SERVICES DESCRIPTION AND TERMS

These Services Description and Terms apply to Customer's use of Services and, where specified herein, certain third-party products. The Services are only as expressly described in these Services Description and Terms. Capitalized terms used in these Services Descriptions and Terms but not defined below have the meanings in the Master Subscription Agreement (the "***Agreement***"). Aryaka reserves the right to update these Services Descriptions and Terms from time to time without notice. Aryaka reserves the right to upgrade the Services and/or add additional functionality from time to time with or without notice.

New Service Offerings Effective February 2025

A. Definitions

"***Activate***" ("Activated" and "Activation" as grammatically appropriate) shall mean Aryaka has completed the connectivity of the Services and the Servicesare ready for use by the Customer regardless of whether Customer is actually utilizing the Services.

"***AI***" means artificial intelligence.

"***ANAP***" means the Aryaka Network Access Point (ANAP), a device that provides bandwidth optimization, SD-WAN capabilities, Layer4 thru Layer 7 security, web security, visibility for monitoring and application acceleration over a WAN Link that is connected to an Aryaka Network Point of Presence (AN POP or Aryaka POP).

"***CDN***" means content delivery network.

"***CPU***" means Central Processing Unit.

"***CSX***" means Cloud Services Extension, where Aryaka leverages ISP's backbone or fabric to extend to other regions, both locally and remotely.

"***Customer***" means the organization that has entered into an Agreement under which it has purchased and deployed Services.

"***Elastic***" allows for the on-demand incremental consumption of Aryaka Services already purchased, including but not limited to the need for additional sites or other Aryaka Services.

"***Enterprise LMC Services***" shall include Dedicated Internet Access (DIA), Ethernet Virtual Private Line (EVPL or P2P).

"***Internet Service Provider***" ("***ISP***") means any third-party carrier proving a Link to a Customer site.

"***IT***" means Information Technology-based.

"***Last Mile Circuit***" ("***LMC***") means the physical Link (wired or wireless) that is used to connect Customer's premise to the closest Aryaka POP.

"***Link***" means the pair of sites connected using the Services.

"***Optimized Capacity***" means subscribed bandwidth for all the sites per region.

"***Order Form***" means the ordering document for purchases hereunder, including addenda thereto, that are entered into between the Parties from time to time.

"***Oversubscription***" means a Customer has a temporary need to go beyond its subscription units as set forth in the Order Form. Units may be bandwidth, sites, LastMile Management, and/or High Availability ANAPs.

"***POP***" means point of presence.

"***SaaS***" means Software as a Service.

"***SASE***" means Secure Access Service Edge.

"***SD-WAN***" or "***SDWAN***" means software-defined wide area network.

"***Services***" means all services provided by Aryaka and any and all Aryaka downloaded materials (including but not limited to Java Applets, soft-ANAP, and browser/User Interface components), user guides, code, user interface passwords, accessories and other documents, that are purchased by Customer or its' Affiliates under a fully executed Order Form, including associated offline components as may be further described in an Order Form or as set forth herein. Third-party products provided or made available in connection with Services may be subject to third-party terms or otheradditional terms as set forth herein, and as referenced in the Order Form.

"***SLA***" means the Service Level Agreement referenced in the Agreement.

"***SKU***" means Stock Keeping Unit.

"***Small & Medium Business*** ("***SMB***") ***LMC Services***" shall include Broadband, DSL, any wireless service and any future LMC Link technology not explicitly included in "Enterprise" Services.

"***Strategic Network Optimization***" means Aryaka initiated strategic resourcing activities of links, which Aryaka, at its sole discretion, deems appropriate to support ongoing performance, responsiveness and quality consistent with the SLA provided to the Customer. When appropriate, links are replaced to minimize the need for mitigation. In the event the Customer refuses a recommended Strategic Network Optimization event, the remaining Link shall no longer qualify for credits under Aryaka's SLA.

"***uCPE***" means Universal Customer Premise Equipment, a software appliance virtualized for Linux/KVM systems to run on Intel x86 hardware. "Aryaka Network" means Aryaka's geographically distributed network of proprietary servers and software.

"***vANAP***" means Virtual ANAP, a virtualized software that runs on compute instances of public cloud providers such as Amazon Web Services ("AWS").

"***VPN***" means Virtual Private Network.

B. <u>Description of Aryaka Services</u>

Aryaka Services: The Aryaka Services portfolio provides a cloud-first SASE service that combines a global optimized private core, SD-WAN functionality, security functionality, cloud connectivity, wide area network optimization capabilities (including compression, data de-duplication, application acceleration proxies) with cloud-based management, and visibility using the MyAryaka portal.

The Aryaka Services portfolio consists of the following:

1. Aryaka SDWAN Service
2. Aryaka Unified SASE Service
3. Aryaka Advanced Security Service
4. Aryaka SaaS Acceleration Service
5. Aryaka AI>Observe Service
6. Aryaka Professional Service
7. Aryaka Managed Firewall Service
8. Aryaka CDN Service
9. Aryaka Premium Support Service

Aryaka offers the following two pricing models:

- **"Standard" pricing model** includes all services and related subscription pricing plans for all deployment scenarios.
- **"Enterprise Flex" pricing model** includes all services and related subscription pricing plans for all deployment scenarios, additionally it includes Elastic Subscription.

C. Common Available Functionality

The following may be available to Aryaka SDWAN, Aryaka Unified SASE, and Aryaka Advanced Security Services:

a. Elastic with Enterprise Flex pricing model. Without Elastic means not allowing for the on-demand incremental consumption (also called Elastic Subscription) of specific Aryaka Services already purchased at any time, including but not limited to additional sites, remote users or any other service. With Elastic, on-demand incremental consumption is allowed. The charges with multiplier related to on-demand service Elastic Subscription are billed monthly in arrears, with the option to cancel the Elastic Subscription at any time.

b. High Availability (HA) option provides additional levels of redundancy for enterprise sites consuming specific Aryaka Services.

- ANAP-HA Redundancy is enabled at the ANAP device level for a site. Should the active ANAP fail as described in the SLA, the redundant ANAP will automatically become active and start routing traffic to the designated Aryaka POP. The redundant ANAP is included in this service. ANAP-HA is available in different tiers: Small, Medium, Large and X-Large.
- POP-HA Redundancy enabled in case of POP failure and traffic is routed to a backup Aryaka POP. POP-HA includes a redundant ANAP enabling the rerouting to another Aryaka POP in case of POP failure. POP-HA is available in different tiers: Small, Medium, Large and X-Large.
- High Availability for ZTNA Service is ensured through Aryaka's globally distributed PoPs. In case of a PoP or service node failure, user sessions are automatically redirected to the next available PoP with minimal disruption.

c. Last Mile Management option gives Customers 24x7 proactive Link Monitoring and management of Customer's procured last mile links that connect an enterprise site to specific Aryaka Services.

- Aryaka's Support team proactively works with the Customer's ISP, utilizing a Letter of Authorization (LOA) to raise and resolve any technical issues on the Customer's behalf. Last Mile Management is a per Link service and utilizes Aryaka's ANAP technology.
- At Aryaka's option, Last Mile Management Links may be converted to Last Mile Service at or around the Customer's vendor expiration date.

d. Last Mile Service allows Customer to purchase last mile internet connection services like DIA, Broadband, Fixed Wire etc. from Aryaka, which include enhanced features compared to typical "ISP" service.

- Last Mile Service always comes with Last Mile Management which provides Aryaka with

enhanced visibility of each Link, utilizing the ANAP.

- Last Mile Service is always sold separately from all other Services on a separately processed and signed Order Form.

e. Remote User service includes a Managed Zero Trust Network Access (ZTNA) Service that provides secure, policy-based access to Customer-designated applications and services and does not grant unrestricted network-level access. Access decisions are identity- and context-aware and can be enforced on Aryaka's Unified SASE platform. The ZTNA Service is delivered as a Managed Service, under which Aryaka will provide subscribing Customers with:

- The Remote User license is assigned per individual remote user and may vary by geographic region.
- The Remote User service provides access to globally distributed, redundant ZTNA gateways hosted within Aryaka's PoPs and delivered as a Cloud-based Managed Service.
- A ZTNA client application will be provided by Aryaka for installation by end users on supported devices, including PCs, laptops, and mobile phones.
- Aryaka will perform 24x7 health monitoring and handle incident management issues related to the ZTNA Gateways in addition to providing technical support for Remote User Service. Aryaka completely manages the configuration and policy management of ZTNA Gateways in alignment with Customer-provided access requirements.
- The Remote User service may be integrated with other Aryaka services, subject to the availability and procurement of applicable licenses by the Customer.
- Customer responsibilities are outlined below:
    i. Distribution and installation of the ZTNA Client Application provided by Aryaka onto authorized end-user devices (e.g., laptops, desktops, mobile devices), in accordance with deployment guidelines.
    ii. Ensuring that no conflicting network access software (such as legacy VPN clients or other tunneling agents) is active on the end-user device running the Aryaka ZTNA Client, as such conflicts may lead to interoperability or connectivity issues that fall outside the scope of Aryaka's support obligations.
    iii. Providing Level 1 support and troubleshooting for the Customer's corporate users, based on the documentation, configuration guidelines, and troubleshooting procedures supplied by Aryaka to the Customer's IT support team.
- The ZTNA option of Remote User is powered by the remote access technology offered by Cloudbrink, Inc. ("***Cloudbrink***"). By installing the Remote User client (powered by Cloudbrink), end users are agreeing to the license agreement with Cloudbrink (or affiliate) as follows: https://cloudbrink.com/eula/
- CUSTOMER ACKNOWLEDGES AND AGREES THAT CLOUDBRINK INC. AND PRODUCT OFFERINGS ARE THIRD-PARTY COMPONENTS AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO CLOUDBRINK FROM PRODUCT OR OPERATIONS PERSPECTIVE.
- Terms of Use for Remote User:

i. Remote User is licensed based on a 'per user' licensing. A user is identified by a unique identity/user id as captured in the Customer's authentication server or identity provider (such as Microsoft Active Directory, LDAP server, etc.) connecting to Remote User during each month.

ii. Remote User has two offerings: One offering for “Mainland China” and one offering for “Global” which excludes Mainland China. Customer can have access to Mainland China POPs of ZTNA gateway only with a Mainland China Remote User subscription.

iii. Remote User license packaging is available as different tiers based on the size of the user block Customer has opted to commit in for. Per user pricing depends on the committed user count as opted in by the Customer as mentioned in the Order Form.

iv. Subject to the below, Customer will be billed based on the committed user count in the Order Form or actuals whichever is higher.

v. All user licenses purchased by the Customer in the Order Form will be billed from the date of Activation of the Service or Service Commencement Date, whichever is earlier.

vi. At the end of the month, if the number of unique users connected to Remote User has exceeded the committed user count, the additional usage will be invoiced in arrears. Excess users will be billed based on the Burst multiplier as agreed upon in the Order Form.

vii. Aryaka reserves the right to provision additional POPs to support larger Global deployments at minimal to no additional cost to Customer.

viii. Each Remote User shall have no more than three (3) end point devices connecting to the Service.

ix. Aryaka does not provide Internet Breakout (any mechanism) from any of the POPs located outside Mainland China for traffic originating in Mainland China.

x. Aryaka reserves the right to choose the location and number of Remote User ZTNA gateway POPs that will be reserved for the Customer users to connect to the service, while every effort will be undertaken by Aryaka to provide the optimal connectivity and experience to end users subject to resource availability on infrastructure side and compliance needs.

xi. Aryaka reserves the right to throttle the bandwidth usage for any Remote User if an abusive pattern of consumption is observed on a consistent basis.

xii. Aryaka reserves the right to list of supported capabilities and that will be reflected on the product documentation made available to Customers. Notwithstanding the foregoing, Aryaka shall ensure that the Services purchased by Customer under the Order Form will not materially, adversely deviate from what is agreed to by the Parties thereon.

D. Detailed Description of Aryaka Services

1. Aryaka SD-WAN Service

SD-WAN Service provides connectivity services, including first, middle, and last mile, to enterprise sites, such as branch offices, stores, service centers, data centers and remote users. Aryaka SD-WAN leverages Aryaka's global Private Core to connect enterprise sites at high performance with a managed SLA. It includes global optimized Private Core, SD-WAN functionality, Cloud Connectivity, WAN Optimization capabilities (including compression, Data Deduplication, Application Acceleration proxies) with cloud-based management, and visibility using the MyAryaka portal. SDWAN Service comes with the ability to directly connect enterprise sites securely over the internet using Site-2-Site InternetVPN and/or MPLS, including service management.

SDWAN for site license comes in different tiers - Small ("S"), Medium ("M"), Large ("L") and X-Large ("XL"). The SDWAN site license also includes always-on monitoring, and 24x7 support by Aryaka's Global network operations centers (NOC). Optionally, ANAP hardware and shipment thereof are included. Aryaka's ANAP is a hardware appliance that hosts Aryaka's operating system and, of which some hardware models can host certified virtual machines ("VM"). The ANAP is included and is part of Aryaka Service. The capacity and specification of the optional ANAP hardware included with the site license differs for each tier and are subject to change. Aryaka Service site licenses such as S, M, L or XL can also be applied for uCPE where the hardware (x86 platform), OS (Linux) and hypervisor (KVM) are provided by the Customer and Aryaka provides the virtualized ANAP software.

