verizon

DDoS Shield for Internet Dedicated Services
Service Level Agreement

1. **Overview**. This Service Level Agreement ("SLA") defines the service metrics which Verizon strives to meet in the delivery of DDoS Shield for Internet Dedicated Services and the credits Customer is eligible to receive if those metrics are not met. This SLA sets forth Customer's sole remedies for any claim relating to failure to meet any standard set forth in this SLA. Verizon's records and data will be the basis for all SLA calculations and determinations.

2. **Claims**. To receive a remedy under this SLA, Customer must notify Verizon within 40 business days of an SLA metric having not been met, with the exception of Clause 4.3 (Filtered Mitigation) where the Customer must notify Verizon within five calendar days of an SLA metric having not been met. No Service Credits will be issued if Customer does not notify Verizon within the five-day period. Verizon will verify any requested Service Credit and will confirm the amount of the credit, if applicable. Verizon's Service Credit calculation is the final and definitive assessment of any credit payable. If a number of unmet service metrics arise out of the same SLA failure, Customer will be entitled to the highest value Service Credit for one unmet metric. The total number of Service Credits for any cumulative SLA failure may not exceed the MRC.

3. **Credits**. Customer has the right to receive credits ("Service Credits") in case Verizon fails to meet such metrics. The SLA will become effective when Verizon has issued the Verification Notice except Installation SLA items which become active upon Verizon's acceptance of Customer's configuration submission. During any calendar month that the metrics set forth below are not met, Customer may be eligible for one Service Credit. Subject to Section 2 above, each subsequent SLA violation will result in an additional Service Credit. Each Service Credit is equal to 10% of the MRC. If Customer receives more than four Service Credits in three consecutive months or 10 Service Credits in a single month, the customer shall have the right to terminate its Contract for DDoS Shield for Internet Dedicated Services without liability on written notice to Verizon.

4. **DDoS Shield for Internet Dedicated Services SLA Metrics**

4.1 **Installation**. Verizon will perform standard installation within 10 business days of an approved order or the Internet Dedicated Services being made available to Customer, whichever is later.

4.2 **Availability of Service**. DDoS Shield for Internet Dedicated Services will have 99.999% availability to mitigate DDoS attacks.

4.3 **Time to Filtered Mitigation**

4.3.1 **Service activation**. Within 15 minutes of receiving a request from a Customer, Verizon will activate BGP redirection of the Customer's inbound traffic to Verizon's DDoS Shield for Internet Dedicated Services mitigation platform.

4.3.2 **Mitigation**. Within 30 minutes after Customer's inbound traffic being redirected to the Verizon DDoS Shield for Internet Dedicated Services mitigation platform, Verizon will initiate mitigation of inbound DDoS attack traffic.

4.4 **BGP Routing Change**. Verizon will announce Customer's BGP route changes, for pre-configured IP ranges, to the Internet within 15 minutes after Verizon's receipt of Customer's request for such routing change.

4.5 **Availability of DDoS Shield Portal**. The Service Portal will have 99.9% availability, and the DDoS detection and mitigation capabilities will remain available.

4.6 **Customer Activated BGP Redirection**. If used, within 5 minutes after Customer's Inbound Traffic is fully redirected to the Verizon DDoS Shield mitigation platform, Verizon will mitigate any DDoS attack traffic as Customer pre-specified in the policies in the DDoS Shield Portal. This mitigation under such Policies will ensure that no more than 5% of malicious attack traffic will be passed to Customer endpoint(s), based on the preconfigured rules. Customers should notify Verizon of the attack (phone or via portal) to ensure that any additional countermeasures are configured as required. In order for customer-activated BGP redirection to function, the customer must either: 1) peer with Verizon Route Servers as per the BGP Peers section of the portal; or 2) start a redirection of type "Under Attack" via the DDoS Shield portal.

4.7 **Phone Activation**. Within 15 minutes after receiving a telephone request from a Technical Point of Contact, Verizon will perform Verizon activated BGP redirection of the Customer's inbound traffic to Verizon DDoS Shield mitigation platform. Verizon will mitigate any DDoS attack traffic to the traffic levels mutually agreed upon by Customer and Verizon during provisioning. This mitigation will ensure that no more than 5% of malicious traffic will be passed to Customer endpoint(s), based on the preconfigured, mutually agreed rules.

4.8 **Ongoing Mitigation Tuning**. During the duration of active DDoS attack, Verizon DDoS Operations will perform ongoing tuning of needed mitigation perimeters to ensure total malicious traffic returned to Customer endpoint(s) does not exceed 5% defined in 4.6.

5. **Exclusions**. The metrics set forth in Section 4 are not applicable in the case of any of the following circumstances:

5.1 Customer provides inaccurate or insufficient configuration information.

5.2 A violation of Verizon's Acceptable Use Policy. The applicable AUP is available at the following URL: https://www.verizon.com/business/terms/ or other URL designated by Verizon. Customer shall ensure that each user of DDoS Security adheres to the AUP. Verizon reserves the right to change the AUP from time to time, effective upon posting of the revised AUP at the designated URL or other notice to Customer.

5.3 Traffic redirection delays due to causes beyond Verizon's reasonable control.

5.4 Non-performance, negligent, unlawful acts or failure to act by Customer, its agents or suppliers.

5.5 Failure of non-Verizon network(s) connected to the Customer's endpoint(s).

5.6 Failure of Customer to implement access control lists (ACLs).

5.7 Failure of Customer to participate in DDoS Security mitigation efforts, including the inability of Verizon to reach Customer by telephone or Customer's failure to make available English-speaking points of contact to coordinate and communicate with Verizon during a DDoS attack.

5.8 Acts of God or events of Force Majeure.

5.9 Scheduled or emergency maintenance.

5.10 Suspension or termination of DDoS Security by Verizon in accordance with the terms of the Contract.

verizon

6. **Maintenance**. Verizon may perform maintenance on its systems at any time, but will limit such maintenance to a maximum of eight hours of scheduled maintenance during any one calendar month and six hours of maintenance during any single maintenance window. Scheduled maintenance may result in Customer's inability to access client side web-based and mobile user interfaces, applications programming interfaces (APIs), or other Customer accessible software, but will not impact Verizon's ability to mitigate DDoS attacks on Customer's behalf. Additionally, Verizon may take an emergency maintenance outage of no more than 4 hours once per month with one-hour prior notice. During all maintenance windows, Verizon DDoS Operations will operationally withdraw the targeted device ensuring minimal traffic impact and the total remaining service platform will remain operational to service any ongoing or newly started mitigation.