Akamai Service Terms of Use

I. General Service Terms

These terms apply to the purchase and use of Akamai's products and services, including without limitation professional services and support, ("Services") and shall be deemed incorporated into the Agreement between you (the customer, reseller, or partner, i.e. the "Customer") and Akamai. Service descriptions, billing methods, and technical requirements applicable to the Services (collectively "Service Documents") are accessible via http://www.akamai.com/service and the Akamai customer portal. Akamai may terminate or modify any Service and corresponding Service description if the termination or modification is generally applicable to all Customers. In the event of such a termination or modification of a Service, Customer may terminate the applicable Transaction Document without termination charge if, as a result of such changes, Customer experiences a material decrease in the functionality of the affected Service and Akamai fails to remedy the decrease in functionality within thirty days of written notice from Customer. Capitalized terms used but not defined herein shall have the meanings ascribed to them in Akamai's Terms & Conditions, Customer's Agreement, and/or Service Documents.

Service Delivery

For Professional Services and support Services, Service delivery is evidenced by Customer's ability to submit to Akamai a request for the relevant level of support. For all other Services, Service delivery is evidenced by (i) the provisioning of Akamai customer portal access credentials to Customer and (ii) the ability of either Customer or Akamai to configure and/or deploy an initial Service configuration. As detailed in Customer's Agreement and/or applicable Service Documents, certain Services include limitations or entitlements as to the types or quantities of sites, applications, URLs, networks, domains or other digital properties, usage, attacks, security control combinations and configurations, and/or other services with which the Services can be provided. Customer's use of Services alone does not guarantee conformity with any compliance standard, and Customer is responsible for deploying and configuring Services in a manner that meets applicable compliance standards. Services not explicitly labeled as compliant with a compliance standard (e.g. "PCI compliant") are not compliant with that standard; and, subject to data protection terms agreed upon by Customer and Akamai, Customer assumes all liability associated with using Services to transmit, process, or store data in a manner that contravenes a compliance standard. Customer's use of a Service is subject to the corresponding SLA, which is available in the Akamai customer portal or otherwise incorporated into Customer's Agreement.

Akamai provides no guarantee or warranty that Services shall be delivered from within any specified geography; and, unless specified otherwise in Customer's Agreement, Services may be delivered from any geography or point of presence that Akamai determines to be appropriate for performance and availability purposes. The geo-blocking/filtering capabilities included with a Service do not prevent or eliminate access via anonymous proxy or anonymizing VPN, and there is no guarantee that the IP addresses accurately reflect country boundaries. Akamai shall not be liable to Customer or any third party for acts of a government authority or network provider – including without limitation new or modified laws or regulations or efforts to filter, block, alter, throttle, or otherwise damage data or traffic sent with the use of a Service – that, in Akamai's reasonable discretion, prevent or make infeasible, delivery of traffic or provision of Services from, into, or in a specific geography. Unless required by law, Akamai shall not be required to assist Customer with laws, policies, or regulations that apply to Customer's content, services, or business, nor shall Akamai be liable for the disclosure of Customer content or other information to a government authority upon direct inquiry by such authority. Services are delivered in English only.

In using Akamai's Secure Socket Layer ("SSL") network, Customer will configure and maintain its Akamai metadata to use encryption algorithms, key lengths, origin certificate verification, and other applicable metadata. Failure to do so may expose information in the SSL session to a third party. In using Akamai Services, Customer may transmit the following types of information only over the Akamai SSL network and via no other Akamai network: (i) the numbers assigned by card issuers to identify cardholders' accounts and data about card transactions placed by Customer's end-users on Akamai's SSL network; (ii) information

that constitutes Protected Health Information under the Health Insurance Portability and Accountability Act; and (iii) any personally identifiable information entered by a user on a designated portion of Customer's site, application, or other digital property for the purpose of fulfilling a transaction or account access process and which is identified to be replaced by a token pursuant to the configuration defined and approved by Customer in connection with an applicable Service.

Requests not directly related to Customer's use of Akamai Services, the Akamai platform, or the extended use thereof shall be considered out of scope. Unless specified in Customer's Agreement or applicable Service Documents, Services do not include in-person meetings at Customer's facilities, onsite training for Customer by Akamai, or shipping or installation of any hardware or software. For Services designed to test Customer's sites or applications, Customer is, unless explicitly specified otherwise in Customer's Agreement, solely responsible for all costs, expenses, liabilities, and responsibility for testing, including, where applicable, infrastructure, back-up, hosting, telecommunication costs, internal and external internet access, third party cloud services, scripts, generation of native applications, passwords and user account access control. Akamai may charge Customer for traffic bursts or increased usage resulting from Customer's actions or deviation from requirements or suggested procedures, settings, or configurations specified in Service Documents or otherwise conveyed to Customer via Customer's specified contacts. Akamai may limit Customer's use of the Akamai network if a force majeure event beyond Akamai's reasonable control results in extraordinary traffic levels on Akamai's network. Services do not include penetration, performance, or load testing, and neither Akamai nor Customer shall perform such testing or network scanning on the other's environment.

