

DISTRIBUTED DENIAL OF SERVICE (DDoS) MITIGATION SERVICE

1.0 Service

1.1 Description. Distributed Denial of Service (DDoS) Mitigation Service ("DDoS Service") is an optional service feature that may be acquired and used with various internet access services provided by XO, including Dedicated Internet Access (DIA) Service and others offered with DIA, such as MPLS IP-VPN, SIP and IP Flex (Underlying Internet Access Service"). The option assists customers in lessening potentially damaging denial of service attacks that can occur between a Customer or End User Premises and the public Internet by re-routing, subject to size and duration limitations, specifically, no more than ten (10) GBps or less than forty-eight (48) hours, respectively, Customer or End User traffic to a XO location after XO receives an authorized request from Customer to initiate DDoS Service. XO in its sole discretion may refuse a Customer request for DDoS Service.

1.2 Requirements. In all instances Customer must comply with the configuration recommendation provided by XO to Customer with regard to the use of the Underlying Internet Access Service with which DDoS Service is associated. XO's recommendation will take into account Customer's or End User's Network, Internet configuration, applications and IP addressing scheme. Under no circumstance will XO be liable or otherwise responsible to Customer or others for: (i) any delay, reduction or inability of Customer to obtain access to its Network as a result of Customer's or End User's non-compliance with XO's recommendation; or (ii) any change made by Customer or End User to its Network that has not been communicated to and approved by XO prior to the change being made. In addition, when XO is providing DDoS Service, an outage allowance claim or claim for another SLA remedy or remedies pertaining to the Underlying Internet Access Service will not be entertained if the proximate cause of the claim is in any way related to the deployment of DDoS Service.

2.0 Escalation Procedures. The Parties must comply in all instances with the escalation procedures, if any, applicable to an associated Underlying Internet Access Service.

3.0 Point-of-Termination or Demark. The Point-of-Termination (demark) for DDoS Service is the same as applies to the associated Underlying Internet Access Service.

4.0 Rights and Obligations. Except as modified or supplemented in this herein, each Party's rights and obligations pertaining to DDoS Service are the same as those that apply to the associated Underlying Internet Access Service.

5.0 Customer's Representations and Warranties

5.1 Network Modifications. Customer represents and warrants it will assume all risks, losses and liabilities arising from, or related to, unauthorized changes made to its or its End User's Network, including those involving services provided by XO, if such changes result in a lower level of Customer or End User Network security or unsecured access to its Customer's or End User's Network.

5.2 Service Monitoring. Customer represents and warrants it has acquired and will retain all required consents from third parties that allow XO to access and investigate

information packets constituting Customer's or End User Internet traffic.

5.3 Export Control. Customer acknowledges that the DDoS Service governed by the Agreement is subject to U.S. export laws and regulations and that any use or transfer of the DDoS Service must be authorized under those laws and regulations. Further, use of the DDoS Service outside of the U.S. may subject Customer and/or Customer's End Users to export or import regulations in other countries. Without limiting the foregoing, goods, software or technical data related to the DDoS Service are prohibited for export or re-export to Cuba, Iran, Sudan, North Korea, Syria or foreign nationals thereof, or any other country that is subject to U.S. economic sanctions or comprehensive export controls restricting such export or re-export, as well as to persons or entities barred from engaging in export transactions by the U.S. Departments of Commerce, State or Treasury (see Country Group E at http://www.export.gov/ecr/eg_main_023148.asp, as such list may be updated from time to time). Customer represents and warrants that it will comply with such export controls set forth above. Customer is responsible for notifying its End Users of such restrictions and agrees to be responsible for End Users' use. Customer will not use, distribute, transfer or transmit, directly or indirectly, information or any immediate product (including processes and DDoS Services) utilizing the DDoS Service, except in compliance with U.S. export laws and regulations.

6.0 Limitations of Liability. In addition to the limitations of XO's liability as set forth in Section 3.2 of the General Terms and Conditions and in any applicable Service Exhibit, XO shall not be liable to Customer or others for:

6.1 (i) discarding traffic when an attack exceeds ten (10) GBps or lasts more than forty-eight (48) hours; (ii) discontinuing DDoS Service when XO determines an attack has ended or has not occurred within the past forty-eight (48) hours; or (iii) terminating DDoS Service in its entirety when XO, in its sole discretion, determines Customer is overusing DDoS Service, specifically, using it on a continuous basis or employing it as a precautionary rather than a corrective measure;

6.2 the receipt of any unauthorized traffic or the non-receipt of legitimate traffic; or

6.3 any failure of DDoS Service to detect and prevent other possible threats, vulnerabilities, or security breaches of Customer's or End User's Network.

7.0 Indemnification. Customer shall indemnify, defend and hold XO and its officers, directors, employees, agents, affiliates and suppliers harmless from and against any claims, actions, demands, regulatory or government inquiries, losses, damages and expenses, including attorney's fees, relating to any violation including, but not limited to, a breach by Customer, its End Users, or others of its account or their obligations with regard to DDoS Service, the placement or transmission of any message, information, software or other materials on the Internet by Customer, its End Users or other users of its account, a violation of the AUP, Customer's or End User traffic being processed through XO's switch, port or node, or privacy and data security matters arising from the provision of DDoS Service. This Customer indemnification obligation shall survive the termination of DDoS Service.