknowledges that it is Customer's responsibility to ensure that the Customer Environment is interoperable with each Serviced Device.

2.4.4 **Installation Sites and Equipment.** Customer shall prepare any installation site and/or Customer Environment in accordance with Verizon's instructions to ensure that any equipment which enables a Verizon interface to the Customer's device(s) is properly configured as required and operates in accordance with the manufacturer's specifications. Customer is responsible for any costs associated with preparation of the installation site and Customer Environment. If Customer fails to make any preparations required herein and this failure causes Verizon to incur costs during the implementation or provision of Policy Management then Verizon reserves the right to invoice Customer for such costs.

2.4.5 **User Interface.** In connection with the provision of Policy Management services, Verizon may provide Customer with ~~1~~ one or more user Logins to access the portal. Customer shall at all times keep its Login strictly confidential and shall take all reasonable precautions to prevent unauthorized use, misuse or compromise of its Login. Customer agrees to notify Verizon promptly upon learning of any actual or threatened unauthorized use, misuse, or compromise of its Login. Verizon is entitled to rely on Customer's Login as conclusive evidence of identity and authority. Customer shall be liable for all activities and charges incurred through the use of Customer's Login, and will indemnify, defend and hold Verizon harmless from all liabilities, losses, damages, costs and expenses (including, without limitation, reasonable attorneys' fees and costs) incurred by Verizon resulting from the use and/or compromise of Customer's Login, unless the unauthorized use, misuse or compromise of Customer's Login is solely attributable to a Verizon's gross negligence or willful misconduct.

2.4.6 **Protected Health Information (PHI).** Absent terms to the contrary in the Agreement, Policy Management is implemented without specific controls that may generally be required or customary for Customers in any particular industry and is not designed to satisfy any specific legal obligations. Customer agrees to use Policy Management in accordance with all applicable laws and not to use the service in any manner that imposes obligations on Verizon under any laws other than those laws with which Verizon agrees to comply as specifically set forth in the Agreement. Without limiting the generality of the foregoing, Customer agrees not to cause, or otherwise request that Verizon create, receive, maintain or transmit protected health information (as defined at 45 C.F.R. § 160.103) for or on behalf of Customer in connection with Policy Management or in any manner that would make Verizon a business associate (as defined at 45 C.F.R. § 160.103) to Customer. In the event Customer acts or uses Policy Management in a manner not permitted under this Section 2.4.6, Customer shall (a) be in material breach of the Agreement, including this Service Attachment; (b) ~~indemnify, defend and hold harmless Verizon for any losses, expenses, costs, liabilities, damages, penalties, investigations or enforcement~~

~~proceedings (including attorneys' fees) arising from or relating to Customer's breach of this Section 2.4.6; (c)~~ take, at Customer's expense, prompt action to correct and/or mitigate the effects of Customer's breach of this Section 2.4.6; and (c~~d~~) provide Verizon with reasonable cooperation and support in connection with Verizon's response to Customer's breach of this Section 2.4.6. Customer shall assume and be solely responsible for any reporting requirements under law or contract arising from Customer's breach of this Section 2.4.6.

2.5 Warranties

2.5.1 **Verizon Warranties.** Verizon warrants to Customer that it will perform its obligations in a good and workmanlike manner. The remedies set forth in the service level agreement (SLA) portion of this Service Attachment are Customer's sole and exclusive remedies in connection with the portions of Policy Management related to the failure to meet any standard set forth in the SLA.

2.5.2 **Third Party Warranties.** For any third party products and/or services incorporated as part of Policy Management, Customer shall receive only the warranties offered by such third party to the extent Verizon may pass through such warranties to Customer.

