NaaS CLOUD MANAGEMENT

1.   GENERAL

1.1   **Service Definition.** NaaS Cloud Management (NaaSCM) is a networking and security solution that enables mesh connectivity across cloud service providers (CSPs) and CSP regions. NaaS Cloud Management leverages Verizon's IP backbone, NaaSCM Bandwidth Connectivity, and NaaSCM Data Volume Connectivity products and third party management software as a service under the Network as a Service (NaaS) framework.

1.2   **NaaSCM Service Components:** NaaSCM offers the below set of services. Customers can procure all or a subset of these services in order to meet their specific needs. Customers must procure either one of the Connectivity Services at each site. Customers must procure both Fabric/OverlayMesh Services and Managed Services as part of the solution.

1.2.1 **NaaSCM Bandwidth Connectivity:** With NaaSCM Bandwidth Connectivity, Verizon provides an interconnection across a third party vendor's network between a Customer's Verizon-provided service and their collocated equipment or CSP - within select third party data centers. Customer must have a suitable existing arrangement with the third party vendor network or suitable CSP agreement, and Customer must separately have a contract for the Verizon Private IP service in order to utilize NaaSCM Bandwidth Connectivity as an access method for that service.

1.2.2 **NaaSCM Data Volume Connectivity:** With NaaSCM Data Volume Connectivity, Verizon provides an interconnection with the network of select third-party cloud providers (with whom the customer has separately contracted) in select data centers locations, enabling Customer to utilize those third-parties'

cloud services over Verizon's Private IP network. Verizon interconnects either directly to the cloud providers or with partners that in turn connect to the cloud providers.

1.2.3 **NaaSCM Fabric/Overlay Mesh:** The NaaSCM solution creates an overlay mesh network or fabric that enables applications running anywhere in the cloud to communicate with each other as though they are on the same network. The mesh features are provided either on Regional Edge Nodes located in Verizon POPs or on Customer Edge Nodes located in customer's environment. The features provided in each of these locations are as follows:

- *Regional Edge features*: DDoS Protection, Web Application Firewall, Rate Limiting Capability, API Security, Multi-cloud Load Balancing, SSL Termination, Application Performance/Health Visibility, Secure Event Visibility
- *Customer Edge Tier 1 features*: Load Balancing (network or application), Multi-cloud Networking, Application Proxying, SSL Termination, Application Performance Observability, Service Discovery, Routing Capability, Multi-cloud Networking Virtual Router, Network Firewall, Network Request Rate Limit
- *Customer Edge Tier 2 features*: Web Application Firewall, App Security, API Security, Layer 7 Application DDoS Protection

1.2.4 **NaaSCM Managed Services:** NaaSCM provides a comprehensive suite of Verizon managed services that manage all of the NaaS Cloud Management services on behalf of the customer. These managed services include orchestration, automation for connectivity across public, private clouds, enterprise sites and remote users, integrated visibility, performance monitoring and service assurance of both underlay and overlay are in scope for this offering. NaaSCM Managed Services offer the following capabilities:

- Deployment and ongoing management of the Verizon NaaS Cloud Management solution elements.
- Respond to alarms generated that indicate an availability/health condition of cloud workloads has occurred.
- Open trouble tickets on the customer's behalf.
- Proactively notify the customer that an outage condition exists, backed by Service Level Objectives.
- Configure and manage all NaaS Cloud Management policies and connections on behalf of the customer.
- Work with the customer to resolve any issues that the customer is facing after applying policy updates.

1.3 **Mutli-Cloud Fabric.** NaaS Cloud Management includes the following software components listed below.

1.3.1 **Global Controller.** The Global Controller operates in a combination of Verizon's global infrastructure and/or a public cloud provider. This is the primary Software component of NaaS Cloud Management and includes a portal of the service and logging functions. This component provides a multi-tenanted solution to manage the lifecycle of the infrastructure, applications, and services.

1.3.2 **Regional Edge.** The Regional Edge instances are deployed in Verizon data centers to process Customer traffic. Regional Edges directly access the Verizon network infrastructure and are the hub of the data plane managed by the Global Controller instance. Regional Edges also act as IPSec tunnel endpoints for the Customer Edge software.

1.3.3 **Customer Edge.** A Customer Edge instance is licensed to Verizon's Customers on a subscription basis and can reside in a Customer location, public cloud, private cloud or other Customer-controlled edge sites. In order for Verizon to provide software or services to its Customers utilizing NaaS Cloud Management, Verizon will require that the Customer site have one (1) or more instances of the Customer Edge deployed, which creates a software appliance managed from the Global Controller. Certain use-

cases of the NaaS Cloud Management services run on one (1) or more CE appliances. Customer location may have more than one (1) site, and those sites may optionally connect to each other directly using site-to-site tunnels.

