verizon

MANAGED SECURITY SERVICES – DEVICE MANAGEMENT +

1. GENERAL

1.1 **Service Definition.** Managed Security Services (MSS) - Device Management + (Device Management) services for Serviced Devices offers device troubleshooting, hardware management replacement (where available), device back up, device restoration, and critical security software patches/upgrades. The Serviced Devices may be located on the customer's premises (Premises Based Devices) or may be located in a Verizon Virtual Network Service (VNS), Verizon Hosted Network Service (HNS), or Third Party Cloud environment (Microsoft Azure or Amazon Web Services). Device Management must be purchased with Health Monitoring and Policy 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 Device 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 Device Management service after Customer has approved the project plan.

1.3 **Service Features.** Device Management services include device troubleshooting, hardware management and hardware replacement for Premises Based Devices, device back up, device restoration, and critical security software patches/upgrades.

1.3.1 **Device Troubleshooting.** Verizon investigates the cause of an incident on the Serviced Device through remote problem diagnosis and initiates device troubleshooting to remedy the problem remotely. Verizon may conduct root cause analysis of the problem and communicates the results to Customer, if applicable.

Verizon will not conduct analysis if the source of the problem lies within the Customer responsibility (for example, Customer networking issues or Subordinate Devices not under Verizon's management). The Mean Time to Resolution (MTTR) SLA applies to Availability, Health and Other Incident Tickets for Severity 1 tickets.

1.3.2 **Premises Based Device Hardware Management.** Hardware management is provided for Premises Based Devices if Customer has purchased vendor maintenance and provides Verizon with all the associated maintenance and support credentials for such Premises Based Devices. Customer must have 24x7 maintenance support for the Serviced Device and authorize Verizon to act on Customer's behalf for such maintenance support. Customer must coordinate with Verizon for any upgrade, replacement or removal of a Serviced Device.

1.3.2.1 **Hardware Failure.** In the event of a hardware failure, Verizon escalates the problem to the vendor or the manufacturer of the Premises Based Device. Verizon coordinates the on-site servicing of the hardware by the relevant third party maintenance service provider. Verizon does not provide any on-site maintenance for hardware unless agreed under a separate written work agreement and charged at the Applicable Rates. An escalation to the manufacturer or vendor, followed by a hardware replacement or maintenance, is subject to and pursuant to the terms and conditions and the service level agreements of the equipment manufacturer/vendor and its Return Material Authorization (RMA) policies. Hardware replacement and RMA is not supported for end-of-life devices.

1.3.2.2 **Customer Managed Hardware.** When Customer directly manages its maintenance and support contract with the vendor, Customer will authorize Verizon with the third party vendor to raise support cases on its behalf.

1.3.3 **Premises Based Device 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 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 hardware and/or software updates 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 Back-up and Restoration**

1.3.4.1 **Verizon VNS/HNS Device.** Verizon will take on-demand backups before major changes, such as Software Upgrades, 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. Software Upgrades. 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 **Premises Based Device Hardware Replacement.** Verizon will notify Customer on the end-of-life of a Premises Based Device. 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. Customer is responsible for replacing end-of-life or unsupported devices. Hardware replacements may be planned and carried out by Verizon if agreed under a separate written work agreement and charged at the Applicable Rates.

1.3.6 **Software Patches.** Verizon monitors the release of security vulnerabilities and notifies Customer on critical security patches for the Serviced Device after they have been validated by Verizon and if applicable for Customer. Verizon informs Customer of critical security patch or upgrade installations, which are installed during an agreed Maintenance Window, and confirms with the Authorized Contacts when the installation of a critical security patch or upgrade has been completed.

