I. Service Description

TWTC's DDoS Scrubbing Service, DDoS Scrubbing DCMSP, and DDoS Scrubbing Protected Hosts ("Services") monitor Customer's Internet traffic as it traverse TWTC's Network to detect anomalies that are symptomatic of a denial or distributed denial of service attack. The Services are available for purchase as an add-on feature to TWTC's Internet Access and if applicable, Converged Services. The Services do not require Customer to install its own hardware or software.

When provisioning the Services, TWTC will sample Customer's Internet traffic to establish baseline measurements. Traffic thresholds are then established based on the baseline measurements. Although the thresholds are typically based on industry best practices, they may be set at levels requested by Customer. The baseline measurements and thresholds may be reviewed periodically by the parties for any changes in Customer's usage patterns.

When the Service detects an anomaly that is symptomatic of a DDoS attack, due to triggered thresholds or indicators of protocol misuse, it generates an alert to TWTC's NOC. TWTC will investigate such anomaly and, when a DDoS attack is indicated, TWTC will contact Customer to validate whether a DDoS attack is occurring or Customer's usage is causing the anomaly.

If Customer confirms that a DDoS attack is occurring, TWTC will route Customer's inbound traffic to its DDoS Scrubbing platform and begin applying countermeasures to help minimize the effects of the DDoS attack. The Service and associated countermeasures are configured to reduce disruption of Customer's legitimate traffic. TWTC personnel will remain on the telephone with Customer only so long as needed to validate the DDoS attack, support installation of the countermeasures and verify completion of the countermeasures.

TWTC will review the countermeasures 24 hours after initial implementation and will remove them if TWTC determines the DDoS attack has ended. TWTC will then redirect Customer's inbound traffic to its normal path and notify Customer that countermeasures have been removed.

If a DDoS attack is impacting, or may impact, TWTC's Network, TWTC may take any action, including but not limited to blackhole filtering Customer's traffic, which filtering would result in all traffic destined to Customer being dropped.

Customer may elect to enable auto-mitigation, which is a capability that automatically redirects Customer's inbound traffic to the DDoS Scrubbing platform when a predefined anomaly is detected, and will begin to apply countermeasures pre-associated with the detected anomaly.

II. Service Level Agreement

A. Customer Notification

TWTC will contact Customer within fifteen (15) minutes after a high severity alert is generated on TWTC's monitoring system and is deemed by TWTC to be indicative of a DDoS attack.

Time to Respond	Credit
Less than 15 minutes	No Credit
15 minutes or greater	5% of the MRC

B. Application of Countermeasures

TWTC will begin applying countermeasures within fifteen (15) minutes after Customer validates the DDoS attack and authorizes TWTC to apply countermeasures.

Time to Begin Mitigation	Credit
Less than 15 minutes	No Credit
15 minutes or greater	5% of the MRC*

- Not applicable when auto-mitigation is enabled

C. Additional Provisions

- TWTC shall issue a credit for each instance of a failure to meet the metric specified in the tables above. Credits are calculated by multiplying the percentage in the table by the MRC for the applicable Service. Customer shall only be entitled to one credit per day and, for any billing month, credits cannot exceed the MRC of the applicable Service.

- Customer is responsible for keeping the contact information for its technical representative up to date with TWTC's Customer Network Reliability Center at 800-829-0420. TWTC cannot initiate DDoS countermeasures promptly if Customer's representative cannot be reached.

- TWTC's failure to meet the above requirements shall not constitute a "Service Outage" for purposes of the underlying agreement between the parties. If the performance of Customer's Internet Access or Converged Services is affected by the DDoS countermeasures, the SLAs for those Services will not apply during the time period that the countermeasures are in place.

- The above credits are Customer's sole and exclusive remedy for TWTC's failure to meet the applicable metric or failure to mitigate a DDoS attack. Credits are only issued if requested by Customer, and such requests must be submitted to TWTC within sixty (60) days following the DDoS event.

- Customer acknowledges that the use of auto-mitigation may result in unintended blocking of non-attack traffic

Customer acknowledges that it is important to notify TWTC of anticipated changes to its network security architecture, including exceptions to Customer's normal network activity (i.e. unscheduled back-ups, increase traffic due to marketing events) to avoid false high-severity alerts to the Service.