1.4 **NaaS Cloud Management Center Console.** The status and performance of the NaaS Cloud management service design and functions can be monitored by the customer within the Verizon NaaS Management Center console. Users will be able to view analytics for both network and security services, and in the future, the ability to manage, add/update network and security policies for both internal and external user personas will be enabled. This client dashboard will allow for integrated monitoring and management of the NaaS Cloud Management service elements. The dashboard will provide a Single Pane of Glass view of the network with drilldown insight into the performance and configuration of the sites, network, clusters, devices, etc. that comprise the end-to-end solution.

2. **SUPPLEMENTAL TERMS**

2.1 **Customer Edge Rights and Licenses.** Subject to the terms and conditions of the Agreement, and any applicable Orders, we grant you a limited, revocable, non-exclusive, non-transferable, non-sublicensable right to: (a) permit Users to install, execute and use the Customer Edge Software on Authorized Devices, in executable code form only; (b) permit Users to access and use the NaaS Cloud Management, solely through the Customer website portal specified in an Order; and (c) permit End Users to access and use the Customer Dashboard, solely through the Customer website portal specified in an Order, solely in connection with your internal business purposes during the applicable Service Term.

2.2 **Reservation of Rights.** We and our suppliers and licensors retain all right, title and interest in and to the Services and any software or other technology used in the provision of the Services and all modifications and derivative works thereof; all trademarks, names, logos; and all Documentation for the Services, including without limitation, all rights to patent, copyright, trade secret and other intellectual property rights. Other than as specifically described in Section II, you have no right under the Agreement to any of the Services, Documentation, or to any of Verizon or its suppliers and licensors' trademarks, patents, copyrights, or other intellectual property rights. Verizon and its suppliers and licensors retain all rights not granted herein.

2.3 **Use Restrictions.** You are responsible for all activities conducted by you and your Users with respect to the Services. You shall not directly or indirectly: (a) copy, modify, or create derivative works of the Services, any software component of the Services, or Documentation; (b) rent, lease, lend, sell, license, sublicense, assign, distribute, publish, transfer, or otherwise make available the Services or Documentation except as expressly permitted under this Agreement; (c) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to any software component of the Services; (d) remove any proprietary notices from the Services or Documentation; (e) disassemble any hardware made available to you as part of the Services; (f) use the Services or Documentation in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property right or other right of any person, or that violates any applicable laws; or (g) access or use the Services or Documentation for purposes of competitive analysis thereof or the development, provision or use of a competing software service or product.

2.4 **Third Party Access.** As part of the Services, you may have the opportunity to grant any third-party entity or website the ability to access your Account. Should you elect to do so, you acknowledge and agree that neither Verizon nor its licensors' shall be responsible for damages, harm, or losses that may arise from the third-party's access to your Account.

2.5 **Security and Privacy.** You will obtain any consents and provide any notices that are legally required for your use of the Software.

2.6 **Export Control; Government Restricted Rights.** The Software is subject to export control legal requirements of various countries, including the laws of the United States. You shall comply with the U.S. Foreign Corrupt Practices Act and all applicable export laws, restrictions and regulations of the U.S. Department of Commerce, and any other applicable U.S. and foreign authority.

2.7 **Notice to U.S. Government End Users.** The Customer Edge Software and Documentation qualify as "commercial items," as that term is defined in Federal Acquisition Regulation ("FAR") 48 C.F.R. 2.101 and consist of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contrary provision in any agreement into which this Agreement may be incorporated, you may provide to a government end user or, if this Agreement is entered into directly with a government end user, you will acquire, the Customer Edge Software and Documentation with only those rights set forth in this Agreement. Use of the Customer Edge Software and/or Documentation constitutes an agreement by the government that the Customer Edge Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes your acceptance of the rights and restrictions herein.

2.8 **Third Party Beneficiary.** Verizon and its suppliers and licensors are express and intended third-party beneficiaries of the Agreement and may claim the benefits, exercise the rights, and enforce the terms set forth in the Agreement.

2.9 **Customer Data.** As part of providing NaaS Cloud Management, Verizon may transfer, store and process Customer Data in the United States or any other country in which Verizon or its agents maintain facilities. By using NaaS Cloud Management services, Customer consents to this transfer, processing and storage of Customer Data.

2.10 **Outage Backup.** In the case of an outage, customer's traffic may be routed over a private, third-party partner network. This private, third-party network serves as an additional layer of redundant connectivity utilized in the event of an outage.

2.11 **Customer Responsibilities**

2.11.1 **Cloud Service Provider Access.** Verizon requires customer-specific administrative Login credentials to the Cloud Service Providers associated with NaaS Cloud Management. Customer will provide administrative Login access credentials to Verizon during service implementation and will provide updated credentials to the extent they change during the term in which Customer uses NaaS Cloud Management.

2.12 **Turkey Use Prohibition.** Connections to and use of the public Internet, world wide web, and social media by a user in Turkey requires the exclusive use of the service of a locally licensed Internet service provider (such as Verizon) in a manner that is compliant with all applicable laws and with any licenses, codes of practice, instructions, or guidelines issued by regulatory authorities. Customer must immediately notify Verizon of any known contravention of the foregoing. Any violation of this express prohibition may result in immediate suspension of the relevant Services by Verizon until, in Verizon's sole judgement, the violation

has been cured. Customer is responsible for any fines, penalties, losses, damages, costs or expenses incurred by Verizon due to Customer's violation of this prohibition.