1.3.6.1 **Software Upgrades.** Verizon monitors the manufacturer release of software version upgrades for Serviced Devices and will notify Customer on the end-of-life of a software version. The end-of-life date is the date communicated by the relevant manufacturer when the support ceases for the software so that Customer can foresee a software version upgrade. Customer may request software upgrades released by the vendor or manufacturer, provided Verizon supports the requested software version. Verizon does not proactively upgrade features for each Serviced Device. Software upgrades or migrations may be planned and carried out by Verizon under a separate written work agreement and charged at the Applicable Rates. Verizon does not provide on-site software maintenance.

1.3.7 **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.

1.3.8 **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 Device 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.

1.3.8.1 **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.

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

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

2. SUPPLEMENTAL TERMS

2.1 **Excluded Serviced Device.** Device 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 Device 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;
- 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 Device 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 Device 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~~ six 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 Device 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 Device Management (ii) comply with Device 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 Device 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 Device Management then Verizon reserves the right to invoice Customer for such costs.

2.4.5 **User Interface.** In connection with the provision of Device 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~~ responsible for all activities and charges incurred through the use and/or compromise 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, Device 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 with regard to PHI. Customer agrees to use Device 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 Device 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 Device 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 Device 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 Device 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 Device 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 Device 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 Device Management service prior to the Service Activation Date as set forth under this provision, or Verizon terminates a Device 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 Device 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 Device 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 Device 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 Device 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 Device Management services or materials delivered pursuant Device Management service. Customer retains all right title and interest in and to the underlying factual data gathered through the provision of Device 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 Device 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.** Device 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-Operations (RFO) notice. These SLAs do not apply to Unsupported Devices, devices in EOL status, or implementation of a Major Change Request.

3.1.1 **Mean-Time-to-Resolution (MTTR) SLA for Device Management.** The MTTR SLA Severity 1 tickets applicable for Availability/Health and Other Incident service tickets is ~~4~~ four hours for Severity 1 tickets only for Customers who experience an outage of the Serviced Device. There is no SLA for Severity 2, 3 and 4 tickets. SLA communication and reporting is provided as follows:

- Verizon will communicate with Customer's Authorized Contacts through email.
- The Customer Portal contains Customer's MTTR report for Severity 1 for Availability/Health and Other Incident service ticket and is refreshed every 15 minutes.
- Verizon's SLA time is as follows:
  - Response time: ≤ 15 minutes after an Availability/Health or Other Incident ticket creation time.

- SLA time: MTTR SLA for Severity 1 tickets < 4 hours if the root cause of the outage is a device or software failure.
- SLA start: SMC Time Stamp when Severity 1 ticket is created.
- SLA stop: SMC Time Stamp when a ticket is resolved or reduced to a Severity 2 due to a Workaround.

3.1.2 **MTTR SLA.** The following conditions are applicable to MTTR SLA:

- The Serviced Devices are equipped with a Verizon accessible serial console interface allowing device-level access.
- The vendor maintenance and support agreements must provide the ability of a ticket to be opened with a vendor support desk on a 24x7 basis.
- Customer must provide on-site assistance if required e.g., re-booting, verification of cables of the Serviced Device, etc.
- Customer is required to call the SOC when creating a Severity 1 Other Incident ticket though the Customer Portal.
- The MTTR SLA start time is measured as the SMC Time Stamp when the Severity 1 ticket is created, or the Time Stamp when the priority of an existing ticket is raised to Severity 1
- The MTTR SLA stop time is measured as the SMC Time Stamp when the severity 1 ticket is closed, or when the priority has been reduced due to a Workaround or lack of Customer feedback.

3.1.3 **SLA Time.** Certain conditions apply to the time of SLAs.

3.1.3.1 **SLA Time Pause.** The SLA clock will be paused when:

- Verizon is awaiting feedback or during an approved Maintenance Window from Customer.
- The ticket status is 'On Hold' status as requested by Customer.
- A ticket is raised with the vendor to initiate a hardware replacement.
- The problem is caused by a software bug for which no Workaround or patch is available.
- Verizon monitors the stability of the service after an incident is perceived to be resolved.

