AKAMAI SERVICES

The following definitions, billing methodologies, service descriptions and additional terms are applicable to the purchase and use of Akamai's various products and Services and shall be deemed incorporated into the Order Form or other Transaction Document between Customer/Reseller/Channel Partner/NetAlliance Partner (as applicable) and Akamai. Akamai is constantly working to improve its Services for the benefit of all its global customers, and as a result we need to retain the right to make changes to all Services so long as the changes do not negatively impact our customers. Akamai may modify or terminate any Service if such modification or termination is generally applicable to all customers. In the event of such a modification or termination, Customer/Reseller/Channel Partner/NetAlliance Partner (as applicable) may terminate the applicable Order Form or other Transaction Document without termination charge if Akamai fails to remedy a material decrease in the functionality of the affected Service within thirty days of written notice from such Customer/ Reseller/Channel Partner/NetAlliance Partner (as applicable). Capitalized terms used but not defined herein shall have the meanings set forth in the Terms & Conditions governing Customer's purchase of Akamai offerings.

SELECTED ACRONYMS/DEFINITIONS

95/5: The billing and measurement methodology shorthand describing a process of determining the 95th percentile of usage or the uncompressed equivalent as measured by Akamai over five minute intervals. The 95/5 methodology is used to measure usage of NetStorage, Concurrent Users, and Services billed in Mbps, Gbps or any other bit per second methodology.

API: Application Programming Interface

Application or "App": Any discrete instance of computer software that performs a particular function for a Customer or Customer's end user and can be accelerated by any Akamai acceleration Service. For billing purposes, each instance of any such software is considered an independent "Internet Application" or "App". For example, each Application running on a particular platform (e.g., Force.com, Amazon AWS, Microsoft Azure, SAP, .NET, etc.) is considered a discrete App, while the platform itself would not be considered an App. Also, a portal consisting of many Applications will be counted as more than one application.

Card Information: Personally identifiable information entered by a user on a designated portion of Customer's Site for the purpose of fulfilling a transaction or account access process and which is identified to be replaced by a token pursuant to the Edge Tokenization Module configuration defined and approved by Customer. Such information may include a user's name, address, personal account number, credit card number, debit card number, bank account number, check number or other financial account number.

Content Adaptation Engine: Generates optimized, mobile device-specific content adapted from Customer's origin website content.

Content Type: An HTTP response header that describes the file type that follows and that the browser uses to render the content properly.

CP Code: Content provider code used to track Customer's individual usage of the applicable Service(s).

Customer Portal: Luna Control Center located at https://control.akamai.com.

Custom Rule: The capability to create a rule in Akamai metadata language and implemented by Akamai's WAF module.

Datacenter: Any destination IP address outside of the Akamai network used as a source location for Customer content (and would not include any Akamai IP address or Service, such as Akamai NetStorage).

DDoS (distributed denial-of-service) or DoS (denial-of-service) Attack: An ongoing traffic increase where (i) Site traffic is four or more times higher than the average Site traffic, per unit, over the immediately preceding two month period, (ii) Customer and Akamai mutually agree that the traffic spike is malicious, and/or unwanted, and Customer requests Akamai to declare the traffic as a DDoS Attack, and (iii) Customer informs Akamai that they are willing to NOT serve the unexpected traffic and are willing to allow Akamai to determine the approach for mitigating potential negative impacts of the DDoS traffic (e.g., blocking the traffic, redirecting the traffic, serving the traffic, etc.).

Digital Property means a Site requiring separately configured and distinct Application Services deployed on the Akamai platform, reporting feeds or invoicing. A Digital Property may consist of at most one domain name and ten hostnames.

DNS: Domain Name System.

Emergency Security Configuration Assistance: Any Managed Kona Site Defender Security Configuration Assistance request made with less than 24 hours' notice, or delivered outside of normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

Error: A failure in software to materially conform to the specifications described in http://www.akamai.com/service and the applicable product documentation.

Extended Validation (EV) Digital Certificate: A special type of X.509 digital certificate that requires more extensive investigation of the requesting entity by the certificate authority before being issued. The requirements for issuing EV Digital Certificates are defined by the Certification Authority Browser Forum ("CA/Browser Forum") located at http://www.cabforum.org. Extended Validation certificates may be issued as single-hostname or Subject Alternative Name (SAN) certificates.

FISMA: Federal Information Security Management Act

Gbps: gigabit(s) per second. One (1) Gbps is equal to 1,000 Mbps.

GB: gigabyte(s). One (1) GB is equal to 1,000 MB.

HD Client: Combination of the HD Network Player Component and the NetSession Interface to enable delivery of HD Network Services.

HD Network Player Component: Akamai's client-side software used to enable delivery of Akamai HD Network Services. The Akamai HD Network Player Component is provided subject to the applicable license agreement located at www.akamai.com/product/licenses, and Customer's purchase and use of the Akamai HD Network Player Component constitutes Customer's acceptance of the terms of such license.

HIPAA Security Rules: Health Insurance Portability and Accountability Act, the current version can be found here: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html.

Hit: An HTTP request to an Akamai server to access an object.

HTML: HyperText Markup Language.

HTTP: Hypertext Transfer Protocol. HTTP is an Application-level protocol for distributed, collaborative, hypermedia information systems.

HTTP Dynamic Streaming ("HDS"): Supports Adobe Flash.

HTTP Live Streaming ("HLS"): Supports Apple iPhone/iPad.

HTTPS: HTTP combined with a network security protocol.

Identity Provider: A service provider that creates, maintains, and manages identity information for Customer and provides principal authentication to Akamai.

Initial Response Time: The time it takes a customer to get a response on the reported issue from an Akamai technical support representative. The measurement of the Initial Response Time is the elapsed time from the receipt of the request by Akamai, to the response to Customer by an appropriate service resource to acknowledge the request, respond with a service request number and begin working the issue. This includes time until a response is received in the form of a call back or e-mail or any other customer-facing communication. The degree of urgency can vary based upon the issue's Priority Level.

IP: Internet protocol.

IP Blacklist: A list of IP addresses that are explicitly denied a connection to an Akamai edge server.

IP Rate Control: The ability to monitor and block excessive request rates made by client systems for websites, applications and related objects accelerated by Akamai's edge platform.

IP Whitelist: A list of IP addresses that are explicitly accepted without further security analysis.

ISO: Industry Organization for Standardization

KB: kilobyte(s). One KB is equal to 1,000 bytes.

Luna Control Center: See Customer Portal.

Map: A specific and limited collection of Akamai servers, selected by Akamai and consisting of a list of IP network address ranges denoted using classless inter-domain routing ("CIDR") notation, that are configured within the Akamai network infrastructure to communicate with Customer's origin server(s).

Mbps: megabit(s) per second.

MB: megabyte(s). One MB is equal to 1,000 KB.

Midgress Traffic: additional traffic from a midgress server to an edge server generated by certain Services.

Mobile Site: A set of URLs used to deliver content and applications targeted at mobile devices for a discrete and individual corporate unit (e.g., legal entity, company business unit, publishing group, product brand or Application) that may consist of at most one domain and up to 3 sub-domains. For example, in the case of mobile.customer.com and images-mobile.customer.com, "customer.com" is the domain and "mobile" and "images-mobile" are sub-domains.

MPV: million Page Views.

NetSession Interface: Akamai's client-side software used in conjunction with various Akamai Services. The NetSession Interface is provided subject to the terms of the applicable license agreement located at www.akamai.com/product/licenses, and Customer's purchase and use of the NetSession Interface constitutes Customer's acceptance of the terms of such license.

NetSession Interface Software Development Kit: An API, sample applications, and documentation that enables Customer to programmatically access features and functions of the NetSession Interface. This kit supports the C programming language. and is subject to the applicable licenses included therewith.

Optimized Mobile Page: Delivery of a file by Akamai that (1) represents the primary container for Customer's requested web page; (2) has been optimized by the Akamai Content Adaptation Engine; and (3) has one of the following content type: text/html, text/plain, application/xhtml+xml, text/xhtml, text/xml, application/xml, excluding redirects (HTTP response code 301/302) and File Not Found error page (HTTP response code 404). Akamai aggregates the number of these files delivered each month.

Output Minutes: Unit of measure used by Video On-Demand Transcoding (VODT). Videos output from this system are rounded up to the next whole second. All videos transcoded in a given billing period will be added together in seconds and then rounded to the next whole minute. In the case of multiple bitrate encoding (MBR), the number of output seconds can be determined by multiplying the length of the source video in seconds by the number of renditions created for the MBR set for each source video, and then the total is rounded up to the next minute.

Page View: The delivery of a file by Akamai that has Content Type "text/html" but excludes redirects (HTTP response code 301/302) and File Not Found error page (HTTP response code 404). Akamai aggregates the number of "text/html" files delivered each month.

PB: petabyte(s). One PB is equal to 1,000 TB.

PCI Standard: Payment Card Industry Data Security Standard, the current version of which can be found at: https://www.pcisecuritystandards.org/).

Peak Usage: the peak Mbps traffic on the Akamai network at any given time.

Play Attempt: An attempt to run a live or on demand stream on a media player. A single Play Attempt may result in successful play back that lasts many hours or the stream may not start at all due to errors or user initiated termination of play back. The number of Play Attempts will be tracked via the "Play Attempts" metric in the Media Analytics Service. Total Play Attempts for a month are calculated by summing the Play Attempts metric across all active instances of Audience Analytics, QoS Monitor, and Server Side Analytics modules. Bitrate switching during adaptive bitrate streaming does not constitute a new Plays Attempt. For 24x7 streams or playlists that have multiple titles in a single stream, each new title accessed within the playlist will constitute a new Play Attempt.

Priority Level: The following is a guide for assigning appropriate priority levels for Support Requests:

Priority Level	Impact	Description
Priority 1 ("P1")	Critical	Service is significantly impaired and unavailable to multiple user locations. Example: Multiple Sites are affected.
Priority 2 ("P2")	Major	Repeatable inability to use the applicable Service from a single location or region. Example: Localized denial of service issue. This might be to a single Site or even a single server.
Priority 3 ("P3")	Low	Non-urgent matter or information request. Examples: Planned configuration change request, information requests, reports or usage questions, clarification of documentation, or any feature enhancement suggestions.

Product Support: the provision of telephone or web-based technical assistance by Akamai to Customer's technical contact(s) with respect to Errors related to the corresponding products and features licensed for use on the Akamai network by the Customer. The available variants of Product Support are: Standard Support, Priority Support, Enhanced Support SLA and Premium Support. Product Support is provided in accordance with the service descriptions and service levels included in http://www.akamai.com/service for each of these variants.

Product Support does not include assistance related to errors encountered under the use of Akamai products for any purpose not stated in the service description or features of the supported products licensed by the Customer. For example, Product Support for Akamai's performance or media products does not include Akamai Support or Professional Services assistance related to the use of the Akamai network features to defend against volumetric, or application layer attacks.

Product Support for Akamai Kona Products: is provided in accordance with the service descriptions and service levels included in http://www.akamai.com/service under each of the Akamai Support Service levels (Standard Support, Priority Support, Enhanced Support SLA & Premium Support.)

Under Product Support for Akamai Kona Products, Akamai's security analysts will perform an analysis of a Security Event. Whether or not a Security Event is considered a Security Incident is determined solely by Akamai. Identified events will be classified, prioritized, and escalated as Akamai deems appropriate.

Security Incidents are classified into one of the three priority levels described below:

Priority Level: The following is a guide for assigning appropriate priority levels for Kona Site Defender Support Requests:

Priority Level	Impact	Description
Priority 1 ("P1")	Critical	This class exhibits: a) loss or outage on any portion of a Kona protected property, b) data breach (exfiltration or infiltration) confirmed in progress, or c) defacement of a protected property.
Priority 2 ("P2")	Major	This class exhibits: a) degradation in performance on any portion of a Kona protected property, b) suspected data breach, or c) excessive bot activity that may lead to intellectual property compromise.
Priority 3 ("P3")	Low	This class exhibits: a) signs of a potential small-scale security incident (log event evidence of malicious traffic that does not impact the origin and may be false positive, b) is a proactive action; "heightened attention" in response to a public threat, for instance, c) includes a possible fraud investigation without immediate evidence of data breach, or d) low-level site scraping activity.

Product Support for Akamai Kona Products Includes:

- Support for product Errors encountered by the Customer
- Initial response and acknowledgement of Security Events identified and reported to Akamai Customer Care by the Customer
- Verification that a Security Event is indeed the result of a third party attack that is taking place (declare a Security Incident)
- Customer is responsible for making changes to their Kona configuration via available mechanisms
- Customer assistance related to solving customer problems with basic use of Kona products for Remedial Mitigation of the known active attack vectors via Luna Control Center
- CCare assistance and initial instruction is limited to up to:
    - Two (2) hours per Security Event for Customers with Standard Support, Priority Support or Enhanced Support SLA Support—no more than 25 hours total in any given year.
    - Six (6) hours per Security Event for Customers with Premium Support. -- no more than 150 hours total in any given year.
- For assistance beyond these limits, Akamai Professional Services would need to be engaged at additional cost.

Product Support for Kona Products does not include:

- Ongoing monitoring of Security Monitor or Alerts by Akamai
- Monitoring of Customer bridge calls by Akamai
- Professional Services required to identify or assess attack vectors, conduct attack response planning, provide Configuration Assistance, or custom rule development.

Real-Time Reporting (RTR): An Akamai proprietary log delivery technology used for intercommunication with customer-operated log management systems.

Remedial Mitigation: the use of any standard mitigation tactic against known attack vectors

Request: a request to an Akamai server to retrieve an item of anonymous non-personally identifiable user data from an Akamai proprietary database or to perform a certain function based upon one or more Segments specified by Customer.

Secure Web Transaction: An SSL Network HTTPS request and response that may carry Card Information.

Security Event: any event causing suspicion of an actual or anticipated application level or denial of service attack.

Security Incident: any Security Event which has been reasonably confirmed by Akamai CCare services to be an actual attack against a Customer's Digital Property.

Segment: a characteristic selected by Customer and assigned to an anonymous user based upon such user's online activity.

Service Level Agreements or SLA: Use of any Service is subject to the applicable Akamai service level agreement located on the Akamai Customer Portal.

Site means a set of URLs used to deliver content and Applications for a discrete and individual corporate unit (e.g., legal entity, company business unit, publishing group, product brand or Application) that may consist of at most one domain and up to 10 hostnames. For example, in the case of www.customer.com and images.customer.com "customer.com" is the domain and "www" and "images" are hostnames.

SmoothHD: an Akamai offering that supports Microsoft Silverlight.

SSL: secure sockets layer.

SSL Network Access: A network resource allocated to Customer for the purpose of accelerating SSL sessions with a X.509 digital certificate. Customer purchases the type of digital certificate to be included with the SSL Network Access, such as Standard (Single-Hostname), Wildcard, SAN, Extended Validation (EV), Extended Validation SAN or Third Party.

Standard or Single-Hostname Digital Certificate: A X.509 digital certificate identifying a single hostname that is issued by either Akamai or an Akamai-chosen certificate authority.

Strict IP Whitelist: A configuration option within the Web Application Firewall ("WAF") network-layer controls in which requests are processed solely for the IP addresses within the IP Whitelist, whereas requests from all other IP addresses are explicitly denied a connection to an Akamai edge server.

Subject Alternative Name (SAN) Digital Certificate: A X.509 digital certificate standard that can be used to identify more than one entity or device. Digital certificate products identified as SAN Digital Certificates can sign more than one hostname.

Support Requests: Service support calls or online support tickets initiated by Customer where the underlying issue is determined to reside in Customer's host environment (not in the Akamai Services or Akamai network) or other requests outside the scope of support. Additional Support Requests beyond those included in a particular Service package may be subject to Akamai's standard rates.

TB: terabytes delivered. One (1) TB is equal to 1,000 GB.

Third Party: an entity or person other than Akamai or Customer.

Third Party Component: any solution, application, technology or component thereof provided by a 3rd Party.

Third Party Digital Certificate: A X.509 digital certificate furnished by the customer to Akamai for use with the purchased Service(s).

Thps: thousand Hits per second.

TPV: thousand Page Views.

Universal Streaming: an Akamai offering that supports HDS and HLS.

Wildcard Digital Certificate: A X.509 digital certificate that signs multiple hostnames within a specified domain. For example, the wildcard *.example.com specifies the domain "example.com" and can sign hostnames such as "www.example.com" and "images.example.com". Wildcard Digital Certificates are issued by either Akamai or an Akamai-chosen certificate authority. In cases where Akamai issues the wildcard certificate there is a 10 hostname limit under the primary domain. Otherwise, Wildcard Digital Certificates can sign an unlimited quantity of hostnames in the specified domain.

GENERAL SERVICE INFORMATION

Provides general Service-related information applicable to purchase and use of Akamai's offerings.

Akamai Network Data: As between Akamai and Customer, Akamai retains all right, title and interest worldwide in the Akamai Services and all models, reports, analyses, statistics, databases and other information created, compiled, analyzed, generated or derived by Akamai in connection with delivery of the Akamai Services and the operation of Akamai's network (collectively, "Akamai Network Data"), regardless of the media in which such Akamai Network Data is embodied, now or in the future. Akamai Network Data may be created, compiled, analyzed, generated or derived from (a) aggregated network utilization and performance data generated and collected via the operation of Akamai's network and/or in connection with the delivery of Akamai Services to Customer, (b) anonymous and non-personally identifiable user data collected by Akamai from Customer's Site(s) solely with and to the extent of the written consent of Customer, and (c) Akamai's proprietary information, software, code, technology and other intellectual property.

Customer Portal: Upon execution of the initial Transaction Document, Customer shall be provided access to the Customer Portal where a variety of billing, reporting and SLA information is available.

Data Collection Limitations: The data collection for Customer's reports has a limit on the amount of information collected per Transaction Document per day. The limits vary across the reports and are subject to change. Information about the data collection limits can be found at the Akamai Customer Portal.

Default Protocols and Configurations: For certain Services, Akamai may from time to time recommend the use of certain protocols, configurations or security parameters. Customers shall bear the risk associated with decision by it not to follow, or to modify or disable, such default protocols and configurations.

Streaming Limitations during Force Majeure: Akamai reserves the right to limit Customer's use of the Akamai streaming network in excess of Customer's committed usage in the event that force majeure events, such as war, natural disaster or terrorist attack, result in extraordinary levels of traffic on Akamai's network.

BILLING

This section provides certain information regarding Akamai's billing methodology, as well as certain usage requirements and general Service-related information applicable to the purchase and use of Akamai's offerings. Common usage-based billing methodologies include the following:

- **Active NetSession Instance**: an Akamai NetSession Interface that has downloaded Customer content from other clients or from HTTP sources over a defined period.
- **Certified Download –** a download where Akamai NetSession Interface retrieved all bytes of the object and validated every byte against a secure hash of the object**.**
- **CPU Milliseconds:** Where central processing unit ("CPU") millisecond measurements are involved, such measurements are normalized for Akamai's standard CPU processing power.
- **DNS Traffic:** Unless otherwise indicated, all traffic to Akamai DNS servers in excess of 50 Mbps as measured by Akamai will be billed at $.02 per MB.
- **Invoicing:** One-time fees are billed in advance on the applicable Billing Effective Date. Monthly recurring fees are billed each calendar month in advance starting on the applicable Billing Effective Date. For the avoidance of doubt, the Term on the applicable Transaction Document begins on the Billing Effective Date. Overage and similar fees are billed monthly in arrears. If the overage rate is not outlined on the order form, activation form, or other Transaction Document, then the usage rate set forth therein shall also apply as the overage rate. Selecting multiple Services may in certain circumstances result in Customers receiving multiple invoices. All components of the Services are accepted and billed on a per installation basis; billing will commence upon delivery of the Service for each component thereof.
- **Per Digital Property:** Unless otherwise indicated, all fees reflected on an Order Form are per Digital Property.
- **Regional Traffic Measurements:** Akamai reserves the right to measure 95/5 on a per region basis if Customer's usage exceeds 20 Mbps.
- **Superbursting Charges:** Unless otherwise indicated, for all Services billed based in Mbps, Gbps or any other bit per second methodology, an additional charge of $.02/MB, or an alternative amount stated in the applicable local currency, will be applied to the sum of MBs in excess of two times the commitment, to the extent such usage is in the top 5% of 5 minute intervals.
- **SureRoute (Route Optimization Midgress):** If the SureRoute Service is enabled, Midgress Traffic will be generated. Midgress Traffic in the form of Mbps or GB will be billed in addition to other usage traffic at the usage rate set forth on the order form. Note: For Dynamic Site Accelerator Services, midgress page view traffic is not billed.
- **Tiered Distribution (Cache Hierarchy Midgress):** If Tiered Distribution is enabled, Midgress Traffic will be generated. Midgress Traffic will be billed in addition to other usage traffic at the usage rate set forth on the applicable Order Form.
- **Usage:** Unless otherwise indicated, Services indicated as being measured on the basis of Mbps, Gbps or any other bit per second methodology, as well as NetStorage, are billed on a 95/5 basis. Other usage is based on total use or the uncompressed equivalent as measured by Akamai, commonly reflected in MB, GB or TB or, in the case of Services based on pages viewed, Page View or MPV or, in the case of Services based on Hits or million Hits, and in the case of Services that are based on Requests, the number of Requests made as indicated in the relevant agreement.

