DQE Communications LLC

Service Schedule A-4: DDoS Mitigation

The Distributed Denial of Service (DDoS) Schedule ("Service Schedule") is subject to, and made a part of, the Master Service Agreement ("MSA") entered into by and between DQE and Customer. Capitalized terms not defined herein will be the meaning ascribed to them in MSA.

A. Definitions. The following definitions shall apply to DDoS Mitigation Service:

1. **Abuse -** Improper or illegal activity that has a deleterious effect on either DQE Communications network or other DQE customer services is classified as Abuse. The DQE Acceptable Use Policy published and periodically updated on our web site provides a more detailed listing of traffic and activity that is classified as Abuse.

2. **Commencement Date –** The date upon which the Service Activation Notice ("SAN") is delivered to Customer or the Emergency Order was signed and DDoS Mitigation Service began.

3. **Customer Data –** Any information held or maintained by Customer on their systems or network or information stored in off-premise services.

4. **Customer Contact Center (CCC) –** The customer web application portal that DQE maintains to provide information about service and tickets to customers.

5. **Distributed Denial of Service ("DDoS") Attack** – An attempt(s) to make an online service/server unavailable by overwhelming it with traffic from multiple sources.

6. **Distributed Denial of Service ("DDoS") Mitigation Service** – set of tools and techniques for resisting or mitigating the impact of DDoS Attack.

7. **Endpoints –** Customer controlled network device(s) that is receiving traffic on the internet circuit.

8. **Network Operations Center ("NOC") –** DQE's network monitoring and customer call center.

9. **Non-Attack Incident Fee (NAIF) –** fee for use of the DDoS Mitigation Service during a Non-Attack Incident. A "Non-Attack Incident" is when the customer incorrectly or falsely claims a DDoS Attack is underway. This fee shall be 25% of the monthly MRC per Non-Attack Incident.

10. **Per Incident Fee –** Should Customer have more than 25 Incidents in a 12 month period, DQE reserves the right to charge a one-time fee equal to 50% of the Customer's MRC per each additional Incident. An Incident is defined as when the DQE NOC and Customer agree to open a NOC ticket for this Service.

11. **Service –** the DDoS Mitigation Service.

12. **Service Level (SLA) –** The service level applicable to the relevant DDoS Mitigation Service as set out in Section D below.

B. DDoS Mitigation Service Description. DDoS Mitigation Service is a network-based traffic analysis service for mitigating the impact of Distributed Denial of Service (DDoS) Attacks for DQE Internet Customers. DQE will proactively monitor a Customer's internet traffic and assess for a possible DDoS Attack. If DQE identifies a possible DDoS Attack, DQE will proactively contact the Customer to discuss commencing DDoS Mitigation Service. Customer may also contact the DQE NOC to report a DDoS Attack. After DQE and the Customer collectively agree that a DDoS Attack is taking place, DQE will commence the DDoS Mitigation Service. When

system and/or network capacity is exceeded, DQE reserves the right to pass through the Customer's IP traffic without scrubbing the IP traffic. Post-mitigation, DQE will route the Customer's traffic back to standard traffic flow. Once traffic is restored to standard traffic flow, the DDoS Mitigation Service shall be deemed completed and closed.

C. Customer Obligations.

1. Customer must notify the NOC at 877-263-8638 in the event Customer experiences, or anticipates, a DDoS Attack. Upon receipt of notification, the NOC opens a trouble ticket and commences monitoring. The Customer shall notify DQE immediately in the event of a problem or disruption, but not later than 2 hours after the event has started.

2. Customer may opt instead to pre-authorize DQE to monitor and begin DDoS Mitigation Services under specific parameters. Such pre-authorization must occur in writing.

3. The Customer must coordinate with the NOC to determine whether, and to confirm that, a DDoS Attack is taking place, and authorize DQE to begin DDoS Mitigation Service.

4. Customer must provide a list of employees (title, name, mobile phone number and email) to DQE and keep it updated continuously via the CCC portal on who may report a possible DDoS Attack and approve DDoS Mitigation Service.

5. The Customer is responsible for the security of managing network components of customer data environment such as routers, firewalls, databases, physical security, or servers.

6. The Customer accepts and agrees that the Service shall be provided through common and shared infrastructure and should multiple DQE Customer DDoS Attacks occur simultaneously DQE, in its sole discretion, reserves the right to prioritize the order in which Customer's receive DDoS Mitigation Service.