Virtual ANAP that runs on public cloud providers, has its Aryaka Service site license S, M, L and XL SKUs. These come with specific hardware resource requirements such as number of CPU cores, memory and storage required to run the Aryaka-provided virtualized software.

Terms of Use for Aryaka SDWAN Service:

i. Aryaka reserves the right to match the ANAP device type with the Customer subscription and capabilities desired.

ii. Aryaka reserves the right to determine the POP for connecting a site to its network based on providing optimal service delivery.

iii. Aryaka SDWAN Service can be purchased through the Standard pricing model or Enterprise Flex pricing model.

iv. If Elastic-Multiplier is not included in the Order Form, Customers shall not exceed the purchased number of site licenses, users and/or service limits ("Increase") as set forth in the Order Form. If such Increase does occur, Customer will be notified, in writing, and the Parties shall execute an amended Order Form.

Table 1: Aryaka SDWAN Service regions are defined as:

Aryaka Regions	Different regions of the world
Global	Any countries or regions except Mainland China
Mainland China	Mainland China

2. Aryaka Unified SASE Service

Unified SASE Service provides integrated connectivity services, including first, middle, and last mile, and comprehensive security services to enterprise sites, such as branch offices, stores, service centers, data centers and remote users. Aryaka Unified SASE leverages Aryaka's global Private Core to connect enterprise sites at

high performance with a managed SLA. It includes global optimized Private Core, SD-WAN functionality, Cloud Connectivity, WAN Optimization capabilities (including compression, Data Deduplication, Application Acceleration proxies), plus Next-Generation Firewall (NGFW), Secured Web Gateway (SWG), Intrusion Detection and Prevention System (IDPS) and Anti-Malware with cloud-based management, and visibility using the MyAryaka portal. Unified SASE comes with the ability to directly connect enterprise sites securely over the internet using Site-2-Site Internet VPN and/or MPLS, including service management.

Unified SASE Service for site license comes in different tiers Small ("S"), Medium ("M"), Large ("L") and X-Large ("XL").The site license also includes activating, orchestration, always-on monitoring, and 24x7 support by Aryaka's Global network operations centers (NOC). Optionally, ANAP hardware and shipment thereof are included. Aryaka's ANAP is a hardware appliance that hosts Aryaka's operating system and, of which some hardware models can host certified virtual machines ("VM"). The ANAP is included and is part of Aryaka Service. The capacity and specification of the optional ANAP hardware included with the site license differs foreach tier and are subject to change. Aryaka Service site licenses such as S, M, L or XL can also be applied for uCPE where the hardware (x86 platform), OS (Linux) and hypervisor (KVM) are provided by the Customer and Aryaka provides the virtualized ANAP software.

Virtual ANAP that runs on public cloud providers, has its Aryaka Service site license S, M, L and XL SKUs. These come with specific hardware resource requirements such as number of CPU cores, memory and storage required to run the Aryaka-provided virtualized software.

a. Unified SASE includes Internet VPN up to site tier limit. Internet VPN means the ability for two sites to communicate securely over the Internet using site-2-site VPN.
b. Unified SASE provides port to connect to MPLS service. MPLS means the ability for a site-to-peer with a Customer Edge MPLS Router.
c. Unified SASE includes NGFW-SWG. It is Aryaka's Next-Generation Firewall ("NGFW") and Secured Web Gateway ("SWG") service. It provides application and user-aware protection to networks, users and cloud infrastructure.
d. Unified SASE includes IPS service. It is Aryaka's Intrusion Protection Service ("IPS"). IPS provides advanced intrusion detection and protection with threat intelligence.
e. Unified SASE includes Anti-Malware service. It provides advanced malware detection and protection using threat intelligence.

<u>Terms of Use for Aryaka Unified SASE Service:</u>

i. Aryaka reserves the right to match the ANAP device type with the Customer subscription and capabilities desired.
ii. Aryaka reserves the right to determine the POP for connecting a site to its network based on providing optimal service delivery.
iii. Aryaka Unified SASE Service can be purchased through the Standard pricing model or Enterprise Flex pricing model.
iv. If Elastic is not included in the Order Form, Customers shall not exceed the purchased number of site licenses, users and/or service limits ("Increase") as set forth in the Order Form. If such Increase does occur, Customer will be notified, in writing, and the Parties shall execute an amended Order Form.

Table 2: Aryaka Unified SASE Service regions are defined below:

Aryaka Regions	Different regions of the world
Global	Any countries or regions except Mainland China
Mainland China	Mainland China

3. Aryaka Advanced Security Service

Advanced Security provides integrated connectivity services, including first, middle, and last mile, and advanced security services to enterprise sites, such as branch offices, stores, service centers, data centers and remote users. Aryaka Advanced Security Service leverages Aryaka's global Private Core to connect enterprise sites at high performance with a managed SLA. It includes global optimized Private Core, SD-WAN functionality, Cloud Connectivity, WAN Optimization capabilities (including compression, Data Deduplication, Application Acceleration proxies), plus Next-Generation Firewall (NGFW), Secured Web Gateway (SWG), Intrusion Detection and Prevention System (IPS), Anti-Malware and Cloud Access Security Broker (CASB) with cloud-based management, and visibility using the MyAryaka portal. Advanced Security Service comes with the ability to directly connect to enterprise sites securely over the internet using Site-2-Site Internet VPN and/or MPLS, including service management.

Advanced Security Service for site comes in different tiers Small ("S"), Medium ("M"), Large ("L") and X-Large ("XL").The site license also includes activating, orchestration, always-on monitoring, and 24x7 support by Aryaka's Global network operations centers (NOC). Optionally, ANAP hardware and shipment thereof are included. Aryaka's ANAP is a hardware appliance that hosts Aryaka's operating system and, of which some hardware models can host certified virtual machines ("VM"). The ANAP is included and is part of Aryaka Service. The capacity and specification of the optional ANAP hardware included with the Advanced Security site license differs foreach tier and are subject to change. Aryaka Service site licenses such as S, M, L or XL can also be applied for uCPE where the hardware (x86 platform), OS (Linux) and hypervisor (KVM) are provided by the Customer and Aryaka provides the virtualized ANAP software.

Virtual ANAP that runs on public cloud providers, has its Aryaka Service site license S, M, L and XL SKUs. These come with specific hardware resource requirements such as number of CPU cores, memory and storage required to run the Aryaka-provided virtualized software.

a. Advanced Security includes Internet VPN. Internet VPN means the ability for two sites to communicate securely over the Internet using site-2-site VPN and Aryaka Hybrid WAN technology.

b. Advanced Security includes MPLS. MPLS means the ability for a site-to-peer with a Customer Edge MPLS Router.

c. Advanced Security includes NGFW-SWG. It is Aryaka's Next-Generation Firewall ("***NGFW***") and Secured Web Gateway ("***SWG***") service. Part of Aryaka Secure Access Service Edge (SASE) architecture, it provides application and user-aware protection to networks, users and cloud infrastructure.

d. Advanced Security includes IPS service. It is Aryaka's Intrusion Protection Service ("***IPS***"). Aryaka IPS, part of SASE architecture, provides advanced intrusion detection and protection with threat intelligence.

e. Advanced Security includes Anti-Malware service. Part of SASE architecture, it provides advanced malware detection and protection using threat intelligence.

f. Advanced Security Service includes Aryaka CASB. It is Aryaka's Cloud Access Security Broker ("***CASB***"), part of SASE architecture provides comprehensive visibility and control over SaaS

applications, including sanctioned, unsanctioned, and unclassified apps, via a centralized dashboard. It helps discover and monitor use of those software or applications that are without explicit approval from the IT department, reducing risks from unauthorized SaaS usage.

Terms of Use for Aryaka Advanced Security Service:

i. Aryaka reserves the right to match the ANAP device type with the Customer subscription and capabilities desired.

ii. Aryaka reserves the right to determine the POP for connecting a site to its network based on providing optimal service delivery.

iii. Aryaka Advanced Security Service can be purchased through the Standard pricing model or Enterprise Flex pricing model.

iv. If Elastic is not included in the Order Form, Customers shall not exceed the purchased number of site licenses, users and/or service limits ("***Increase***") as set forth in the Order Form. If such Increase does occur, Customer will be notified, in writing, and the Parties shall execute an amended Order Form.

Table 3: Aryaka Advanced Security Service regions are defined as:

Aryaka Regions	**Different regions of the world**
Global	Any countries or regions except Mainland China
Mainland China	Mainland China

4. Aryaka SaaS Acceleration Service

Aryaka SaaS Acceleration Service enables multi-cloud networking delivered as-a-service, leveraging Aryaka's Global Private Core to connect enterprise sites to SaaS.

SaaS-APP is a site license required to connect a SaaS application to Aryaka's Global Private Core.

Table 4: Aryaka's SaaS Regions are as defined below:

Aryaka Regions	**Different regions of the world**
Global	Any countries or regions except Mainland China
Mainland China	Mainland China

Terms of Use for SaaS:

i. Pricing for subscription to Aryaka's core for these SaaS Service differs per region, as defined by Aryaka.

ii. Hosted locations for SaaS are assigned to one specific region.

iii. CSX Remote Connection charge is based on the bandwidth and distance between the two ends of the connection. The CSX connection is considered remote when they connect different metro regions.

5. Aryaka AI>Observe Service

Aryaka AI>Observe Service is an AI-driven cybersecurity observability service to provide organizations with a powerful combination of secure networking and advanced threat detection. It provides AI/ML-based log data analytics to enhance threat detection capabilities with real-time analysis and anomaly identification.

Terms of Use for AI>Observe:

i. Aryaka AI>Observe can be purchased through the Standard pricing model or Enterprise Flex pricing model.

ii. Aryaka AI>Observe must be purchased for sites and users with Aryaka Services.

iii. The AI>Observe is powered by the technology offering from SEQURETEK INC. ("***SEQURETEK***"). CUSTOMER ACKNOWLEDGES AND AGREES THAT SEQURETEK AND PRODUCT OFFERINGS ARE THIRD-PARTY COMPONENTS AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO SEQURETEK FROM PRODUCT OR OPERATIONS PERSPECTIVE.

6. Aryaka Professional Services

A. Day0 Professional Services are Aryaka professional services to assist customers with initial configuration, design and implementation of Aryaka security services. Day0 Professional Services are ordered as credit by unit of hour. These services include comprehensive guidance and hands-on assistance, and are designed to ensure seamless onboarding experience, enabling Customers to leverage Aryaka's network and cloud solutions effectively.

Terms of Use for Day0 Professional Services:

i. Pricing for subscription to Aryaka's Day0 Professional Services is based on an hourly rate.

ii. Day0 Professional Services is not included in the Unified SASE or Advanced Security for sites or Remote Users. It needs to be purchased separately.

iii. Day0 Professional Services can be applied to supported service types according to the menu of Services.

iv. Day0 Professional Services must be pre-ordered prior to commencement of service delivery.

v. Day0 Professional Services are intended solely for one-time engagements.

B. Smart Hands Professional Services are Aryaka professional services to assist customers with initial configuration, activation and implementation of Aryaka SD-WAN service for sites. These services include on-site, hands-on assistance, and are designed to ensure seamless site onboarding experience, enabling Customers to leverage Aryaka's advanced network and cloud solutions effectively.

Terms of Use for Smart Hands Professional Services:

i. Pricing for subscription to Aryaka's Smart Hands Professional Service is based on an hourly rate.

ii. Smart Hands Professional Service is billed in arrears after each billing cycle.

iii. Smart Hands Professional Service is intended solely for one-time engagements.

7. Aryaka Managed Firewall Services

A. Hosted VM Firewall Service provides the ability to host select third party virtual firewalls licensed by Customer from its third-party provider (not by or through Aryaka) (a "Customer-OwnedFirewall") on an ANAP. In addition to hosting capability, Aryaka provides VM life cycle management consisting of initial Activation,

start, stop and deletion of the firewall virtual machine as part of this offering. Security policy and configuration management of firewalls, monitoring of threat events, and procurement of the third-party firewall license are outside the scope of the Hosted VM Firewall Service and are the sole responsibility of the Customer.

The Hosted VM Firewall Service is available in different tiers: Compact and Standard.