SERVICE DESCRIPTIONS AND ADDITIONAL TERMS

Provides brief descriptions of what is included in certain Akamai offerings. Detailed Service descriptions, including system requirements and configuration guidelines for all Akamai products and Services, can be found in the configuration guide for the applicable offering, available from your Akamai representative.

Access Control: Includes access to specific metadata tags providing additional security controls governing how users connect to the Akamai infrastructure, and how the Akamai infrastructure connects to Customer's origin server(s). These metadata tags are grouped into the following categories: edge authorization, edge to origin authorization, enhanced availability, caching controls, security related controls. The majority of the Access Control metadata tags are configurable solely by Akamai, however, some of the available tags can be selected and implemented by Customer directly.

Adaptive Image Compression: Adaptive Image Compression is designed to detect the current network conditions between a client request for a JPEG image from an Akamai Edge server, and may dynamically re-compress the image file according to Customer configured levels, reducing file size and assisting in faster transmission of the image file. Customer agrees to abide by all copyright, trademark, and other intellectual property laws worldwide in connection with the use of Adaptive Image Compression. Customer hereby grants permission and license, where applicable, for Akamai to copy, alter, modify, resize, crop, watermark, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise make derivative versions of images for which the Adaptive Image Compression module is activated, including intermediary graphical stages which may be cached internally in image server software in addition to customary object caching at Edge servers. Customer acknowledges that due to capacity and network deployment constraints, the Adaptive Image Compression functionality may not have a positive impact on performance.

Advanced Cache Optimization (or Control): Includes access to optimization features that help in improving the cacheability of complex content on Akamai edge servers.

Akamai Cloud Catalyst: Akamai Cloud Catalyst provides Customers that are IaaS Storage, IaaS Compute and/or PaaS providers with the ability to provide Akamai content delivery (CDN) capabilities to their end-users as part of Customer's cloud services/product offerings. For example, an end-user who signs up for cloud storage with Customer and wants Akamai CDN benefits could also purchase "CDN services" when purchasing other cloud services/products from Customer. Cloud Catalyst allows Customer to then provide that end-user with CNAME instructions to point to a target domain that resolves to Akamai and receives Akamai CDN services. These CDN services are preconfigured by Akamai, and can be used by any of the Customer's end-users by simply following a pre-defined CNAMEing pattern to turn on access with no additional configuration required.

Akamai® DDoS Defender ("DDoS Defender"): Designed to reduce the potential likelihood and impact of many common types of DDoS Attacks by absorbing some DDoS traffic, deflecting attacks, and authenticating valid traffic at the network edge. The DDoS Defender Service includes pre-provisioning and configuration of key functionality through metadata and support services to respond to many types of DDoS events by applying security response mechanisms and standard operating procedures specifically designed to identify and remediate DDoS Attacks, and providing protection from burst charges associated with unexpected or malicious traffic spikes. DDoS Defender is managed by Akamai Global Services and Support, and includes no customer self-service capabilities. DDoS Defender includes DDoS Fee Protection.

Additional DDoS Defender Terms:

- Customer acknowledges and agrees that DDoS Defender does not prevent or eliminate all DDoS Attacks.
- DDoS Defender requires the purchase of DSA, DSD, RMA, and/or WAA Services.
- Customer is required to provide Akamai the URL(s) and/or domain(s) to be covered by DDoS Defender. The Customer Sites covered by DDoS Defender shall be limited as outlined in the Agreement.
- DDOS Defender services are delivered in English only.
- Customer agrees to provide an escalation matrix including a minimum of three contacts that Akamai may need to reach during suspected DDoS Attacks. Contact information must include name, email address and mobile phone information.
- Customer agrees that Akamai will capture AkaID and other relevant data.
- Akamai is not responsible for any Customer action that might result in DoS, availability issues or performance degradation
- Akamai reserves the right to charge Customer for usage fees associated with traffic bursts or increased usage resulting from Customer actions.

- Any requests that are not directly related to Customer's use of the Akamai platform or extended use thereof, and are not related to the preparation or mitigation of malicious DDoS Attacks, shall be considered out the scope of this Service.

Akamai Identity Services ("AIS"): AIS Services are designed to integrate certain end user information into Customer's content (website, player, etc.) by using an authentication and authorization layer. The AIS standard authentication and authorization layer provides Customer an interface to use with multiple Identity Providers. In addition, AIS provides an anonymous "cloud identity" through tokenization based on attributes provided by Customer's Identity Provider(s). AIS does not do direct authentication or store usernames/passwords of end users and only stores anonymous attributes of end user identity provided by Customer's Identity Provider(s). Customer shall not provide Akamai with personally identifiable information and shall not use AIS data to track end users across non-Customer owned Sites.

Akamai Media Delivery: Includes access to Akamai's network for content delivery for one or more of the following products: On-Demand Streaming (in one or more of the following formats: Adobe® Flash®, Microsoft Windows® Media, or Apple QuickTime®), Live Streaming (in one or more of the following formats: Adobe Flash, Microsoft Windows Media, Apple QuickTime), HTTP Downloads, AdaptiveEdge Streaming for Microsoft Silverlight or Progressive Media Downloads.

> **Additional Akamai Media Delivery Terms**: Files served using the HTTP Downloads Service must be 100 KB or larger. Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput. Akamai reserves the right to make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the Service resulting from its failure to comply with the requested changes. Akamai may, at its sole discretion, utilize the Akamai NetSession Interface to provide a portion of the delivery Services to Customer.

Akamai Media Player – Flash: Akamai software used to enable delivery of streaming and progressive download content in various formats. Unless otherwise specified all components of the Akamai Media Player are delivered in binary format without source code. Branding, customization and configuration of the Akamai Media Player is limited to what is available using FlashVars, the XML Configuration file, and the JavaScript API. The use of the Akamai Media Player for Flash requires the use of one or more of the Akamai delivery services for Flash (On-Demand Streaming for Flash, Live Streaming for Flash, On-Demand Streaming for HD Flash, Live Streaming for HD Flash, or Progressive Downloads). The Akamai Media Player is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer's purchase and use of the Akamai Media Player constitutes Customer's acceptance of the terms of such license.

Akamai Mobile Accelerator: Akamai Mobile Accelerator ("AMA") is designed to accelerate content over mobile networks and to mobile devices. AMA includes access to the features of Dynamic Site Accelerator, Mobile Detection and Redirect and Akamai Mobile Protocol. Customer is required to purchase DSA or WAA in order to use AMA. Customer can also purchase AMA as a stand-alone solution that includes DSA. AMA does not accelerate non-mobile properties and does not work for software downloads.

Akamai Mobile Accelerator Secure: Includes access to the features of Akamai Mobile Accelerator and, in addition, access to Access Control, Secure Content Delivery, and provision of one of the following SSL Network Digital Certificates: Standard (single-hostname), Wildcard, SAN or Third Party.

Akamai Mobile Protocol: Includes access to certain network enhancements and transport protocol optimizations designed for mobile networks.

Aqua Ion: Includes access to Akamai's network and site acceleration services, which include one or more of the following features: pre-fetching; route optimization; or transport protocol optimization.

Aqua Ion Mobile: Aqua Ion Mobile is designed to accelerate web content to mobile devices. Aqua Ion Mobile includes access to Mobile Detection and Redirect, Akamai Mobile Protocol, Device Characterization and Adaptive Image Compression. Aqua Ion Mobile only accelerates Mobile Sites. Customer agrees that Aqua Ion Mobile shall not be used for downloads of objects with a file size greater than 20 megabytes. If Customer has purchased Aqua Ion Mobile as a stand-alone product Customer shall also get access to Dynamic Site Accelerator Premier.

Aqua Ion Mobile Secure: Includes access to the features of Aqua Ion Mobile and, in addition, access to Access Control, Secure Content Delivery, and provision of one of the following SSL Network Digital Certificates: Standard (single-hostname), Wildcard, SAN or Third Party.

Aqua Ion Secure: Includes access to the features of Aqua Ion plus access to the Access Control module, Secure Content Delivery module; and provisioning of one of the following SSL Network Access Digital Certificates – Standard (Single-hostname), Wildcard, SAN or Third Party.

Aqua Mobile: See Aqua Ion Mobile.

China CDN: System requirements and configuration guidelines can be found in the EdgeSuite Configuration Guide.

Additional Terms for China CDN. China CDN Services are provided on the same basis as the Service outlined on the applicable Transaction Document for those Services with the following additional terms. Customer understands and acknowledges that:

1. Akamai provides no guarantee or warranty that the China CDN Services shall be delivered from within China;
2. China CDN Services may be delivered from any geography that Akamai determines to be the appropriate geography for performance and availability purposes;
3. Customer shall comply with all applicable laws in China, including but not limited to any registration requirements for .cn Sites, and agrees to supply Akamai with any documentation or registration information (including origin IP addresses) reasonably requested by Akamai;
4. Akamai is not liable for any acts of a government authority or network that may prevent delivery of content from a specific geography or such authority filtering, blocking, altering, or damaging data sent by Customer over the Akamai network including use of the China CDN Services outlined in the applicable Transaction Document;
5. Customer shall not require Akamai to assist Customer with any laws, policies or regulations that apply to Customer's content implemented by a government authority;
6. Akamai shall not be liable for the disclosure of the originator of any Customer content to a government authority upon direct inquiry by such authority;
7. Akamai may deliver all or part of the China CDN Services through the use of third party suppliers; and
8. Akamai reserves the right to limit or restrict the amount of traffic purchased hereunder.

Client Access Control ("CAC") Module. Supplies a set of IP addresses to Customer that Akamai uses to serve Customer's content and also provides Customer with assistance in managing a change process for this set of IP addresses as they change over time. In addition, Customer will have access to a configuration page in the Luna Control Center to configure a secure edge hostname for Client Access Control and the delivery of the set of IP addresses for Customer through the Luna Control Center Client Access Control CIDR Lists page. Customer must acknowledge receipt of new IP addresses within 90 days of notification by Akamai. Should Customer fail to provide such acknowledgement, Akamai will continue to serve the traffic covered by the base Service offering; however Akamai shall no longer provide any commitment regarding the performance of the base Service offering or the CAC Module, and Customer expressly acknowledges and agrees that degradation of base Service offering (including performance against the applicable SLA) may occur as a result. Should Customer fail to provide acknowledgement within 180 days of notification, Akamai reserves the right to degrade Customer to a different Map and to charge Customer's then-current usage rate for a custom Map over and above the existing charges for CAC which shall continue to apply. Such new custom Map may also have degraded performance from the up-to-date IP addresses supplied by Akamai for the CAC Module. Customer acknowledges and agrees that if CAC is purchased with Session Accelerator (SXL), Customer shall no longer obtain the performance SLA in place with the base SXL Service.

Client-side Downloads ("CSD"): Includes access to the NetSession Interface Software Development Kit, which enables use of the Akamai CSD network for the HTTP Downloads Service.

Additional Terms for Client-side Downloads. CSD Services are provided on the same basis as the Service(s) outlined on the applicable Transaction Document for those Services with the following additional terms. Customer understands and acknowledges that:

1. Akamai may, at its sole discretion, utilize the Akamai NetSession Interface to provide a portion of the delivery services to Customer.
2. Akamai performs the CSD Services through the transmission and retransmissions of the content as stored on the computer systems of multiple end users and that such end users

must be prompted to download and install the Akamai NetSession Interface onto such computer systems and agree to an end user license agreement provided by Akamai.

3. The Akamai NetSession Interface is subject to U.S. export jurisdiction. Customer agrees to comply with all applicable international and national laws that apply to the Akamai NetSession Interface, including the U.S. Export Administration Regulations, as well as end-user, end-use destination restrictions issued by U.S. and other governments.

4. To ensure end users are provided adequate notice and Akamai receives end user acceptance, the following paragraph must be presented to the end user before the Akamai NetSession Interface is installed:

   "The <insert customer application name> uses the Akamai NetSession Interface, which may utilize a limited amount of your upload bandwidth and PC resources to connect you to a peered network and improve speed and reliability of Web content. The Akamai NetSession Interface is secure client-side networking technology that harnesses the power of your computer to deliver software and media available on the Akamai network. Your Akamai NetSession Interface works collectively with other Akamai NetSession Interfaces, along with thousands of Akamai edge servers, and runs as a networking service utilizing a limited amount of your computer's available resources. More information about the Akamai NetSession Interface is available here: http://www.akamai.com/client. By clicking "Accept" you accept the Akamai License Agreement."

   Customer agrees to include a hyperlink to http://www.akamai.com/eula with the text "Akamai License Agreement". When the end user accepts the Akamai License Agreement, Customer application must make an API call to NetSession to indicate end user acceptance of the Akamai License Agreement, allowing NetSession to begin serving content from the Akamai network. Customer agrees that it shall not send any API call to NetSession that is not preceded by an "Accept" click to the paragraph above.

Compliance Management: A collection of documentation and tools designed to assist Customer in understanding how Akamai Services relate to its own compliance initiatives through supporting documentation of Akamai policies and procedures mapped to sections of specific compliance frameworks. Customer may select one or more framework modules to help support relevant compliance initiatives (a minimum of one framework module is required). Available framework modules are:

a. Compliance Management – PCI Compliance

- Akamai shall undertake an annual audit in accordance with the PCI Standard for purposes of ongoing information security compliance verification.
- Akamai will provide an SSL network designed to be compliant with the current PCI Standard(s) (the "Akamai SSL network" or the "Akamai Secure Content Delivery Network"). In the event the PCI Standard is updated, Akamai's Compliance Management - PCI Compliance will be updated within twelve (12) months of the last applicable date of the older PCI Standard.
- Akamai shall make available to Customer upon request:
  - A copy of the Report on Compliance Acceptance Letter issued to Akamai upon completion of its most recent PCI audit; and
  - An executive summary of recent quarterly network vulnerability scans performed on the Akamai SSL network.
- Akamai will provide a level of security against unauthorized access to, and/or use of Cardholder Data equal to or greater than that required by the PCI Standard. For purposes of this section, "Cardholder Data" means the numbers assigned by card issuers to identify cardholders' accounts and data about card transactions placed by Customer's end-users on the Akamai SSL network.
- Customer shall only use Akamai Services to transmit Cardholder Data in a secure fashion in accordance with the PCI Standard.
- Customer agrees to configure and maintain its Akamai metadata to use encryption algorithms, key lengths, and other applicable metadata that are consistent with the PCI Standard.
- Customer shall configure and maintain its Akamai metadata so as not to cache nor store and Cardholder Data via Akamai NetStorage.
- Customer agrees that, in using Akamai Services, it will only transmit Cardholder Data over the Akamai SSL network and via no other Akamai network.
- Customer will not provide Akamai with Cardholder Data outside of the use of the Akamai SSL network, whether through urls, cookies, logging, queries or any other means.

- Neither Akamai nor Customer shall perform network scanning or penetration or similar testing on the other's environment.
- Customer shall have access to end-user session logs through the use of the Akamai Log Delivery Service. Akamai shall not be required to maintain an independent historical record of these end-user session logs.
- In the event of a Cardholder Data compromise, both Customer and Akamai shall provide commercially reasonable support to the other in connection with any investigations into such compromise.

b. Compliance Management – ISO

- Akamai shall undertake an annual self-assessment against the security section of the ISO standard ISO 27002.
- Akamai's Compliance Management – The ISO Compliance Management Module will be updated within twelve (12) months of the applicable date of revisions to the ISO Standard.
- The ISO assessment yields reports against the deployed networks that transmit customer data as well as on Akamai Technologies as a whole to gauge Akamai's internal processes and policies. The ISO Compliance Management module includes:
    - An executive summary report from the most recent assessment; and
    - Selected documentation on Akamai policies and procedures reviewed as part of the most recent assessment.

Definition: ISO 27002 is a set of guidelines regarding security (as compared to the ISO 27001 standard). Assessment against ISO 27002 is not an assessment of the effectiveness of any processes, only verification that such policies exist, are well documented, clearly communicated, and universally followed.

c. Compliance Management – FISMA

- Akamai's Compliance Management – FISMA Compliance Management Module will be updated within twelve (12) months of the applicable date of the update to NIST 800-53.
- The FISMA Compliance Management module includes:
    - Documentation on Akamai policies and procedures reviewed as part of the FISMA self-assessment effort against NIST 800-53.
- Definition: FISMA is the act of Congress that established the requirements for each federal agency to have a comprehensive system for managing security of information and information systems including those provided or managed by another agency, contractor, or other source. The National Institute of Standards and Technology (NIST) maintains the role of developing information security standards (Federal Information Processing Standards) and guidelines (Special Publications in the 800-series), including NIST Special Publication 800-53, "*Recommended Security Controls for Federal Information Systems".*

d. BITS Compliance Management

- "BITS" is a division of The Financial Services Roundtable <http://www.fsround.org>, and a not-for-profit industry consortium whose members are 100 of the largest financial institutions in the United States.
- Akamai's Compliance Management – BITS Compliance Management Module will be updated within twelve (12) months of the applicable date of the update to the BITS standard.
- The BITS Compliance Management module includes:
    - Documentation on Akamai policies and procedures reviewed as part of the BITS self-assessment effort.

e. HIPAA Compliance Management

- Akamai shall undertake an annual audit for the purposes of ongoing verification of HIPAA compliance for its SSL network.
- Akamai will provide an SSL network designed to be compliant with the current HIPAA standards. In the event that the HIPAA standard is updated, Akamai's Compliance Management – HIPAA Compliance will be updated within 12 months of the last applicable date of the older HIPAA standard.

- Neither Akamai nor Customer shall perform network scanning or penetration or similar testing on the other's environment
- Customer shall have access to end-user session logs through the use of the Akamai Log Delivery Service. Akamai shall not be required to maintain an independent historical record of these end-user session logs.
- In the event of a Protected Health Information (PHI) compromise, both Customer and Akamai shall provide commercially reasonable support to the other in connection with any investigations into such compromise.

For a breach of any of the following limitations, Customer shall indemnify and hold Akamai harmless from any claims or damages Customer or Akamai may incur as a result of Customer's breach of the requirements below:

- Customer agrees to configure and maintain its Akamai metadata to use encryption algorithms, key lengths and other applicable metadata that are consistent with HIPAA.
- Customer agrees to configure and maintain its Akamai metadata so as not to cache nor store PHI on Netstorage.
- Customer agrees to configure and maintain its Akamai metadata as not to process PHI in EdgeComputing Applications.
- Customer agrees that, in using Akamai Services, it will only transmit PHI over the Akamai SSL network and via no other Akamai network.
- Customer will not provide Akamai with PHI outside of the use of the Akamai SSL network, whether through URLs, cookies, logging, queries or any other means.
- Customer will indemnify Akamai for any configuration changes required or approved by the Customer.

Customer's use of Compliance Management Services and accompanying framework modules do not guarantee Customer's compliance with any compliance standard. Such determination can only be made directly between Customer and its applicable compliance auditors.

On-Site Audit Compliance Management: An engagement specific to a single compliance framework module, delivered by Akamai's Information Security ("InfoSec") team. The On-Site Audit Compliance Management Service will be delivered by the InfoSec team at Akamai's corporate offices in Cambridge, Massachusetts over a period of up to five (5) consecutive business days and will provide a deeper review of Akamai's policies and procedures relative to the Customer's deployed Akamai Services.

Content Targeting: Includes access to specific metadata tags providing IP based information of end users connecting to the Akamai network. With the Content Targeting module, the following attributes can be identified based on IP: country code, region code, network code, network type, device type, city, marketing area, metropolitan statistical area, primary metropolitan statistical area, area code, latitude, longitude, country, time zone, zip code, and connection speed.

DDoS Fee Protection: The DDoS Fee Protection module provides Customer with a credit for overage fees incurred due to a DDoS Attack. For eligible requests, Customer's overage fees for the month in which the DDoS occurred are reversed and replaced with the "Capped Burst Fee" value set forth on the applicable Transaction Document (unless actual overage fees are less than the Capped Burst Fee amount in which case the actual overage fees will apply). The DDoS Fee Protection module is only available with the APS Enterprise, Dynamic Site Accelerator Enterprise, Dynamic Site Accelerator Offload, Dynamic Site Accelerator Secure Offload, Dynamic Site Accelerator Secure, Dynamic Site Accelerator Standard, Dynamic Site Delivery, Rich Media Accelerator Enterprise, Rich Media Accelerator, Rich Media Accelerator: Infrastructure Offload Edition, and Web Application Accelerator Services, and requires that Customer also purchase the Web Application Firewall and/or DDOS Defender Service. For the avoidance of doubt, the DDoS Fee Protection module cannot be offered to customers who receive consolidated invoices aggregating usage from more than one Service and/or Transaction Document. In addition, by electing to purchase the DDoS Fee Protection module, Customer (i) authorizes Akamai to impose technical measures available in the Akamai Services that control and/or mitigate a DDoS Attack, even if such measures result in degraded application and/or site performance, and (ii) acknowledges that Service Level Agreements do not apply during the period of a DDoS Attack.