7. Customer acknowledges and agrees that the DDoS Mitigation Service does not prevent or eliminate all DDoS Attacks.

8. Customer acknowledges and agrees that DQE may use various tools in its sole discretion to protect its network, including but not limited to "black holing" traffic, suspension of Internet service, and/or termination of Internet service.

9. Customer represents and warrants that Customer has all right, title and interest or is the licensee with right to use and/or access all of the Endpoints, applications and/or content Customer delivers to DQE to perform the DDoS Mitigation Service. Customer represents and warrants that Customer has the right to grant DQE the access rights and licenses set forth herein and has obtained or will obtain prior to DQE's performance of DDoS Mitigation Service all rights, authorizations or permissions required for DQE to perform the DDoS Mitigation Service.

10. During a DDoS Attack, Customer shall:

i) Have a technical contact available during the entirety of an open trouble ticket to enable Customer to interact with DQE's support team;

ii) Ensure other mitigation equipment is disabled within the Customer's environment; and

iii) Will cooperate with DQE and any requests as needed.

D. Service Level Requirements. DQE's Service Level (SLA) for mitigation response time is within thirty (30) minutes of the Customer reporting a DDoS Attack and DQE opening a NOC trouble ticket pursuant to which Customer authorized DQE to begin DDoS Mitigation Service.

1. Response Time:

In the event that the DQE fails to initiate a DDoS Mitigation Service response within 30 minutes after a NOC ticket is opened and Customer authorized DDoS Mitigation Service, and such failure affects Customer's ability to use DDoS Mitigation Service while under attack, the following Service Level Credits apply:

DQE Response Time in Minutes	Service Level Credit
0-30	N/A
31-90	10%
91-120	20%
121-240	30%
241-480	40%
481+	50%

2. Service Level Credits:

In the event that DQE does not achieve a particular Service Level in a given month, for reasons other than an Excused Outage (as defined below), DQE will issue a credit to Customer as set forth in the applicable service level table above, upon Customer's request ("Service Level Credit"). To request a credit, Customer must contact DQE's Customer Service by calling toll free in the U.S. and Canada 1-866-GO-FIBER or delivering a written request within thirty (30) days of the end of the month for which a credit is requested. Customer's total credits in any one (1) month shall not exceed one (1) month's DDoS MRC for the affected Service for that month and cannot be applied to MRC for any other services obtained through DQE.

An "Excused Outage" is an outage caused by: (a) the configuration, failure or malfunction of non-DQE equipment or systems (including any products introduced as part of a fix or modification agreed to between the Parties); (b) scheduled maintenance or planned enhancements or upgrades to the DQE network; (c) DQE not being given reasonable access to the premises; (d) Customer exceeding the maximum capacity of a port connection or any other rate limitation as set forth in the applicable Service Order; (e) documented delays resulting from Customer's failure to respond to troubleshooting requests or other reasonably requests from DQE; or (f) a Force Majeure Event as defined in the Master Service Agreement.

E. Modifications, Term, Termination and Suspension.

1. Modifications:

A Customer's DDoS Mitigation Service must coincide with the size of the Customer's purchased Internet Bandwidth. If a Customer's Internet service bandwidth is modified (either upgraded or downgraded), Customer's DDoS Mitigation Service bandwidth will be automatically upgraded or downgraded to match. Any increase or decrease in price will become effective on the next available billing cycle and will be prorated.

2. Term:

The Term of this Schedule shall commence on the Commencement Date, and the duration of the Term for DDoS Mitigation Service shall be as set forth in the Service Order, but for no less than one year ("Initial Term"). Thereafter this Service Schedule shall continue on a month-to-month basis (each month a "Renewal Term"), unless Customer gives written notice of its intention to terminate not less than thirty (30) days prior to the expiration of the Initial Term or then current Renewal Term, as applicable.

3. Termination:

(i) If the Customer terminates Internet service prior to the end of any Term for this DDoS Mitigation Service, Customer shall pay any past due balances, plus, as liquidated damages, all remaining monthly Service Fees due under the remaining Term.

(ii) DQE may terminate the Services performed under any one or more Customer Service Orders hereunder for convenience by giving at least one hundred and eighty (180) days prior written notice to the Customer.