3. **SERVICE LEVEL OBJECTIVES.** The NaaS Cloud Management Service Level Objectives (SLO) defines and sets forth the requirements and other terms and conditions agreed to between the Customer ("Customer") and Verizon with respect to the support Verizon shall provide in order to maintain the delivery of NaaS Cloud Management service. The SLO can be found at: www.verizon.com/business/service_guide/reg/Naas-Cloud-SLO.pdf.

4. **FINANCIAL TERMS.** Customer will pay the charges for NaaS Cloud Management service specified in the Agreement, including those applicable charges provided at the following URL: www.verizon.com/business/service_guide/reg/applicable_charges_toc.htm.
Charges are in U.S. dollars and will be billed in the invoice currency of the associated service.

4.1 **Customer Edge Charges.** Customer Edges (CE) are hosted by the customer at their hosting expense. Customers can use as many services as they wish to be provided by their CE, up to the compute limitations of the CE. Customers can choose from either 4vCPU, 8vCPU or 16vCPU. These are dimensioning considerations which are priced incrementally. Customers can choose either standard (single node) or High Availability (three nodes) CEs.

4.2 **Change Orders.** Customers are allowed a certain number of no-fee change orders per month based on the number of NaaSCM Customer Sites. Specifically, the maximum number of no-fee change requests per month is calculated by multiplying the number of NaaSCM Customer Sites by 15. For example, the limit for a Customer with six (6) NaaSCM Customer Sites would be 90 change requests per month. In the event that Customer exceeds this limit, Verizon reserves the right to issue Customer an overage charge of $60 for each change order over the limit. Change orders that are subject to this policy include, but are not limited to, the following:
- Scurity policy additions and changes
- Load balancer additions and network changes
- Networking changes with CSPs
- IP address changes and additions
- 4.1 Border Gateway Protocol (BGP) configuration and network changes

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

Term	Definition
API Security	Blocks API attacks in real time and eliminates vulnerabilities at the source. The portal enables users to manage threat analytics, forensics, and troubleshooting.
Application Performance/Health Visibility	Detailed application telemetry in the form of metrics, logs, alerts and events are collected from across the platform. This data is available in graphical format in the console, via APIs for programmatic consumption.
Application Performance Observability	Detailed metrics, logs, requests, and notifications are centrally collected from every site to provide rich observability across application, infrastructure, network, and security services across the entire system. These metrics are used to provide a holistic view of application health, service connectivity, API requests, and infrastructure resource

2311131428-32

	consumption. This gives the ability to easily debug and trace issues across the system while the centralized service can be used to integrate logs and metrics with external performance management systems like Datadog, Splunk, etc.
DDoS Protection	Web Application Firewall protection against OWASP vulnerabilities and the ability to configure custom Layer 7 policies.
Application Proxying	Ability to control the flow of application and API traffic by terminating incoming TCP connections or UDP streams from a client and initiating a new connection to the server.
DNS Domain Delegation	Ability to assign authority over part of the DNS namespace to NaaS Cloud Management, enabling services to manage the namespace in an authoritative manner.
IP Reputation	Ability to allow or deny IP addresses based on a threat category or a threat score that is determined by a continuously updated malicious IP database.
L3 Routing Capability	The ability to connect virtual network segments by forwarding packets based on IP address.
Load Balancing	A centrally managed globally distributed load balancer and proxy with service discovery, health checking, application micro-segmentation, and application policy providing the most advanced implementation of edge load-balancer with ingress/egress capability for any service mesh.
Multi-cloud Load Balancing	A centrally managed globally distributed load balancer and proxy with service discovery, health checking, application micro-segmentation, and application policy providing the ability to terminate to back-end services residing in one or more public and/or private clouds.
Multi-cloud Networking	Seamless and secure connectivity to public and private clouds over the Verizon Private IP (PIP) Network.
Multi-cloud Networking Virtual Router	Provides the ability to route packets from a network segment on one cloud to a network segment on another cloud.
Network Firewall	An object that contains all the network security configuration for a site and serves as a single place to configure network policies, service policies, and ACLs.
Network Request Rate Limit	A method of protecting applications by controlling the rate of traffic coming into or out of an application.
Rate Limiting Capability	A method of protecting applications by controlling the rate of traffic coming into or out of an application.
Secure Event Visibility	Ability to view firewall events, logs, statistics and incidents via a graphical dashboard in the console.
Service Discovery	Ability for a site or virtual-site to automatically discover service endpoints and publish VIP's. This can be accomplished using the DNS, K8S, or Consul methods.
SSL Termination	The process of decrypting encrypted traffic before passing it to the back-end web/application server.
Web Application Firewall	Provides protection from a range of attacks on HTTP traffic with the ability to identify and act upon threats. Actions include logging and blocking.