2.5.3 **Customer Warranties.** Customer represents and warrants that (a) it has and will continue to have all rights, power, permissions and authority necessary to have Verizon perform Policy Management services in the Customer Environment (including, without limitation, all rights, power, permissions, authority and network user consents necessary in respect of any IP address assigned to a Serviced Device and consent from its network users to Verizon's logging and monitoring activities hereunder), and (b) will not provide any PHI to Verizon for purposes of Verizon's performance of services hereunder. Customer hereby assumes the sole responsibility for the accuracy of the IP addresses and domains provided to Verizon. Customer will be liable for all costs and expenses from any third party claims of loss, damage (including reasonable attorneys' fees) and liability of any kind that may be incurred as a result of Customer's breach of the foregoing warranty.

2.6 Term and Termination

2.6.1 **Service Commitment.** The Service Commitment is for a ~~1~~ one-year term, ~~2~~ two-year term or, ~~3~~ three-year term. At the end of a Service Commitment, the Agreement will automatically renew for subsequent ~~1~~ one-year terms at the then current ~~1~~ one-year term price, unless a Party provides the other Party with notice of its intent not to auto-renew the Agreement at least 60 days prior to the expiration of the Service Commitment term. Customer may opt to purchase a different Service Commitment term with advance notice 60 days prior to the expiration of a Service Commitment or auto renewed term.

2.6.2 **Pre-RFS Termination.** Either Party may terminate a request for Policy Management services prior to the Service Activation Date with or without cause, effective 30 days after written notice of cancellation. If Customer requests a termination of a Policy Management service prior to the Service Activation Date as set forth under this provision, or Verizon terminates a Policy Management service as a result of Customer's failure to provide the necessary information or reasonable assistance required by Verizon to provision the service Customer will pay any set-up fees and other provisioning charges.

2.6.3 **Post-RFS Termination.** Either Party may terminate Policy Management service, with or without cause, effective 60 days after written notice of termination is given to the other Party. Customer accepts and agrees that, in the event (i) Customer terminates any Service for convenience, or (ii) Verizon terminates any Service for cause prior to the end of any contracted Service Commitment, then Customer will pay Verizon Early Termination Charges. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

2.6.4 **Termination for Chronic SLA Failure.** In the event that Verizon breaches the SLAs described in Section 3 for ~~6~~ six or more consecutive months, Customer shall have the right to terminate this Agreement in whole or in part, so long as such SLA failure is not remedied within 90 days after Verizon has received a registered written notice of the service problems.

2.7 **Third Party Products or Services.** The Parties agree that Verizon shall not be liable for any damages caused by hardware, software, or other products or services furnished by parties other than Verizon, its agents, or subcontractors, or any damages caused by the products and/or services delivered by or on behalf of Verizon which have been modified, serviced, or otherwise attended to by parties other than Verizon or without Verizon's prior written and express consent. Customer acknowledges that Verizon shall not be liable for any damages resulting, directly or indirectly, from any act or failure to act by Customer or any third party, including, without limitation, the non-performance, defaults, omissions or negligence of any third party that provides telecommunications services in the country or countries in which Customer's premises or systems are situated and other countries from, across, to or in respect which Policy Management is provided by or on behalf of Verizon.

2.8 **Industry Alerts and Third Party Updates and Patches.** With regard to services which provide information sharing and/or industry alerts, Verizon disclaims any liability to Customer, and Customer assumes the entire risk for (a) information from third parties provided to Customer which to the best of Verizon's information, knowledge and belief did not contain false, misleading, inaccurate or infringing information; (b) Customer's actions or failure to act in reliance on any information furnished as part of Policy Management; and/or, (c) the use of any third party links, patches, updates, upgrades, enhancements, new releases, new versions or any other remedy suggested by any third party as part of Policy Management.