Service Configuration

When Akamai configures Customer's configurations, Customer shall provide all necessary configuration information to Akamai to enable the configurations in advance. Subject to additional parameters specified in Customer's Agreement or applicable Service Documents, configurations may take up to twenty-four (24) hours to become active. For certain on-demand Services, Customer may be required to notify Akamai of the need to re-route traffic or otherwise activate Service functionality. Customer agrees to provide and appropriately update an escalation matrix that includes the names, email addresses, and phone numbers of at least three (3) individuals who are authorized and accountable for representing Customer in communicating technical requirements and giving approval for project schedules and milestones and whom Akamai may contact for configuration, support, or security purposes, including data breach incidents. Customer is solely responsible for (i)distributing and managing access control keys and user login credentials associated with Services (ii) ensuring that Customer's origin infrastructure has the capacity required to accommodate any additional load generated by Customer's ordered Services.

As needed to provide Services to Customer, Akamai reserves the right to make, or to require Customer to make, technical configuration changes, which may impact links, URLs, or embedded files deployed by Customer. In implementing such changes, Akamai will adhere to the terms of the relevant Service Documents, and Akamai will provide Customer with reasonable advance notification of any such required changes unless doing so would pose a legal, regulatory, security, or technical risk. Customer shall be solely responsible for Service disruptions that result from Customer's failure to comply with requested configuration changes or implement updates or upgrades to the Service or associated software. For any Service that includes access to emergency security configuration assistance, Customer pre-authorizes Akamai to make customizations and other changes designed to defend against security incidents or address Service-related issues.

Customer shall have the right to use deliverables and work product provided by Akamai to Customer during the term of the applicable Transaction Document; but Akamai shall retain all rights in, and title to, deliverables and work product created while rendering Services. No activity performed in the course of Akamai's rendering Services shall be considered joint development. Customer shall not attempt to reverse engineer, disassemble, decompile, or otherwise discover the source code, trade secrets, or methods of operation of the Services, nor shall it knowingly permit any third party to perform any of the aforementioned activities.

Data

As between Akamai and Customer, Akamai retains all right, title and interest worldwide in the 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 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 and shall have the right to use such data for purposes of providing, maintaining, developing and improving its products and services. 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) user/usage data collected by Akamai from Customer site traffic (which data may not be used to positively identify end users), and (c) Akamai's proprietary information, software, code, technology, and other intellectual property.

Akamai shall have the right to monitor and inspect traffic on the Akamai network, as well as logs related to such traffic, as necessary to provide the Services and to derive and compile information relating to the type, nature, content, identity, behavior, signature, source, frequency, reputation, and other characteristics of Internet traffic and activity to help to identify attacks, malware, viruses, fraud, exploits, and other malicious activity that threatens Akamai customers on the Internet ("Threat Data"). Akamai shall be free to use, distribute, and make derivative works of Threat Data for the purpose of (a) providing, maintaining, developing, and improving the Services offered to Akamai's customers and partners; and (b) assisting in the detection, identification, analysis, mitigation and prevention of fraud and attacks against Akamai customers and partners. If Akamai distributes Threat Data or derivative works incorporating Threat Data, to any third party, such distribution shall not directly identify Customer or its end users. To the extend personal information or personal identifiable information is included in the Threat Data or otherwise processed when Threat Data is generated, Akamai ensures its compliance with applicable data protection laws. Data processing agreements covering the processing of personal information by Akamai when providing its services are available in Akamai's Privacy Trust Center, www.akamai.com/compliance/privacy.

For Services that include a data collection and/or reporting component, Customer acknowledges that (i) data may be aggregated and/or limited to the data available to Akamai in certain jurisdictions and (ii) data collection limits vary across reports and are subject to change at Akamai's discretion. Unless specified otherwise in Customer's Agreement or applicable Service Documents, Akamai does not provide any guarantee for volume, collection rate, or applicability of such data. Additionally, such data (i) is intended solely for assessing media, web and/or security performance, (ii) is for Customer's internal use only, and (iii) constitutes Confidential Information.