Additional DDoS Fee Protection Terms: To be eligible for a credit (a) the DDoS Attack must result in overage charges in excess of twice the average monthly overage fee measured in the preceding six months, and excluding months in which a mutually agreed DDoS Attack occurred, (b) Customer must notify Akamai's CCare organization of a DDoS Attack, (c) Akamai's CCare organization must verify reported DDoS Attack is a legitimate Attack eligible for credit, and (d) the credit requests must be submitted no later than 30 days following a disputed Service invoice. When issuing a credit Akamai shall have sole authority in determining whether the reported Service incident qualifies for credit. If Customer's average monthly Service fee exceeds their selected tier or if more than two credits are requested in any given calendar year, then Akamai shall have the right to require Customer to pay a higher Capped Burst Fee. A single credit shall be applied on a monthly basis, even when multiple Attacks occur in the month. Credit shall be issued as a credit memo and not a revised invoice.

Device Characterization: Device Characterization provides Customer access to the Customer Portal to activate cache key augmentation and HTTP header augmentation with characteristics drawn from a database of mobile devices. The matching mechanism to identify mobile devices at the edge, and the database of related characteristics, is defined and updated periodically by Akamai, at Akamai's sole and reasonable discretion, and Customer agrees that there are no guarantees around specific device inclusion in such mechanisms or data accuracy or breadth in the database. Customer is prohibited from accruing any device data added by Akamai to HTTP headers except in logs for Customer's internal analysis and debugging purposes. Customer is prohibited from publishing any device data added by Akamai to HTTP headers. Akamai may, without notice, make substantial and fundamental changes to the Device Characterization module that affect the handling of web traffic to Customer's digital properties, including but not limited to changes to the database, including addition and removal of devices and characteristic fields, changes to the data or relevant interpretation of the data.

Download Manager ("DLM"): Connects Customer to the Akamai network and is designed to improve download speed, availability and file integrity, and help manage download workflow tasks. The DLM module provides access to two download manager implementations: (i) browser plug-in - an ActiveX control or java applet browser plug-in, subject to the applicable license agreement located at www.akamai.com/product/licenses, designed to improve download speed, availability and file integrity, and help manage download workflow tasks, and (ii) installed application that provides access to the DLM features provided by the NetSession Interface. The installed application allows access to the JavaScript user-interface library for programmatically controlling the NetSession Interface from a browser. The JavaScript application is subject to the applicable license agreement located at www.akamai.com/product/licenses.

DLM to DLM Traffic: Enables access to all features available in, and is subject to the terms for, the "Client-side Downloads" Service as outlined hereinabove.

Downloads Analytics: Includes Customer Portal access credentials to Akamai's analytics platform for downloads, with support for server side data sources, and optionally client-side data sources, as selected by Customer. Server-side data sources utilize log data generated by Akamai's HTTP Downloads Delivery Service. If the optional client-side data sources are selected by Customer, then client-side data sources will utilize data delivered to Download Analytics from Akamai's NetSession Interface.

Dynamic Content Assembly ("DCA"): Includes access to the following page assembly features available at the Akamai edge server: "Include", "Conditional Logic" and "Error and Exception Handling", as outlined in the ESI 1.0 specification document. Any functionality beyond page assembly and the pre-outlined features identified above will require the purchase of the EdgeComputing solution.

Dynamic Page Caching: Includes access to a rules engine that enables granular caching, segmentation and downstream policies for content based on request criteria such as name/value pairs found in cookies, request headers, and query-strings.

Dynamic Site Accelerator ("DSA"): includes access to Akamai's network for content delivery and access to Akamai's Site acceleration Services, which include one or more of the following features: pre-fetching; route optimization; or transport protocol optimization. DSA is to be used for web sites only, not for web applications.

Dynamic Site Accelerator – Premier ("DSA Premier"): Includes access to the features of the DSA Service, plus Advanced Cache Optimization, Enhanced Akamai Protocol, Dynamic Page Caching modules, object pre-fetching, page pre-fetching and content delivery using IPv6.

Shopper Prioritization Module: includes access to Akamai's Shopper Prioritization functionality that provides the ability to control traffic to customer's origin server by redirecting users selectively to a pre-configured alternate web-page (i.e., overflow site).

Dynamic Site Accelerator - Secure: Includes access to the features of Dynamic Site Accelerator plus access to the Access Control module, Secure Content Delivery module; and provisioning of one of the following SSL Network Access Digital Certificates – Standard (Single-hostname), Wildcard, SAN or Third Party.

Dynamic Site Accelerator Secure – Premier ("DSA Secure Premier"): Includes access to the features of the DSA Secure Service, plus Advanced Cache Optimization, Enhanced Akamai Protocol and Dynamic Page Caching modules.

Dynamic Site Accelerator - Enterprise: Includes access to the features of Dynamic Site Accelerator – Secure, plus access to the Advanced Cache Optimization, Site Failover, Dynamic Content Assembly and Content Targeting modules.

Billing Methodology: If monthly HTTP/HTTPS traffic delivery exceeds 200 GB delivered per MPV, Akamai will bill for overage fees at $3 per GB. Overages are based on the greater of actual or committed Page Views. Page View overages will be charged at the Additional MPV rate. Midgress Traffic is included in the GB metric, but not the MPV metric. Mbps and GB billing models are also available. Midgress Traffic is included in both of these metrics. Note 1: HTTP/HTTPS traffic includes all HTTP methods. Note 2: China CDN and China CDN Secure traffic is measured and billed separately at the usage rate set forth on the Order Form.

Site Fees: Fees are per Site. If more than 1 domain and/or 10 hostnames is required, an additional Site must be purchased.

Large File Support: With the Dynamic Site Accelerator Service, individual files cannot exceed 100 MB in size. For files that exceed 100 MB in size, please use the Electronic Software Delivery Service.

Page Views: Akamai aggregates the number of "text/html" files delivered each month in order to determine Page View count.

Dynamic Site Delivery ("DSD"): Includes access to Akamai's network for content delivery, NetStorage infrastructure and on-demand streaming networks.

Billing Methodology: If monthly HTTP traffic delivery exceeds 200 GB delivered per MPV, Akamai will bill for overage fees at $3 per GB. Overages are based on the greater of actual or committed Page Views. Page View overages will be charged at the Additional MPV rate. Midgress Traffic is included in the GB metric but not the MPV metric. Mbps and GB billing models are also available. Midgress Traffic is included in both of these metrics. Note: HTTP traffic includes all HTTP methods.

Site Fees: Fees are per Site. If more than 1 domain and/or 10 hostnames is required, an additional Site must be purchased.

Large File Support: With the Dynamic Site Delivery Service, individual files can not exceed 100 MB in size. For files that exceed 100 MB in size, please use the Electronic Software Delivery Service.

Page Views: Akamai aggregates the number of "text/html" files delivered each month in order to determine Page View count.

EdgeComputing: Includes deployment of Applications provided by Customer on the Akamai EdgeComputing platform; EdgeSessions (persistent session state); remote use of one Akamai EdgeComputing QA server for testing Applications in a simulated Akamai environment; and standard reporting. Pricing is based upon a threshold of 250 CPU milliseconds per request and a cumulative Application server memory usage threshold of 75MB as measured by Akamai. Akamai reserves the right to remove Applications from the Akamai network or charge additional fees if Customer's usage exceeds either threshold as measured by Akamai.

EdgeComputing with EdgeApplication: Includes use of EdgeComputing (subject to functionality and limitations described above), plus access to EdgeApplication(s) referenced on the EdgeApplication Schedule attached to the Order Form.

EdgeApplication Worksheet: Recurring and one-time fees are billed in advance. Overage and similar fees are billed in arrears. Akamai disclaims responsibility or liability for any Third Party Component used by Customer, or Third Party professional services provided to Customer, in

connection with EdgeComputing Services. Although Akamai may provide invoicing for a combined solution or professional services on behalf of a Third Party, Akamai itself is not providing the Third Party Component of the combined solution. All Third Party professional services and all obligations relating thereto, including support, are the responsibility of such Third Party and not Akamai. Customer agrees to look solely to such Third Party for support or other obligations relating to the Third Party Component or professional services and expressly acknowledges that its obligation to pay Akamai for the EdgeComputing component of a combined solution is independent of the performance of any Third Party Component.

Application Support: Includes troubleshooting issues related to EdgeComputing Applications.

User Prioritization Application: includes access to Akamai's User Prioritization application that provides the ability to control traffic to the origin server by redirecting users selectively to a pre-configured alternate web-page (overflow site).

EdgeConnect Cloud Monitor (ECM): ECM is a data API for monitoring activity and performance of Internet applications delivered through Akamai. Customer shall receive a single data feed and the set of data that may be viewed shall be determined by a single Customer-selected ECM data schema with a defined set of fields.

EdgeConnect Performance Metrics (ECPM): Customer must have purchased EdgeConnect Cloud Monitor to purchase ECPM. ECPM entitles Customer to access additional metrics (in addition to those data fields received in ECM). Customer shall still receive a single data feed as in ECM and the set of data that may be viewed shall be determined by a single Customer-selected ECPM data schema with a defined set of fields.

Edge Device Characterization: Edge Device Characterization provides Customer access to the Customer Portal to activate cache key augmentation and HTTP header augmentation with characteristics drawn from a database of mobile devices. The matching mechanism to identify mobile devices at the edge, and the database of related characteristics, is defined and updated periodically by Akamai, at Akamai's sole and reasonable discretion, and Customer agrees that there are no guarantees around specific device inclusion in such mechanisms or data accuracy or breadth in the database. Customer is prohibited from accruing any device data added by Akamai to HTTP headers except in logs for Customer's internal analysis and debugging purposes. Customer is prohibited from publishing any device data added by Akamai to HTTP headers. Akamai may, without notice, make substantial and fundamental changes to the Edge Device Characterization module that affect the handling of web traffic to Customer's digital properties, including but not limited to changes to the database, including the addition and removal of devices and characteristic fields, changes to the data or relevant interpretation of the data.

Edge Media Buying ("EMB"): Includes access to Akamai's acceleration Services (which include one or more of the following features: pre-fetching; route optimization; and/or transport protocol optimization) for the limited purpose of enabling Akamai to order and/or purchase media inventory from Customer. The limitations and restrictions on use for the EMB Service shall be set forth on the applicable Transaction Document.

EdgeScape: Akamai shall provide to Customer access to its EdgeScape Database of information identifying the geographic and network point-of-origin of Site requests.

Additional Definitions and Terms for EdgeScape:
"Database" means the proprietary database, and all information included therein, compiled by Akamai and currently used by Akamai to provide Site content providers with the Identification Code for assigned, route-able addresses in the commercial IP space. "Identification Code" means the information provided by the Database for each Site request, including, but not limited to identifying the geographic and network point-of-origin of such request. More specifically, the Database shall provide the following information: country code, region code (US state/non-AOL only and province (Canada only)) and network and connection type for certain networks (as selected by Akamai)). Customer's use of the Services are subject to the following restrictions: Customer shall not (i) integrate both the Identification Code(s) and the IP address obtained from the Database with any of its databases; or (ii) use the Services to provide a managed identification service that competes with Akamai's EdgeScape Service or (iii) provide both the Identification Code(s) and the IP address to a third party. As between Akamai and Customer, Akamai retains all right, title and interest worldwide in the Database, regardless of the media in which the Database is embodied, now or in the future. Customer agrees that it does not have any ownership or other proprietary rights of any kind, express or implied, in the Database, other than

access to the information contained therein as part of the Services. Customer agrees not to dispute any of Akamai's ownership rights in the Database.

EdgeSuite Delivery: Includes access to Akamai's network for delivery of content. Unless otherwise indicated, charges for EdgeSuite Delivery are based on usage, measured in Mbps or actual usage, as indicated on the Order Form.

EdgeSuite Enterprise: Includes access to Akamai's network for delivery of content and Secure Content Delivery (1 Standard Certificate); and SureRoute (1 Map).

Edge Tokenization Module: Includes access to Akamai's edge tokenization functionality that provides a way to replace Card Information with a token provided by Customer's third party payment gateway partner supported by Akamai (as used herein, the "Payment Gateway Partner") as part of a Secure Web Transaction, typically for a shopping or account access operation. The Payment Gateway Partner will provide the token generation and credit card storage services, and Akamai shall not be responsible for the delivery of such services. The Edge Tokenization Module intercepts Secure Web Transactions which include Card Information, securely forwards the Card Information to the Payment Gateway Partner via Akamai's SSL Network, obtains the token from the Payment Gateway Partner and replaces the Card Information with the token, which shall be provided to Customer.

Edge Tokenization Limitations and Requirements:

1. The Edge Tokenization Module is restricted to replacing Card Information for only those Secure Web Transactions that are identified via a URL, web page or other means in the applicable Edge Tokenization Module configuration.
2. Akamai shall only work directly with the applicable Payment Gateway Partner and/or disclose relevant Cardholder Data of user's to the Payment Gateway Partner on behalf of and for the benefit of the Customer and/or the applicable user and/or as necessary to provide the Services.
3. Customer shall provide Akamai with account credentials for the payment processor and/or payment gateway that are limited to permissions for validation of Card Information and token creation only and that do not allow Akamai to view, modify, or retrieve Card Information via API or other method once the Card Information has been converted into a token.
4. Customer shall configure and maintain its Akamai metadata so as not to cache nor store any Card Information via Akamai NetStorage.
5. Customer agrees that, in using Services, it will only transmit Card Information over the Akamai SSL network via no other Akamai network.
6. Customer will not provide Akamai with Card Information outside the use of the Akamai SSL network, whether through urls, cookies, logging, queries or any other means.
7. The Edge Tokenization Module is only available in conjunction with Customer's use of Akamai's Dynamic Site Accelerator, Dynamic Site Delivery, Rich Media Accelerator and Web Application Accelerator Services.
8. The Edge Tokenization Module does not provide any functionality for Customer's self-service configuration and reporting on the Customer Portal.
9. Use of the Edge Tokenization Module does not guarantee compliance with the PCI Standard. Such determination can only be made directly between Customer and its applicable compliance auditors.
10. Akamai expressly disclaims all representations and warranties regarding any Payment Gateway Partner's services, including, without limitation, whether such services comply with the PCI Standard or other security standards. Akamai shall have no liability for any breach or unauthorized access to or use of Customer data resulting from the Payment Gateway Partner's services or software.

EdgeView Powered by BMC Software ("EdgeView"): EdgeView provides performance monitoring and reporting for Sites and Applications accelerated by Akamai Services. EdgeView provides web performance measurements and end-to-end transaction times as perceived by actual end users. EdgeView enables comparison of Site and Application performance before and after using the Akamai Services and also provides information that may be used in the analysis of non-accelerated Sites and Applications to determine if Akamai Services may provide a more optimal end-user experience. EdgeView is delivered as a software-based virtual appliance using VMware's Open Virtualization Format deployed on-premise at the Site or Application origin along with Java scripts inserted into monitored pages. The EdgeView module includes (i) access to a BMC Software portal where real-time interactive dashboards and live reports display the performance impact of the Akamai Services, and (ii) one (1) license and support for up to twenty (20) precise segments of web traffic (Watchpoints) unless specified

otherwise on a Transaction Document. In addition, Customer use of the EdgeView module is subject to the following Customer acknowledgements and conditions:

1. Customer's use of the EdgeView module is subject to the terms of an End User License Agreement with BMC, and will include access on BMC's portal during the Term of the applicable Akamai DSA or WAA contract.
2. EdgeView is provided on an as-is basis with no guarantee of accuracy or reliability and does not supply comprehensive data for determining service levels or issue resolution.
3. Data from EdgeView shall not be used for determining Akamai SLA performance nor will Customer request debugging from Akamai based on EdgeView reports.
4. Customer must acknowledge and commit resources to work directly with BMC Software to install and resolve all issues related to the EdgeView Service.
5. Customer shall renew any EdgeView licenses every December via the BMC Software portal.
6. Customer acknowledges and agrees that Akamai is not responsible for the delivery or performance of EdgeView and may discontinue offering EdgeView at any time.

Electronic Software Delivery ("ESD"): All files served using the Akamai Electronic Software Delivery Service must be 100 KB or larger. Akamai may, at its sole discretion, utilize the NetSession Interface to provide a portion of the ESD Services to Customer.

Enhanced Akamai Protocol: Includes access to certain network enhancements and transport protocol optimizations.

Enhanced DNS ("eDNS"): The Enhanced DNS Service provides an outsourced primary and secondary DNS service via a distributed network of DNS servers deployed across multiple networks designed to improve DNS performance, security and scalability.

Enhanced DNS Service commitment: The Enhanced DNS Service commitment includes:

1. Primary DNS which enables use of the Akamai Intelligent Platform to host Customers' DNS zones as the master authority name server.
2. Secondary DNS where the Customer may retain ownership of zone data in a master name server and transfer zone.
3. Up to the number of DNS zones specified in an Order Form. Additional zones will be charged at the overage rate specified in the Order Form.
4. Enhanced DNS zones may have up to 25,000 records. Delivery of the Service is evidenced by the provisioning of the Customer's Luna Control Center Customer Portal access credentials.

Features: DNSSEC is a protocol extension that works by digitally signing answers to DNS lookups using public key cryptography. Two add-on DNSSEC modules are available with the eDNS service:

Sign and Serve DNSSEC: Enables transfer of unsigned zone from Customer's hidden master DNS server to Akamai. Requires annual update of a signing key reference called a DS record.

Serve DNSSEC: Enables transfer of signed zone to Akamai for serving DNSSEC queries.

Enterprise Edge: A software-based virtual appliance that shall be deployed on Customer-provided hardware at the Application origin. Customer must provide hardware meeting Akamai's specifications for the Enterprise Edge software. Customer's use of Enterprise Edge is subject to the terms of an end user license agreement, accepted at time of download via the Customer Portal. Customer is solely responsible for the upkeep of the Customer-provided hardware as well as the installation and ongoing patch management of applicable software. Akamai shall not be responsible for outages that occur as a result of Customer-provided hardware failure or Customer's failure to patch the applicable software as directed by Akamai via the Customer Portal.

FastDNS: The FastDNS Service provides an outsourced primary and secondary DNS service via Akamai's new FastDNS all Anycast network of DNS servers deployed across multiple networks designed to improve DNS performance, security and scalability.

FastDNS Service commitment: The FastDNS Service commitment includes:

1. Primary DNS which enables use of the Akamai Intelligent Platform to host Customers' DNS zones as the master authority name server.

2. Secondary DNS where the Customer may retain ownership of zone data in a master name server and transfer zone.
3. Zone Apex Mapping which allows Customers to direct their users directly to select Akamai acceleration Services designed to improve performance.
4. Up to the number of DNS zones specified in an Order Form. Additional zones will be charged at the overage rate specified in the Order Form.
5. Vanity Name Server support that enables Customers to use their own DNS names for name servers rather than Akamai hostnames.
6. Enhanced DNS zones may have up to 25,000 records. Delivery of the Service is evidenced by the provisioning of the Customer's Luna Control Center Customer Portal access credentials.

Security Module: The security module of FastDNS provides the following additional services:

Sign and Serve DNSSEC: Enables transfer of unsigned zone from Customer's hidden master DNS server to Akamai. Requires annual update of a signing key reference called a DS record.

Serve DNSSEC: Enables transfer of signed zone to Akamai for serving DNSSEC queries.

Log Delivery Service: Allows Customers to retrieve logs of DNS requests for further analysis purposes. Note: if a Customer comes under large sustained DDos attacks, only samples of the logs will be available during the time period of the DDos.

DNS Monitor: Provides access to dashboard with near real-time reports to monitor security oriented activity on their DNS systems. The dashboard provides Customers with information on where the attack originates, including such things as IP addresses, geographies and request types.

Fast File Upload: Includes access to Akamai's network for content delivery and access to Akamai's file upload acceleration services, which includes route optimization for uploads and/or transport protocol optimization for uploads.

Fast-IP Blocking (FIPB) Module for IPA/SXL: Includes access to one or more of the following network layer controls: IP Blacklist, IP Whitelist, Strict IP Whitelist and Geographic controls. The FIPB module is designed to help Customers mitigate attacks against the Customers' origin servers by filtering traffic from pre-specified sources. AKAMAI DOES NOT WARRANT OR GUARANTEE THAT THE FIPB MODULE WILL MITIGATE ALL POSSIBLE ATTACKS AND/OR THREATS. AKAMAI RECOMMENDS ALL CUSTOMERS MAINTAIN APPROPRIATE SECURITY CONTROLS AT THEIR ORIGIN SERVERS AND/OR DATA CENTER. CUSTOMER ASSUMES ALL RISK WITH THE USE NETWORK LAYER CONTROLS AVAILABLE THROUGH THE FIPB MODULE, INCLUDING POTENTIAL SERVICE OUTAGES DUE TO MISCONFIGURED RULES. THE IPA/SXL SERVICE LEVEL AGREEMENT DOES NOT APPLY TO END USERS THAT CUSTOMERS HAVE BLOCKED USING NETWORK LAYER CONTROLS.