2.9 **Intellectual Property Rights.** Neither Party acquires right, title or interest in or to the other Party's information, data base rights, data, tools, processes or methods, or any copyrights, trademarks, service marks, trade secrets, patents or any other intellectual or intangible property or property rights of the other Party by virtue of the provision of Policy Management services or materials delivered pursuant Policy Management service. Customer retains all right title and interest in and to the underlying factual data gathered through the provision of Policy Management service. Verizon owns all right title and interest in and to Verizon's use cases, trade secrets, confidential information or other proprietary rights in any creative or proprietary ideas, information or other material used by Verizon or presented to Customer (each, a Technical Element), including, but not limited to: data, software, modules, components, designs, utilities, databases, subsets, objects, program listings, tools, models, methodologies, programs, systems, analysis frameworks, leading practices, report formats, manner of data expression and specifications. Verizon grants Customer a nonexclusive, royalty-free license to use each Technical Element integrated into any deliverable solely for Customer's internal business purposes during the term of this Service Attachment. Customer may disclose a Technical Element integrated into a deliverable to a third party as long as such third party is subject to a written nondisclosure agreement, requiring such third party to maintain the confidentiality of such Technical Element and to use such Technical Element only for the benefit of Customer. Notwithstanding anything contained herein to the contrary, Customer is prohibited from creating derivative works of all or any portion of a Technical Element.

2.10 **Confidential Information.** Customer acknowledges that the following information constitutes Confidential Information hereunder: (a) the methods, systems, data and materials used or provided by Verizon in connection with the provision of Policy Management service; and (b) the results of Verizon's assessment of Customer and all reports issued by Verizon in connection with such results including, without limitation, security analyses and insight (Net Intel Information). Customer will disclose Net Intel Information only to Customer employees with a need to know for the purposes set forth in this Service Attachment and who are bound to confidentiality obligations at least as restrictive as those set forth in the Agreement and this Service Attachment. In no event may Customer use lesser efforts to protect Net Intel Information from use or disclosure not permitted under the Agreement than it uses to protect its own highly-sensitive confidential

information, or less than reasonable efforts. Confidential Information shall not include information that is comprised of statistical information, or other aggregated information regarding security vulnerabilities, security configurations and the like insofar as such information does not identify Customer or Customer's computer network or computer systems.

2.11 **Restriction on ~~Selling~~ Encryption ~~Functionality~~Services in India.** Prior to connecting any encryption equipment to Verizon facilities in India Customer must obtain prior evaluation and ~~Customer will not use bulk encryption equipment in connection with Verizon Facilities in India. Customer may use encryption up to 40 bit key length in RSA algorithm. If Customer requires encryption higher than this limit, then Customer will obtain~~ approval from the relevant telecom authority.

~~2.12 **General Data Protection Regulation.** Policy Management is compliant with the General Data Protection Regulation (GDPR).~~

3. SERVICE LEVEL AGREEMENT (SLA)

3.1 **Key Performance Indicators.** This SLA defines the service metrics for which Customer has the right to receive credits (Service Credits) in case Verizon fails to meet such metrics. In relation to a particular Serviced Device, the SLA will become effective when Verizon has issued the Ready- for-Operation (RFO) notice. These SLAs do not apply to Unsupported Devices, EOL status devices, or the implementation of a Major Change Request.

3.1.1 **Regular Change Request SLA.** The Regular Change Request SLAs are as follows:

Regular Change Request	Timeframe
Accepted	≤ 24 hours after request
Implementation	During Maintenance Window

3.1.1.1 **Regular Change Request Service Credits.** The Regular Change Request SLA Service Credits are as follows:

Response Time	Instances per Month ≥ X/Y	Service Credit
Acceptance > 24 hours	≥ 1/10	1

3.1.2 **Fast Track Change Request.** The Fast Change Request SLAs are as follows:

Fast Track Change Request	Timeframe
Accepted	≤ 4 hours after request
Implementation	≤ 36 hours after acceptance
Cost	6 Service Tickets

3.1.2.1 **Fast Track Change Request Service Credits.** The Fast Track Change Request SLA Service Credits are as follows:

Response Time	Instances per Month ≥ X/Y	Service Credit
Acceptance > 4 hours	≥ 1/10	1
Implementation > 36 hours after acceptance	> 0/10	1

3.1.3 **Urgent Change Request SLA.** The Urgent Change Request SLAs are as follows:

Urgent Change Request	Timeframe

Accepted	≤ 2 hours after request
Implementation	≤ 4 hours after acceptance
Cost	8 service Tickets