Equipment Furnished by Akamai

Akamai is not responsible for Customer or third party charges to install and configure Akamai-furnished equipment necessary for Service provisioning ("Akamai Equipment") on Customer's premises. If Akamai installs Akamai Equipment on Customer's premises, Customer shall make available to Akamai at no charge the facilities, rack space, connectivity, and other infrastructure reasonably deemed necessary by Akamai. Akamai Equipment and all technology, operating systems, and software on the Akamai Equipment are and shall remain, as between Akamai and Customer, the sole property of Akamai. Unless specified otherwise in Customer's Agreement or Service Documents, (i) Akamai shall be solely responsible for monitoring, maintaining, and operating Akamai Equipment and related operating systems and software and (ii) Customer shall not (a) operate Akamai Equipment; (b) load or operate any software, programs, or other technology or functionality on Akamai Equipment; (c) remove, open, modify, interfere or interconnect with, or otherwise attempt to gain access to Akamai Equipment or Akamai systems, software, or technology deployed thereon or used therewith; or (d) permit a third party to do any of the foregoing. Customer shall permit Akamai's employees and agents, upon reasonable notice to Customer, to enter Customer's facilities to monitor and/or maintain Akamai Equipment. Unless specified otherwise in applicable Service Documents, Customer shall also provide Akamai remote access to Akamai Equipment twenty-four (24) hours per day, seven (7) days per week. Customer shall use reasonable care to protect Akamai Equipment from loss, damage, destruction, and other harm. If Customer violates Akamai's intellectual property rights in Akamai Equipment or the related software, Akamai may terminate the Agreement immediately and seek any other available remedies. If Customer does

not return Akamai Equipment within thirty (30) days of termination or expiration of the corresponding Transaction Document, Customer shall pay a per-device replacement fee reasonably determined by Akamai based on applicable market rates and shall remain obligated to immediately return the Akamai Equipment to Akamai. Customer shall have no option to purchase Akamai Equipment.

Software

Any application programming interface, software development kit, or other software component ("Akamai Tools") provided by Akamai for use with a Service constitutes Akamai intellectual property that is licensed, not sold, to Customer. Akamai hereby grants Customer a nonexclusive, non-transferable, non-sublicensable, worldwide license to use Akamai Tools solely to access and use the corresponding Services. Akamai Tools may be subject to additional terms that accompany the Akamai Tool; and, by accessing and/or using any such Akamai Tool, Customer accepts the license terms. Customer shall not use Services, including without limitation Akamai Tools, to track end users across non-Customer owned sites.

Non-Akamai Products and Services

Unless specified otherwise in Customer's Agreement, Customer shall be solely responsible for the installation, maintenance, and support of appliances, hardware, software, and services acquired from third parties. If Customer relies on a third party to manage Services, Customer shall provide Akamai with a delegated point of contact for such third party. Customer authorizes Akamai to provide the third party with all access and information required by the third party to manage the Services. Customer acknowledges and agrees that third party products, software, and services may be subject to separate license agreements, warranties, or other terms and conditions provided or required by the supplier or manufacturer of such third party offerings. Customer's use of a non-Akamai service, product, or application is subject to the provider making it available for interoperation with the relevant Akamai Service.

If Akamai provides support in connection with third party warranties, such support may be contingent upon Customer's continued compliance with requirements outlined in applicable Service Documents, the subject third party products or services, and/or Customer's efforts to address problems implicating the third party provider's warranty and technical support policies directly with such third party. For Services used with non-Akamai products or services, Customer acknowledges that its obligation to pay Akamai for the Akamai component of a combined solution is independent of the performance of any third party component or service. Additionally, for Services that integrate with, collect data from, or otherwise operate in concert with non-Akamai products or services, Customer represents and warrants that it has an active contract with the authorized provider of the relevant products and/or services.

II. Delivery Services

General

As detailed in Service Documents, certain media Services require the purchase of a compatible delivery Service. For Services that apply Akamai's protocol downgrade feature, protocol downgrade capabilities may not be used for any data that exposes personally identifiable information. Additionally, with Akamai's protocol downgrade feature, only HTTPS connections terminated using Standard TLS certificates will be allowed to be downgraded to HTTP, and connections terminated using Enhanced TLS certificates will not be allowed to be downgraded. No protocol downgrade will be applied on Akamai's PCI Standard compliant network. Customer assumes all liability for information transferred using a Service's protocol downgrade capabilities. For Services that deliver, store, or otherwise manipulate encrypted media, the level of encryption may impact playback performance depending on Customer's system. NetStorage Customers acknowledge that the associated file transfer protocol is insecure and that use of this protocol may leak access credentials and data transmitted. Akamai cannot improve the original quality of video submitted to Services and, unless specified otherwise in a Service Document, Akamai shall not be responsible for video quality degradation that may result from the use of certain media Services.