Front-End Optimization (FEO): Front-End Optimization is designed to improve web page performance by modifying the page and associated embedded objects for faster rendering in the browser. FEO provides Customer with an assortment of performance optimizations that can be applied to an HTML page (or grouping thereof). An HTML page is defined as an object served with a HTTP Content-Type header of text/html. Customer represents and warrants that it has full rights to any content to which FEO is applied, and grants permission and license for Akamai to copy, alter, modify, resize, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise manipulate and make derivative versions of pages for which FEO is activated, including intermediary stages which may be cached internally in addition to customary caching at Edge servers. Customer hereby indemnifies Akamai against any losses associated with applying FEO to its content. Customer acknowledges that Akamai may at any time and without notice alter FEO, which may result in web page errors. Akamai shall use reasonable commercial efforts to avoid web page errors however Customer acknowledges and agrees that Akamai shall not be responsible or held liable for errors or site slowdown due to use of FEO.

Geographic Controls: A configuration option within the Web Application Firewall ("WAF") network-layer controls in which requests from a source IP address can be explicitly denied based upon the country from which the request originates.

Global Traffic Management ("GTM" or "FirstPoint"): The Global Traffic Management Service is a DNS-based load balancing solution that is designed to route traffic between different resources based on configurable rules that can increase availability and performance. Customer shall not combine the GTM Service with any Third Party accelerated content delivery service similar to EdgeSuite Delivery without the prior written consent of Akamai. Traffic policies based on CIDR mapping are subject to Akamai approval. Customer is limited to 100 Digital Properties under management and up to 5000 hits per second of peak DNS traffic.

GTM Datacenter: A GTM Datacenter represents a co-located set of servers to which GTM will route Customer traffic. A GTM Datacenter exists within the context of a GTM Domain but may be used by all GTM Properties within that GTM Domain.

GTM Domain: A GTM Domain is a grouping of GTM Properties. The type of domain determines the type of properties that can be created inside that domain. The available domain types are Failover, IP intelligence, Weighted Round Robin, Performance or Performance Plus. Additionally permissions on the Luna Control Center are set at the domain level.

GTM Property: A GTM Property is an entity (domain or subdomain) for which Customer uses the Akamai GTM system. The GTM rules to be applied for this entity could be of type Failover, IP intelligence, Weighted Round Robin or Performance.

IPv6 for Global Traffic Management: Adds two pieces of functionality to the GTM Service

1. GTM will support AAAA-only properties, which respond to AAAA record DNS requests with IPv6 addresses, and no answer for A record DNS requests. AAAA-only properties can be of any type except Performance Plus. Server liveness tests will be performed over IPv6.
2. GTM will support a new property type called "IP Version Selector". Such a property will require two properties in the same domain as traffic targets: an A-only property to answer A requests, and a AAAA-only property to answer AAAA requests. This property type is suitable for managing a dual stack Site.

GTM will support "A-only" properties, which respond to A record DNS requests with IPv4 addresses and no answer for AAAA record DNS requests. No domain name service will be provided over IPv6 (i.e. all A or AAAA requests must go over IPv4).

Granular Cloud Reporting: Allows customized reporting by one or more business identifiers with the ability to capture time intervals ranging from five (5) minutes or greater. Customer can create or delete multiple reports based on immediate or long-term needs to capture usage and traffic patterns for business identifiers such as unique domains, paths or query parameters based on time intervals.

HD Network Solution: Includes (i) access to the HD Client, (ii) access to the HD Network Player Component code under the terms set forth at www.akamai.com/product/licenses, and (iii) Customer Portal access credentials for HD network for delivery of HD On Demand Streaming and/or HD Live Streaming (in Universal Streaming and/or SmoothHD).

Additional HD Network Solution Terms: Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput. Akamai reserves the right to require that Customer make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash, Microsoft Silverlight, and/or Apple iPhone/iPad files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the Service resulting from its failure to comply with the requested changes. Akamai may, at its sole discretion, utilize the Akamai NetSession Interface to provide a portion of the delivery Services to Customer.

Token Authorization: An add-on security module for the HD Network Solution designed to help limit link sharing attacks. This security mechanism authorizes the user based on a token generated using a shared secret string. Token Authorization provides access to the Customer Portal to create an initial Token Authorization configuration for the HD Network Solution. In addition, Customer will receive token generation software development kit for supported platforms using which Customer will generate time bound tokens. The following additional terms apply to Customer's use of Token Authorization Services:

1. All terms and limitations of the HD Network Solution apply to use of Token Authorization;
2. Available for Adobe Flash platform and HTTP live streaming by Apple iPhone and iPad only; and
3. Protection of segmented streaming formats with Token Authorization requires the use of cookies based tokens by Customer.

Player Verification: An add-on security module for the HD Network Solution designed to help limit deep linking attacks by helping to ensure only an approved player is used to play the content delivered by the HD Network Solution. Player Verification provides access to the Customer Portal to create an initial player verification configuration for the HD Network Solution and the HD Network Player Components to be used with the player. For Apple IPhone and iPad devices, Akamai offers device verification capability, which helps verify that content is delivered to a registered Apple iPhone and iPad device. The following additional terms apply to Customer's use of Player Verification:

1. All terms and limitations of the HD Network Solution apply to use of Player Verification;
2. Up to 100 players may be enabled on an approved list of players provided by Customer. Adding additional players to the approved player list requires written authorization from Akamai;
3. Up to 100,000 Apple iPhone and iPad devices may be supported as part of device verification. The registration rate for these devices must not exceed 50 Apple iPhone and iPad device registrations per second and device verification rate must not exceed 500 device verifications per second;
4. Available for Adobe Flash platform and HTTP live streaming by Apple iPhone and iPad only; and
5. Customer must use an HD Network Player Component.

Secure Media: A security Service designed to help limit stream ripping attacks. This mechanism enables Akamai to deliver encrypted content from an Akamai edge server all the way to the player run-time. Secure Media provides access to the Customer Portal to create an initial Secure Media configuration for the HD Network Solution. In addition, Customer will receive HD Network Player Components to be used with the Adobe Flash player. The encryption key used to encrypt the content can be static or can be randomly generated to enable unique encryption per user session. The following additional terms apply to Customer's user of Secure Media:

1. All terms and limitations of the HD Network Solution apply to use of Secure Media;
2. Available for HTTP dynamic streaming by Adobe Flash platform and HTTP live streaming by Apple iPhone and iPad only;
3. Requires Adobe Flash Player 10.1 or later for Adobe Flash platform;
4. Customer must use an HD Network Player Component; and
5. Customer is responsible for securing the static encryption key. Optionally, access to an alternative encryption key can be secured using Token Authorization and keys can be delivered over SSL to the player, when supported by the client environment.
6. The level of encryption may impact playback performance depending on the Customer system. Currently supported algorithms are AES-128 bit and RC4. Partial encryption, based on a percentage of the payload to be encrypted, is also supported.

Secure Media Transport: A security product designed to help limit stream ripping attacks. This mechanism enables Akamai to deliver media content over HTTPS (HTTP + SSL/TLS) to players. Secure Media Transport provides access to the Customer Portal to create an initial Secure Media Transport configuration for the HD Network Solution. The following additional terms apply to Customer's user of Secure Media Transport:

1. All terms and limitations of the HD Network Solution apply to use of Secure Media Transport;
2. Available for Adobe Flash platform only;
3. Customer utilizing server-side SSL must use Akamai wildcard certificates;
4. Customer acknowledges that Customer's content is not protected at rest or while in cache; and
5. SSL Encryption may impact playback performance, depending on the client system, and Customer acknowledges that the SSL connection terminates at the browser.

HTTP Content Delivery: Includes access to Akamai's network for content delivery, cache optimization, content availability and basic reporting and monitoring.

Image Converter: Image Converter provides Customer access to call graphical manipulations using a specified URL API upon images supplied by Customer on origin web servers, or on Akamai NetStorage, delivered by Akamai Services. Customer agrees to abide by all copyright, trademark, and other intellectual property laws worldwide in connection with the use of Image Converter. Customer hereby gives permission and license, where applicable, for Akamai to copy, alter, modify, resize, crop, watermark, reformat, resave, compress, decompress, rewrite, store, transmit, cache, strip metadata and otherwise make derivative versions of images for which the Image Converter module is activated, including intermediary graphical stages which may be cached internally in addition to customary HTTP

object caching at Edge servers. Customer acknowledges that (a) the effects of the Image Converter module must be caused by Customer by altering HTML to make calls conforming to the specified URL API, (b) Akamai may at any time and without notice alter the URL API, which may result in web page errors, and (c) an image derivative requested from an Edge server which is not cached requires calculation, resulting in some additional latency in the HTTP request time. Image Converter requires the purchase of a compatible Akamai delivery solution.

Insight for Publishers: Akamai's Insight for Publishers Service relies on anonymous non-personally identifiable user data collected by Akamai across multiple participating Sites for customers who have executed a Transaction Document for such Service with Akamai. By its use of the Insight for Publishers Service, Customer represents and warrants that it has the right to authorize Akamai to collect and use such anonymous user data from its participating Sites on its behalf and authorizes and directs Akamai to do so in connection with the Services.

InstantConfig: Allows management of multiple unique domains for non-secure (HTTP) traffic. Customer must CNAME its wildcard domains and hostnames to the Akamai CNAME that enables InstantConfig capabilities. Customer will be responsible for any automation and workflow/ coordination to successfully deploy 3rd party CNAMEs. Standard aggregate traffic reporting features are unchanged and there is no detailed reporting for InstantConfig traffic. Detailed reporting is the responsibility of Customer with the purchase of Akamai Log Delivery Service. Enhanced cache control is not available with InstantConfig and Customer may have to translate purge requests as guided by Akamai. Available only with Akamai Cloud Catalyst, Alta Enterprise Accelerator and DSA Services.

IP Application Accelerator ("IPA"): Includes access to Akamai's IP Acceleration; and access to Akamai's Application acceleration services, which include one or more of the following features: route optimization, transport protocol optimization, dynamic mapping, forward error correction and dynamic packet replication.

Billing Methodologies: Concurrent Users is the number of users simultaneously using the Akamai network. For purposes of the IP Application Accelerator Services only, a User is defined as a unique combination of source IP, destination IP, source port, and destination port – typically a TCP connection.

Additional Definitions and Terms for IP Application Accelerator: Customer shall make available to Akamai at no charge such facilities, rack space, connectivity and other infrastructure that Akamai deems reasonably necessary to enable Akamai to install, manage and operate Akamai servers (the "Servers") used to provide the Service. Upon execution of the Agreement, Akamai shall provide to Customer the Servers, and other equipment necessary for the provisioning of the Services (collectively, the "Akamai Equipment"). Customer shall provide a reasonable level of security at such facility and use reasonable care to protect the Akamai Equipment from loss, damage or destruction. Upon Akamai's reasonable request, Customer shall provide basic "hands and eyes" technical assistance including installing, swapping, or de-installing Customer premise equipment and basic configuration using a keyboard and monitor on same. Customer shall permit Akamai's employees and agents, upon reasonable notice to Customer, to enter Customer's facilities where the Akamai Servers are located. Customer shall provide remote access to such Servers twenty-four hours a day, seven days a week. The Akamai Equipment and all operating systems and other software placed on the Akamai Equipment by Akamai are and shall remain at all times, as between Akamai and Customer, the sole property of Akamai. Akamai shall be solely responsible for monitoring, maintaining and operating the Akamai Equipment and the related operating systems and software. Nothing in the Agreement shall be construed to grant Customer any rights or license in the Akamai Equipment or the software or technology on the Akamai Equipment. Unless otherwise agreed in writing, Customer shall not (i) operate the Akamai Equipment, (ii) load or operate any software, programs or other technology or functionality on such Akamai Equipment, (iii) remove, open, modify or interfere or interconnect with the Akamai Equipment, (iv) gain or attempt to gain access to the Akamai systems, software or technology or reverse engineer, reverse compile or attempt to derive the composition or underlying information of any software or computer programs in or on the Akamai Equipment, or (v) permit a third party to do any of the foregoing. Customer will not create, suffer or allow any, liens or claims on the contents of its location that could attach to or otherwise be placed on the Akamai Equipment. Customer shall perform such acts reasonably requested by Akamai to evidence Akamai's or an Akamai Affiliate's ownership of the Akamai Equipment, protect the Akamai Equipment from claims, liens or other rights of third parties or, if legal title was transferred to Customer via the importation process, operation of law or some other means, to transfer title back to Akamai or the appropriate Akamai entity. In the event Customer violates Akamai's intellectual property rights in the Akamai Equipment and the related software and technology, Akamai shall have

the right to terminate the Agreement immediately and seek specific performance, injunctive relief and/or equitable relief, in addition to any other remedies which may be available. Upon termination or expiration of the Order Form, Customer shall cooperate with Akamai or its agents to return the Akamai Equipment to Akamai within 30 days. If Customer fails to return the Akamai Equipment to Akamai within 30 days, Customer shall pay a fee of $12,500 and shall remain obligated to immediately return the Akamai Equipment to Akamai. For the avoidance of doubt, Customer shall have no option to purchase Akamai Equipment upon the termination or expiration of the Order Form.

IPv6 Module: Includes HTTP delivery (and HTTPS delivery for products with Secure Delivery) of content and Applications on a dual-stack hostname ("dual-stack digital property" such as "www.example.com") for which Akamai DNS name servers respond to both A and AAAA requests with corresponding Akamai edge servers capable of serving both IPv4 and IPv6 HTTP(S) requests, and access to the Customer Portal to set up dual-stack hostnames and provide applicable IPv6 visitor and traffic reporting.

IPv6 Module Limitations:

1. IPv6 may not be available for all products.
2. IPv6 content will be delivered from a subset of Akamai locations and performance will not be indicative of the expected performance or availability of any future generally available IPv6 Module. Akamai will not provide any SLA for Customer's users who request AAAA records for the duration of the LA. This should not have an adverse impact on Customer's users who are requesting content over only IPv4.
3. Unsupported features for IPv6 clients related to HTTP(S) delivery include, but are not limited to: AkamaiHD, DLM (Download Manager), Analytics, in-China delivery for China CDN, and Client Access Control. Content Targeting functionality may also be limited in some cases. The Customer may need to make changes to handle IPv6 addresses in HTTP(S) request headers, delivered log lines, download receipts, ESI scripts, and any authentication schemes that rely on the client IP.

IPv6 Module for IPA/SXL: Includes IP application delivery (including HTTPS delivery for SXL) of content and Applications on a dual-stack hostname ("dual-stack digital property" such as "www.example.com") for which Akamai DNS name servers respond to both A and AAAA requests with corresponding Akamai edge servers capable of serving both IPv4 and IPv6 requests, and access to the Customer Portal to set up dual-stack hostnames and provide applicable IPv6 visitor and traffic reporting. The SXL Performance Service Level Agreement does not apply when end users receive an AAAA response and connect to Akamai via IPv6 Module for IPA/SXL.

IPv6 Module for IPA/SXL Limitations:

1. IPv6 may not be available for all products.
2. IPv6 content will be delivered from a subset of Akamai locations and performance will not be indicative of the expected performance or availability of any future generally available IPv6 Module. Akamai will not provide any SLA for Customer's users who request AAAA records for the duration of the LA. This should not have an adverse impact on Customer's users who are requesting content over only IPv4.

Kona IP Defender: Kona IP Defender is designed to improve the security posture of Customer's IP-based applications and reduce the likelihood and impact of security events by mitigating attacks at the Akamai network edge. Kona IP Defender includes configurable functionality designed to help protect Customer Applications by reducing the risk and impact of network layer attacks. It provides request rate control protections to mitigate the risk of Denial of Service and Distributed Denial of Service. It provides tools that enable the definition and enforcement of security policy specific to source IP, destination port and other parameters. Kona IP Defender also provides protection from burst charges associated with unexpected or malicious traffic spikes.

Additional Kona Site Defender Terms:

- Customer acknowledges and agrees that Kona IP Defender does not prevent or eliminate all attacks. Akamai does not warrant or guarantee that Kona IP Defender will detect and mitigate all possible attacks and/or threats.
- Kona IP Defender applies only to those digital properties associated with the applicable Service contractually associated with Kona IP Defender.
- Customer is required to provide Akamai the IP address(es) and/or hostname(s) to be covered by Kona IP Defender. The Customer Applications covered by Kona IP Defender shall be limited as outlined in the Agreement.

- Customer agrees to provide an escalation matrix including a minimum of three (3) contacts that Akamai may need to reach during suspected attacks. Contact information must include name, email address and mobile phone information and be updated by Customer as applicable.
- Customer agrees that Akamai may capture service-specific session information for purposes of identifying the source of DDoS traffic.
- Akamai is not responsible for any Customer action or non-action that might result in Service disruption, availability issues or performance degradation.
- Akamai reserves the right to charge Customer for usage fees associated with traffic bursts or increased usage resulting from Customer actions.
- Any requests that are not directly related to Customer's use of the Akamai platform or extended use thereof, and are not related to the preparation or mitigation of malicious security events, shall be considered outside of the scope of this Service.
- Akamai recommends that all customers maintain appropriate security controls on their application server(s).

Kona Site Defender: Kona Site Defender is designed to improve the security posture of Customer's Sites and reduce the likelihood and impact of security events by mitigating attacks at the Akamai network edge. Kona Site Defender includes configurable functionality designed to help protect Customer Sites by reducing the risk and impact of attacks at the network and application layers. It provides request rate control protections to mitigate the risk of Denial of Service and Distributed Denial of Service as well as common attack methodologies such as SQL Injection, Cross-Site Scripting, trojan backdoors, and malicious bots. It provides tools that enable the definition and enforcement of security policy specific to client IP, HTTP method and other request parameters. Kona Site Defender also provides protection from burst charges associated with unexpected or malicious traffic spikes. Kona Site Defender includes Web Application Firewall, Origin Cloaking (formerly known as Site Shield), Site Failover, Access Control, Security Monitor and DDoS Fee Protection.

Additional Kona Site Defender Terms:

- Customer acknowledges and agrees that Kona Site Defender does not prevent or eliminate all attacks. Akamai does not warrant or guarantee that Kona Site Defender will detect and mitigate all possible attacks and/or threats.
- Kona Site Defender provides protection for only those digital properties associated with the applicable Service contractually associated with Kona Site Defender.
- Customer is required to provide Akamai the URL(s) and/or domain(s) to be covered by Kona Site Defender. The Customer Sites covered by Kona Site Defender shall be limited as outlined in the Agreement.
- Customer agrees to provide an escalation matrix including a minimum of three (3) contacts that Akamai may need to reach during suspected attacks. Contact information must include name, email address and mobile phone information and be updated by Customer as applicable.
- Customer agrees that Akamai may capture relevant service-specific session information for purposes of identifying the source of DDoS traffic.
- Akamai is not responsible for any Customer action or non-action that might result in Service disruption, availability issues or performance degradation.
- Akamai reserves the right to charge Customer for usage fees associated with traffic bursts or increased usage resulting from Customer actions.
- Any requests that are not directly related to Customer's use of the Akamai platform or extended use thereof, and are not related to the preparation or mitigation of malicious security events, shall be considered outside of the scope of this Service.
- Akamai recommends that all customers maintain appropriate security controls on their origin server(s).

License Delivery for Windows Media DRM: Includes access to Akamai's network for provisioning and generation of Windows Media DRM licenses.

Live Streaming: Includes access to Akamai's network for live content delivery in one or more of the following formats: Adobe Flash, Microsoft Windows Media, Apple QuickTime.

> **Additional Live Streaming Terms:** Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput. Akamai reserves the right to require that Customer make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash or Microsoft Silverlight files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the Service resulting from its failure to comply with the requested changes.

Media Analytics: Media Analytics is a suite of analytic products including Audience Analytics, QoS Monitor, Viewer Diagnostics, and Server Side Analytics modules. The Media Analytics Services include Customer Portal access credentials to Akamai's analytics platform for media, with support for both server-side and/or client-side data sources, as selected by Customer. Audience Analytics, QoS Monitor, and Server Side Analytics are required modules of Media Analytics, while Viewer Diagnostics is an optional module that a customer can choose to order.