Terms of Use for Hosted VM Firewall Service:

i. Hosting capabilities of the Hosted VM Firewall Service and the Activation of the Hosted VM Firewall Service are limited to third-party next-generation firewall vendor solutions and form factors that are approved and qualified by Aryaka ("***Approved Hosted Firewalls***").

ii. In order to receive the Hosted VM Firewall Service, Customer must first acquire appropriate license rights with respect to the Customer-Owned Firewall sufficient to allow Aryaka to host the Customer-Owned Firewall and to access the Customer-Owned Firewall as necessary in connection with its Activation of the Hosted VM Firewall Service (for example, during set-up to ensure traffic flows are acceptable and interface settings are correct) and provide proof to Aryaka of such license rights. Thereafter, Customer must always maintain such license rights while receiving the Hosted VM Firewall Service. Customer represents and warrants to Aryaka that Customer has obtained and will maintain such license rights, and Customer agrees to indemnify and hold harmless (without application of any exclusions of damages or exclusions or limitations of liability in the Agreement), and at Aryaka's request, defend Aryaka and its affiliates, successors and assigns (and its and their officers, directors and employees) from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including, without limitation, attorneys' fees and court costs) which arise out of or relate to Customer's failure to have obtained and maintained such license rights. Customer hereby grants to Aryaka and its affiliates the right and license to host the Customer-Owned Firewall and to access the Customer-Owned Firewall in connection with Aryaka's Activation of the Hosted VM Firewall Service to Customer.

iii. CUSTOMER ACKNOWLEDGES AND AGREES THAT CUSTOMER-OWNED FIREWALLS ARE NOT AN ARYAKA SERVICE OR PRODUCT AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO CUSTOMER-OWNED FIREWALLS.

B. Managed Firewall Service is comprised of the operations management described below by Aryaka of select third-party firewalls licensed by Customer from its third-party provider (not by or through Aryaka) (a "Customer-Owned Firewall") hosted on an ANAP or physical firewall appliances. This service is compromised of the following functions with respect to the Customer-Owned Firewall:

- Configuration and change management
- Firewall and network access policy rules as determined and approved by the Customer
- Software patching
- 24x7 support
- Firewall device health monitoring

Terms of Use for Managed Firewall Service:

i. The Activation of the Managed Firewall Service is limited to third party next-generation firewall vendor solutions and form factorsthat are approved and qualified by Aryaka ("Approved Managed Firewalls").

ii. Security policy design and formulation and managed SOC (Security Operation Center) are not part of the scope of the Managed Firewall Service offering, and Customer is solely responsible for these functions.

iii. Security posture is determined solely by Customer, and Aryaka will only be acting as the implementor of Customer's security policies under direction and authorization by Customer is solely responsible for its security policies.

iv. Day 0 firewall policy formulation or configuration migration from a third-party firewall is not part of the scope of Managed Firewall Service.

v. In order to receive Managed Firewall Service, Customer must first acquire appropriate license rights with respect to the Customer-Owned Firewall sufficient to allow Aryaka to access, manage and otherwise perform Managed Firewall Services with respect to the Customer-Owned Firewall on behalf of the Customer and provide proof to Aryaka of such license rights. Customer must always thereafter maintain such license rights in effect while receiving the Managed Firewall Services. Customer represents and warrants to Aryaka that Customer has obtained and will maintain such license rights, and Customer agrees to indemnify and hold harmless (without application of any exclusions of damages or exclusions or limitations of liability in the Agreement), and at Aryaka's request, defend Aryaka and its affiliates, successors and assigns (and its and their officers, directors and employees) from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including, without limitation, attorneys' fees and court costs) which arise out of or relate to Customer's failure to have obtained and maintained such license rights. Customer hereby grants to Aryaka and its affiliates the right and license to access, manage and otherwise perform Managed Firewall Services with respect to the Customer-Owned Firewall on behalf of the Customer in connection with the Activation of Managed Firewall Services.

vi. CUSTOMER ACKNOWLEDGES AND AGREES THAT CUSTOMER-OWNED FIREWALLS ARE NOT AN ARYAKA SERVICE OR PRODUCT AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO CUSTOMER-OWNED FIREWALLS.

C. Firewall-High Availability provides additional levels of redundancy for enterprise sites with a hosted and, optionally, a Managed Firewall Service. Firewall ("FW") High Availability ("HA"), in all cases, requires ANAP-HA and/or a POP-HA.

- Hosted VM FW HA: Provides the ability to enable firewall redundancy at the virtual machine ("VM") level by hosting a redundant firewall on a redundant ANAP. Should the active hosted firewall fail, the redundant firewall on the redundant ANAP will automatically become the active firewall. The Hosted VM FW is available in different tiers: Compact and Standard.
- Firewall Manage HA: Provides Firewall Manage for a redundant firewall (hosted on an ANAP or a firewall appliance). Firewall Manage is available in different tiers: Compact and Standard.

Terms of Use for Firewall-High Availability offerings for Managed Firewall Service:

i. Definition of Compact and Standard Size Firewall is based on thedefinitions under Hosted VM Firewall Service and Managed Firewall Service.

ii. Firewall-High Availability will be an optional add-on service, and subject to the terms and conditions and Terms of Use set forth herein.

iii. Firewall-High Availability requires ANAP-HA.

8. Aryaka CDN (IADS) Service

Aryaka CDN provides IP Application Delivery-as-a-Service ("IADS") as a usage-based service. IADS is used for accelerating any web or IP-based public applications, such as web servers and VDI farms, over Aryaka's Global network using capabilities, such as TCP optimization, caching, and compression with cloud-based management and visibility, when using the MyAryaka portal.

Terms of Use of Aryaka CDN Services (IADS):

i. Aryaka reserves the right to choose the edge POPs and origin POPs todeliver the Services on its global network.

ii. Aryaka reserves the right to limit the maximum data transfer rates achieved over the Aryaka Network based on the aggregate data purchased.

9. Aryaka Premium Support Service

Aryaka Premium Support Services are designed with the intention to facilitate the sustained operational health of customer systems whereby customer is aligned with one or more dedicated technical support engineer(s) (hereby referred to as "Named Engineer(s)") to act as an extension of the customer's IT/network team. This Service ensures deep familiarity with the customer's environment, infrastructure, and business priorities to provide effective resolution. Aryaka Premium Support is available in two options:

A. Designated Support Personnel (DgSP)

Designated Support Personnel (DgSP) provide customers with multiple Named Engineers familiar with the customer's network infrastructure and environment. The DgSP service model is non-exclusive, with Named Engineers allocated to support more than one customer account. DgSP subscription scope includes:

a. Advanced Troubleshooting: Deep-dive analysis, RCA, and resolution of complex issues.
b. Architecture & Design Guidance: Best practices, optimization, and infrastructure advisory.
c. Customer Engagement: Lead monthly/quarterly reviews, strategic escalation point.
d. Training & Mentorship: Enablement sessions for customer teams and junior support staff.
e. Change Management: Validate and review planned changes for risk mitigation.

B. Dedicated Support Personnel (DSP)

Dedicated Support Personnel (DSP) provide a single, Named Engineer exclusively assigned to one customer account. Acting as a strategic escalation point, DSP promotes maintaining faster resolution, continuity of knowledge, and alignment with customer's long-term infrastructure goals. DSP subscription scope includes:

a. Advanced Troubleshooting: Deep-dive analysis, RCA, and resolution of complex issues.
b. Architecture & Design Guidance: Best practices, optimization, and infrastructure advisory.
c. Proactive support: Regular health checks, trend analysis, capacity planning.
d. Customer Engagement: Lead monthly/quarterly reviews, strategic escalation point.
e. Performance Metrics: SLA tracking, custom reporting, and continuous improvement plans.
f. Training & Mentorship: Enablement sessions for customer teams and junior support staff.
g. Change Management: Validate and review planned changes for risk mitigation.

Terms of Use for Aryaka Premium Support Services:

i. Aryaka Premium Support is a subscription-based service. Subscriptions for either DSP or DgSP can be purchased for a minimum term of twelve (12) months.

ii. Aryaka Premium Support is delivered during local customer business hours (8 hours, Monday to Friday). Coverage for extended hours, including 24x7 operations, may be arranged through the purchase of multiple subscriptions.

iii. Unless otherwise specified, support will be provided from Aryaka's India service centre with applicable time-zone alignment. Customers may request region-specific Named Engineer(s), subject to additional subscription fees.

iv. Pricing for both services is available under Aryaka "Standard" and "Enterprise Flex" models.

v. Aryaka Premium Support applies to all Aryaka Services subscribed to by a customer; however, it does not replace Network Operations Centre (NOC) or Customer Success functions.

vi. The following activities are not included under Aryaka Premium Support unless expressly agreed:

- Initial deployment and migrations.
- Onsite presence.
- Any work outside the agreed subscription scope.

vii. Aryaka reserves the right to reassign support personnel as needed to support continuity of services.

viii. Aryaka Premium Support is subject to and provided in accordance with the Service Level Agreement found at aryaka.com/sla.

[*End of New Service Offerings*]

ARYAKA SMARTSERVICES

A. Definitions

"Activate" ("Activated" and "Activation" as grammatically appropriate) shall mean Aryaka has completed the connectivity of the Services and the Services are ready for use by the Customer regardless of whether Customer is actually utilizing the Services.

“ANAP” means the Aryaka Network Access Point (ANAP), a device that provides bandwidth optimization, SD-WAN capabilities, Layer4 thru Layer 7 security, web security, visibility for monitoring and application acceleration over a WAN Link that is connected to an Aryaka Network Point of Presence (AN POP or Aryaka POP).

“Bursting” allows Customer to use bandwidth greater than the Activated bandwidth capacity.

“CPU” means Central Processing Unit.

“CSX” means Cloud Services Extension, where Aryaka leverages ISP’s backbone or fabric to extend to other regions, both locally and remotely.

“Customer” means the organization that has entered into an Agreement under which it has purchased and deployed Services.

“Enterprise LMC Services” shall include Dedicated Internet Access (DIA), Ethernet Virtual Private Line (EVPL or P2P).

“IaaS” means Infrastructure as a Service.

“Internet Service Provider” (“ISP”) means any third-party carrier proving a Link to a Customer site.

“IT” means Information Technology-based.

“L2 Private Core” or “Private Core” (without “L2” prefix) means Layer-2 based network within Aryaka’s Global Private network.

“L3 Private Core” means Layer-3 based network within Aryaka’s Global Private network.

“Last Mile Circuit” (“LMC”) means the physical Link (wired or wireless) that is used to connect Customer’s premise to the closest Aryaka POP.

“Link” means the pair of sites connected using the Services.

“Optimized Capacity” means subscribed bandwidth for all the sites per region.

“Order Form” means the ordering document for purchases hereunder, including addenda thereto, that are entered into between the Parties from time to time.

“Oversubscription” means a Customer has a temporary need to go beyond its subscription units as set forth in the Order Form. Units may be bandwidth, sites, Last Mile Management, and/or High Availability ANAPs.

“POP” means point of presence.

“ROW” means rest of the world, excluding Mainland China.

“SaaS” means Software as a Service.

“SASE” means Secure Access Service Edge.

“SD-WAN” means software-defined wide area network.

“Services” means all services provided by Aryaka and any and all Aryaka downloaded materials (including but not

limited to Java Applets, soft-ANAP, and browser/User Interface components), user guides, code, user interface passwords, accessories and other documents, that are purchased by Customer or its' Affiliates under a fully executed Order Form, including associated offline components as may be further described in an Order Form or as set forth herein. Third-party products provided or made available in connection with Services may be subject to third-party terms or other additional terms as set forth herein, and as referenced in the Order Form.

"SLA" means the Service Level Agreement referenced in the Agreement.

"SKU" means Stock Keeping Unit.

"Small & Medium Business ("SMB") LMC Services" shall include: Broadband, DSL, any wireless service and any future LMC Link technology not explicitly included in "Enterprise" Services.

"Strategic Network Optimization" means Aryaka initiated strategic resourcing activities of links, which Aryaka, at its sole discretion, deems appropriate to support ongoing performance, responsiveness and quality consistent with the SLA provided to the Customer. When appropriate, links are replaced to minimize the need for mitigation. In the event the Customer refuses a recommended Strategic Network Optimization event, the remaining Link shall no longer qualify for credits under Aryaka's SLA.

"uCPE" means Universal Customer Premise Equipment, a software appliance virtualized for Linux/KVM systems to run on Intel x86 hardware. "Aryaka Network" means Aryaka's geographically distributed network of proprietary servers and software.

"vANAP" means Virtual ANAP, a virtualized software that runs on compute instances of public cloud providers such as Amazon Web Services ("AWS").

"VPN" means Virtual Private Network.

B. Description of Aryaka Services

The description for Aryaka's Services is as set forth below:

Aryaka SmartServices: The Aryaka SmartServices portfolio provides a cloud-first SD-WAN service that combines a global optimized Layer 2 ("L2") Private Core, Layer 3 ("L3") Private Core, SD-WAN functionality, L3 VPN connectivity, Cloud Connectivity, WAN Optimization capabilities (including compression, Data Deduplication, Application Acceleration proxies) with cloud-based management, security and visibility using the MyAryaka portal.