Services designed to accelerate and/or improve media delivery may consume end users' device resources and/or increase end users' network and data usage on end users' network service plans. Any Customer application incorporating such a Service and any Customer website accessible via a supported browser must include terms describing the applicable Service for notice to and acceptance by Customer's end users and viewers. Although the following does not constitute legal advice, such terms should be comparable to the following: THIS APPLICATION OR WEBSITE USES AKAMAI'S [SERVICE NAME]. BY ACCESSING THIS APPLICATION OR WEBSITE, YOU UNDERSTAND AND AGREE THAT AKAMAI MAY EMPLOY THE USE OF MULTICAST TECHNOLOGY AND TECHNOLOGY TO FACILITATE MEDIA DISTRIBUTION DIRECTLY BETWEEN END USERS, USING THE END USERS' IP ADDRESSES, FOR PURPOSES OF IMPROVING VIDEO QUALITY FOR END USERS AND REDUCING NETWORK TRAFFIC. AKAMAI'S [SERVICE NAME] MAY USE END USERS' DEVICE RESOURCES, SUCH AS CPU, STORAGE, AND BANDWIDTH, AND MAY INCREASE NETWORK AND DATA USAGE ON END USERS' NETWORK SERVICE PLANS. ADDITIONALLY, IF USE OF THE [SERVICE NAME] TECHNOLOGY IS DEPENDENT UPON THE USE OF A CPU, STORAGE, BANDWIDTH, AND/OR DATA PLAN OWNED OR CONTROLLED BY A THIRD PARTY, YOU ACKNOWLEDGE AND AGREE THAT YOUR LICENSE TO USE THE [SERVICE NAME] TECHNOLOGY IS SUBJECT TO YOUR OBTAINING CONSENT FROM THE RELEVANT THIRD PARTY FOR SUCH USE. YOU REPRESENT AND WARRANT THAT, BY ACCEPTING THESE TERMS, YOU HAVE OBTAINED SUCH CONSENT.

When Akamai supplies IP addresses to Customer, Customer must acknowledge receipt of the IP addresses within ninety (90) days of notification by Akamai. If Customer fails to do so, Akamai will continue to serve the traffic covered by the base Service; but Akamai shall no longer provide any commitment regarding the performance of the base Service or the relevant access control module, and degradation of the base Service (including performance against the applicable SLA) may occur. If Customer fails to provide acknowledgement within one hundred eighty (180) days of notification, Akamai may degrade Customer to a different server map and charge Customer's then-current usage rate for a custom server map over and above the existing charges, which shall continue to apply. The new custom server map may also have degraded performance from the up-to-date IP addresses supplied by Akamai. Akamai reserves the right to reclaim IP addresses when it determines that Customer is no longer using them. Akamai will notify Customer in advance before reclaiming IP addresses. Once Akamai notifies Customer of its IP address reclaim, Customer shall be solely responsible for ensuring that the IP addresses are no longer in use by its service providers, and Akamai shall not be responsible for any liabilities arising out of continued use of reclaimed IP addresses.

For Services that involve identification and/or detection of mobile devices, the matching mechanism to identify or detect mobile devices at the edge, as well as the database of related characteristics, are defined and updated periodically by Akamai, at Akamai's sole discretion. Customer acknowledges that there are no guarantees around specific device inclusion in such mechanisms or data accuracy or breadth in the database. Customer is prohibited from (i) accruing any device data added by Akamai to HTTP headers except in logs for Customer's internal analysis and debugging purposes and (ii) publishing any device data added by Akamai to HTTP headers.

China CDN and Russia CDN

Akamai reserves the right to limit or restrict the amount of traffic purchased for delivery via Akamai's Russia CDN and/or China CDN Services. Customers using Akamai's Russia CDN and/or China CDN Services shall comply with all applicable laws in Russia and/or China, including without limitation: (i) laws that address the storage of any personal information inside Russia and/or China; and (ii) registration requirements for .ru and/or .cn sites. Customer agrees to supply Akamai with all documentation or registration-related information (including origin IP addresses) reasonably requested by Akamai. Akamai provides no guarantee or warranty that the Russia CDN Service or China CDN Service shall be delivered from within Russia or China, respectively. Akamai may deliver all or part of the China CDN Service with the use of third party suppliers, which may collect their own log files.