> **Audience Analytics Module:** includes access to dashboards and reports to understand audience behavior and analyze the drivers of this behavior via the Akamai Customer Portal. Audience Analytics aggregates data from client side data sources.
>
> **QoS Monitor Module:** Includes access to the real time quality of service monitoring portion of Akamai's Media Analytics product. QoS Monitor provides quality of service trends across various dimensions including time, geography, format, ISP, city, etcetera. QoS Monitor aggregates data from client side data sources. Customer shall provide Akamai at least 15 days advance notice if Customer intends to use QoS Monitor to track greater than 50,000 concurrent viewers at any point in time or more than 1 million plays within a single 60-minute period and work with Akamai to ensure a supportable configuration is set up for the event.
>
> **Server Side Analytics Module:** includes access to dashboards and reports to understand and analyze media consumption and audience behavior via the Akamai Customer Portal. Server Side Analytics aggregates data from server side data sources. Server Side Analytics was also known as Media Analytics in previous versions of the Media Analytics product.
>
> **Viewer Diagnostics Module:** includes access to a dashboard that lets customers find individual viewers and analyze that viewer's video consumption activity over a period of 60 days. Each viewer's video play activity is displayed in a calendared view with information regarding connection characteristics as well as a summary of the quality of experience for that individual play.
>
> **Additional Media Analytics Terms:** Depending on which Media Analytics module is ordered by Customer, either or both of the following may apply:
>
> - Server-side data sources utilize log data generated by Akamai's delivery Services. Server-side data sources include support for one or more of the following products: On Demand Streaming (in Adobe Flash and/or Microsoft Windows Media format), Live Streaming (in Adobe Flash and/or Microsoft Windows Media format), and/or HTTP Downloads.
> - Client-side data sources utilize data delivered to Media Analytics from Customer's audio/video player applications utilizing Akamai's analytics plug-in for Adobe Flash, Microsoft Silverlight, iPhone, or HTML5 applications. The Media Analytics plug-in is subject to the terms of the applicable license agreement located at www.akamai.com/product/licenses, and Customer's purchase and use of the Akamai client-side Media Analytics Service constitutes acceptance of the terms of such license. Client-side data sources include support for the following delivery formats and playback technologies: RTMP, Smooth Streaming, HLS, or Progressive Media Downloads using Flash, Silverlight, HTML5, iOS Applications, Android Applications, Roku Applications, or Xbox Applications for on demand or live video content. In addition, Client-Side data sources can be utilized with non-Akamai delivery services for data aggregation and reporting purposes.

Mobile Detection and Redirect Service: The Mobile Detection and Redirect Service provides Customer access to the Customer Portal to activate mobile detection and redirect functionality. The matching mechanism to detect mobile devices at the edge is defined and updated periodically by Akamai, at Akamai's sole and reasonable discretion, and Customer agrees that there are no guarantees around specific device inclusion in such mechanisms. Customer shall be provided access to a whitelist and a blacklist in the Customer Portal to override current default behavior. The Mobile Detection and Redirect Service does not include deployment of the configuration to either the Akamai staging network or the Akamai production network.

Billing Methodology: Billing includes a one-time activation fee and a monthly maintenance fee for the first domain.

Domain Fees: Additional monthly fees are charges each additional domain that is redirected.

Mobile Front-End Optimization (Mobile FEO): Mobile FEO includes all performance optimizations described in FEO but is limited to Mobile Sites.

Mobile Optimization Service Management Module: Includes access to mobile device detection, identification and Akamai content adaptation engine optimization features generating Optimized Mobile Pages for mobile devices from existing web site content. Existing Sites may be programmed in a variety of languages. Akamai aggregates the number of mobile page files of specific content types processed by the Akamai content adaptation engine each month in order to determine Optimized Mobile Page count.

Billing Methodology: Billing is based on a monthly usage commitment of Page Views. Usage overages may result in billing at the then prevailing overage rate.

Site Fees: Fees are per Mobile Site. If more than 1 domain and/or 3 sub-domains is required, an additional Mobile Site must ne purchased.

Optional Module Fees: Additional purchased modules will be billed on a flat monthly fee basis in addition to the Platform tier pricing and/or usage commitment rate as applicable.

Mobile Optimization eCommerce: is a subset of normal content adaptation, handled by the module with the focus on generating and handling Optimized Mobile Pages for mobile devices from existing web site content, including but not limited to the ability to add, remove, view and change shopping cart items for most origin web sites.

Mobile Optimization Analytics: is an integration effort to provide integration to specific third party analytics or tracking packages for mobile web site Metrics, using primarily the server-to-server API's of those systems to avoid a reliance on mobile device features such as scripting.

Mobile Video: is a subset of normal content adaptation, the Mobile Video module can provide mobile transcoded video for pre-identified video assets for the iPhone family and Android family from FLV and MPG input files.

Multi Domain Config: Allows management of many unique domains. Customer can achieve integration of many unique domains by CNAMEing its wildcard domains and hostnames to the Akamai. The customer will be responsible for any automation and workflow/ coordination to successfully deploy 3rd party CNAMEs. Standard aggregate traffic reporting features are unchanged; there is no detailed reporting for Multi Domain Config traffic. Detailed reporting is the responsibility of Customer supported via Akamai Log Delivery Service. Enhanced cache control is not available with Multi Domain Config and Customer may have to translate purge requests as guided by Akamai. Available only with DSA, WAA, DSD or RMA Services.

Multiple Origin Configuration ("MOC"): Provides Customer with the capability to direct traffic for one configured IPA or SXL hostname to up to ten (10) origin datacenters. The MOC Service also provides Customer with the capability to direct requests to the origin data center based either on Akamai-provided performance statistics or failover capabilities from one origin data center to another in a pre-defined order.

NetStorage: Includes access to Akamai's network-based storage Service that may be used with Akamai's content delivery Services as an origin or source for files that are delivered across Akamai's network. The NetStorage Service includes the following restrictions and limitations:

- The maximum size of a single storage group is 10 TB.
- The maximum size of a file that can be uploaded to NetStorage is 25 GB.

- The maximum number of files in any given directory is 50,000.
- There are no guarantees regarding the number of operations per second that may be provided.

NetStorage File Manager: Includes access to functionality on the Customer Portal for uploading and management of Customer data in NetStorage.

Aspera Upload Acceleration Module (Beta): Includes access to the use of Aspera Upload Acceleration products for uploading Customer data into NetStorage. Customers can download Aspera Client Software and activate, configure and manage Aspera Upload Acceleration through the Luna Control Center. Aspera Client Software is subject to a license between Aspera and the Customer, which is contained in the Aspera Client Software. Customer's purchase and use of Aspera Upload Acceleration constitutes Customer's acceptance of the terms of such license and agreement that Akamai shall not be held liable for any of the requirements or terms contained therein. Aspera Upload Acceleration also includes Standard Support. Aspera Upload Acceleration is provided in English only.

Billing Methodology: Usage is billed as GB transferred per month. Billing is based on bytes sent and received.

Signiant Module: Includes access to the use of Signiant products for uploading Customer data into NetStorage. Customer acknowledges and agrees that in the event Customer elects to utilize content delivery networks other than Akamai for their content delivery needs, then Akamai shall have a corresponding right to discontinue provision of the Signiant Module Services, at its sole and reasonable discretion.

Network Conditions: Provides Customer access to functionality on the Luna Control Center to activate HTTP header augmentation of the representation of the network conditions between the edge server and the end user device as seen by the Akamai platform. This lever provides better visibility of the network and also can help with content management and cache key augmentation.

Object Visibility Module: Includes access to functionality on the Customer Portal to configure generation of real time logging data from the Akamai platform and delivery of this logging data to Customer. Customer acknowledges and agrees that the Object Visibility Module does not supply comprehensive data for determining service levels and therefore data from this module is provided on an as-is basis, with no guarantee of accuracy or reliability, and further such data shall not be used for determining Akamai SLA performance. In addition, Customer hereby acknowledges that it shall be responsible for ensuring Customer's origin infrastructure has the capacity required to accommodate any additional load generated by the Object Visibility Module.

Object Delivery (or Caching): Includes access to cache optimization, content availability and basic reporting and monitoring. The following additional terms are applicable to Object Delivery:

Billing Methodology: If the monthly traffic delivery exceeds 20 GB per million Hits, Akamai will bill for overage fees at $3 per GB.

Large File Support: Individual files over 100 MB will not be delivered. For files that exceed 100 MB in size, Customer should use the Electronic Software Delivery Service.

HTML Support: With the Akamai Object Delivery Service, files of Content Type "text/html" will not be delivered. To deliver such files, please use the Web Application Accelerator, Dynamic Site Accelerator, or Dynamic Site Delivery Service.

Hit Count: Each Web page typically has many embedded objects so one Page View can result in multiple Hits for the objects that make up the Web page. For billing and reporting, Akamai counts all Hits (includes "success" response codes that deliver content as well as redirects, permission and other "error" Hits).

Offline Content Protection: Akamai will provide offline playback support leveraging Microsoft PlayReady DRM technology. Akamai will encrypt the content with PlayReady tools and provide the application interfaces to access the cloud based PlayReady license services. The Akamai Service is targeted for Silverlight-based content.

On Demand Streaming: Includes access to Akamai's network for on demand content delivery in one of more of the following formats: Adobe Flash, Microsoft Windows Media, Apple QuickTime.

Additional On Demand Streaming Terms: Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput. Akamai reserves the right to require that Customer make certain technical configuration changes, which may impact links, URLs or embedded Adobe Flash

or Microsoft Silverlight files deployed by Customer. Akamai will provide Customer with reasonable advance notification of any such required changes. Customer will be solely responsible for any possible disruption of the Service resulting from its failure to comply with the requested changes.

Origin Access Control ("OAC"): Supplies access to a list of IP addresses to Customer that Akamai uses to contact Customer's origin. OAC provides assistance in managing a change process for this set of IP addresses as they change over time. Customer must acknowledge receipt of new IP addresses within ninety (90) days of notification by Akamai. Should Customer fail to provide such acknowledgement, Akamai will continue to serve the traffic covered by the base Service offering; however, Akamai shall no longer provide any commitment regarding the performance of the base Service offering or the OAC module, and Customer expressly acknowledges and agrees that degradation of base Service offering (including performance against the applicable SLA) may occur as a result. Should Customer fail to provide acknowledgement within 180 days of notification, Akamai reserves the right to degrade Customer to a different Map and to charge Customer's then-current usage rate for a custom Map over and above the existing charges for the OAC Service, which shall continue to apply. Such new custom Map may also have degraded performance from the up–to-date IP addresses supplied by Akamai for the OAC Service. Akamai's OAC Service is not intended to be a security offering that limits communication to the list of IP addresses supplied to Customer, and in failure situations Customer's end users will connect directly to Customer's origin for access to content. Customer acknowledges and agrees that if OAC is purchased with Session Accelerator (SXL), Customer shall no longer obtain the performance SLA in place with the base SXL Service.

Origin Cloaking: Includes access to the Customer Portal containing information regarding current status of the applicable Origin Cloaking Map(s), any pending changes to the Origin Cloaking Map(s), as well as the Origin Cloaking firewall rules.

Premium Reporting: Metrics and reporting on content, streams, downloads and visitors (Specific reporting based on the applicable Akamai Service).

Progressive Media Downloads: Includes access to Akamai's network for content delivery, with optional optimizations for certain media files.

Real User Monitoring (RUM): RUM is a technology used to aggregate and analyze performance for certain data collected directly from Customer's end-user's browser, providing information on Customer's website performance from the browser. Customer acknowledges that Akamai does not provide any guarantee for volume, collection rate, or availability of RUM data, and in addition that specific data collected may change from time to time at Akamai's sole discretion. Customer acknowledges and agrees that Customer is responsible for the terms for any data collection from Customer's end-users, including those collected by RUM, and Customer hereby indemnifies Akamai for any claims arising out of Customer's use of RUM or RUM data, including, but not limited to, website errors caused by the use of the RUM beacon or performance slowdown associated with the use of RUM on Customer's website.

Rich Media Accelerator ("RMA"): Includes access to Akamai's network for content delivery and access to Akamai's rich media acceleration Services, which include one or more of the following features: pre-fetching; route optimization; or transport protocol optimization.

Rich Media Accelerator - Enterprise: Includes access to the features of Rich Media Accelerator, plus access to the Advanced Cache Optimization, Site Failover, Dynamic Content Assembly and Content Targeting modules.

Billing Methodology: Usage is billed as Mbps or total GB delivered per month. Midgress Traffic is included in both of these metrics. Note 1: HTTP/HTTPS traffic includes all HTTP methods and request/response traffic. Note 2: China CDN and China CDN Secure traffic is measured and billed separately at the usage rate set forth on the Order Form.

Additional Site Fees: Fees are per Site. If more than 1 domain and/or 10 hostnames is required, an additional Site must be purchased.

SecureHD: SecureHD provides security services for the HD Network and is comprised of individual features that together provide complete and robust security protection for streaming content. The solution consists of: media encryption, Token Authentication, Player Verification, and Content Targeting.

Billing Methodology:

Media Encryption: Billing is based on either a flat monthly fee with an overage component or a commitment to deliver a certain number of encrypted GB per month with an overage component.

The flat monthly fee is a fixed fee that entitles Customer to deliver X encrypted GB. Any overage will be billed as an uplift and calculated at a predetermined percentage of normal delivery costs. For example, if Customer is paying Akamai $.10 per GB, is being billed an overage that is 45% of normal delivery costs and exceeds their allotment by 200 encrypted GB, then Customer's per encrypted GB rate would be $.10 for normally delivery, + $.045 for the overage or $.145. At 200GB, this would lead to a total overage fee of $29.

Minimum commitments for encrypted GB will be calculated as 45% of Customer's normal delivery commitment. For example if a customer commits to 500 GB of normal delivery @ .10 per GB for a total of $50, the minimum commitment for Media Encryption will be 225 encrypted GB or $22.50. Any overages will be calculated using the same model as described above. However, overages will be calculated at the agreed upon percentage above normal delivery and not at 45%.

Token Authentication: Billing is based on a flat monthly fee
Player Verification: Billing is based on a flat monthly fee
Content Targeting: Billing is based on a flat monthly fee

Security Monitor: Security Monitor provides access to dashboards and near real-time reports to monitor security-related activity via the Akamai Customer Portal. Security Monitor aggregates data from the Customer's Web Application Firewall implementation, and provides Customers the ability to monitor in near real-time when they are under attack by providing visibility into the nature of the attack, the source(s) of the attack and an indication of what resource or asset is being attacked. Security Monitor provides the ability to review data around attack activity, such as the geographies from which the attack traffic is coming and what defense capabilities triggered the attack declaration.

Service & Support

Professional Services: Unless otherwise indicated, Professional Services are charged on an hourly basis at the rate set forth in the Transaction Document. If no rate is indicated, Akamai's then current list price shall apply. Depending on the nature and scope of the project, a separate statement of work may need to be provided. Per terms of the applicable statement of work, upon completion of integration, Akamai Professional Services will contact Customer to let them know that the Service is available. Upon notification that the Service is implemented, Akamai will begin billing for the integrated Service on the billing effective date or after ten (10) business days, whichever occurs earlier. Billing will commence regardless of the readiness of Customer DNS changes and/or problems due to unavailability of Customer's origin server, data center, Application or Site. If Customer has purchased additional consulting Services to project manage, architect, optimize the configuration or integrate other products and Services, these Services will be considered above and beyond the current integration and will not affect billing of the integrated Service as defined above.

Professional Services – Standard Integration: Includes activation of the applicable Akamai Service as set forth on the associated Transaction Document. This may include any or none of the following:

- Telephone support to (i) conduct a training session for Akamai's online tools for configuration management, reporting, and troubleshooting, and (ii) answer specific implementation questions
- E-mail and/or web conferencing support to assist Customer with the activation process
- Standard Integration Services are provided at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

NOTE: Standard Integration Services do not include in person meetings at Customer's facilities by Akamai personnel. Unless otherwise indicated in an applicable Transaction Document, Standard Integrations are limited to up to eight (8) hours of assistance from an integration specialist and/or other Akamai professionals.

Professional Services – Managed Integration: Includes Standard Integration Services plus one or more of the following related to the implementation and consumption of Akamai Services:

- Enterprise Services Methodology (ESM)
- Total project ownership and schedule
- Requirements gathering and analysis
- Implementation plan specific to Customer
- Change management process definition

- Configuration test plan
- Full life cycle project management and status reporting
- Deployment plan
- Risk assessment
- Support for go-live and associated monitoring
- Post implementation review

Managed Integration Services are provided via phone, email and/or web conferencing at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time). Off-hours support must be requested in advance by Customer no fewer than ten (10) business days prior to the date at which point Akamai will assess the request to determine if the request can be accommodated and if any additional fees are required to fulfill the request. If the scope of Customer's requirements changes during the course of the project, a separate Transaction Document may be required. Customer agrees to reasonable additional fees for travel and living related expenses for Akamai's technical team. Customer shall provide a single point of contact as well as a backup point of contact, authorized and accountable for representing Customer in communicating technical requirements and giving approval for the project milestones and schedule. Customer shall provide technical resources to answer any technical questions that Akamai personnel may have regarding the requirements and deliverables in a timely manner. Customer will be responsible for coordinating and managing any changes to their infrastructure that may be required for integration as referenced in the applicable Transaction Document. Customer will be responsible for conducting functional testing via Akamai for all web properties referenced in the associated Transaction Document prior to going live on the platform. Customer agrees only the web properties referenced in the associated Transaction Document are in scope for this Service. Managed Integration Services are not available for web properties that require custom user client, other than standard web browsers. During the Term of the applicable Transaction Document, Customer may use any deliverables and work products provided in conjunction with the delivery of Managed Integration Services; provided however, Akamai retains all rights in such deliverables and work products created. Unless otherwise indicated in an applicable Transaction Document, Managed Integration Services are limited to up to forty (40) hours of assistance from an Akamai technical team and/or other Akamai professionals.

Professional Services – Emergency Integration: An additional emergency integration fee may be applied to either a Standard or Managed Integration if all or part of the integration must be completed with less than ten (10) business days' notice. In order to accommodate timelines the integration may be split into two tracks, with components requiring expedited implementation being done separately from components that do not. Emergency integrations are subject to resource availability and integration scope and must be reviewed and approved by Akamai Professional Services on a case by case basis.

Professional Services – Enterprise: Includes access to Akamai's Professional Services. The terms and scope of the engagement will be defined in an applicable statement of work.

Professional Services – Event Services: Includes pre-event preparation, enhanced support during the event, and post-event review. The terms and scope of the project will be defined in an applicable statement of work.

Professional Services – Mobile Services: Includes initial implementation as well as on-going support of the Mobile Optimization Service Management Module. The terms and scope of the project will be defined in an applicable statement of work.

Professional Services – Packaged Solutions: Includes access to Akamai's Professional Services for value-added consulting. The terms and scope of engagement will be defined in an applicable statement of work.

Professional Services – WAF Service Management: Required service for customers purchasing Akamai Web Application Firewall. Includes access to one or more of the following:

- WAF Log File Review: Statistical analysis of Customer's WAF log files for rules triggered. Reviews to be performed up to twice per year with up to one (1) WAF configuration and up to two (s) Sites included in each review.
- WAF Configuration Assistance: Up to specified hours on the Transaction Document per quarter of ongoing Professional Services to assist Customer with their WAF configuration.

- Additional WAF Service Management Terms:
  - Customer acknowledges and agrees that WAF Service Management does not prevent or eliminate all possible attacks and/or threats.
  - WAF Log File Review and Reporting does not include implementation of specific configuration recommendations, as these are the responsibility of Customer.
  - Overage fees for WAF Service Management are billed quarterly in arrears.
  - Quarterly allocation and measurement of WAF Configuration Assistance hours starts on the first full month that includes the applicable Billing Effective Date.
  - Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
  - Service does not include in person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Standard Support: Included with all Akamai Services unless otherwise set forth on the applicable Transaction Document or in the Service Description of the applicable Service. Standard Support includes access to all of the following:

- Self-service configuration tools
- Pooled technical support account team
- Standard Initial Response Times
  - Two (2) hours or less for P1 issues
  - Four (4) hours or less for P2 issues
  - Two (2) business days or less for P3 issues
  - All Support Requests reported via e-mail will be considered as P3
- Live support during regular business hours for P2 and/or P3 issues
- Live 24x7X365 support for P1 issues
- Multiple ways to contact Akamai's support team
  - E-mail (ccare@akamai.com)
  - Online (https://control.akamai.com)
  - Phone (1.877.4.AKATEC or 1.617.444.4699)
- Online troubleshooting/diagnostic tools
- Up to 15 Support Requests per year across all Akamai Services

Named Enhanced Support: Includes access to all items included in Standard Support, plus:

- Proactive Support. Up to eight (8) hours per month of proactive services from Customer's designated primary technical support engineer. May be allocated to services such as:
  - Customer support advocacy
  - Quarterly review calls
  - Monthly touch point calls
- Faster Initial Response Times from the Akamai technical support team
  - Thirty (30) minutes or less for P1 issues (must be opened via phone)
  - Two (2) hours or less for P2 issues
  - One (1) business day or less for P3 issues
  - All Support Requests reported via e-mail will be considered as P3
- Named Enhanced Support live support availability
  - Live 24x7X365 support for P1 and/or P2 issues
  - Live support during regular business hours for P3 issues
- Unlimited support requests
- Two (2) seats per year in instructor-led Akamai training courses, located at an Akamai training facility (a.k.a. "Akamai University")
- Each unit of Named Enhanced Support includes above service coverage for up to four (4) Sites or Applications. For Customers under percentage based pricing, the number of sites is not limited.

  Named Enhanced Support Plus Technical Advisory Service: Includes access to all items included in Named Enhanced Support, plus Technical Advisory Service.

  Named Enhanced Support Plus Aqua Service Management: Includes access to all items included in Named Enhanced Support, plus Aqua ION Service Management.

  Named Enhanced Support Plus Terra Service Management: Includes access to all items included in Named Enhanced Support, plus Terra Alta Service Management.