The Aryaka SmartServices portfolio consists of the following services ("SmartServices"):

1. Aryaka SmartManage ("SmartManage")
2. Aryaka SmartConnect ("SmartConnect")
3. Aryaka SmartCloud ("SmartCloud")
4. Aryaka SmartSecure ("SmartSecure")
5. Aryaka Day 0 Professional Services ("Day0 Professional Services")

Aryaka SmartServices portfolio is available under two pricing models:

- **Standard pricing model**, including all SmartServices and related subscription pricing plans for Global deployment scenarios only;
- **Enterprise Flex pricing model** additionally includes, besides Global deployment scenarios, regional deployment scenarios, Elastic Subscription, and Bandwidth Pooling options, as described below.

Global deployment is used for enterprises operating in multiple regions, with traffic traversing the Aryaka core globally.

Regional deployment is used for enterprises operating primarily in a single region, as defined by Aryaka, where traffic traversing the Aryaka core stays within the region.

1. **Aryaka SmartManage Services**

SmartManage provides the foundational capabilities required to power the SmartServices platform for deployments at enterprise sites, such as branch offices, stores, service centers, and data centers.

a. **SmartManage-SiteLicense** means the basic SmartManage service required to connect enterprise sites. SmartManage-SiteLicense comes in different tiers (Bring Your Own – ("BYO"), Small ("S"), Medium ("M"), Large ("L") and X-Large ("XL")). The SmartManage-SiteLicense service includes activating, orchestration, always-on monitoring, and 24x7 support by Aryaka's Global network operations centers (NOC). Optionally, ANAP hardware and shipment thereof are included. Aryaka's ANAP is a hardware appliance that hosts Aryaka's operating system and, of which some hardware models can host certified virtual machines ("VM"). The ANAP is included and is part of Aryaka SmartServices. The capacity and specification of the optional ANAP hardware included with the SmartManage-SiteLicense differs for each tier and are subject to change. The ANAP 1500 or equivalent is provided with the Small Tier; the ANAP 2600 or equivalent with the Medium Tier; the ANAP 3000 or equivalent with the Large Tier. Global and Regional pricing plans are available for each of the above SmartManage - SiteLicense tiers. SmartManage site licenses such as S, M, L or XL can also be applied for uCPE where the hardware(x86 platform), OS (Linux) and hypervisor (KVM) are provided by the Customer and Aryaka provides the virtualized ANAP software.

b. **Virtual ANAP** that runs on public cloud providers, has its SmartManage S,M,L and XL SKUs. These come with specific hardware resource requirements such as number of CPU cores, memory and storage required to run the Aryaka-provided virtualized software.

c. **SmartManage-ElasticSubscription-Multiplier** means allowing for the on-demand incremental consumption (also called Elastic Subscription) of Aryaka SmartServices already purchased at any time, including but not limited to incremental bandwidth, additional sites, or any other SmartService. The charges related to Elastic Subscription are billed monthly in arrears, with the option to cancel the Elastic Subscription at any time.

Terms of Use for SmartManage Services:

(i) Aryaka reserves the right to match the ANAP device type with the Customer subscription and capabilities desired.

(ii) Aryaka reserves the right to determine the POP for connecting a site to its network based on providing optimal service delivery.

(iii) SmartManage can be purchased through the Standard pricing model or Enterprise Flex pricing model.

2. **Aryaka SmartConnect Services**

SmartConnect Global/Regional Services provide connectivity services, including first, middle, and last mile, to enterprise sites, such as branch offices, stores, service centers, and data centers. SmartConnect Global/Regional Services leverage Aryaka's global L2 Private Core to connect enterprise sites at high performance with a managed SLA. SmartConnect Global/Regional Services come with the option to directly connect enterprise sites securely over the internet using Site-2-Site InternetVPN and/or MPLS, including

service management. All SmartConnect Global/Regional Services require a SmartManage-SiteLicense, as defined above.

The Aryaka SmartConnect Global/Regional Services consists of the following features:

- InternetVPN
- MPLS
- L2 Private Core Subscribed Bandwidth ("SBW")
- Inter-Region Multiplier
- Bursting
- High Availability ("HA")
- Last Mile Management
- Last Mile Service

a. SmartConnect-InternetVPN means the ability for two sites to communicate securely over the Internet using site-2-site VPN and Aryaka HybridWAN technology.

b. SmartConnect-MPLS means the ability for a site-to-peer with a Customer Edge MPLS Router.

c. SmartConnect-L2PrivateCore-SBW means the ability for enterprise sites to connect over Aryaka's middle-mile L2 Private Core. Pricing of subscribing to Aryaka's SmartConnect-L2PrivateCore-SBW differs per region, as defined by Aryaka in Table 1 below. Enterprise sites are assigned to one specific Region (as defined below) based on the nearest proximity to one of the Aryaka POPs.

Table 1: Aryaka SmartConnect-L2PrivateCore-SBW regions are defined as:

Aryaka Regions	Different regions of the world
UCM	USA, Canada, Mexico
EUR	Europe (excluding Russia)
IND	India
APJK	Asia (excluding India, Mainland China)
MLCHN	Mainland China
SAF	South-Africa
SAM	South America
ISR	Israel
DUB	Dubai
AUSNZ	Australia and New Zealand

Customers can subscribe to bandwidth on the Aryaka middle-mile L2 Private Core on a per-site per-Region basis. Subscribed bandwidth is abbreviated as SBW. Aryaka provides "Global" and "Regional" pricing plans for SmartConnect-L2PrivateCore-SBW. With a Global bandwidth subscription, sites can connect from their respective Aryaka Region to any other Region. Regional bandwidth subscriptions allow sites to connect within their respective Aryaka Region only. Global and Regional pricing tiers are available for most Aryaka Regions.

d. **SmartConnect-InterRegion-Multiplier** allows Regional Sites to communicate to sites in Regions other than the Region in which the site resides. Any traffic sent to or from a Regional Site to any site not located in the same Region is InterRegion traffic. All InterRegion traffic is metered and billed at the end of the month based on the Inter Region-Multiplier on the Sales Order Form. Without the

InterRegion- Multiplier enabled it is not possible for a Regional Site to send to and receive traffic from any site located outside of its region.

e. **SmartConnect-HighAvailability (HA)** provides additional levels of redundancy for enterprise sites consuming SmartServices.

- SmartConnect-ANAP-HA Redundancy is enabled at the ANAP device level for a site. Should the active ANAP fail as described in the SLA, the redundant ANAP will automatically become active and start routing traffic to the designated Aryaka POP. The redundant ANAP is included in this service. SmartConnect- ANAP-HA is available in different tiers: Small, Medium, and Large.
- SmartConnect-POP-HA Redundancy enabled in case of POP failure and traffic is routed to a backup Aryaka POP. SmartConnect-POP-HA includes a redundant ANAP enabling the rerouting to another Aryaka POP in case of POP failure. SmartConnect-ANAP-HA is available in different tiers: Small, Medium, Large.

f. **Bursting-Multiplier** allows Customers to exceed the purchased SmartConnect-L**2**PrivateCore-SBW by up to 50% of the SBW per site with an upper limit of 100 Mbps per site. All Bursting usage, exceeding the SBW, is calculated and billed at the end of the month based on the multiplier on the valid Order Form. The calculation for Bursting usage is based on the 99th percentile of the consumed bandwidth. Customers will pay an additional usage fee, as set forth in the Order Form, for the extra bandwidth used.

g. **SmartConnect-LastMileManagement** gives Customers 24x7 proactive Link Monitoring and management of Customer's procured last mile links that connect an enterprise site to Aryaka Services.

- Aryaka's Support team proactively works with the Customer's ISP, utilizing a Letter of Authorization (LOA) to raise and resolve any issues on the Customer's behalf. Last Mile Management is a per Link service and utilizes Aryaka's ANAP technology.
- At Aryaka's option, SmartConnect-Last Mile Management Links may be converted to SmartConnect-LastMileService at or around the Customer's vendor expiration date.

h. **SmartConnect-LastMileService** allows a Customer to purchase enhanced last mile connection services from Aryaka, which includes enhanced features compared to typical "ISP" service.

- SmartConnect-LastMileService always comes with SmartConnect-LastMileManagement which provides Aryaka with enhanced visibility of each Link, utilizing the ANAP.
- SmartConnect-LastMileService is an enhanced LastMileService which extends Performance Monitoring to "Strategic Network Optimization."
- Customer may also request "Smart Insight", which includes Customer portal access and Customer visibility into each Link.
- SmartConnect-LastMileService is always sold separately from all other SmartServices on a separately processed and signed Sales Order Form.

Terms of Use for SmartConnect Global/Regional Enterprise Services:

(i) Customer's purchase of the Optimized Capacity will be on a per Region basis and can be allocated only among the sites in a particular Region as defined in Table 1 above. Site moves (excluding Last Mile Services), bandwidth reallocation and add-on relocations are limited to no more than one (1) change per site in any

given month.

(ii) If Elastic-Multiplier is not included in the Order Form, Customers shall not exceed the purchased aggregate bandwidth, number of site licenses and/or service limits ("Increase") as set forth in the Order Form. If such Increase does occur, Customer will be notified, in writing, and the Parties shall execute an amended Order Form.

(iii) Any billing schedule based on the deployment dates shall be set forth in the Order Form.

(iv) SmartConnect Global can be purchased through Standard pricing model or Enterprise Flex pricing model.

SmartConnect Regional can be purchased through Enterprise Flex pricing model only.

3. **Aryaka SmartCloud Services**

SmartCloud enables multi-cloud networking delivered as-a-service. SmartCloud leverages Aryaka's global L2 Private Core to connect enterprise sites to SaaS and IaaS.

a. **SmartCloud-Azure-VWAN** This service allows Customers to connect to the Azure VWAN Hub from Aryaka's endpoint (ANAP) over the Internet. Aryaka manages connectivity to Azure VWAN Hub. SmartCloud-Azure- VWAN requires a SmartManage-SiteLicense.

b. **SmartCloud-SaaS-APP-License** is a site license required to connect a SaaS application to Aryaka's global L2 Private Core.

c. **SmartCloud-IaaS-License** is a site license required to connect an IaaS site (*i.e.*, AWS, Azure) to Aryaka's global L2 Private Core.

d. **SmartCloud-L2PrivateCore-SBW** provides the ability for IaaS and SaaS sites to connect over Aryaka's middle-mile L2 Private Core. SmartCloud-L2PrivateCore-SBW always requires at least one or more of SmartCloud-SaaS-App-License and/or SmartCloud-IaaS-License. Pricing of subscribing to Aryaka's core for these services differs per Region, as defined below by Aryaka. Hosted locations for IaaS and SaaS are assigned to one specific Region, as defined in Table 2 below.

e. **SmartCloud-CSX-RemoteConnection** is used when Aryaka leverages the POP provider's fabric to connect to Service Providers (or Customer data centers that are also connected to the provider's fabric) in a remote metro location.

Table 2: Aryaka's SmartCloud Regions are as defined below:

Aryaka Regions	Included POPs
Mainland China	Beijing, Shanghai
Rest of World	Every other Region excluding Mainland China

Terms of Use for SmartCloud:

(i) Pricing for subscription to Aryaka's core for these SmartCloud Services differs per region, as defined by Aryaka.

(ii) Hosted locations for IaaS and SaaS are assigned to one specific region.

(iii) SmartCloud-CSX-RemoteConnection charge is based on the bandwidth and distance between the two ends of the connection. The CSX connection is considered remote when they connect different metro regions.

4. **Aryaka SmartSecure Services**

SmartSecure includes all security capabilities offered on the Aryaka platform, including native security capabilities on the ANAP and certain management functions with respect to select third-party firewall services.

SmartSecure-EdgeEssentials service includes native security capabilities offered on the ANAP, including a stateful firewall (L3/L4), zones, and micro-segmentation. The stateful firewall delivers north-south access protection. Zones provide site-segmentation to secure east-west branch traffic. Micro-segmentation enforces end-to-end network isolation between different network segments. SmartSecure-EdgeEssentials is available in different tiers: Small, Medium, and Large.

Terms of Use for SmartSecure-EdgeEssentials:

Tiering of SmartSecure-EdgeEssentials (Small, Medium, Large) is mapped to the SmartConnect Global/Regional Site license sizing.

a. **SmartSecure-CloudSecurity-ANAP-Connector** service allows Customers to connect to select third-party Cloud Secure Internet Gateway solutions licensed by the Customer from its third-party provided (not by or through Aryaka) (such as Zscaler, Palo Alto Prisma, Check Point CloudGuard connect, Symantec) from an ANAP over the Internet. Aryaka monitors and manages connectivity to the respective Cloud Security providers.

Terms of Use for SmartSecure-CloudSecurity-ANAP-Connector:

Procurement of Secure Internet Gateway licensing is not included as part of the offering.

b. **SmartSecure-Hosted-VM-Firewall-Service** provides the ability to host select third party virtual firewalls licensed by Customer from its third- party provider (not by or through Aryaka) (a "Customer-Owned Firewall") on an ANAP. In addition to hosting capability, Aryaka provides VM life cycle management consisting of initial Activation, start, stop and deletion of the Firewall virtual machine as part of this offering. Security policy and configuration management of Firewalls, monitoring of threat events, and procurement of the third-party firewall license are outside the scope of the SmartSecure Hosted-VM-Firewall- Service and are the sole responsibility of the Customer. The SmartSecure-Hosted-VM-Firewall- Service is available in different tiers: Compact and Standard.