3.1.3.2 **SLA Time Resumption.** The SLA clock will resume once the replacement device is installed and connectivity is restored to the SMC, or when Verizon received feedback from the vendor or manufacturer on a software or configuration problem.

3.2 **MTTR Service Credits.** MTTR service credits are calculated in accordance with the table below:

MTTR	Instances per Month ≥ X/Y	Service Credit
≤ 4 hrs.	N/A	N/A
> 4 hrs. ≤ 6 hrs.	≥ 1/ 10	2
> 6 hrs.	0/10	3

3.2.1 **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 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.

3.2.2 **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.

3.2.3 **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 monthly recurring charge (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 Device 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). Device 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. three3 billing cycles, 4four 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 Device 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.
Availability	Verizon monitors the availability of the Serviced Device 24x7.
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 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.
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.
Health	Verizon monitors the health of the Serviced Device 24X7 by measuring disk space, CPU resource usage, memory and swap usage, network utilization, time synchronization, failover status, Log intake, and other device and service level statistics depending on the device type. Verizon establishes a health threshold for each of the health parameters reported by the Serviced Device and creates a Health incident if ~~1~~ one or more thresholds are exceeded.
~~**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.
Logs	A collection of various IT, compliance, network, application, and security related information created by Subordinate Devices.
Major Change Request	A Major Change Request involves any of the following: • Activating a previously unused function on a Serviced Device. • Minor, major & maintenance software upgrades to patch software vulnerabilities or bugs. • Standard major software version upgrades. • Adding a new Site-to-Site VPN. • MSS backend changes related to the move of equipment where the management IP address or connectivity does not change. Minor and major software upgrades may be requested via the Customer Portal. Maintenance software upgrades are performed by Verizon during Maintenance Windows. Service level agreements do not apply for implementation of Major Change Requests.
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 Device Management 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.
Non-Premises Based Device	Serviced Device in a Verizon hosted environment or third party cloud.

Managed Security Services – Device Management+

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.
Other Incident	Service tickets that Verizon or Customer can create for service related incidents on the Serviced Devices that are not related to an Availability or Health incident, which can be logged on a 24x7 basis.
Out-Of-Band	Out-Of-Band connectivity enables Verizon to access the Serviced Devices in the event that standard remote access methods become unavailable.
Premises 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 Device Management implementation process. 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 five~~5~~ sites at an additional charge.
RFI	Request for Information – A Customer inquiry regarding a Serviced Device or Device 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 Device Management on a Serviced Device. The RFS date may vary for each device.
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 Device 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 Roles and Responsibilities in the form of a RACI Matrix for complex and/or custom solutions • Network topologies and asset inventories of systems
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 premises which is monitored by Verizon's Managed Security Services. Serviced Devices do not include Subordinate Devices
Severity 1	A critical error causes the Serviced Device or the Services to fail. Normal day-to-day business is not possible, e.g. system failure, or an inaccessible or inoperable production system.

Severity 2	An error significantly affects the functions of a serviced device in a high availability set-up and impacts normal day-to-day business. Non-critical performance degradation. A severity 1 incident where a Workaround exists.
Severity 3	An isolated error impacts the functions of the Serviced Device and there is no important impact on the day-to-day business. A severity 2 incident where a Workaround exists.
Severity 4	An error has been identified. There are no problems with the Serviced Device, and there is no immediate impact on the production environment. A severity 3 incident where a Workaround exists.
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.
SMC Time Stamp	A time stamp recorded by Verizon at the SMC and reported on the Customer Portal. The time stamps are used as the reference for measuring the Service Level Agreement. The SMC Time Stamp is recorded in UTC and synchronized worldwide using the Network Time Protocol (NTP).
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 premises or on the Customer's third party provider's premises and which integrates with the Serviced Devices but which is NOT monitored or managed by Verizon under Device Management.
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 Device Management platform. Certain limitations and conditions with respect to the availability of Device Management services apply for Unsupported Devices.
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 (e.g., 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.