Miscellaneous

Akamai resellers and participants in Akamai's Net Alliance Program must enter into a written agreement with each subcustomer of Akamai's Cloud Embed Service binding the subcustomer to an acceptable use policy no less stringent than Akamai's Acceptable Use Policy. IoT Edge Connect is provided "as is", and Customer acknowledges that IoT Edge Connect is not designed or intended for use or resale in situations requiring fail-safe performance where the failure of IoT Edge Connect could lead to death, personal injury, or physical or environmental damage.

III. Security Services

Customer acknowledges that the Services do not prevent or eliminate all attacks or security threats. Akamai may, without notice, make changes to a Service's application layer controls at Akamai's sole discretion. If necessary to apply application layer rule exceptions to Customer's configuration to facilitate an update, Customer shall provide support as needed by Akamai in an expedient fashion so that Akamai can implement necessary changes. Customer authorizes Akamai to impose technical measures available in the Services in order to control or otherwise mitigate DDoS attacks. Measures taken to address DDoS attacks may result in degraded application and/or site performance; and, for Customers that order Akamai's DDoS Fee Protection Service, Service Level Agreements associated with the underlying DDoS mitigation Service do not apply during the period of a DDoS attack that implicates the credits associated with the DDoS Fee Protection Service. With respect to Akamai's Prolexic Service (the GRE or Connect options), Akamai reserves the right to rate limit above the associated Committed Information Rate, as defined in the Akamai Services Page.

In the course of consuming or providing Services, as applicable, Customer or Akamai may report or identify events causing suspicion of an actual or anticipated application level or denial of service attack. Whether any such event constitutes an attack shall be determined solely by Akamai. AKAMAI DOES NOT WARRANT OR GUARANTEE THAT: (I) THE SERVICES WILL DETECT OR MITIGATE ALL POSSIBLE ATTACKS, BOT REQUESTS, OR OTHER THREATS; (II) THE SERVICES WILL CORRECTLY CATEGORIZE AS BOTS ALL DETECTED REQUESTS; OR (III) CLIENT SCORES WILL ACCURATELY REPRESENT A CLIENT THREAT LEVEL. AKAMAI RECOMMENDS ALL CUSTOMERS MAINTAIN APPROPRIATE SECURITY CONTROLS AT THEIR ORIGIN SERVERS AND DATA CENTERS.

IV. Analytics Services

Certain data that Customer receives in connection with its use of analytics Services may consist of elements, e.g. client IP addresses, that are categorized as personal information under data protection laws. Customer shall comply with applicable data protection laws when processing personal information. Customer shall not use Services to develop or provide a product or service that competes with one or more of Akamai's Services.

V. Professional Services and Support

For Services that involve pre-provisioning, configuration assistance, a managed service component, or other support or professional service function (collectively "Support") to be performed or managed by Akamai, the scope of Support will be established in the Customer's Agreement and applicable Service Documents. For changes to the agreed scope of Support, Akamai and Customer will execute a change order specifying the additional work to be performed by Akamai. Unless specified otherwise in the Customer's Agreement and/or Service Documents, Standard Support is included with all Services. Akamai's obligations to perform Support are contingent upon Customer's allowing Akamai, as needed, to install updates and access (either remotely or otherwise) computer systems, software, and data. Support is, unless specified otherwise in Customer's Agreement or applicable Service Documents, provided at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

An additional emergency integration fee may be applied if all or part of a standard or managed integration must be completed on less than ten (10) business days' notice. Emergency integrations are subject to

resource availability, and must be reviewed and approved by Akamai on a case by case basis. Each Customer relying on self-service integration acknowledges that, although technical support will be available at the level purchased by Customer, Akamai technical support does not provide integration services.

Unless specified in applicable Service Documents, Akamai does not provide any service level agreement for managed delivery services or managed integration services, warrant or guarantee that such services will detect or mitigate all possible changes adversely impacting end user experience, or make recommendations for potential performance improvement. Customer acknowledges that Support does not prevent or eliminate all possible attacks or threats. For persistent attacks or security incidents outside the scope of the applicable security product, Akamai may declare security event management complete without successful mitigation, in which case other Services may be required to continue attempts to mitigate the malicious activity.

VI. Carrier Services

The Aura Operator Portal is a SaaS-based management and reporting tool for Customers of Akamai's Aura Managed CDN (MCDN) Services. Use of the Aura Operator Portal is subject to the Customer's agreement with Akamai for Akamai Accelerated Network Program or Aura MCDN, as the case may be. Information provided by or on behalf of Akamai via the Aura Operator Portal is for internal use only and shall be treated as Akamai confidential information subject to the confidentiality obligations in effect between Akamai and Customer.