3.1.3.1 **Urgent Change Request Service Credits.** Urgent Change Request SLA Service Credits are as follows:

Response Time	Instances per Month ≥X/Y	Service Credit
Acceptance > 2 hours	≥ 1/10	1
Implementation > 4 hours, ≤ 8 hours after acceptance	>0/10	1
Implementation > 8 hours after acceptance	>0/10	2

3.1.4 **Emergency Change Request SLA.** The Emergency Change Request SLAs are as follows:

Emergency Change Request	Timeframe
Implementation	≤ 2 hours after acceptance of the request
Cost	Monthly recurring charge per device

3.1.4.1 **Emergency Change Request Service Credits.** Emergency Change Request SLA Service Credits are as follows:

Response Time	Instances per Month ≥X/Y	Service Credit
Implementation > 2 hours, ≤ 8 hours after acceptance	>0/5	1
Implementation > 8 hours after acceptance	>0/5	2

3.2 **Service Credit Amount.** Service Credits will be calculated monthly. Service Credits are only available starting ~~1~~one month after the service has reached the ready-for-service (RFS) milestone. Service Credits are calculated as follows:

- ~~1~~ one Device Service Credit equals the daily charge (calculated based on the applicable monthly recurring charge divided by the number of days in the month) for the affected Serviced Device.
- Instances per Month ≥ X/Y means that if Verizon exceeds the SLA Response Time X time(s) out of Y instances per month then the Customer may be eligible for a Service Credit.

3.3 **Service Credit Claims.** The following conditions apply to service credit claims:

- Customer will notify Verizon within 30 Business Days following the calendar month where an SLA metric has not been met. No Service Credits will be issued if Verizon is not notified.
- Verizon will verify any requested Service Credit, and will confirm the amount of the credit, if applicable. Verizon's Service Credit calculation is the final and definitive assessment of any credit payable.
- Service Credits will be offset against future charges.

3.4 **Service Credit Conditions.** The following additional conditions apply to service credits:

- Customer will only receive a single Service Credit if a series of unmet SLA response times arise out of the same Availability, Health Incident, or Other Incident and will receive the highest value Service Credit.
- The total number of Service Credits may not exceed 50% of the MRC payable for the affected Serviced Device during that month.
- Service Credits will not be due if the failure to meet SLA response times is due to:
  - A failure by Customer (or entity under Customer's control) to comply with Customer's obligations as described herein.

- The non-performance, default, error, omission or negligence of any entity not under Verizon's reasonable control (such as, but not limited to, failure of any of Customer's third party providers of telecommunications services or problems with equipment Customer has provided).
- The performance of routine maintenance work on Service Equipment or on any of the equipment used to provision Policy Management during the applicable Maintenance Window or emergency maintenance.
- Tests performed or commissioned by or on behalf of Customer.
- Any Force Majeure Event.

4. **FINANCIAL TERMS**

4.1 **Rates and Charges.** Unless expressly indicated otherwise, all non-recurring charges (NRCs) will be invoiced upon Order Confirmation Date. The monthly recurring charges (MRCs) will be invoiced upon Service Activation Date known as Ready-for-Service (RFS). Policy Management is subject to a ~~1~~ one-year Service Commitment.

4.2 **Per-Device Billing and On-boarding.** Customers will be billed a monthly recurring, per-device charge for the number of devices under management. Per-device charges are determined by pricing tiers based on the number of devices (e.g. 0-25, 26-50, 51-100, etc.) whereby the effective per-device rate declines as the quantity increases. At contract execution, Verizon defines an on-boarding period, expressed in billing cycles, based on the planned number of devices in scope for management. The on-boarding period (e.g. ~~3~~ three billing cycles, ~~4~~ four billing cycles, etc.) is automatically determined by the number of devices and the effective on-boarding period increases as the device quantity increases. During the on-boarding period the per-device rate is derived from the tier representing the total number of devices planned for management. The on-boarding period is only applied to the devices included in the initial order. The on-boarding period is not applied to, or modified as a result of, subsequent orders and change orders. The per-device rate applied during the on-boarding period is set for the auto-calculated number of on-boarding billing cycles and will not change even if the actual on-boarded device counts exceed the initial estimated amounts. After the on-boarding period, the per-device rate is derived from the tier representing the actual number of devices under management.