Terms of Use for SmartSecure-Hosted-VM-Firewall-Service:

(i) Hosting capabilities of the SmartSecure Hosted VM Firewall Service and the Activation of the SmartSecure Hosted VM Firewall Service are limited to third-party next-generation Firewall vendor solutions and form factors that are approved and qualified by Aryaka ("Approved Hosted Firewalls").

Currently, Approved Hosted Firewalls are the following:

- Approved Hosted Firewalls - Compact: Palo Alto Networks VM-50 and Check Point CloudGuard Edge/Quantum Edge (2 vCPU form factors).
- Approved Hosted Firewalls - Standard: Palo Alto Networks VM-100 and Check Point CloudGuard Edge/Quantum Edge (4 vCPU form factors).

(ii) In order to receive the SmartSecure-Hosted VM Firewall Service, Customer must first acquire appropriate license rights with respect to the Customer-Owned Firewall

sufficient to allow Aryaka to host the Customer- Owned Firewall and to access the Customer-Owned Firewall as necessary in connection with its Activation of the SmartSecure-Hosted VM Firewall Service (for example, during set-up to ensure traffic flows are acceptable and interface settings are correct) and provide proof to Aryaka of such license rights. Customer must always thereafter maintain such license rights in effect while receiving the SmartSecure-Hosted VM Firewall Service. Customer represents and warrants to Aryaka that Customer has obtained and will maintain such license rights, and Customer agrees to indemnify and hold harmless (without application of any exclusions of damages or exclusions or limitations of liability in the Agreement), and at Aryaka's request defend, Aryaka and its affiliates, successors and assigns (and its and their officers, directors and employees) from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including, without limitation, attorneys' fees and court costs) which arise out of or relate to Customer's failure to have obtained and maintained such license rights. Customer hereby grants to Aryaka and its affiliates the right and license to host the Customer-Owned Firewall and to access the Customer-Owned Firewall in connection with Aryaka's Activation of the SmartSecure-Hosted VM Firewall Service to Customer.

(iii) CUSTOMER ACKNOWLEDGES AND AGREES THAT CUSTOMER-OWNED FIREWALLS ARE NOT AN ARYAKA SERVICE OR PRODUCT AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO CUSTOMER-OWNED FIREWALLS.

d. **SmartSecure-Managed-Firewall-Service** is comprised of the operations management described below by Aryaka of select third- party firewalls licensed by Customer from its third-party provider (not by or through Aryaka) (a "Customer-Owned Firewall") hosted on an ANAP or physical firewall appliances. This service is compromised of the following functions with respect to the Customer-Owned Firewall:

(i) configuration and change management,

(ii) firewall and network access policy rules as determined and approved by the Customer,

(iii) software patching,

(iv) 24x7 support, and

(v) firewall device health monitoring.

This service excludes (x) security policy design, formulation, Firewall configuration migration services, managed Security Operation Center ("SOC") services, and (y) procurement of the Customer Owned Firewall, each of which is the sole responsibility of the Customer.

Terms of Use for SmartSecure-Managed-Firewall Service:

The Activation of the SmartSecure Managed Firewall Service is limited to third party next-generation Firewall vendor solutions and form factors that are approved and qualified by Aryaka ("Approved Managed Firewalls"). Approved Managed Firewalls are:

Palo Alto Networks

- Compact Firewall: Palo Alto 200 series, 500 series, VM-50
- Standard Firewall: Palo Alto 800 series, VM-100
- Full Size Firewall: Palo Alto 3000 series

Check Point

- Compact Firewall: CloudGuard Edge/Quantum Edge 2 vCPU
- Standard Firewall: CloudGuard Edge/Quantum Edge 4 vCPU, SMB/Quantum Spark 1530, 1550
- Full Size Firewall: SMB/Quantum Spark 1570, 1590, 1600, 1800

(i) Full Size Managed Firewall is restricted to physical Firewall appliances only.

(ii) Security policy design and formulation and managed SOC (Security Operation Center) are not part of the scope of the SmartSecure Managed Firewall Service offering, and Customer is solely responsible for these functions.

(iii) Security posture is determined solely by Customer, and Aryaka will only be acting as the implementor of Customer's security policies under direction and authorization by Customer is solely responsible for its security policies.

(iv) Day 0 Firewall policy formulation or configuration migration from a third- party Firewall is not part of the scope of SmartSecure Managed Firewall Service.

(v) In order to receive SmartSecure-Managed-Firewall Services, Customer must first acquire appropriate license rights with respect to the Customer- Owned Firewall sufficient to allow Aryaka to access, manage and otherwise perform SmartSecure-Managed-Firewall-Services with respect to the Customer-Owned

Firewall on behalf of the Customer and provide proof to Aryaka of such license rights. Customer must always thereafter maintain such license rights in effect while receiving the SmartSecure-Managed-Firewall Services. Customer represents and warrants to Aryaka that Customer has obtained and will maintain such license rights, and Customer agrees to indemnify and hold harmless (without application of any exclusions of damages or exclusions or limitations of liability in the Agreement), and at Aryaka's request defend, Aryaka and its affiliates, successors and assigns (and its and their officers, directors and employees) from and against any and all claims, losses, liabilities, damages, settlements, expenses and costs (including, without limitation, attorneys' fees and court costs) which arise out of or relate to Customer's failure to have obtained and maintained such license rights. Customer hereby grants to Aryaka and its affiliates the right and license to access, manage and otherwise perform SmartSecure- Managed-Firewall-Services with respect to the Customer-Owned Firewall on behalf of the Customer in connection with the Activation of SmartSecure- Managed-Firewall Services.

(vi) CUSTOMER ACKNOWLEDGES AND AGREES THAT CUSTOMER-OWNED FIREWALLS ARE NOT AN ARYAKA SERVICE OR PRODUCT AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO CUSTOMER-OWNED FIREWALLS.

e. **SmartSecure-Check Point-Managed-Firewall-Service** is comprised of the same scope of service as provided for the SmartSecure- Managed- Firewall Service (Section 4.d., above) and further includes a subscription license to Customer for the firewall product(s) offered by Check Point Software Technologies Ltd. ("Check Point") and set forth on the applicable Order Form ("Check Point Products").

Terms of Use for SmartSecure-Check Point Managed Firewall Service:

Check Point Products are Activated through Aryaka solely for use in connection with the SmartSecure-Check Point Managed Firewall Services and are licensed by Check Point to the Customer pursuant to the Check Point End-User License Agreement located at: **https://www.checkpoint.com/support-services/software-license- agreement-limited-hardware-warranty/** and **https://www.checkpoint.com/about-us/cloud-terms/** (as may be updated from time to time), as provided by Check Point or which accompany the Check Point Products ("Check Point EULA"). By ordering the Check Point Products pursuant to an order, Customer acknowledges that its use of the Check Point Products is subject to the Check Point EULA. Customer further authorizes Aryaka, acting as agent for Customer, to accept the Check Point EULA on behalf of Customer as part of the installation process of the Check Point Products. Customer's license and use of Check Point Products and Check Point's use of personal information that it collects or generates both in relation to the Check Point website (www.checkpoint.com) and Check Point Products are subject to the terms of Check Point's Privacy Policy located at https://www.checkpoint.com/privacy/ (as may be updated from time to time). Customer consents to the use of such personal information in accordance with Check Point Privacy Policy.

Customer further acknowledges and agrees:

(i) Any software contained in the Check Point Products is licensed in object code form only. Customer agrees: (a) not to reverse engineer, decompile

or disassemble Check Point Products; (b) not to remove any identification or proprietary notices from Check Point Products; (c) except for back-up copies, not to copy Check Point Products or develop any derivative works thereof; (d) not to develop any other products based on Check Point's intellectual property contained in any Check Point Products; and (e) not to develop methods to enable unauthorized parties to use Check Point Products.

(ii) Check Point, and its licensors, own and shall retain all right (except those expressly and unambiguously licensed in the Check Point EULA), title and interest in and to the Check Point Products, including all hardware and software incorporated therein, as well as any accompanying documentation, including but not limited to, all intellectual property rights embodied therein.

(iii) EXCEPT FOR ANY PRODUCT WARRANTY MADE BY CHECK POINT DIRECTLY TO CUSTOMER PURSUANT TO THE CHECK POINT EULA, CHECK POINT MAKES NO WARRANTIES WITH RESPECT TO ANY PRODUCT, LICENSE OR SERVICE AND DISCLAIMS ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTIES OF NONINFRINGEMENT. CHECK POINT DOES NOT WARRANT THAT THE CHECK POINT PRODUCT(S) WILL MEET ANY REQUIREMENTS OR THAT THE OPERATION OF CHECK POINT PRODUCTS WILL BE UNINTERRUPTED OR ERROR FREE. ARYAKA MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE CHECK POINT PRODUCTS AND EXPRESSLY DISCLAIMS ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING AS SET FORTH ABOVE.

(iv) EXCEPT TO THE EXTENT EXPRESSLY SET FORTH IN THE CHECK POINT EULA, CHECK POINT WILL HAVE NO LIABILITY ASSOCIATED WITH THE CHECK POINT PRODUCTS. CHECK POINT PRODUCTS ARE NOT AN ARYAKA SERVICE OR PRODUCT AND ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO CHECK POINT PRODUCTS.

(v) By subscribing to the SmartSecure Check Point Managed Firewall service, Customer is agreeing to a 'non-cancellable' Check Point subscription for the applicable Check Point Products valid for the duration specified in the Order Form.

(vi) Security posture is determined solely by Customer, and Aryaka will be only acting as the implementor of Customer's security policies under direction and authorization by Customer. Customer is solely responsible for its security policies.

(vii) Check Point Products available in connection with the SmartSecure Check Point Managed Firewall belong to (1) NGTP – Next Gen Threat prevention or (2) NGTX – Next Gen Threat Prevention and Sandboxing subscription

categories, based on user selection, as such products are described by Check Point in its Product Datasheet.

(viii) Customer will have access rights to the Check Point Products Activated in connection with the SmartSecure Check Point Managed Firewall service only when the Aryaka Managed Firewall Service on Check Point is active. Customer's subscription and license to the Check Point Products will not be valid after discontinuation of SmartSecure-Check Point-Managed-Firewall- Services from Aryaka.

f. **SmartSecure-Managed-CloudGuard Connect-Service (cloud service)** is comprised of a similar scope of service as provided for the SmartSecure-Check Point-Managed-Firewall-Service (Section 4.c., above), this Service is however provided as a cloud solution, delivered on the CloudGuard Connect Product (CGC) offered by Check Point Software Technologies Ltd. ("Check Point"), and set forth on the applicable Order Form. This Service includes a subscription license (NGTP/NGTX) to Customer for CheckPoint CloudGuard Connect.

Terms of Use for SmartSecure-Managed-CloudGuard-Connect-Service:

(i) SmartSecure-CheckPoint-Managed-CloudGuard-Connect-Service is subject to the same terms and conditions and Terms of Use, as in the Section for SmartSecure-Check Point-Managed-Firewall-Services.

(ii) SmartSecure-CheckPoint-Managed-CloudGuard-Connect-Service is licensed based on 'Per user' licensing. A user is identified by a unique identity/userid as captured in the Customer's authentication server or identity provider (such as Microsoft Active Directory, LDAP server, etc.) connecting to the Private Access Service during each month.

(iii) SmartSecure-CheckPoint-Managed-CloudGuard-Connect-Service covers only for users connecting into CloudGuard Connect using (a) ANAP at a Smart Connect Site and (b) Remote user coming in through Aryaka Private Access Client.

(iv) Upon Activation of the SmartSecure-Check Point-Managed- CloudGuard-Connect-Service, all user licenses purchased by the Customer in the Order Form will be billed from date of Activation of the Service, or Service commencement date, whichever is earlier.

(v) At the end of the month, if the number of unique users connected to the SmartSecure-Check Point-Managed-CloudGuard-Connect-Service has exceeded the committed user count, then the additional usage will be invoiced in arrears. Excess users will be billed based on the Burst multiplier as agreed upon in the Order Form.

(vi) Each Remote user using the SmartSecure Private Access client to connect into SmartSecure-Check Point-Managed-CloudGuard-Connect shall have no more than three (3) end point devices connecting to such Service.

(vii) SmartSecure-Check Point-Managed-CloudGuard-Connect-Service is not available in Main Land China.

g. **SmartSecure-Managed-CloudFirewall-CheckPoint-Harmony- Internet-Access-Service** is comprised of a similar scope of service as provided for the **SmartSecure-Managed-CloudGuard Connect-Service** (stated above), delivered on the Harmony Connect Internet Access offering from Check Point, which is the rebranded naming for Check Point CloudGuard Connect and set forth on the applicable Order Form. This Service includes a subscription license (Internet Access) to Customer for Check Point Harmony Connect offering. Same Terms & Conditions apply as stated above.

h. **SmartSecure-HighAvailability** provides additional levels of redundancy for Enterprise Sites with a hosted and, optionally, a Managed Firewall Service. SmartSecure-HighAvailability, in all cases, requires SmartConnect-ANAP-HA and/or a SmartConnect-POP-HA.