- Named Enhanced Support delivery is evidenced by Customer having the ability to submit Support Requests.

Priority Support: Includes access to all items included in Standard Support, plus:

- Named support team
  - Quarterly business reviews
  - Assistance with configuration of scheduled reports and real-time alerts
- Priority case handling and status updates
  - Every four (4) hours for P1 issues
  - Daily for P2 or P3 issues
- Priority Initial Response Times
  - One (1) hour or less for P1 issues
  - Two (2) hours or less for P2 issues
  - One (1) business day or less for P3 issues
  - All Support Requests reported via e-mail will be considered as P3
- Priority live support availability
- Unlimited Support Requests
- Two (2) seats per year in instructor-led Akamai training courses, located at an Akamai training facility (a.k.a. “Akamai University”)

Priority plus Download Service Management Support Package: Includes access to all items included in Priority Support, plus Download Service Management.

Priority plus DSA Service Management Support Package: Includes access to all items included in Priority Support, plus DSA Service Management.

Priority plus Technical Advisory Service Package: Includes access to all items included in Priority Support, plus Technical Advisory Service.

Priority plus WAA Service Management Support Package: Includes access to all items included in Priority Support, plus WAA Service Management.

Premium Support: Includes access to all items included in Priority Support, plus

- Enterprise program management and ongoing professional services assistance (limited to agreed upon scope)
- Focused technical account team and technical support handling procedures
- Proactive Service monitoring
- Premium case status updates
  - Hourly for P1 issues
- Premium Initial Response Times
  - Thirty (30) minutes or less for P1 issues (must be opened via phone)
  - One (1) hour or less for P2 issues
  - All Support Requests reported via e-mail will be considered as P3
- Unlimited Akamai University training seats (subject to availability of courses)
- Priority beta participation. (Note: Akamai's Service roadmap does not constitute a promise or obligation of delivery of any functionality, and Akamai, at its sole discretion, reserves the right to at any time alter the design, specifications and forecasted time-to-market of all of its products and Services on any roadmap, as part of its continuing program of product development.)
- Up to two (2) days of custom on-site training per year

Enhanced Support SLA: Provides the following in addition to all items included with Standard Support and/or Priority Support (as set forth on the applicable Transaction Document or in the Services description of the applicable Service):

- Faster Initial Response Times from the Akamai technical support team
  - Thirty (30) minutes or less for P1 issues (must be opened via phone)
  - Two (2) hours or less for P2 issues
  - One (1) business day or less for P3 issues
  - All Support Requests reported via e-mail will be considered as P3
- Unlimited Support Requests

- One (1) one-time seat in an instructor-led Akamai training course, located at an Akamai training facility (a.k.a. "Akamai University")

Enterprise Command Center Support: An optional support module available as a supplement to Priority or Premium Support. Enterprise Command Center Support includes:

- Direct support from a dedicated Akamai Command Center team for Akamai Session Accelerator issues
- Customized incident response procedure
- Direct access to a named Akamai incident manager
- Service Level Agreement for Enterprise Command Center Initial Response Times
- Under limited availability, Enterprise Command Center Support is available during North America (GMT – 5:00) East Coast business hours of 8:00 AM to 8:00 PM ET. Service outside of this timeframe will be provided in accordance with the Customer's baseline Priority or Premium Support Package Service Level Agreement.

Holiday Monitoring and Alerting: Provides the following from US Thanksgiving Day (of the year ordered) to January 1st of the following year:

- Akamai walk-though of recommended portal alert settings and thresholds
- Proactive Service Monitoring during the effective time period for up to 4 CP Codes
- Standard and Priority Support customers purchasing this module will receive an additional 20 Support Requests during the effective time period

On Call Event Support: Includes access to Akamai event coordinator who will:

- Engage with your IT team prior to the event to assess infrastructure and business process readiness
- Review your Akamai configuration and recommend improvements
- Devise contingency plans and escalation procedures
- Advise on the creation of appropriate event alerts

During the event, your staff will have access to a named representative from the Akamai support team to contact for expedited issue resolution.

- A minimum of 21 calendar days of notice is required to ensure Event Support coverage for your event.

Live Event Support: Includes all the features of On Call Event Support, plus the following:

- Akamai will fully manage the implementation of any configuration updates identified in the review phase
- Access to Akamai's Stream Analyzer or Akamai's Site Analyzer solutions for a limited period, to monitor Customer's event performance and check for delivery degradation
- A comprehensive post-event report that documents key traffic metrics and summarizes root cause and resolution for any issues during the event

For the duration of the event, Customer will have access to a named Akamai support representative on call or via a live phone bridge.

- A minimum of 21 calendar days of notice is required to ensure Event Support coverage for your event.

Professional Services – Akamai Media Player Maintenance: Available to Customers who have purchased the Akamai Media Player. Provides access to periodic Akamai Media Player software updates which may include feature enhancements, platform library upgrades, best practice enhancements, and/or bug fixes.

Professional Services – Akamai University

- Provides instructor-led public classroom training course(s) located at an Akamai training facility
- Training delivered by Akamai's Professional Services members
- Each purchased unit is equal to one (1) one-time seat, and can be used to attend any of the training instances listed on www.akamai.com/training

Professional Services – Aqua Ion Service Management: Available for Aqua Ion customers. Includes access to one or more of the following:

- Aqua Ion Assessment and Optimization: Technical review of existing Akamai Aqua Ion configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Aqua Ion configurations included in each review.
- Up to the specified hours on the Order Form per quarter or month (default of eighteen (18) hours per quarter or six (6) hours per month) of ongoing Professional Services to perform updates to existing Aqua Ion configurations.
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Service does not include in person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Assessment: A Professional Services assessment and written report on at least one of the following topics related to the Customer's websites or applications specified: Architecture Evaluation, High Performance Best Practices, Security Best Practices, Industry Best Practices, Infrastructure Scaling and Offload Best Practices, Akamai Service and Configuration Recommendations.

Professional Services – Download Service Management: Available for Electronic Software Delivery, Download Manager and Download Analytics customers. Includes access to one or more of the following:

- Download Manager consulting – activation and basic customization of Akamai's Download Manager JavaScript UI templates for up to one hostname per month.
- Download Analytics setup and ongoing review - Customization of Akamai's Download Analytics service, including a monthly review of data.
- Up to the specified hours on the Order Form per month (default of eight (8) hours per month) of ongoing Professional Services to perform updates and enhancements to existing ESD configurations.
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Service does not include in person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – DSA Service Management: Available for Dynamic Site Accelerator customers. Includes access to one or more of the following:

- Site Optimization Review: Technical review of existing Akamai Site configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) DSA Sites configurations included in each review.
- Up to the specified hours on the Order Form per month or quarter (default of six (6) hours per month) of ongoing Professional Services to perform updates to existing Site configurations (limited to agreed upon scope).
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Service does not include in person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Enterprise Service Management: Available for customers receiving Standard or Priority Support. Includes access to one or more of the following:

- Technical Configuration Review: Technical review of existing Akamai configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Akamai configurations included in each review.
- Up to the specified hours on the Order Form per quarter or month (default of sixty (60) hours per quarter or twenty (20) hours per month) of ongoing Professional Services to perform updates or new integrations for existing Service configurations.
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Service does not include in person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Protect and Perform Service Management: Required service for Customers purchasing Akamai Protect and Perform. Includes access to one or more of the following:

- Threat Update Reviews: Statistical analysis of the Customer's log files for WAF rules triggered, and written report and recommendations for improvement. Reviews to be performed up to three (3) times per year, with up to one (1) configuration and up to two (2) Sites included in each review.
- Web Performance Technical Reviews: Technical review of existing Akamai Aqua Ion or Terra Alta configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Aqua Ion or Terra Alta configurations included in each review.
- Configuration Assistance and Updates: Up to the specified hours on the Order Form per quarter of ongoing Professional Services to help Customers perform updates to existing Aqua Ion or Terra Alta and Site Defender configurations.
- Additional Terms:
  - Customer acknowledges and agrees that Protect and Perform Service Management does not prevent or eliminate all possible attacks and/or threats.
  - Site Defender Log File Review does not include implementation of specific configuration recommendations, as these are the responsibility of the Customer.
  - Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
  - Service does not include in-person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Rule Update Service: Recommended service for Customers purchasing Kona Site Defender or Web Application Firewall. Includes access to one or more of the following:

- Threat Update Reviews / Reviews: Statistical analysis of the Customer's log files for WAF rules triggered. Reviews to be performed up to the specified number of times per year in the Order Form for one (1) delivery configuration and up to two (2) WAF policies in each review.
- No more than 1/3 of the Reviews may be used in any single calendar quarter.
- All Reviews must be consumed during the contract term.
- Security Configuration Assistance: Up to the specified hours on the Order Form per month of ongoing Professional Services to assist Customer with its Site Defender configuration.
- Additional Terms:
  - Customer acknowledges and agrees that Site Defender Service Management does not prevent or eliminate all possible attacks and/or threats.
  - Site Defender Log File Review does not include implementation of specific configuration recommendations, as these are the responsibility of the Customer.
  - Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
  - Security Configuration Assistance is not intended to provide security incident emergency response.
  - Service does not include in-person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Security: Includes access to Akamai's Professional Services for Security Services. The term and scope of the engagement will be defined in an applicable statement of work.

Professional Services – Service Management: Available for customers receiving Standard Support or Priority Support Services. Includes access to one or more of the following:

- Technical Configuration Review: Technical review of existing Akamai configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Akamai configurations included in each review.
- Up to the specified hours on the Order Form per month or quarter (default of six (6) hours per month) of ongoing Professional Services to perform updates to existing Service configurations.
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

- Service does not include in person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Site Defender Service Management: Recommended service for Customers purchasing Kona Site Defender. Includes access to one or more of the following:

- Site Defender Log File Review: Statistical analysis of the Customer's log files for WAF rules triggered. Reviews to be performed up to twice per year with up to one (1) configuration and up to two (2) Sites included in each review.
- Site Defender Configuration Assistance: Up to the specified hours on the Order Form per month of ongoing Professional Services to assist Customer with their Site Defender configuration.
- Additional Site Defender Service Management Terms:
  - Customer acknowledges and agrees that Site Defender Service Management does not prevent or eliminate all possible attacks and/or threats.
  - Site Defender Log File Review does not include implementation of specific configuration recommendations, as these are the responsibility of the Customer.
  - Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
  - Service does not include in-person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – Terra Alta Service Management: Available for Terra Alta customers. Includes access to one or more of the following:

- Up to the specified hours on the Order Form per month or quarter (default of six (6) hours per month) of ongoing Professional Services to perform updates to existing Terra Alta configurations.
- Technical Configuration Review: Technical review of existing Akamai Terra Alta configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) Terra Alta Applications included in each review.
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Service does not include in person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Professional Services – WAA Service Management: Available for WAA customers. Includes access to one or more of the following:

- Application Optimization Review: Technical review of existing Akamai WAA configurations, and recommendations for improvement. Reviews to be performed up to twice per year, with up to two (2) WAA Applications included in each review.
- Up to the specified hours on the Order Form per month or quarter (default of six (6) hours per month) of ongoing Professional Services to perform updates to existing WAA configurations.
- Work to be conducted at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Service does not include in person meetings at Customer's facilities by Akamai personnel unless otherwise indicated in an applicable Transaction Document.

Technical Advisory Service: Includes access to a designated technical advisor during standard business hours, up to an agreed upon number of hours or Business Days (stated on the Order Form), for advisory services that can include any one or more of the following activities:

- Provide pre- and post-sales technical consultation
- Assist with strategic initiatives through ongoing engagement
- Schedule periodic status meetings
- Conduct periodic Engagement Reviews
- Share industry and technology best practices with Customers

For travel to Customer's premises, Customer agrees to reasonable additional fees for travel and living related expenses for Akamai's technical team.

Technical Advisory Service – Enterprise: Includes access to all items included in Technical Advisory Service, plus one or more of the following:

- Two (2) blue-sky workshops annually – The designated technical advisor will work with Customer to understand and develop a technology roadmap to help map technical solutions with business needs. Each workshop will be limited to forty (40) hours.

- Technical Consulting Assessment – an annual technical engagement, analysis and review in one of the following areas:
  - Site Assessment
  - Application Assessment
  - Performance Assessment
  - Configuration Review
- Four (4) Akamai University training seats (subject to availability of courses).

For travel to Customer's premises, Customer agrees to reasonable additional fees for travel and living related expenses for Akamai's technical team

Customer Travel Expense Policy: This policy applies when necessary and reasonable travel is conducted by Akamai personnel to a customer premises or a choice of the customer's location for authorized Akamai business. The applicable charges are pursuant to the following:

- One (1) business day trip: USD 750
- Each additional business day: USD 500
- A fixed PS fee may be uplifted to include the travel costs
- A per hour PS rate may be uplifted to include the travel costs

Session Accelerator ("SXL"): Includes access to Akamai's IP Acceleration network; and access to Akamai's Application acceleration Services, which include one or more of the following features: route optimization, transport protocol optimization, dynamic mapping, forward error correction, and dynamic packet replication.

Billing Methodologies: Concurrent Users is the number of users simultaneously using the Akamai network. For purposes of the Session Accelerator Services only, a User is defined as a unique SSL session ID.

Additional Definitions and Terms for Session Accelerator: Customer shall make available to Akamai at no charge such facilities, rack space, connectivity and other infrastructure that Akamai deems reasonably necessary to enable Akamai to install, manage and operate Akamai servers (the "Servers") used to provide the Service. Upon execution of the Agreement, Akamai shall provide to Customer the Servers, and other equipment necessary for the provisioning of the Services (collectively, the "Akamai Equipment"). Customer shall provide a reasonable level of security at such facility and use reasonable care to protect the Akamai Equipment from loss, damage or destruction. Upon Akamai's reasonable request, Customer shall provide basic "hands and eyes" technical assistance including installing, swapping, or de-installing Customer premise equipment and basic configuration using a keyboard and monitor on same. Customer shall permit Akamai's employees and agents, upon reasonable notice to Customer, to enter Customer's facilities where the Akamai Servers are located. Customer shall provide remote access to such Servers twenty-four hours a day, seven days a week. The Akamai Equipment and all operating systems and other software placed on the Akamai Equipment by Akamai are and shall remain at all times, as between Akamai and Customer, the sole property of Akamai. Akamai shall be solely responsible for monitoring, maintaining and operating the Akamai Equipment and the related operating systems and software. Nothing in the Agreement shall be construed to grant Customer any rights or license in the Akamai Equipment or the software or technology on the Akamai Equipment. Unless otherwise agreed in writing, Customer shall not (i) operate the Akamai Equipment, (ii) load or operate any software, programs or other technology or functionality on such Akamai Equipment, (iii) remove, open, modify or interfere or interconnect with the Akamai Equipment, (iv) gain or attempt to gain access to the Akamai systems, software or technology or reverse engineer, reverse compile or attempt to derive the composition or underlying information of any software or computer programs in or on the Akamai Equipment, or (v) permit a third party to do any of the foregoing. Customer will not create, suffer or allow any, liens or claims on the contents of its location that could attach to or otherwise be placed on the Akamai Equipment. Customer shall perform such acts reasonably requested by Akamai to evidence Akamai's or an Akamai Affiliates' ownership of the Akamai Equipment, protect the Akamai Equipment from claims, liens or other rights of third parties or, if legal title was transferred to Customer via the importation process, operation of law or some other means, to transfer title back to Akamai or the appropriate Akamai entity. In the event Customer violates Akamai's intellectual property rights in the Akamai Equipment and the related software and technology, Akamai shall have the right to terminate the Agreement immediately and seek specific performance, injunctive relief and/or equitable relief, in addition to any other remedies which may be available. Upon termination or expiration of the Order Form, Customer shall cooperate with Akamai or its agents to return the Akamai Equipment to Akamai within 30 days. If Customer fails to return the Akamai Equipment to

Akamai within 30 days, Customer shall pay a fee of $12,500 and shall remain obligated to immediately return the Akamai Equipment to Akamai. For the avoidance of doubt, Customer shall have no option to purchase Akamai Equipment upon the termination or expiration of the Order Form.

SHUTR: A performance enhancement that enables support for an HTTP protocol enhancement named "Suppressed Headers for Upstream Traffic Reduction" (the SHUTR Protocol) to be engaged when a compliant device makes an HTTP request to an enabled Digital Property on the Akamai network. SHUTR Protocol compliant devices are available from third parties; Akamai does not market, sell, control, support, or debug such devices, or the relevant logic that they employ.

Site Analyzer: Includes access to Akamai's speed note network for monitoring websites and transactions; and access to the Customer Portal which includes instant check, e-mail reports and alerting.

Site Failover: Includes functionality for in-metadata failover. In the event that the origin Site becomes unavailable, Site Failover can be used to achieve one of the following actions (a) serve what is in cache, (b) serve content from NetStorage, or (c) regenerate request to another datacenter.

SPDY: The SPDY module is designed to support use of the SPDY protocol on Akamai's secure network. The beta will include support for SPDY draft 2 only. SPDY will be supported in the last mile only (client-to-edge), and edge-to-origin will be delivered using regular HTTPS. Stream prioritization (as set by the client) will be supported. SPDY Push or Hint directives will not be supported. The number of concurrent SPDY streams will be limited during the SPDY beta. SPDY will be available to supporting clients only. Customer acknowledges that SPDY is a third party protocol and Akamai will not be responsible for any bugs or performance issues resulting in its design or implementation. Customer acknowledges that SPDY may not have a positive impact on performance at all times.

Steelhead Cloud Accelerator Service: Steelhead Cloud Accelerator Service provides Customer's enterprise network users with access to Akamai's SureRoute for IP network, combined with Riverbed's Cloud Steelhead software, for purposes of accelerating the performance of specified Software as a Service ("SaaS") applications being accessed by those enterprise users from Customer's network. The Service also includes access to Riverbed's technical support services, the terms of which are set forth at www.riverbed.com/termsandconditions. Activation of the Service occurs through the Riverbed Cloud Portal, and Riverbed will provide the Service to Customer during the term of the paid subscription to the Service. Customer may access the Service from its network only via Riverbed Steelhead appliance(s) running specified versions of Riverbed WAN optimization software that are current on Riverbed support and maintenance.

Usage of the Service is limited by the number of users purchased. Certain features or SaaS application packages may be subject to additional restrictions or terms set forth at www.riverbed.com/additionalcloudacceleratorterms. In addition, usage of the Service is limited to the particular SaaS application package(s) purchased by Customer. Use of the Akamai network in connection with the Service is subject to Akamai's acceptable use policy located at www.akamai.com/html/policies/index.html, and use of the Akamai Cloud Proxy enablement software to access the Service is subject to the standard Riverbed end user license agreement located at www.riverbed.com/us/license. For the avoidance of doubt, for Customer to benefit from the acceleration for the SaaS application package(s) purchased in connection with the Service, Customer must (1) have the necessary Riverbed Steelhead appliances and/or software required to access the Service, and (2) ensure such appliances and/or software are covered by a then current Riverbed maintenance and support plan. Riverbed and Akamai retain ownership of any intellectual property resulting from the Service.

Stream Analyzer: Includes access to a media delivery network for streaming and HTTP Content Delivery; one NetStorage group; and one Digital Property for all content delivery. Such capabilities include one or more of the following features: on-demand streaming and HTTP content management and delivery; metadata and RSS feed management and delivery; live streaming content provisioning and delivery; and policy management and delivery.

Terra Alta Enterprise Accelerator ("Terra Alta" or "Alta"): Includes access to Akamai's SSL network for secure content delivery; provisioning of one of the following SSL Network Access Digital Certificates: Wildcard or SAN; access to Akamai's application acceleration and cloud management services, which in turn includes one or more of the following features: object pre-fetching, page pre-fetching, route optimization, transport optimization and Edge Load Balancing. The Edge Load Balancing module included with Terra Alta provides entitlement to use Akamai's Global Traffic Management Service with

either performance or weighted load balancing. Terra Alta also includes access to Akamai's FastDNS, which includes access to Primary DNS and Enhanced DNS.

Terra Alta Enterprise Accelerator 2.0 ("Terra Alta 2.0" or "Alta 2.0"): Includes access to Akamai's SSL network for secure content delivery; provisioning of one of the following SSL Network Access Digital Certificates: Wildcard or SAN; access to Akamai's Application acceleration Services, which in turn includes one or more of the following features: Web Deduplication, object pre-fetching, page pre-fetching, route optimization, protocol optimizations, front end optimizations and edge load balancing for up to two (2) physical locations. Alta 2.0 also provides entitlement to use Akamai's Global Traffic Management Service with weighted load balancing for the same two (2) physical locations used with edge load balancing. Alta 2.0 also includes access to Primary DNS as well as access to Edge Connect Cloud Monitor.

Terra Alta with Kona Site Defender ("Alta with Kona Site Defender"): Includes access to Terra Alta and Kona Site Defender Services as described herein. The terms for each of these Services shall apply to Customer's use of the Terra Alta with Kona Site Defender Services.