4. Suspension:

DQE may suspend provision of the DDoS Mitigation Service and/or Internet services if, in the DQE's reasonable determination, an Abuse occurs. Such suspension shall remain in effect until Customer corrects the applicable Abuse. In the event that, in DQE's reasonable determination, an Abuse is critically impacting, or threatens to critically impact, the DQE's network or servers, DQE may suspend provision of the DDoS Mitigation Service and/or Internet service, as applicable, immediately and without prior notice. In the event that an Abuse is not critically impacting the DQE network or threatening to do so, DQE shall give Customer prior notice of any suspension. Such suspension shall remain in effect until Customer corrects the applicable Abuse.

If Customer fails to correct any Abuse after notice (whether written or oral) from DQE, DQE may, in its sole discretion, terminate its provision of DDoS Mitigation Service and/or Internet service for breach without any liability or obligation to Customer for any DDoS Mitigation Service suspended or terminated. If it is determined that the Abuse was intentional on Customer's behalf, then DQE in its sole discretion shall charge early termination fees and liquidated damages.

F. Warranty and Limitations. DQE warrants that the Service will meet the specifications on the Customer Service Order. If the Service fail to meet such specifications, DQE will provide support and maintenance to Customer in accordance with the SLAs set forth herein. The SLA will be effective on the applicable Commencement Date, but credits will not apply until the first full calendar month in which a Service is provided. If the Service fail to meet the specifications on the Customer Service Order then Customer shall be entitled to remedies set forth in the applicable SLA.

EXCEPT AS SET FORTH HEREIN, THE CREDIT CALCULATIONS SET FORTH IN THE SLA SHALL BE CUSTOMER'S SOLE REMEDY IN THE EVENT OF ANY FAILURE OF THE SERVICE TO MEET THE SPECIFICATIONS. THE TOTAL AMOUNT OF CREDIT THAT WILL BE EXTENDED TO CUSTOMER AS A RESULT OF DQE'S FAILURE TO MEET THE SPECIFICATIONS SET FORTH IN THE SLA SHALL BE LIMITED TO 100% OF ONE MONTH'S RECURRING CHARGE IN ANY SINGLE MONTHLY BILLING PERIOD. EXCEPT AS SET FORTH IN THIS SECTION, DQE MAKES NO WARRANTIES TO CUSTOMER WITH RESPECT TO THE SERVICE, EXPRESSED OR IMPLIED. DQE EXPRESSLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY AND OF FITNESS FOR A PARTICULAR

PURPOSE. DQE EXPRESSLY DISCLAIMS ANY WARRANTY OF CONTINUOUS OR UNINTERRUPTED SERVICE.

If Customer is delinquent on any invoice, any SLA credits due to Customer shall be deducted from said delinquent amount. The application of credits does not waive Customer's obligation to pay any remaining balances or any future amounts under this Service Schedule.

DQE reserves the right to stop DDoS Mitigation Service at its sole discretion when a DDoS Attack has not occurred or has ceased. DQE does not warrant that the Service will operate error free, uninterrupted or fail-safe; that DQE will correct all product or Service errors, or that the Service will lead to certain results. Any advice or information provided by the DQE or its providers or agents cannot represent guarantees.

DQE will not be liable for any: (i) disruptions in the security of the Customer network, system or equipment; (2) loss, corruption, or theft of Customer Data during the use of the Service; or (iii) loss or damage in connection with or arising out of the interruption or loss or use of the Service.

Neither DQE nor DQE's third party suppliers will be liable for any punitive, special, consequential, incidental or indirect damages, including but not limited to, loss of profits or review, business interruption, or lost data, even if the Party has been advised of the possibility of such loss or damage.

G. License. Customer acknowledges that operation and performance of the DDoS Mitigation Service involves repeated filtering of traffic to the Endpoint and Customer herby expressly consents to the same. Customer hereby grants DQE a non-exclusive, non-transferrable, and royalty-free license to access the Endpoint and the internet traffic flowing thereto and any applications contained therein for the sole purpose of performing the DDoS Mitigation Service.

H. Network Management. Use of the DDoS Mitigation Service in a manner that, in DQE's reasonable determination, directly or indirectly produces or threatens to produce a material negative effect on the DQE's network or that materially interferes with the use of the DDoS Mitigation Service or DQE's network by other Customers or authorized users, including, without limitation, overloading servers or causing portions of DQE's network to be blocked; and altering any aspect of the DDoS Mitigation Service where such is not authorized by DQE; enables DQE to take any action at its sole discretion to preserve the integrity and/or operations of DQE's network.