- SmartSecure-HostedVM-FW-HA: provides the ability to enable firewall redundancy at the virtual machine ("VM") level by hosting a redundant firewall on a redundant ANAP. Should the active hosted firewall fail, the redundant firewall on the redundant ANAP will automatically become the active firewall. The SmartSecure- HostedVM-FW is available in different tiers: Compact and Standard.
- SmartSecure-FirewallManage-HA: provides SmartSecure FirewallManage for a redundant firewall (hosted on an ANAP or a firewall appliance). SmartSecure-FirewallManage is available in different tiers: Compact, Standard, and Full Size.
- SmartSecure-Check Point-Managed-Firewall-Services-HA: this service is the same as the SmartSecure-FirewallManage-HA, while including the subscription to a Check Point Product on and subject to the same Terms of Use set forth above with respect to the Check Point Managed Firewall Service.

Terms of Use for SmartSecure-HighAvailability offerings for Managed Firewall Service and Check Point Managed Firewall Service:

(i) Definition of Compact, Standard and Full Size Firewall is based on the definitions under SmartSecure Hosted VM Firewall Service and Managed Firewall Service.

(ii) **SmartSecure-HighAvailability** offerings will be an optional add-on on top of SmartSecure services defined above, and subject to the terms and conditions and Terms of Use of the above respective sections.

(iii) SmartSecure-Check Point-Managed-Firewall-Services-HA is subject to the same terms and conditions and Terms of Use, as in the Section for **SmartSecure-Check Point-Managed-Firewall-Services.**

(i) **SmartSecure-HighAvailability** requires **SmartConnect-ANAP-HA service.**

i. **SmartSecure-VPN Accelerate** provides accelerated connectivity to virtual private networks ("VPN") for remote and mobile users across Aryaka's private core.

- **SmartSecure-VPN Accelerate VPN-License** privately connects a specific VPN concentrator procured by Customer from its third-party provider (not by or through Aryaka) on the Customer site to Aryaka's global L2 Private Core (the origin POP). Per VPN concentrator license, a maximum of eight (8) entry-points (the edge POP) are

enabled on the Aryaka L2 Private Core.

- SmartSecure-VPN Accelerate SBW Worldwide provides a single worldwide bandwidth pool to connect remote and mobile users to the Customer's VPN concentrator using Aryaka's middle L2 Private Core.

Terms of Use for SmartSecure-VPN Accelerate:

For legal compliance purposes, in the case of Mainland China users of SmartSecure-VPN Accelerate, Aryaka requires that the Customer only tunnel corporate internal traffic over SmartSecure-VPN Accelerate, and not use SmartSecure-VPN Accelerate to tunnel Internet traffic to a VPN concentrator located outside of Mainland China.

j. **SmartSecure Private Access** is a managed VPN as a Service offering from Aryaka that provides the Customers with VPN Gateway infrastructure for enabling remote user access to Customer's Private network over Aryaka L2 Private Core. SmartSecure Private Access is delivered as a Managed Service from Aryaka where Aryaka will provide Customers subscribing to the Service with:

- Access to Globally distributed and redundant VPN Gateways (referred to as Private Access Instances) deployed on Aryaka POPs as a Cloud Service.
- Private Access VPN client application (referred to as Private Access Client) provided to the Customer by Aryaka (which will be deployed by the Customer's end users on their devices such as PCs, laptops, and mobile phone).
- 24 X 7 health Monitoring of Private Access Instances and technical support for the Private Access Service.
- Configuration and policy management for Private Access Instances.
- Incident management of Private Access Instances.
- Integration into Aryaka SmartConnect Global/Regional Services and SmartCloud services (subject to SmartConnect / SmartCloud licensing as required to be purchased by the Customer).

The responsibilities below are retained by the Customer:

- Distribution and installation of Private Access clients.
- Ensuring no conflicting VPN Apps/Agents are running on the end-user device that is running the Aryaka Private Access Client, as that may result in interoperability issues and connectivity troubles which will be outside the scope of Aryaka support.
- Level 1 troubleshooting and support for corporate users of Customer based on the documentation and guidance provided by Aryaka to Customer's IT Department.

Terms of Use for SmartSecure Private Access:

(xiv) SmartSecure Private Access is licensed based on a 'Per user' licensing. A user is identified by a unique identity/user id as captured in the Customer's authentication server or identity provider (such as Microsoft Active Directory, LDAP server, etc.) connecting to the Private Access Service during each month.

(xiv) SmartSecure Private Access has two offerings: One offering for Mainland China and one offering for ROW which excludes Mainland China. Customer can have

access to Mainland China POPs of Private Access only with a Mainland China Private Access subscription.

(xiv) SmartSecure Private Access ROW license packaging is available as different tiers based on the size of the user block Customer has opted to commit in for. Per user pricing of SmartSecure Private Access ROW depends on the committed user count as opted in by the Customer as mentioned in the SOF.

(xiv) Subject to subsection (v) below, Customer will be billed based on the committed user count in the Order Form.

(xiv) All user licenses purchased by the Customer in the Order Form will be billed from the date of Activation of the Service or Service commencement date, whichever is earlier.

(xiv) At the end of the month, if the number of unique users connected to the SmartSecure Private Access Service has exceeded the committed user count, then the additional usage will be invoiced in arrears. Excess users will be billed based on the Burst multiplier as agreed upon in the Order Form.

(xiv) Each Customer subscribing to Private Access ROW can be provisioned with up to 10 ROW POPs based on the geographical location of the users. Aryaka reserves the right to provision additional POPs to support larger global deployments at no additional cost to Customer.

(xiv) Each Customer subscribed to Mainland China SmartSecure Private Access can be provisioned with up to 3 Mainland China POPs.

(xiv) Each end user using the SmartSecure Private Access Service shall have no more than three (3) end point devices connecting to the Service.

(xiv) Aryaka does not provide Internet Breakout (using a VO, Cloud Security Solution or any other such mechanism) from any of the POPs located outside Mainland China for traffic originating in Mainland China.

(xiv) Aryaka reserves the right to choose the location and number of SmartSecure Private Access POPs that will be reserved for the Customer users to connect to the Service, while every effort will be undertaken by Aryaka to provide the optimal connectivity and experience to end users subject to resource availability on infrastructure side and compliance needs.

(xiv) Aryaka reserves the right to throttle the bandwidth usage for any remote user if an abusive pattern of consumption is observed on a consistent basis.

(xiv) Aryaka reserves the right to decide what capabilities will be added/ modified/removed from the list of supported capabilities and that will be reflected on the product documentation made available to Customers. Notwithstanding the foregoing, Aryaka shall ensure that the Services procured by Customer under the Agreement will not materially adversely deviate from what is agreed by the Parties thereon.

(xiv) The SmartSecure Private Access offering is powered by the remote access technology offering from NCP-engineering, Inc. (“NCP”). By installing the SmartSecure Private Access client (powered by NCP), end users agree to the

license agreement with NCP (or affiliate) as follows:

https://www.ncp-e.com/fileadmin/_NCP/pdf/info/NCP_License_Terms_Client_EN.pdf

CUSTOMER ACKNOWLEDGES AND AGREES THAT NCP TECHNOLOGY AND PRODUCT OFFERINGS ARE THIRD-PARTY COMPONENTS AND THAT ARYAKA AND ITS AFFILIATES DISCLAIM AND ARE NOT RESPONSIBLE FOR DAMAGES OR LIABILITIES ARISING FROM OR RELATED TO NCP FROM PRODUCT OR OPERATIONS PERSPECTIVE.

k. **SmartSecure NGFW-SWG** is Aryaka's managed Next-Generation Firewall ("NGFW") and Secured Web Gateway ("SWG") service. It provides application and user-aware protection to networks, users and cloud infrastructure. Aryaka's SmartSecure NGFW-SWG service has 2 types of licenses to meet different deployment needs: Site Licenses and User Licenses. Site Licenses are used to provide NGFW-SWG service to a location or site ("Site Licenses"). User Licenses are used to provide NGFW-SWG service to remote users ("User Licenses").

Terms of Use for SmartSecure NGFW-SWG:

(i) SmartSecure NGFW-SWG service Site Licenses require Customers to have SmartManage, SmartConnect or SmartCloud licenses. Supported SmartManage licenses are Global and Regional, with the following sizes: Small, Medium, Large, X-Large, and BYO. Supported SmartConnect EZ and Pro licenses include the following sizes: X-Small, Small, Medium, Medium-Plus, Large and X-Large. Supported SmartCloud licenses are IaaS.

(ii) SmartSecure NGFW-SWG service User Licenses require the remote user to have Aryaka SmartSecure PrivateAccess service. Supported SmartSecure PrivateAccess licenses are SmartSecure PrivateAccess-ROW and SmartSecure PrivateAccess-Mainland China.

(iii) SmartSecure NGFW-SWG service Site Licenses include 7 different sizes: X-Small, Small, Medium, Medium-Plus, Large, X-Large and BYO.

(iv) The size of SmartSecure NGFW-SWG service Site Licenses for a certain site needs to match the SmartManage or SmartConnect license size for the same site, including BYO sites.

(v) SmartSecure NGFW-SWG service can be enabled for SmartCloud IaaS Small or Medium sites with the matching SmartSecure NGFW-SWG service site size. SmartCloud IaaS site with a SmartCloud-ENX-IaaS-License Legacy or SmartCloud-SD-IaaS-License Legacy ("Legacy") license needs to first convert to SmartCloud IaaS Small or Medium to add SmartSecure NGFW-SWG service.

(vi) SmartSecure NGFW-SWG service User Licenses include 2 different regions:

a. Mainland China

b. ROW

(vii) SmartSecure NGFW-SWG service is delivered through an ANAP or a POP, depending on the deployment model. When there is an ANAP in a site deployment model, SmartSecure NGFW-SWG service is delivered on an ANAP. In all other deployment models, SmartSecure NGFW-SWG service is delivered on a POP.

(viii) SmartSecure NGFW-SWG service for remote user is delivered on POPs. Usage is expected to be in accordance with this document and Agreement. Aryaka assumes the average data transfer per subscribed remote user is expected to be less than 6 GB (Gigabytes) per user, per month. If average usage for a Customer exceeds that amount ("Overage"), an Overage charge will be applied. Overage is calculated by subtracting total traffic volume (in Gigabytes) of POP-delivered SmartSecure NGFW-SWG service for the Customer's remote users by 6 Gigabytes multiplied by the total number of SmartSecure NGFW-SWG User Licenses. Overage is billed at the end of the month based on the Overage rates for each Region (ROW and Mainland China) on the valid Order Form.

(ix) Sizes of SmartSecure NGFW-SWG licenses do not provide traffic throughput guarantee. Actual attainable throughput for a site will be affected by, but not limited to, traffic profile, available link bandwidth and ANAP model. Please refer to the SLA for details.

(x) Bursting for SmartSecure NGFW-SWG service for BYO sites or SmartCloud IaaS sites is allowed when the SmartConnect-Bursting-Multiplier option is on the Order Form. Bursting is the actual bandwidth usage above the subscribed bandwidth for BYO sites or SmartCloud IaaS sites as set forth in the Order Form.

(xi) Bursting for SmartSecure NGFW-SWG service for remote user is allowed when the SmartConnect-Bursting-Multiplier option is on the Order Form. Bursting is the actual number of remote users above the contracted number of remote users as set forth in the Order Form.

(xii) Customer is solely responsible for creating, customizing and updating its internal security policies and rules. For an additional fee, Aryaka may provide this as a service to the Customer under a separate Statement of Work.

(xiii) If SmartSecure NGFW-SWG service remote user connection fails, Aryaka has the discretion to redirect the user connection to another POP. Depending on the redirected POP's Region, user experience for internet access may be different from the initial POP.

l. **SmartSecure Anti-Malware** is Aryaka's anti-malware service. It requires SmartSecure NGFW-SWG service to be active. SmartSecure Anti-Malware is an add-on service to SmartSecure NGFW-SWG service. SmartSecure Anti-Malware provides advanced malware detection and protection using threat intelligence. Aryaka's SmartSecure Anti-Malware has 2 types of licenses to meet different deployment needs: Site Licenses and User Licenses. Site Licenses are used to provide Anti-Malware service to a location or site. User Licenses are used to provide Anti-Malware service to remote users.

Terms of Use for SmartSecure Anti-Malware:

(i) SmartSecure Anti-Malware service Site License requires a SmartSecure NGFW-SWG Site License.

(ii) SmartSecure Anti-Malware Service User license requires a SmartSecure NGFW-SWG User License.

(iii) SmartSecure Anti-Malware service Site Licenses include 7 different sizes: X-Small, Small, Medium, Medium-Plus, Large, X-Large and BYO.