Terra Alta with Session Accelerator ("Alta with Session Accelerator"): Includes access to Terra Alta and Session Accelerator Services as described herein. The terms for each of these Services shall apply to Customer's use of the Terra Alta with Session Accelerator Services.

Terra Apex (Beta): Terra Apex is designed to accelerate the performance of Customer configured web content and applications and reduce network link utilization within the Customer's enterprise network. Terra Apex utilizes:

- Network compression and deduplication,
- Application and protocol optimization,
- Caching and serving HTTP content that is typically served from the Akamai Content Delivery Network (CDN), and
- Transparent caching of generic HTTP web content that is not typically served from the Akamai CDN.

Terra Apex is comprised of Terra Apex appliances that reside on the Customer's premises and run supported versions of Terra Apex software. Customers can activate, configure and manage Terra Apex appliances through the Luna Control Center. The software of Terra Apex is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer's purchase and use of Terra Apex constitutes Customer's acceptance of the terms of such license. Terra Apex also includes Standard Support. Use of the Akamai network in connection with the Service is subject to Akamai's acceptable use policy located at www.akamai.com/html/policies/index.html. Customer acknowledges and undertakes all responsibilities for all materials it transmits and/or distributes using Terra Apex.

Akamai offers several levels of bandwidth and TCP connection capacity for a monthly fee. For each location, Customers shall subscribe the capacity appropriate for their usage requirement. Usage of Terra Apex is limited to the capacity purchased by the Customer; traffic that exceeds the purchased bandwidth or TCP connection capacity on any appliance will go to the origin server unoptimized. Akamai reserves the right to deactivate the Terra Apex appliance when the Customer's purchased contract terminates.

Third Party Content Accelerator ("TPCA"): The TPCA Service provides Customer with the ability to direct Akamai to dynamically re-write URLs of third party content referenced by Customer to a hostname established by Customer. The third party content is also configured on Akamai's edge platform to leverage certain of Akamai's DSA features. In addition, TPCA provides access to a rules engine and toolset for a Customer to identify URL patterns in Customer's pages that Customer wants to be directed to and served from the Akamai network on behalf of Customer. Also, traffic reports and alerts are available to Customer in the Customer Portal to provide additional visibility into the traffic behavior for the designated third party content.

Additional terms for TPCA:

1. Customer represents, warrants, and covenants that:

(a) (i) it has all right and authority to direct Akamai to accelerate the third party content; (ii) Customer's use of TPCA or other Akamai Services to accelerate third party content does not, and will not, violate any agreement to which Customer is a party; and (iii) without limitation of any indemnification obligations set forth in the Terms & Conditions governing Customer's purchase of Akamai's offerings, Customer will defend, indemnify, and hold Akamai harmless from and against any claims or damages that arise from the third party content or Customer's use of TPCA or other Akamai Services in conjunction with TPCA to accelerate third party content via the Akamai network.

(b) Customer will not, and will not permit any third party to, use TPCA if: (i) the third party requires a specific hostname or domain be utilized; (ii) the third party, or any contractor, representative, agent, partner or service provider of the third party, is performing user tracking or data collection across many sites based on a cookie or webStorage value that is associated with the third party content; (iii) the third party or any contractor, representative, agent, partner or service provider of the third party has provided an opt-out mechanism for any data tracking activity being conducted in connection with the third party content; or (iv) the third party content (or any portion thereof) to be accelerated is in HTML or Flash.

2. Third party content shall not be deemed part of any Akamai Service by virtue of being located on or served from Akamai servers.

User Validation Module: The User Validation module is designed to help mitigate a suspected or identified attack by introducing a validation challenge in a Web workflow capable of recognizing requests from clients that do not have advanced browser and Flash capabilities. End users are redirected to a validation engine that presents a user challenge to help filter out bad requests such as Botnets and DoS attacks. The User Validation module is not active and remains in standby mode by default until it is activated by Customer via the Luna Control Center.

Video On-Demand Transcoding ("VODT"): Video On-Demand Transcoding is designed to encode Customer videos, provided to Akamai in supported formats, into the appropriate format, bitrates, and frame sizes to enable multi-bitrate delivery over the Akamai HD Network. This service does not support all formats of video and audio. Videos must be provided in a compatible format. Customer grants Akamai permission and license to copy, alter, modify, resize, reformat, resave, compress, decompress, rewrite, transmit, cache, strip metadata and otherwise manipulate and make derivative versions of videos for which VODT is activated and indemnifies Akamai from any losses associated with performing these licensed actions on behalf of Customer. Customer acknowledges that Akamai cannot improve the original quality of video submitted for VODT services and that Akamai shall not be responsible for video quality degradation that may result from use of VODT. VODT requires the use of NetStorage.

Web Application Accelerator ("WAA"): Includes access to Akamai's SSL network for secure content delivery; provisioning of one of the following SSL Network Access Digital Certificates – Standard (Single-hostname), Wildcard, SAN or Third Party; and access to Akamai's Application acceleration Services, which, in turn, includes one or more of the following features: pre-fetching, route optimization and transport control optimization. HTTP/HTTPS traffic includes all HTTP methods.

Billing Methodology: Billed using MPV with GB overage model: if monthly delivery (sum of all traffic types) exceeds 200 GB per MPV, Akamai will bill for overage fees at $3 per GB. Page View overages will be charged at the Additional MPV rate. Mbps and GB billing models are also available.

Page View Count: Akamai aggregates the number of "text/html" files delivered each month in order to determine Page View count.

Web Application Accelerator with On Demand Streaming ("WAA with On Demand Streaming"): Includes access to WAA Services as well as access to Akamai's network for on demand content delivery in Adobe Flash and/or Microsoft Silverlight formats for up to 5% of overall traffic. China CDN Streaming capabilities are not available over China CDN even if purchased for the WAA Service. Akamai reserves the right to limit the sale of WAA with On Demand Streaming to customers whose streaming requirements are not expected to exceed 5% of their overall content acceleration requirements.

Billing Methodology and Page View Count: Same as those set forth above for WAA Services.

Web Application Accelerator with Session Acceleration ("WAA with Session Accelerator"): Includes access to WAA and Session Accelerator Services as described herein. The terms for each of these Services shall apply to Customer's use of the WAA with Session Accelerator Services.

Web Application Firewall ("WAF") Module: Includes access to Akamai's Web Application Firewall functionality, which, in turn, includes one or more of the following features: 1) network layer controls including IP Blacklist, IP Whitelist, Strict IP Whitelist, and Geographic Controls; 2) network layer rules activity report; 3) Application layer controls (firewall rules) both used to mitigate attacks against web Applications and associated systems, where Akamai periodically updates the list of available rules; 4) Application layer rules activity report; 5) Real-Time Reporting (RTR) log functionality; 6) IP Rate controls and activity reports; 7) Custom Rules controls and activity reports; and 8) Security Monitor:

WAF delivery is evidenced by: 1) The provisioning of Luna Control Center access credentials to Customer (enabling Customer Portal access by Customer); and 2) The ability of either Customer or Akamai to configure and/or deploy an initial WAF configuration.

WAF Module limitations include: 1) provides protection for only digital properties associated with the applicable Service contractually associated with WAF Module; 2) Real-Time Reporting (RTR) restricted to logging to servers that are digital properties associated with applicable Transaction Document containing the WAF Module; and 3) availability for use with DSA, DSD, EdgeSuite, RMA and WAA Services only. AKAMAI DOES NOT WARRANT OR GUARANTEE THE WAF MODULE WILL DETECT ALL POSSIBLE ATTACKS AND/OR THREATS. AKAMAI RECOMMENDS ALL CUSTOMERS MAINTAIN APPROPRIATE SECURITY CONTROLS ON THEIR ORIGIN SERVER(S). CUSTOMER ASSUMES ALL RISK OF USE WITH CUSTOM RULES, INCLUDING POTENTIAL SERVICE OUTAGES DUE TO MISCONFIGURED RULES. THE SERVICE LEVEL AGREEMENT DOES NOT APPLY WHEN CUSTOM RULES ARE USED BY THE CUSTOMER.

Web Deduplication: A capability that is designed to improve data transfer on the Akamai platform by eliminating redundant elements with the goal of improving response time to end users.

Web Experience: A set of URLs used to deliver content and Applications for a discrete and individual corporate unit (e.g., legal entity, company business unit, publishing group, product brand or Application) with a shared primary domain name that is used in up to a total of 10 equivalent hostnames or aliases for materially the same content (e.g., mobile or country versions of a domain name). For example, in the case of www.customer.com and images.customer.com, "customer.com" is the domain and "www" and "images" are each additional hostnames. Similarly, m.customer.com, www.customer.mobi, and www.customer.co.uk are the respective examples of mobile and country equivalents for www.customer.com.

WebTrends On-Demand: Includes use of JavaScript Code on HTML pages selected by Customer to be tracked. Specified number of page views each month; five (5) Standard Profiles or fifty (50) Basic Profiles; two hundred (200) selectable or Custom Reports; five hundred (500) exports per month to other formats; and Support. Usage in excess of the monthly usage commitment and up to two times the monthly usage commitment will be charged at the standard order form rate. Usage in excess of two times (2X) the monthly usage commitment will be charged a twenty-five percent (25%) bursting premium. Customer is responsible for configurations unless Akamai Professional Service assistance purchased.

- **WebTrends Professional Service (Customer Consulting Engagements):** WebTrends consulting services subject to WebTrends' Services Terms & Conditions and a Project Authorization to be executed by Customer and WebTrends. Hourly rate is for remote services as it does not include T&E related to services delivery. T&E for actual expenses which will be billed separately.

AURA CDN SOLUTIONS, AURA SUPPORT SERVICES AND AURA HARDWARE:

The following definitions, billing methodologies, service descriptions and additional terms are applicable to the license and use of Akamai's Aura Lumen Software, and purchase and use of Akamai's Aura Spectra Services and Aura Hardware, and shall be deemed incorporated into the Order Form or other Transaction Document between Customer and Akamai. Akamai's Aura Lumen Software, Aura Spectra Services and Aura Hardware are not authorized for resale, sublicense or other distribution under Akamai's Net Alliance Partner Program.

AURA SELECTED ACRONYMS AND DEFINITIONS:

CDN: A content delivery network.

HTTP req/sec: HTTP requests per second.

Network Installation Fee: A one-time fee charged for the installation of the Aura Edge eXchange per 1 Gbps of capacity pursuant to a Transaction Document.

Operator: A fixed line or wireless network operator.

Server: A single physical computer comprised of processing units, memory and input/output capabilities. Each separate physical device (e.g., a blade or a rack-mounted device) that has the required components is considered itself a separate Server.

Server Entitlement: The unit of measure for the number of Servers on which a Customer of Aura Lumen Software is entitled to run the applicable Aura Lumen Software. One Server Entitlement is equal to one (1) Server.

Storage Entitlement: The unit of measure for the amount of non-redundant storage capacity of the Aura Lumen Object Store. One (1) Storage Entitlement is equal to 1 TB of aggregate non-redundant storage.

Workload Entitlement: The unit of measure for the amount of capacity up to which a Customer of Aura Lumen Software is entitled to utilize the applicable Aura Lumen Software at any instant in time. One (1) Workload Entitlement for Aura Lumen CDN is equal to either 1 Gbps or 2000 HTTP req/second of delivered capacity and shall be set forth on the Transaction Document. One (1) Workload Entitlement for Aura Lumen Object Store provides one (1) Gbps of aggregate throughput, where throughput refers to the input or the delivered bandwidth, whichever is higher.

AURA DESCRIPTIONS AND ADDITIONAL TERMS:

Aura CDN Solution: Aura CDN Solution means, collectively, the applicable Aura Lumen Software licensed by an Aura Customer and/or Aura Spectra Services purchased by an Aura Customer pursuant to a Transaction Document.

Aura Control System: The Aura Control System provides access to a management system that allows an Aura Customer to manage components of the Customer's CDN based on the Aura CDN Solution and content delivered via the Aura CDN Solution. The Aura Control System provides a unified suite of management tools that will support the full suite of FCAPS functions (Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management. The Aura Control System is comprised of multiple modules, including software-as-a-service modules and licensed modules. The software-as-a-service modules are the Aura Control Plane and the Luna Control Center. The licensed modules are the Aura Licensed Manager and Aura Licensed Analytics.

AURA LUMEN SOFTWARE:

Aura Lumen Software: Akamai's Aura-Lumen branded licensed CDN software solutions offered to Customers that are Operators, including Aura Lumen CDN, Aura Lumen Object Store and any optional modules for use therewith.

Aura Lumen CDN: Aura Lumen CDN is a suite of licensed software that is offered to Customers that are Operators and which is comprised of the following components: Aura HyperCache, Aura Intercept Service and Aura Request Router. The software used to provide Aura Lumen CDN is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura Lumen CDN constitutes the Customer's acceptance of such license. Use of the Akamai network in connection with Aura Lumen CDN is subject to Akamai's acceptable use policy located at www.akamai.com/html/policies/index.html. Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or distributes using Aura Lumen CDN. Customers of Aura Lumen CDN shall receive access to the Aura Licensed Manager and Aura Licensed Analytics modules within the Aura Control System. All other Aura licensed software components are licensed separately.

Use of Aura Lumen CDN is limited to both (a) the Workload Entitlements and (b) Server Entitlements purchased by Customer pursuant to a Transaction Document. The length of Term of the applicable license agreement for Aura Lumen CDN shall be set forth or incorporated by reference in the applicable Transaction Document.

A Customer must purchase a number of Workload Entitlements for Aura Lumen CDN that meet or exceed the aggregate network-wide daily peak of Customer's actual utilization of such Workload Entitlements. Customer shall reconcile its Workload Entitlements and actual usage once per calendar quarter, by comparing the peak of actual usage for such quarter with the Workload Entitlements already purchased. In the event the actual usage for such quarter exceeds the Workload Entitlements purchased (such excess, the "Overage Lumen CDN Usage"), Customer shall purchase the number of additional Workload Entitlements necessary to cover such Overage Lumen CDN Usage within thirty (30) days after the end of such calendar quarter. Akamai reserves the right to audit Customer's compliance with the foregoing on a quarterly basis.

Aura HyperCache: Aura HyperCache is a node that serves content to end users and also provides local caching storage. The software used to provide Aura HyperCache is subject to the

applicable license agreement for Aura Lumen CDN located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura Lumen CDN constitutes the Customer's acceptance of such license. Aura HyperCache is included with Aura Lumen CDN.

Aura Intercept Service: Aura Intercept Service may be used to transparently intercept and divert HTTP requests into the Aura HyperCache. The software used to provide the Aura Intercept Service is subject to the applicable license agreement for Aura Lumen CDN located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura Lumen CDN constitutes the Customer's acceptance of such license. Aura Intercept Service is included with Aura Lumen CDN.

Aura Request Router: Aura Request Router directs requests via DNS to the optimal cache in a network from which content may be served. The software of used to provide Aura Request Router is subject to the applicable license agreement for Aura Lumen CDN located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura Lumen CDN constitutes the Customer's acceptance of such license. Aura Request Router is included with Aura Lumen CDN.

Aura Lumen CDN– Optional Modules:

Aura Local DNS: Aura Local DNS is used to resolve hostnames of CDN nodes and origins when a Customer does not have a DNS server that is capable of being utilized for this purpose, and is an optional module for Aura Lumen CDN. The software used to provide the Aura Local DNS is subject to the applicable license agreement for Aura Lumen CDN located at www.akamai.com/product/licenses, and the Customer's purchase and use of an Aura Local DNS constitutes the Customer's acceptance of such license. The length of Term of the applicable license agreement for Aura Lumen CDN shall be set forth or incorporated by reference in the applicable Transaction Document.

Aura Licensed CDN – Encryption: Aura Licensed CDN – Encryption enables per-session AES encryption for content delivered by the Aura HyperCache, and is an optional module for Aura Lumen CDN. The software used to provide the Aura Licensed CDN – Encryption is subject to the applicable license agreement for Aura Lumen CDN located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura Licensed CDN – Encryption constitutes the Customer's acceptance of such license. One license to Aura Licensed CDN – Encryption is required for each Workload Entitlement to Aura Lumen CDN that is subject to encrypted delivery. The length of Term of the applicable license agreement for Aura Lumen CDN shall be set forth or incorporated by reference in the applicable Transaction Document.

Aura Lumen Object Store (or "Aura Object Store"): Aura Lumen Object Store is an HTTP object store used to persistently store media content for content origination within a CDN. It supports file ingest from content management systems via multiple ingest protocols and originates content for both linear and VOD applications. The software used to provide Aura Lumen Object Store is subject to the applicable license agreement located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura Lumen Object Store constitutes the Customer's acceptance of such license. Use of the Akamai network in connection with Aura Lumen Object Store is subject to Akamai's acceptable use policy located at www.akamai.com/html/policies/index.html. Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or stores using Aura Lumen Object Store. All other Aura licensed software components are licensed separately.

Use of Aura Lumen Object Store is limited to both (a) the Workload Entitlements and (b) Storage Entitlements purchased by Customer pursuant to a Transaction Document. The length of Term of the applicable license agreement for Aura Lumen Object Store shall be set forth or incorporated by reference in the applicable Transaction Document.

A Customer must purchase a number of Workload Entitlements for Aura Lumen Object Store that equals the greater of the Customer's actual total delivery bandwidth or total ingest bandwidth for the Aura Object Store. Customer shall reconcile its Workload Entitlements and actual total delivery bandwidth or total ingest bandwidth once per calendar quarter, by comparing the applicable actual delivery or ingest bandwidth for such quarter with the Workload Entitlements already purchased. In the event the actual delivery or ingest bandwidth for such quarter exceeds the Workload Entitlements purchased (such excess, the "Overage Object Store Usage"), Customer shall purchase the number of additional Workload Entitlements necessary to cover such Overage Object Store Usage within thirty (30) days after the end of

such calendar quarter. Akamai reserves the right to audit Customer's compliance with the foregoing on a quarterly basis.

Aura Lumen Object Store - Packaged Tools: Packaged third party tools for management and analytics of Aura Lumen Object Store, and an optional module for Aura Lumen Object Store. The software used to provide Aura Lumen Object Store – Packaged Tools is subject to the applicable license agreement(s) for Aura Lumen Object Store located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura Lumen Object Store – Packaged Tools constitutes the Customer's acceptance of such license(s).

Aura Licensed Analytics: Aura Licensed Analytics is a centralized analytics and reporting tool, which provides the logging interface for the components of the Customer's CDN that have been licensed by Akamai. Access to Aura Licensed Analytics is included with Aura Lumen CDN. The software used to provide the Aura Licensed Manager is subject to the applicable license agreement for Aura Lumen CDN located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura Lumen CDN constitutes the Customer's acceptance of such license.

Aura Licensed Manager: Aura Licensed Manager is the centralized element management console for the components of the Customer's CDN that have been licensed by Akamai, and allows for resource provisioning, traffic engineering, feature deployment, element monitoring and real-time monitoring and performance tuning. The Aura Licensed Manager also provides support for multi-tenant CDN services, via partitioned, role-based user control. Aura Licensed Manager is included with Aura Lumen CDN. The software used to provide the Aura Licensed Manager is subject to the applicable license agreement for Aura Lumen located at www.akamai.com/product/licenses, and the Customer's purchase and use of Aura Lumen CDN constitutes the Customer's acceptance of such license.

AURA SPECTRA SERVICES:

Aura Spectra Services: Aura Spectra is a software-as-a-service CDN solution suite offered to Customers that are Operators and is comprised of the following components: Aura Edge eXchange, Aura Edge eXchange Hardware and the SaaS-based components of the Aura Control System (i.e., the Aura Control Plane and the Luna Control Center). Use of the Akamai network in connection with Aura Spectra is subject to Akamai's acceptable use policy located at www.akamai.com/html/policies/index.html. Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or distributes using Aura Spectra.

Aura Edge eXchange (or "AEX"): A software-as-a service CDN solution dedicated for Customer's use and intended to enable delivery of video content and an Aura Customer's retail CDN services to such Customer's subscribers and customers. The Aura Edge eXchange enables the delivery of certain Akamai Sola Sphere Services and Sola Vision Services to the extent set forth in the applicable Transaction Document. As a software-as-a-service, the AEX platform is owned and maintained by Akamai. Use of the AEX is subject to Akamai's acceptable use policy located at www.akamai.com/html/policies/index.html. Customer acknowledges and undertakes all responsibilities for all content and applications it transmits or distributes using AEX. Usage of the Aura Edge eXchange is based on a monthly usage commitment of Gbps measured on the basis of either 95/5 or a fixed peak capacity of aggregate bandwidth throughput. Usage in excess of Customer's monthly usage commitment will overflow to the AEX deployed for Customer subject to the usage rate for overage mutually agreed by the parties and subject to capacity availability. Akamai makes no capacity guarantees, and reserves the right to limit, Customer's usage of the AEX in excess of Customer's usage commitment. Unless otherwise agreed in writing by the parties, Akamai shall have no obligation to deliver Customer traffic via the Akamai Intelligent Platform. Aura Enhanced Support for AEX is included with the purchase of AEX.

Aura Edge eXchange Hardware: A hardware Server that is deployed in an Operator's CDN to enable delivery of the AEX. Unless otherwise agreed in writing by the parties, the Aura Edge eXchange Hardware shall remain at all times owned by Akamai.