5. **DEFINITIONS.** The following definitions apply to Policy Management, in addition to those identified in the Master Terms.

Term	Definitions
24x7	Nonstop service, 24 hours a day, ~~7~~ seven days a week, 365 (366) days a year, independent of time zones and local or international public holidays.
Applicable Rates	The rates that apply for professional services work not covered under this Service Attachment. All such work is subject to the execution of a separate written agreement that describes the activities and the Applicable Rates for performing such work.
Authorized Contacts	Customer personnel authorized by Customer to access the Customer Portal and to interact with Verizon.
Connection Kit	Equipment installed on the Customer Sites used to set up secured monitoring and/or management connections between the Serviced Devices and ~~1~~ one or more Security Management Centers.
Customer Environment	The Customer network and/or information technology infrastructure.
Customer Portal	Online portal where Customers can have a near real time view on the change requests being processed, and where they can view the security posture and effectiveness of the Security Devices
Deployment Kit	A group of documents provided to Customer including various instructions as well as forms for the collection of additional data to enable onboarding.

Emergency Change Request	A Customer initiated Change Request that Verizon implements within two hours after acceptance.
End-of-Life	The end-of-life date is the date communicated by the relevant manufacturer when the support ceases for the Serviced Device so that Customer can foresee a hardware replacement and/or a software version upgrade.
Fast Track Change Request (FCR)	A Customer initiated Change Request that Verizon reviews and accepts within ~~4~~ four hours and implements an accepted FCR within 36 hours after acceptance.
Logs	A collection of various IT, compliance, network, application, and security related information created by Subordinate Devices.
Login	IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or other means of authentication.
Maintenance Window	A time window used for Verizon's performance of maintenance or management services on the Serviced Devices. During a Maintenance Window, the Serviced Devices and/or MSS - Premises Premium services may be temporarily disrupted or unavailable. In the case of Verizon's performance of Customer requested change request(s), the scheduling of Maintenance Windows may be agreed between Customer and Verizon. Maintenance windows are limited to a maximum of ~~6~~ six hours unless otherwise communicated in writing by Verizon.
Major Change Request	A Customer-initiated Change Request requiring more than ~~4~~ four hours (and less than ~~8~~ eight hours) end-to-end, including assessment, preparation and implementation phase. Service level agreements do not apply for implementation of Major Change Requests.
Non-Premises Based Devices	Serviced Device in a Verizon hosted environment or third party cloud.
Order Confirmation Date	Verizon will confirm Customer's Service Order via email and the date of this email is the Order Confirmation Date. The Order Confirmation will confirm the MSS service(s) requested.
Out-Of-Band	Out-Of-Band connectivity enables Verizon to access the Serviced Devices in the event that standard remote access methods become unavailable.
Policy or Policies	Policy are the rules by which the security device functions to protect Customer Environment as intended. Such as firewall policy (also known as Rule Sets), configuration, Whitelist, etc. which define ingress and egress of network traffic.
Premise Based Devices	Serviced Devices located at Customer premises.
Project Manager	A Verizon-designated person who will act as the central point of contact throughout the MSS - Managed Services implementation process and MSS - if applicable. The Project Manager will be responsible for managing the schedule and will also collaborate with Customer to develop a project plan that will specify resources, dates, times, and locations for the tasks described in the project plan. The Project Manager also is responsible for managing the change control process. The Project Manager is not dedicated to Customer. A Dedicated Project Manager may be required if it concerns provisioning more than ~~3~~ three devices over ~~5~~ five sites at an additional charge.
Regular Change Request (RCR)	A Customer initiated Change Request that Verizon reviews and accepts within 24 hours after Customer submission and implements an accepted RCR in the next Maintenance Window as specified in the Service Context, provided that the minimum time between Verizon's acceptance of an RCR and the implementation is at least 48 hours.
RFI	Request for Information – A Customer inquiry regarding a Serviced Device or Policy Management service.

