MANAGED SERVICES

MANAGED WI-FI

1. **SERVICE DESCRIPTION.** As part of its Managed Wi-Fi Service, DQE will (i) install the DQE Equipment, and (ii) provide support and monitoring services for the Customer's managed Wi-Fi network ("Wi-Fi Service") to applicable service location for use solely by the Customer and Customer's guests and visitors that patronize the Service Location ("End Users"). The Wi-Fi will be branded as Customer's Wi-Fi service. Customer acknowledges that the bandwidth and coverage offered by the Wi-Fi Service is not guaranteed, as Wi-Fi Service coverage may vary due to the use of unlicensed spectrum, power supply and equipment mounting location. The Wi-Fi Service is subject to change from time to time to reflect changes in features and technology offered by DQE and applicable laws.

2. **USER ENVIRONMENT.** As part of the Wi-Fi Service, DQE will create and maintain a pre-authentication user environment which, to the extent requested by Customer, will include a landing page requiring an End User to accept terms and conditions Customer may desire to impose as a condition of accessing the Wi-Fi Service. DQE shall update and make changes to the End User environment and landing page, as reasonably requested by Customer.

3. **MAINTENANCE.** DQE shall maintain the Wi-Fi Network as necessary, including managing and modifying (as reasonably requested by Customer) the configuration of equipment and devices, monitoring of the Wi-Fi Network, and, the maintenance, repair, or replacement of DQE Equipment. DQE's obligation to maintain the DQE Equipment shall be limited to:

    - Troubleshooting and remote repair via the DQE NOC; and
    - Site visits by a technician when determined to be appropriate by DQE; provided, that, Customer acknowledges and agrees that it shall be responsible for the payment of all reasonable service charges for visits by DQE technicians.
    - On-site repair or replacement of DQE Equipment as determined necessary by DQE.

4. **MONITORING.** DQE will provide real-time, remote network monitoring to assure that the Wi-Fi is active. DQE will proactively monitor the Wi-Fi Network and will use commercially reasonable efforts to proactively remedy identified issues with Wi-Fi Network.

5. **ONLINE PORTAL.** DQE will provide Customer with an online portal for live monitoring the Wi-Fi Network, including, the routers, switches, and access points. DQE will have access to the standard information provided via the online portal. DQE provides no representations or warranties with respect to the portal beyond those provided by the portal operator to its users.

6. **CUSTOMER OBLIGATIONS.** Customer agrees to the following:

- Customer at their own expense must provide, install, and maintain any required router, firewall and other ancillary equipment/software.

- Customer must report any detected Service or network failure as soon as possible and provide any requested information to the DQE NOC and support personnel at 877-263-8638.

DDoS Mitigation

1. **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 Customers. DQE will proactively monitor a Customer's internet traffic and assess for a possible DDoS Attack. DDoS Mitigation Service can be activated on one of three ways: (i) If DQE identifies a possible DDoS Attack, DQE will proactively contact the Customer to confirm commencing DDoS Mitigation Service; (ii) Customer may contact the DQE NOC to report a DDoS Attack; or (iii) DDoS Mitigation Service can be activated automatically if certain established parameters have been met.. After DQE and the Customer collectively agree that a DDoS Attack is taking place, DQE will commence the DDoS Mitigation Service. When system 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.

2. **DEFINITIONS.** The following definitions shall apply to DDoS Mitigation Service:

   A. **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.

   B. **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.

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

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

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

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

   G. **Excused Outage –** 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.

H. **Non-Attack Incident Fee (NAIF) –** The 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.

I. **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.

3. **CUSTOMER OBLIGATIONS.**

A. **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.

B. **Contacts.** 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.

C. **Acknowledgements.** 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. Customer acknowledges and agrees that the DDoS Mitigation Service does not prevent or eliminate all DDoS Attacks. Customer acknowledges and agrees that DQE may use various tools in its sole discretion to protect its network, including "black holing" traffic, suspension of Internet service, or termination of Internet service. The Customer is responsible for the security of managing network components of customer data environment such as routers, firewalls, databases, physical security, or servers.

D. **Representations and Warranties.** Customer represents and warrants that Customer has all right, title and interest or is the licensee with right to use or access all of the Endpoints, applications 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.

E. **Commencement of DDoS Attack.** Customer must notify the NOC in the event Customer experiences, or anticipates, a DDoS Attack. Upon receipt of notification, the NOC will open a trouble ticket and commence 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. The Customer must authorize DQE to begin DDoS Mitigation Service. 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. During a DDoS Attack, Customer shall:

- Have a technical contact available during the entirety of an open trouble ticket to enable Customer to interact with DQE's support team;
- Ensure other mitigation equipment is disabled within the Customer's environment; and
- cooperate with DQE and any requests as needed.

DQE reserves the right to stop DDoS Mitigation Service at its sole discretion when a DDoS Attack has not occurred or has ceased.

4. **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.

   A. **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%

   B. **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 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. 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.

5. **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 or operations of DQE's network.

6. MODIFICATIONS, TERMINATION AND SUSPENSION.

A. 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.

B. Suspension. DQE may suspend provision of the DDoS Mitigation Service 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 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.

C. Termination. 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. 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 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.

7. 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 fails to meet the specifications on the Customer Service Order, then Customer shall be entitled to remedies set forth in the applicable SLA. 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, 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. 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.

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.