Aura Control Plane: A SaaS-based management and reporting tool as part of the Aura Control System for Customers of Aura Spectra that provides capabilities to monitor traffic delivered by the Aura Edge eXchange and Akamai Accelerated Network Program (AANP) nodes (if any).

AURA SUPPORT SERVICES:

Aura Support Requests: Service support calls or online support tickets initiated by an Aura Customer where the underlying issue is determined to reside in Customer's host environment (not in the Aura CDN Solution or the Akamai Network) are outside the scope of support. Additional Aura Support Requests beyond those included in the Aura Enhanced Support Service package may be subject to Akamai's standard rates.

Aura Severity Levels: The following is a guide for assigning appropriate severity levels for Aura Support Requests:

Severity Level	Impact	Description
Severity 1 ("S1")	Critical	Catastrophic impact to business operations. The Aura CDN Solution is significantly impaired and unavailable to multiple user locations. Example of Severity 1 issues include: - Aura CDN Solution is down causing end-users to experience a total loss of service. - Continuous or frequent instabilities affecting traffic-handling capability on a significant portion of the network/system - Creation or existence of a safety hazard.
Severity 2 ("S2")	High	Significant impact to business operations. Repeatable inability to use the applicable Aura CDN Solution. Example of Severity 2 issues include: - Network or system event causing intermittent impact to end-users. - Loss of redundancy - Loss of routine administrative or diagnostic capability
Severity 3 ("S3")	Low	Limited impact to business operations. Non-urgent matter or information request. Example of Severity 3 issues include: - Issues seen in a test or pre-production environment that would normally cause adverse impact to a production network. - Information requests - Clarification of documentation.

AURA Enhanced Support: Included for the applicable Aura Lumen Software licensed hereunder and for Aura Spectra Services solely to the extent Aura Enhanced Support has been purchased pursuant to an applicable Transaction Document. Aura Enhanced Support includes access to all of the following:

- Self-service configuration tools (where available)
- Named technical support account team
- Live support during regular business hours for S2 and/or S3 issues
- Live 24x7X365 support for S1 issues
- Multiple ways to contact Akamai's support team
    - E-mail: E-Mail address to be provided prior to product install
    - Online: Web address to be provided prior to product install
    - Phone: 1-877-4-AKATEC (1-877-425-2832) or 1-617-444-4699

- Online troubleshooting/diagnostic tools
- Includes Aura Lumen Software Updates and Upgrades, subject to any exclusions and limitations set forth in the applicable Terms & Conditions.
- Enhanced Initial Response Times from the Akamai technical support team
    - Thirty (30) minutes beginning after Customer notifies Akamai of S1 issue by phone
    - Two (2) hours beginning after Customer notifies Akamai of S2 issue by phone
    - One (1) business day or less for S3 issues
      All Aura Support Requests reported via e-mail will be considered as S3

Aura Operational Support Guide
Akamai will provide Customer an operational support guide covering Aura Enhanced Support procedures, including escalation.

AURA HARDWARE:

Aura Hardware: The following products sold by Akamai in connection with the license of Aura Lumen Software:

Aura Hardware: MDS108-AC-32-G8-8SFF-QTX Media Delivery Server

1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 8 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-AC-32-G8-10SFF-QTX Media Delivery Server

1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 10 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-AC-64-G8-8SFF-QTX Media Delivery Server

1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 8 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-AC-64-G8-10SFF-QTX Media Delivery Server

1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 10 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-DC-32-G8-8SFF-QTX Media Delivery Server

1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 8 FF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-DC-32-G8-10SFF-QTX Media Delivery Server

1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 10 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-DC-64-G8-8SFF-QTX Media Delivery Server

1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 8 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS108-DC-64-G8-10SFF-QTX Media Delivery Server

1RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 10 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-AC-32-G8-16SFF-QTX Media Delivery Server

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 16 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-AC-32-G8-25SFF-QTX Media Delivery Server

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 25 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-AC-64-G8-16SFF-QTX Media Delivery Server

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 16 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-AC-64-G8-25SFF-QTX Media Delivery Server

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 25 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-DC-32-G8-16SFF-QTX Media Delivery Server

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 32GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 16 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-DC-32-G8-25SFF-QTX Media Delivery Server

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 25 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-DC-64-G8-16SFF-QTX Media Delivery Server

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 16 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-DC-64-G8-25SFF-QTX Media Delivery Server

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 25 SFF disk cage. Disk storage sold separately.

Aura Hardware: MDS216-AC-64-G8-8LFF-QTX Media Delivery Server (Object Store Server)

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 8 LFF disk cage. LFF Disk storage sold separately.

Aura Hardware: MDS216-AC-64-G8-12LFF-QTX Media Delivery Server (Object Store Server)

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x AC Power Supplies, 4x 1Gbe ports (embedded), 12 LFF disk cage. LFF Disk storage sold separately.

Aura Hardware: MDS216-DC-64-G8-8LFF-QTX Media Delivery Server (Object Store Server)

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 8 LFF disk cage. LFF Disk storage sold separately.

Aura Hardware: MDS216-DC-64-G8-12LFF-QTX Media Delivery Server (Object Store Server)

2RU Server w/ Dual Quad-Core Intel Xeon Processor E5-2620, 64GB Memory, 2x DC Power Supplies, 4x 1Gbe ports (embedded), 12 LFF disk cage. LFF Disk storage sold separately.

Aura Options: Network Interfaces and Transceivers

Aura Interface Hardware 2x10NIC w/XCVR's, SFP-SR (mm): MDS-2XGE-SFP-SR

Adds 2x 10 Gbe ports to 4x embedded 1Gbe ports. Ships with two SFP+ short range transceivers. Transceivers support up to 300m on a multi-mode fiber.

Aura Interface Hardware 2x10NIC w/XCVR's, SFP-SR (mm): MDS-2XGE-SFP-LR

Adds 2x 10 Gbe ports to 4x embedded 1Gbe ports. Ships with two SFP+ long range transceivers. Transceivers support up to 10km on a single-mode fiber.

Aura Options: Storage

Aura 1TB Hard Disk Drive: MDS-1000-SATA-G8-SFF-HDD

1TB 2.5 SATA 7200 RPM HDD Storage Expansion

Aura 500GB Hard Disk Drive: MDS-500-SATA-G8-SFF-HDD

500GB 2.5 SATA 7200 RPM HDD Storage Expansion

Aura 500GB Hard Disk Drive: MDS-500-SATA-G8-LFF-HDD

500GB 3.5 SATA 7200 RPM MDL HDD Storage Expansion (only to be used in Object Store configurations)

Aura 3TB Hard Disk Drive: MDS-3000-SATA-G8-LFF-HDD

3TB 3.5 SATA 7200 RPM MDL HDD Storage Expansion (only to be used in Object Store servers)

Aura Storage Expansion Disk Shelf: MDS2600-G8-SHELF

2RU Disk Enclosure. LFF Disks sold separately

Aura 3TB Hard Disk Expansion Drive: MDS-3000-SATA-OBJ-HDD

3TB 3.5 SATA 7200 RPM MDL HDD Storage Expansion only to be used in Disk Expansion Shelf (not G8 servers)

Aura Accessories & Parts:

Aura Advanced iIO License: MDS-ILO-ADV-RTU

Aura Hardware Parts - 10GbE SFP, 10GBASE-SR, 850 nm optical: SFP-10G-SR-HP

Aura Hardware Parts - 10GbE SFP, 10GBASE-LR, 1310 nm optical: SFP-10G-LR-HP

Aura Spare 460W AC Power Supply: MDS108-AC

Aura Spare 1200W DC Power Supply: MDS108-DC

Aura AC Power Cable, AU, 10A/250V, Type AS/NZ 3112-1993: CBL-PWR-AU

Aura AC Power Cable, CH, 10A/250V, Type GB 2099.1: CBL-PWR-CH

Aura AC Power Cable, EE, 10A/250V, Type CEE(7) VII: CBL-PWR-EU

Aura AC Power Cable, IT, 10A/250V, Type CEI 23-16/VII: CBL-PWR-IT

Aura AC Power Cable, JP, 15A/125V, Type JIS 8303: CBL-PWR-JP

Aura AC Power Cable, NA, 15A/125V, Type NEMA 5-15: CBL-PWR-NA

Aura AC Power Cable, UK, 10A/250V, Type BS 1363A: CBL-PWR-UK

Aura Hardware Limited Warranty Support: Warranty support for Aura Hardware is provided by the third party manufacturer ("Hardware Manufacturer") or an authorized service provider thereof subject to the base limited warranty statements by Hardware Manufacturer accompanying the relevant Aura Hardware, if, where and to the extent applicable. Customer can view, print, or download the global limited warranty and technical support statement for any Hewlett Packard Company ("HP") ProLiant and X86 servers and options which are included in the Aura Hardware at http://h18004.www1.hp.com/products/servers/platforms/warranty/index.html, or a successor website.

Aura Hardware Customer Responsibilities: If the Aura Hardware fails and the suggestions in product documentation do not solve the problem, Customer must contact the Akamai technical support team before contacting the Hardware Manufacturer to properly analyze the cause of the problem. The Hardware Manufacturer is not required to respond to, or supply warranty support for, requests or contacts initiated directly by Customer to Hardware Manufacturer. Customer must be prepared to provide to Akamai's technical support team: (a) the product serial number, model name, and model number; (b) applicable error messages; (c) add-on options; (d) operating system; (e) information about any relevant third party hardware or software, and (f) answers to detailed questions, if any. If Akamai determines that the problem is hardware-related, Akamai will advise the Customer thereof and log a service incident with the Hardware Manufacturer, to the extent permissible under Hardware Manufacturer's warranty and technical support policies. Thereafter, Akamai will use commercially reasonable efforts to act as a point of contact with Hardware Manufacturer if requested by the Customer in assisting to process any warranty or technical support claims with Hardware Manufacturer. Customer hereby permits Akamai to discuss information pertaining to Customer's purchase of Aura Hardware with authorized Hardware Manufacturer personnel or service providers, as necessary for Hardware Manufacturer to provide warranty support. In addition, to enable warranty support to be provided, during the applicable limited warranty periods, Customer must:

- Maintain a proper and adequate environment, and use the Aura Hardware in accordance with the instructions furnished.
- Verify configurations, load most recent firmware, install software patches, run Hardware Manufacturer or other diagnostics and utilities, and implement temporary procedures or workarounds provided by Akamai or Hardware Manufacturer while permanent solutions are being worked.
- Allow Akamai and Hardware Manufacturer to modify Aura Hardware to improve operation, supportability, and reliability or to meet legal requirements.
- Allow Akamai and Hardware Manufacturer to keep resident on Customer systems or sites certain system and network diagnostics and maintenance tools to facilitate the performance of warranty support (collectively, "Hardware Manufacturer Proprietary Service Tools"); Hardware Manufacturer Proprietary Service Tools are and remain the sole and exclusive property of Hardware Manufacturer and are third party products. Additionally, Customer will:
    - Use the Hardware Manufacturer Proprietary Service Tools only during the applicable warranty period and only as allowed by Hardware Manufacturer;
    - Install, maintain and support Hardware Manufacturer Proprietary Service Tools, including any required updates and patches;
    - Return Hardware Manufacturer Proprietary Service Tools or allow Hardware Manufacturer to remove Hardware Manufacturer Proprietary Service Tools upon termination of warranty support;
    - Not sell, transfer, assign, pledge or in any way encumber of convey the Hardware Manufacturer Proprietary Service Tools.
- In some cases, Hardware Manufacturer may require additional software such as drivers and agents to be loaded on Customer systems in order to take advantage of these support solutions and capabilities.
- Use Hardware Manufacturer remote support solutions where applicable. Akamai strongly encourages Customer to use available support technologies provided by Hardware Manufacturer. If Customer chooses not to deploy available remote support capabilities, Customer may incur additional costs due to increased warranty support resource requirements.
- Cooperate with Hardware Manufacturer and Akamai in attempting to resolve the problem over the telephone. This may involve performing routine diagnostic procedures, installing additional software updates or patches, removing third party products or other options, and/or substituting options.

- Make periodic back-up copies of Customer files, data, or programs stored on Customer hard drive or other storage device as a precaution against possible failures, alterations, or loss. Before returning Aura Hardware for warranty support, back up Customer files, data, and programs, and remove any confidential, proprietary, or personal information.

- Maintain a procedure to reconstruct lost or altered files, data or programs that is not dependent on Aura Hardware.

- Provide Hardware Manufacturer or an authorized service provider of Hardware Manufacturer with access to the Aura Hardware; and if applicable, adequate working space and facilities within a reasonable distance of the Aura Hardware; access to and use of information, Customer resources, and facilities as reasonably determined necessary by Hardware Manufacturer to service the Aura Hardware.

- Notify Akamai and Hardware Manufacturer if Customer uses Aura Hardware in an environment that poses a potential health or safety hazard to Akamai and/or Hardware Manufacturer employees or subcontractors. Akamai or Hardware Manufacturer may require Customer to maintain such products under supervision of Hardware Manufacturer and may postpone warranty service by Hardware Manufacturer until Customer remedies such hazards.

- Operate Aura Hardware within any maximum usage limits set forth in Hardware Manufacturer's operating manual or technical data sheets.

- Connect Aura Hardware with cables or connectors that are compatible and pre-qualified or otherwise approved by Akamai.

- Not make any modifications to the Aura Hardware.

- Implement any mandatory changes developed for Aura Hardware or third party products included therein promptly upon notice from Akamai or the applicable third party manufacturer. Mandatory changes are those reasonably designated as mandatory because they address safety, data integrity or legal issues.

- Notify Akamai in writing of any changes to the Customer location of the Aura Hardware, including: order number, product serial numbers, complete physical address of the location of the applicable equipment, Customer contact name at such location. Relocation of Aura Hardware may result in additional fees and reasonable advance notice to Hardware Manufacturer may be required to begin any warranty support after relocation.

- Maintain a list of Aura Hardware under warranty, including the location of the Aura Hardware, serial numbers, the Hardware Manufacturer's-designated system identifiers, and coverage levels. Customer shall keep the list updated during the applicable limited warranty period.

- Designate a reasonable number of callers, as determined by Akamai and Customer, who may contact Akamai's technical support team for the initial report of a hardware problem, or Hardware Manufacturer once an incident has been logged with Hardware Manufacturer by Akamai. Designated callers must be generally knowledgeable and demonstrate technical aptitude in system administration, system management, and if applicable, network administration and management and diagnostic testing. Designated callers must have a proper system identifier.

- Perform additional tasks as defined within each type of warranty service described in the applicable Hardware Manufacturer's limited warranty statements, and any other actions that Hardware Manufacturer or Akamai may reasonably request in order for Hardware Manufacturer to best perform warranty support.

Aura Hardware Customer Self Repair Parts: Warranty repairs may be accomplished, at Hardware Manufacturer's sole discretion, remotely, by the use of a Customer Self Repair (CSR) part, or by a service call at the location of the defective unit. Warranty service terms, service availability, and service response times may vary from country/region to country/region. Customer Self Repair parts are defined by Hardware Manufacturer at: http://h18033.www1.hp.com/support/selfrepair/ww/replace_part.asp?myinc=e003a, or successor website.

Replacement of CSR parts for which Customer self-repair is mandatory must be performed by Customer. If Customer requests Akamai to request Hardware Manufacturer to repair these parts or Customer directly requests Hardware Manufacturer to repair these parts, Customer will be charged additional fees, for travel and labor costs.

If Hardware Manufacturer ultimately determines that an on-site service call is required to repair a defect, the call will be scheduled between Customer and Hardware Manufacturer during standard office hours. Standard office hours are typically 08:00 to 17:00, Monday through Friday, but may vary with local business practices. If the location of the defective unit is outside Hardware Manufacturer's customary service zones, response times may be longer and may be subject to travel charges, reduced restoration or repair commitments, and reduced coverage hours. In order to receive on-site warranty support, Customer must:

- Have a representative present when Hardware Manufacturer provides warranty service at the Customer's site.
- Notify Akamai and Hardware Manufacturer if products are being used in an environment which poses a potential health or safety hazard to Akamai and/or Hardware Manufacturer employees or subcontractors.
- Subject to reasonable security requirements, provide Hardware Manufacturer with sufficient, free and safe access to and use of all facilities, information, and systems determined necessary by Hardware Manufacturer to provide timely warranty support.
- Ensure that all manufacturers' labels (such as serial numbers) are in place, accessible and legible.
- Maintain an environment consistent with product specifications and supported configurations.

Response times set forth in the limited warranty statements are measured from when Hardware Manufacturer receives a valid support request from Akamai that is covered by warranty. Warranty support by Hardware Manufacturer does not cover claims resulting from the following: (a) improper use, site preparation, installation, or site or environmental conditions or other non-compliance with the supporting material for the Aura Hardware; (b) modifications to Aura Hardware or improper system maintenance or calibration not performed by Hardware Manufacturer; (c) failure or functional limitations of any non- Hardware Manufacturer software or product impacting systems receiving Hardware Manufacturer warranty support, (d) malware (e.g., virus, worm, etc.) not introduced by Hardware Manufacturer; (e) abuse, negligence, accident, fire or water damage, electrical disturbances, transportation or other causes beyond Hardware Manufacturer control; (f) non-compliance by Customer of the Customer responsibilities set forth above or in any limited warranty statement applicable to the Aura Hardware; and (g) any other exclusion from warranty coverage set forth in the applicable Hardware Manufacturer's limited warranty statement accompanying the Aura Hardware. Any additional services performed for Customer by Hardware Manufacturer that are not covered by the warranty are chargeable at the applicable rates for such services in the country where such service is performed.

HP Software EULA Supplied with Aura Hardware:

Customer acknowledges and agrees that third party products, including third party software or firmware, may be supplied with the Aura Hardware. Third party software or firmware products may be subject to separate license agreements as required by the supplier or manufacturer of such third party products. Use of any HP software supplied with the Aura Hardware is subject to Customer's acceptance of the HP end-user license or program license agreement provided with such software and located at: http://www8.hp.com/us/en/campaigns/prodserv/software-licensing.html, or a successor website (the "HP EULA"). Customer's purchase of Aura Hardware and use of any such HP software in connection therewith constitutes acceptance of the applicable HP EULA, and a legally enforceable agreement directly between HP and Customer. Without limiting the foregoing, Customer may not exceed any use restrictions or authorizations (if any) applicable to such HP software. If no HP EULA is provided with HP software supplied with Aura Hardware, Customer must request a copy, and Akamai or HP will make it available either in writing or for download.

Akamai Aura Hardware Disclaimers: Akamai does not offer any hardware maintenance or hardware technical support service for Aura Hardware, nor any enhancements to limited warranties (if any) provided by original Hardware Manufacturers of third party products included in Aura Hardware. If Customer

requires additional warranties, hardware maintenance or hardware support service not expressly covered or incorporated herein, Akamai recommends Customer should opt to purchase third party hardware qualified by Akamai for integration with Aura Lumen Software directly from the applicable third party manufacturer and/or any additional support services for such hardware offered by a third party. EXCEPT TO THE EXTENT EXPRESSLY SET FORTH HEREIN, AKAMAI EXPRESSLY DISCLAIMS ALL WARRANTIES, REPRESENTATIONS OR COMMITMENTS OF ANY KIND WITH RESPECT TO THE AURA HARDWARE, ANY THIRD PARTY PRODUCT, OR THE SUPPORT THEREOF, WHETHER EXPRESS OF IMPLIED, PAST OR PRESENT, STATUTORY OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING OR USAGE OF TRADE, TO THE FULLEST EXTENT PERMITTED BY LAW, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, TITLE OR SECURITY. THESE TERMS AND CONDITIONS SUPERSEDE ANY PRIOR AGREEMENTS OR REPRESENTATIONS, INCLUDING REPRESENTATIONS MADE IN AKAMAI SALES LITERATURE OR ADVICE GIVEN TO CUSTOMER BY AKAMAI OR AN AGENT OR EMPLOYEE OF AKAMAI, THAT MAY HAVE BEEN MADE IN CONNECTION WITH CUSTOMER'S PURCHASE OF AURA HARDWARE. AKAMAI DOES NOT WARRANT THAT THE OPERATION OF THE AURA HARDWARE WILL BE UNINTERRUPTED OR ERROR-FREE. AKAMAI IS NOT RESPONSIBLE FOR DAMAGE THAT OCCURS AS A RESULT OF CUSTOMER'S FAILURE TO FOLLOW THE INSTRUCTIONS INTENDED FOR THE AURA HARDWARE. THE WARRANTIES FOR THIRD PARTY PRODUCTS INCLUDED IN AURA HARDWARE ARE EXPRESSLY SET FORTH IN THE EXPRESS LIMITED WARRANTY STATEMENTS OR TERMS AND CONDITIONS ACCOMPANYING SUCH PRODUCTS AND NOTHING HEREIN SHALL BE CONSTRUED AS CONSTITUTING AN ADDITIONAL WARRANTY, REPRESENTATION OR OBLIGATION OF AKAMAI.