RFO	Ready For Operations - The date (following RFS) that Verizon sends RFO notice to Customer and informs Customer that the Serviced Device has been fine-tuned and the escalation parameters, Service Context, and procedures have been set as mutually agreed. The SLA is effective as of this date. RFO is given per Serviced Device.
RFS	Ready For Service - The date on which Verizon starts providing the MSS - Managed Services on a Serviced Device. The RFS date may vary for each device.
Rule Sets	Security Policy.
Security Event	A data record produced by Verizon's security analytics platform based on Verizon's proprietary threat detection policies.
Service Context	A set of documents with version control, posted on the Customer Portal, containing information about Customer that Verizon uses for the provisioning of Policy Management service to Customer. The Service Context is setup during the service initiation phase and is maintained via the change management process. Customer can also add or update host information in the Service Context. The Service Context may include ~~1~~ one or more of the following: • Authorized Contact details and authorization procedure for escalation, notification, and reporting • Service Description • Escalation, notification, reporting, and change control processes • Authorized Contacts • Information on maintenance and support contracts Timeframe of Maintenance Windows • Roles and Responsibilities in the form of a RACI Matrix for complex and/or custom solutions • Network topologies and asset inventories of systems
Service Ticket	A unit for charging certain usage-based services. 24 Service Tickets are provided per Serviced Device under Health Monitoring, annually following RFS. 48 Service Tickets are provided for each Serviced Device under Policy Management, annually following RFS. Verizon may modify the number of Service Tickets provided at its discretion.
Serviced Device	A Serviced Device can be a device, a management station, a (virtual) appliance, virtual appliance located in Third Party Cloud or VNS/HNS, software application or a system located on a security device installed on the Customer Site which is monitored by Verizon's Managed Security Services.
SMC (Security Management Center)	A data center that hosts the Managed Security Services platform and the systems for monitoring, the Serviced Devices. The SMC includes: equipment to connect to the Connection Kit if applicable, management stations, and hosts the Verizon Local Event Collector.
SOC (Security Operations Center)	A data center where the Verizon security analysts work.
Subordinate Device	A subordinate device can be a (virtual) appliance, system, software, and/or log data, application located on a Customer Site or on the Customer's Service Provider's premises and which integrates with the Serviced Devices but which is NOT monitored or managed by Verizon under MSS services.
~~**Urgent Change Request**~~	~~A Customer initiated Change Request that Verizon reviews and accepts within 2 hours and will implement within 4 hours after acceptance.~~
Unsupported Devices	A Serviced Device that is either (i) no longer supported or maintained by its manufacturer; or (ii) an appliance, system, network, or software that is not included in Verizon's portfolio of security products supported on the MSS

	platform. Certain limitations and conditions with respect to the availability of Policy Management services apply for Unsupported Devices.
Urgent Change Request	A Customer initiated Change Request that Verizon reviews and accepts within two hours and will implement within four hours after acceptance.
UTC (Coordinated Universal Time)	Universal Time indication standardized by the Bureau International des Poids et Measures (BIPM) and defined in CCIR Recommendation 460-4. The UTC is the time indicated on atomic clocks. Verizon consults and uses it for its SOC via the Internet protocol NTP. The UTC code uses the 24-hour clock. 4 pm (afternoon) is equal to 16:00 UTC.
Verizon Local Event Collector	The Verizon Hosted Local Event Collector (LEC) or onsite Virtual Local Event Collector (vLEC) is a Verizon proprietary system that acts as a monitoring system, a data collector and a jump host system for the SOC analyst towards the Serviced Devices.
Workaround	An alternative function or method, often using a temporary patch or reconfiguration, to achieve a result equivalent to the original function or method.