(iv) The size of SmartSecure Anti-Malware service Site License for a certain site has to match the SmartSecure NGFW-SWG Site License size for the same site, including BYO sites.

(v) SmartSecure Anti-Malware service can be enabled for a SmartCloud IaaS Small or Medium site that already has SmartSecure NGFW-SWG service with matching SmartSecure Anti-Malware service site size.

(vi) SmartSecure Anti-Malware service is delivered through an ANAP or a POP, depending on the deployment model. When there is an ANAP in a site deployment model, SmartSecure Anti-Malware service is delivered on an ANAP. In all other deployment models, SmartSecure Anti-Malware service is delivered on a POP.

(vii) Sizes of SmartSecure Anti-Malware licenses do not provide traffic throughput guarantee. Actual attainable throughput for a site will be affected by, but not limited to, traffic profile, available link bandwidth and ANAP model. Please refer to the SLA for details.

(viii) Bursting for SmartSecure Anti-Malware service for remote user is allowed when the SmartConnect-Bursting-Multiplier option is t on the Order Form. Bursting is the actual number of remote users above the contracted number of remote users as set forth in the Order Form.

(ix) Customer is solely responsible for creating, customizing, and updating its internal security policies and rules. For an additional fee, Aryaka may provide this as a service to the Customer under a separate Statement of Work.

m. **SmartSecure IPS** is Aryaka's Intrusion Protection Service ("IPS"). It requires SmartSecure NGFW-SWG service to be active. SmartSecure IPS is an add-on service to SmartSecure NGFW-SWG service. SmartSecure IPS provides advanced intrusion detection and protection with threat intelligence. SmartSecure IPS has 2 types of licenses to meet different deployment needs: Site Licenses and User Licenses. Site Licenses are used to provide SmartSecure IPS service to a location or site. User Licenses are used to provide SmartSecure IPS service to remote users.

Terms of Use for SmartSecure IPS:

(i) SmartSecure IPS service site license requires a SmartSecure NGFW-SWG Site License.

(ii) SmartSecure IPS service user license requires a SmartSecure NGFW-SWG User License.

(iii) SmartSecure IPS service Site Licenses include 7 different sizes: X-Small, Small, Medium, Medium-Plus, Large, X-Large and BYO.

(iv) The size of SmartSecure IPS service Site License for a certain site has to match the SmartSecure NGFW-SWG Site License size for the same site, including BYO sites.

(v) SmartSecure IPS service can be enabled for a SmartCloud IaaS Small or Medium site that already has SmartSecure NGFW-SWG service with matching SmartSecure IPS service site size.

(vi) SmartSecure IPS service is delivered through an ANAP or a POP, depending on

the deployment model. When there is an ANAP in a site deployment model, SmartSecure IPS service is delivered on an ANAP. In all other deployment models, SmartSecure IPS service is delivered on POP.

(vii) Sizes of SmartSecure IPS licenses do not provide traffic throughput guarantee. Actual attainable throughput for a site will be affected by, but not limited to, traffic profile, available link bandwidth and ANAP model. Please refer to the SLA for details.

(viii) Bursting for SmartSecure IPS service for remote user is allowed when the SmartConnect-Bursting-Multiplier option is on the Order Form. Bursting is the actual number of remote users above the contracted number of remote users as set forth in the Order Form.

(ix) Customer is solely responsible for creating, customizing and updating its internal security policies and rules. For an additional fee, Aryaka may provide this as a service to the Customer under a separate Statement of Work.

n. **SmartSecure CASB** is Aryaka's Cloud Access Security Broker (CASB), part of Secure Access Service Edge (SASE) architecture provides comprehensive visibility and control over SaaS applications, including sanctioned, unsanctioned, and unclassified apps, via a centralized dashboard. It helps discover and monitor use of software or applications that are without explicit approval , reducing risks from unauthorized SaaS usage. Granular access controls allow fine-tuned access, restricting user access to SaaS apps based on factors like SaaS Apps, SaaS Apps Reputation, user activity, SaaS Organizations, SaaS Suites, SaaS Categories, and schedules, ensuring only authorized users can access sensitive data. With flexible deployment options, it enforces policies across both on-prem and cloud environments. Additionally, Aryaka CASB allows user-based access controls to manage access based on user roles, groups, and assets, and tenant-level policy controls to ensure data remains isolated between different tenants. It requires SmartSecure CASB to be active. SmartSecure CASB is an add-on service to SmartSecure NGFW-SWG. SmartSecure CASB has 2 types of licenses to meet different deployment needs: Site Licenses and User Licenses. Site Licenses are used to provide SmartSecure CASB to a location or site. User Licenses are used to provide SmartSecure CASB to remote users.

Terms of Use for SmartSecure CASB:

(i) SmartSecure CASB site license requires a SmartSecure NGFW-SWG Site License.

(ii) SmartSecure CASB user license requires a SmartSecure NGFW-SWG User License.

(iii) SmartSecure CASB Site Licenses include 7 different sizes: X-Small, Small, Medium, Medium-Plus, Large, X-Large and BYO.

(iv) The size of SmartSecure CASB Site License for a certain site has to match the SmartSecure NGFW-SWG Site License size for the same site, including BYO sites.

(v) SmartSecure CASB is delivered through an ANAP or a POP, depending on the deployment model. When there is an ANAP in a site deployment model, SmartSecure CASB service is delivered on an ANAP. In all other deployment models, SmartSecure CASB service is delivered on POP.

(vi) Sizes of SmartSecure CASB licenses do not provide traffic throughput guarantee. Actual attainable throughput for a site will be affected by, but not limited to, traffic profile, available link bandwidth and ANAP model. Please refer to the SLA for

details.

(vii) Bursting for SmartSecure CASB for remote user is allowed when the SmartConnect-Bursting-Multiplier option is on the Order Form. Bursting is the actual number of remote users above the contracted number of remote users as set forth in the Order Form.

(viii) Customer is solely responsible for creating, customizing and updating its internal security policies and rules. For an additional fee, Aryaka may provide this as a service to the Customer under a separate Statement of Work.

5. Aryaka Day 0 Professional Services

Day0 Professional Services are Aryaka professional services to assist customers with initial configuration, design and implementation of Aryaka SmartManage, SmartConnect, SmartSecure and SmartCloud services. Day0 Professional Services are ordered as credit by unit of hour. These services include comprehensive guidance and hands-on assistance, and are designed to ensure a seamless onboarding experience, enabling customers to leverage Aryaka's advanced network and cloud solutions effectively.

Day0 Professional Services are structured as credit units per hour before service delivery.

ProfessionalServices-ENX-DAY0-Hour

Terms of Use for Day0 Professional Services:

(iv) Pricing for subscription to Aryaka's Day0 Professional Services is based on an hourly rate.

(iv) Day0 Professional Services can be applied to supported service types according to the menu of Services.

(iv) Day0 Professional Services must be pre-ordered prior to commencement of service delivery.

(iv) Day0 Professional Services are intended solely for one-time engagements.

C. Description of Aryaka SmartConnect EZ

Aryaka SmartConnect EZ is Aryaka's SD-WAN managed service offering built on Aryaka's Flexcore (as described below) L3 Private Core.

Aryaka's Flexcore consists of a Layer 2 mesh network for application performance and a Layer 3 mesh network or enhanced Internet for Customers that predominantly use productivity or web/cloud applications.

Aryaka's Layer 2 core provides high levels of application performance with WAN optimization. Aryaka's L3 Private Core is for Customers that want the high-quality Aryaka managed service with predictable performance at a lower cost. This L3 Private Core is provided with advanced loss detection and correction technology without WAN optimization. In the L3 Private Core, all Aryaka POPs in a given Region are interconnected with one another over the Internet, thereby providing increased fault tolerance to outages on any given Link.

Aryaka SmartConnect EZ is offered in four regions (as defined in Table 3 below) and five different sizes (as defined by Aryaka in Table 4 below) per site. Aryaka SmartConnect EZ provides easy-to-consume managed SD-WAN connectivity services to enterprise sites, such as branch offices, stores, service centers, and data centers.

Table 3: Aryaka SmartConnect EZ Regions are defined as:

Aryaka SmartConnect EZ Regions	Different regions of the world
A	USA, Canada, Mexico, European Union
B	Asia-Pacific, Japan, Korea, India, Australia/New Zealand
C	Mainland China
D	South Africa, South America, Dubai, Russia (if available)

Customers can subscribe to one of the five bandwidth capacity sizes on the Aryaka middle-mile L3 Private Core on a per-site per-Region basis, as defined by Aryaka in Table 4 below.

Table 4: Aryaka SmartConnect EZ bandwidth capacity sizes are defined as:

Aryaka SmartConnect EZ Bandwidth Capacity Sizes	Subscribed Bandwidth
X-Small	Up to 10 Mbps
Small	Up to 20 Mbps
Medium	Up to 50 Mbps
Medium-Plus	Up to 200 Mbps
Large	Up to 500 Mbps
X-Large	Up to 1 Gbps

The Aryaka SmartConnect EZ services consist of the following features:

- SmartConnect EZ Sites
- High Availability ("HA")
- Last Mile Management
- Last Mile Service
- Security Services

a. **Aryaka SmartConnect EZ Sites** includes transport over L3 Private Core, five different sizes, in four regions, Cloud IaaS Dedicated Connectivity, Cloud Security Connector, L3/L4 Firewall, Micro-segmentation/Edge Essentials and support (as described in Aryaka Customer Support Policy Document). Subscription price to Aryaka SmartConnect EZ's size differs per region. Enterprise sites are assigned to one specific Region based on the nearest proximity to one of the Aryaka POPs.

b. **Aryaka SmartConnect-EZ-HighAvailability (HA)** provides additional levels of redundancy for enterprise sites consuming Aryaka SmartConnect EZ. High Availability is optional.

- **Aryaka SmartConnect-EZ-ANAP-HA** Redundancy is enabled at the ANAP device level for a site. Should the active ANAP fail as described in the SLA, the redundant ANAP will automatically become active and start routing traffic to the designated Aryaka POP. The redundant ANAP is included in this service. Aryaka SmartConnect-EZ-ANAP-HA is available in all five different Aryaka SmartConnect EZ sizes: X-Small, Small, Medium, Medium-Plus, Large and X-Large.
- **Aryaka SmartConnect-EZ-POP-HA** Redundancy enabled in case of POP failure and traffic is routed to a backup Aryaka POP. Aryaka SmartConnect-EZ-POP-HA includes a redundant ANAP enabling the rerouting to another Aryaka POP in case of POP failure.

Aryaka SmartConnect-EZ-POP-HA is available in all five different SmartConnect EZ sizes: X-Small, Small, Medium, Medium-Plus, Large and X-Large.

c. **Aryaka SmartConnect-LastMileManagement** gives Customers 24x7 proactive Link Monitoring and management of Customer's Links that connect an enterprise site to Aryaka Services. Aryaka's Support team proactively works with the Internet Service Providers of Customers to raise and resolve any issues on the Customer's behalf. Last Mile Management is per last-mile Link. SmartConnect-LastMileManagement is optional.

d. **SmartConnect-LastMileService** allows Customer to purchase first-mile and last-mile Internet circuits from Aryaka. SmartConnect-LastMileService always comes with SmartConnect- LastMileManagement. SmartConnect-LastMileService is always sold separately from all other SmartServices on a separately processed and signed sales order form. SmartConnect-LastMileService is optional.

e. **Security Services** with SmartSecure includes all security capabilities offered on the Aryaka platform, including native security capabilities on the ANAP and certain management functions with respect to select third-party firewall services. SmartSecure service is optional.

Terms of Use for Aryaka SmartConnect EZ Services:

(i) Bandwidth usage shall not exceed subscribed Aryaka SmartConnect EZ size limit per site. Bursting or bandwidth pooling is not available with Aryaka SmartConnect EZ service. Inter-Region Multiplier does not apply to Aryaka SmartConnect EZ services.

(ii) S2S InternetVPN or MPLS are not applicable to Aryaka SmartConnect EZ service.

(iii) Site moves (excluding Last Mile Services), bandwidth size reallocation and add-on relocations are limited to no more than one (1) change per site in any given month.

(iv) If Elastic-Multiplier is not included in the Order Form, Customers shall not exceed the purchased aggregate bandwidth limit for the specific Aryaka SmartConnect EZ service as set forth in the Order Form.

(v) Any billing schedule based on the deployment dates shall be set forth in the Order Form.

(vi) Aryaka SmartConnect EZ can only be purchased under the Enterprise Flex Pricing model.

D. Description of Aryaka SmartConnect Pro

Aryaka SmartConnect Pro is Aryaka's SD-WAN managed service offering built on Aryaka's Flexcore (as described above) Layer 2 Private Core.

Aryaka's Layer 2 Private Core provides high levels of application performance with WAN optimization. In the Layer 2 Private Core, all Aryaka POPs in a given Region are interconnected with one another over a Layer 2 Private Core, thereby providing optimized performance.

Aryaka's Flexcore architecture allows for mixing of sites with different levels of managed SD-WAN or SASE services. SmartConnect Pro sites can connect to sites with other services like SmartConnect EZ. Flexcore path selection is as follows:

- When a SmartConnect Pro site communicates with another SmartConnect Pro site, L2 Private Core will be

used.

- When a SmartConnect Pro site communicates with a SmartConnect EZ site, or vice versa, L3 Private Core will be used.
- When a SmartConnect EZ site communicates with another SmartConnect EZ site, L3 Private Core will be used.

Aryaka SmartConnect Pro is offered in four regions (as defined in Table 5 below) and five different sizes (as defined by Aryaka in Table 6 below) per site. Aryaka SmartConnect Pro provides easy-to-consume managed SD-WAN connectivity services to enterprise sites, such as branch offices, stores, service centers, and data centers.

Table 5: Aryaka SmartConnect Pro Regions are defined as:

Aryaka SmartConnect Pro Regions	Different regions of the world
A	USA, Canada, Mexico, European Union
B	Asia-Pacific, Japan, Korea, India, Australia/New Zealand
C	Mainland China
D	South Africa, South America, Dubai, Russia (if available)

Customers can subscribe to one of the five bandwidth capacity sizes on the Aryaka middle-mile L2 Private Core on a per-site per-Region basis, as defined by Aryaka in Table 6 below.

Table 6: Aryaka SmartConnect Pro bandwidth capacity sizes are defined as:

Aryaka SmartConnect Pro Bandwidth Capacity Sizes	Subscribed Bandwidth
X-Small	Up to 10 Mbps
Small	Up to 20 Mbps
Medium	Up to 50 Mbps
Medium-Plus	Up to 200 Mbps
Large	Up to 500 Mbps
X-Large	Up to 1 Gbps

The Aryaka SmartConnect Pro services consist of the following features:

- SmartConnect Pro Sites
- High Availability ("HA")
- Last Mile Management
- Last Mile Service
- Security Services
- InternetVPN
- MPLS

a. **Aryaka SmartConnect Pro Sites** includes transport over L2 Private Core, five different sizes, in four regions, Cloud IaaS Dedicated Connectivity, Cloud Security Connector, L3/L4/Application Deep Packet

Inspection Firewall, Micro-segmentation/Edge Essentials and support (as described in Aryaka Customer Support Policy Document). Subscription price to Aryaka SmartConnect Pro's size differs per region. Enterprise sites are assigned to one specific Region based on the nearest proximity to one of the Aryaka POPs.

b. **Aryaka SmartConnect-Pro-HighAvailability (HA)** provides additional levels of redundancy for enterprise sites consuming Aryaka SmartConnect Pro. High Availability is optional.

- **Aryaka SmartConnect-Pro-ANAP-HA** Redundancy is enabled at the ANAP device level for a site. Should the active ANAP fail as described in the SLA, the redundant ANAP will automatically become active and start routing traffic to the designated Aryaka POP. The redundant ANAP is included in this service. Aryaka SmartConnect-Pro-ANAP-HA is available in all five different Aryaka SmartConnect Pro sizes: X-Small, Small, Medium, Medium-Plus, Large and X-Large.
- **Aryaka SmartConnect-Pro-POP-HA** Redundancy enabled in case of POP failure and traffic is routed to a backup Aryaka POP. Aryaka SmartConnect-Pro-POP-HA includes a redundant ANAP enabling the rerouting to another Aryaka POP in case of POP failure. Aryaka SmartConnect-Pro-POP-HA is available in all five different SmartConnect Pro sizes: X-Small, Small, Medium, Medium-Plus, Large and X-Large.

c. **Aryaka SmartConnect-LastMileManagement** gives Customers 24x7 proactive Link Monitoring and management of Customer's Links that connect an enterprise site to Aryaka Services. Aryaka's Support team proactively works with the Internet Service Providers of Customers to raise and resolve any issues on the Customer's behalf. Last Mile Management is per Link. SmartConnect-LastMileManagement is optional.

d. **SmartConnect-LastMileService** allows a Customer to purchase first-mile and last-mile Internet circuits from Aryaka. SmartConnect-LastMileService always comes with SmartConnect- LastMileManagement. SmartConnect-LastMileService is always sold separately from all other SmartServices on a separately processed and signed sales order form. SmartConnect-LastMileService is optional.

e. **Security Services** with SmartSecure includes all security capabilities offered on the Aryaka platform, including native security capabilities on the ANAP and certain management functions with respect to select third-party firewall services. SmartSecure service is optional.

f. **SmartConnect-InternetVPN** means the ability for two sites to communicate securely over the Internet using site-2-site VPN and Aryaka HybridWAN technology.

g. **SmartConnect-MPLS** means the ability for a site-to-peer with a Customer Edge MPLS Router.

Terms of Use for Aryaka SmartConnect Pro Services:

(i) Site moves (excluding Last Mile Services), bandwidth size reallocation and add-on relocations are limited to no more than one (1) change per site in any given month.

(ii) If Elastic-Multiplier is not included in the Order Form, Customers shall not exceed the purchased bandwidth size limit for the specific Aryaka SmartConnect Pro service as set forth in the Order Form.

(iii) Any billing schedule based on the deployment dates shall be set forth in the Order Form.

(iv) Aryaka SmartConnect Pro can only be purchased under the Enterprise Flex Pricing

model.

E. Description of Aryaka SmartCDN (IADS)

Aryaka SmartCDN provides IP Application Delivery-as-a-Service ("IADS") as a usage-based service. IADS is used for accelerating any web or IP-based public applications, such as web servers and VDI farms, over Aryaka's global network using capabilities, such as TCP optimization, caching, and compression with cloud- based management and visibility, when using the MyAryaka portal.

Terms of Use of Aryaka SmartCDN Services (IADS):

(i) Aryaka reserves the right to choose the edge POPs and Origin POPs to deliver the Services on its global network.

(ii) Aryaka reserves the right to limit the maximum data transfer rates achieved over the Aryaka Network based on the aggregate commits purchased.

F. Description of Aryaka SmartHands Service

Aryaka SmartHands Service is a professional service offered to a Customer pertaining to the installation and activation of an ANAP to connect a Customer site to Aryaka Services. Aryaka SmartHands Service is offered at a Customer's request for sites which need installation and activation professional services.

Terms of Use for Aryaka SmartHands Service: Unless otherwise stated in the applicable Order Form or statement of work between Aryaka and the Customer, the terms are as follows:

(i) Aryaka SmartHands Service is charged at an hourly rate, for each site that requires the SmartHands Service, and billed monthly in arrears for actual hours delivered.

(ii) Customer will reimburse Aryaka for all reasonable and necessary travel-related expenses.

G. Description of Last Mile Circuits

Last Mile Circuit is the physical Link (wired or wireless) that is used to connect Customer's site to the closest Aryaka POP. The physical Link may be a direct Layer-2 connection or an Internet Circuit. The type of the Last Mile Circuit will be specified in the Order Form.

Terms of Use for Last Mile Circuits:

(i) All charges for each Last Mile Circuit Service will commence when each particular circuit is Activated and ready for service, and the ready for service date ("RFS Date") is communicated to Customer. Such charges shall commence as set forth in the preceding sentence regardless of whether or when other Aryaka Services are Activated.

(ii) Upon completion of the site survey of Customer's sites, the particular third-party service provider will advise Aryaka if there will be: (a) additional charges for providing service above the charges previously quoted to Customer. In any such case, Aryaka will propose the associated cost changes to Customer; (b) "no service available" or equivalent, or if a redesign is required. Aryaka will then undertake to locate an alternate provider for the Last Mile Circuit. Aryaka will propose the alternate Last Mile Circuit together with the associated cost changes to Customer.

(iii) Customer has the right to reject the proposed charges within five (5) days of receipt of the proposal. If Customer rejects the proposal, then the original order for the Last Mile Circuit will be automatically cancelled with no early termination fees. The proposal will be considered accepted if not so rejected by Customer within the 5-day period.

(iv) All start or completion dates provided at the time of signing the Last Mile Circuit order are advisory and non-binding. The final service activation date will be provided after the third-party service provider has completed the site survey of Customer's sites.

(v) Aryaka will not be responsible for delays in (a) completion of internal wiring, (b) Customer responding to requests for additional information, or (c) gaining access to Customer's sites to have the service installed.

(vi) All Last Mile Circuit quotes are based on providing connectivity to the Minimum Point Of Entrance (MPOE). All wiring from the MPOE to Customer's facilities or equipment is the responsibility of Customer. Upon written request from Customer, Aryaka will advise whether it has the capability to provide the internal wiring, together with an estimate of the associated extra cost.

(vii) For all Last Mile Circuits, the Mean Time to Repair and the Service Availability Service Level Agreement will, as provided by (or limited by, as the case may be), the particular third-party service provider, depend upon the type of circuit that is ordered.

H. Description of Link Monitoring

Link Monitoring means the monitoring by Aryaka of Customer's Last Mile Circuit Link to be conducted on a 24x7x365 basis, including reports and support as specified herein. Link Monitoring shall be included with the Last Mile Circuit if and as specified in the Order Form together with a letter of authorization from Customer.

Terms of Use for Link Monitoring

Link Monitoring. If Aryaka receives an executed Letter of Authorization (LOA) from Customer, Aryaka will proceed with the following Link Monitoring services as part of the Last Mile Circuit Management:

(i) Monitor the Link 24x7x365 by pinging between Aryaka's POP and the end-user device.

(ii) Pings occur once per second and Aryaka reports average packet loss and latency by the minute.

(iii) Aryaka monitoring team to be alerted when the rolling average for either latency or packet loss exceeds the applicable thresholds set forth in the SLA.

(iv) As specified in the Last Mile Management SLA terms, in the event of an incident where latency or packet loss exceeds the applicable thresholds, or the last mile tunnel becomes unavailable, Aryaka will follow up with Customer, Customer's Internet Service Provider (ISP), or both.

(v) In working with each ISP, Aryaka will comply with any incident resolution priority or escalation matrix provided by the ISP.

Aryaka is not responsible for any ISP failing to restore service in accordance with the ISP's SLA. Further, Aryaka is not responsible for procuring ISP Links or other non-Aryaka Links for Customer.

I. Service Usage Calculations

With a few exceptions, for most of the above Services, the service usage calculation for billing purposes is based on the committed subscribed quantity, as stated on the Order Form. This section details the service usage calculation methods for usage- based Services where billing is based on actual usage, and not solely on the committed subscribed quantity.

a. Service usage calculation for Elastic Subscriptions

Elastic Subscriptions for all Aryaka Services are allowed when the SmartManage- ElasticSubscription-Multiplier option is present on the Order Form and has been elected by the Customer. Any actual Activated quantity of

a Service exceeding the subscribed quantity for the Service is defined as Oversubscription usage.

The unit price for each unit of oversubscription usage is calculated as the product of the SmartManage-ElasticSubscription-Multiplier and the unit price for the Service, each as set forth in the Order Form.

b. Service usage calculation for InterRegion Traffic

InterRegion traffic for SmartConnect-L2PrivateCore-SBW with regional pricing is allowed when the SmartConnect-InterRegion-Multiplier option is present on the Order Form and has been elected by the Customer. InterRegion traffic for a Regional Site is the max of the 99th percentile of the traffic sent to or received from the Regional Site to all other sites that are not in the same Region. InterRegion traffic for a Region is the sum of the InterRegion traffic for all the Regional Sites in that Region. The unit price for InterRegion traffic is calculated as the product of the SmartConnect-InterRegion-Multiplier and the unit price, per the Regional pricing tier, for the Aryaka SmartConnect-PrivateCore-SBW Service, as set forth in the Order Form. *All Inter-Region traffic is metered and billed at the end of the month based on the multiplier on the signed Order Form.*

c. Service usage calculation for Bursting

Bursting for SmartConnect-L2PrivateCore-SBW is allowed when the SmartConnect- Bursting-Multiplier option is present on the Order Form and has been elected by the Customer. Bursting is the actual bandwidth usage above the subscribed bandwidth for SmartConnect-L2PrivateCore-SBW as set forth in the Order Form. Bandwidth Usage for a site is the max of the 99th percentile for the traffic sent or received over Aryaka's L2 private core. For Regional sites, InterRegion traffic is not accounted for in the Bandwidth Usage. For the Enterprise Flex pricing model, Bursting is calculated for each Region by subtracting the aggregate subscribed bandwidth from the aggregate bandwidth usage for all the sites in that Region. For the Standard pricing model, Bursting is calculated for each site by subtracting the subscribed bandwidth from the bandwidth Usage. The unit price for Bursting is calculated as the product of the SmartConnect-Bursting-Multiplier and the unit price for the Aryaka SmartConnect-L2PrivateCore-SBW service, each as set forth in the Order Form.

Note: For all the above usage-based services, in the case of multiple Order Forms, the unit price and multiplier are determined by the latest Order Form.

[*End of SmartService Descriptions*]