SCHEDULE A: SERVICE DEFINITION FOR DDoS MITIGATION SERVICE

1. DDoS Mitigation Service Description

The Distributed Denial of Service (“DDoS”) Mitigation Service is designed to mitigate DDoS attacks and attack traffic on the Exponential-e network for up to three (3) Exponential-e Internet Services (which can be the Partner’s own Exponential-e Internet Service and/or Internet Services provided to the Partner for use by End Users). The DDoS Mitigation Service supports maximum throughput of 10Gbps per mitigation. Any traffic above this maximum throughput will be discarded. The Exponential-e DDoS mitigation platform will examine the Partner’s / End User’s traffic and auto-generate a “normal” traffic profile. The following are examples of the types of packets that when detected by the DDoS mitigation platform in volumes outside of the “normal” traffic profile will trigger an alert: DNS Amplification, IP Fragment, ICMP, IP Protocol 0, MS SQL Amplification, NTP Amplification, SNMP Amplification, SSDP Amplification, TCP Null, TCP RST, TCP SYN. The triggers are based upon the total amount of any type of traffic going to a monitored IP address. Once an alert is triggered, mitigation is automatically launched. When the Exponential-e DDoS mitigation platform recognises attack traffic or the Partner notifies Exponential-e that the Partner / End User is under attack (where a Diverse Internet Solution exists), traffic destined for the targeted IP address, estate or asset will be re-directed to Exponential-e’s DDoS mitigation platform for inspection. Diverted traffic will be subject to multiple layers of Traffic Cleaning. A network scrubbing platform delivers clean traffic to the hosts under attack. Provides reporting via email and web-interface with the web-interface also providing information on traffic types and trends for up to thirty (30) days. Up to two (2) mitigation profiles are included per Internet Service at no additional charge. Additional mitigation profiles are available at additional charge. These mitigation profiles are tailored per Internet Service and will be set out in the Service Delivery Form. Once the DDoS Mitigation Service has been provisioned, Exponential-e will study traffic patterns in order to inform, report and assist the Partner / End User to identify when a DDoS attack is in progress and advise on specific actions that the Partner / End User should take to lessen their exposure to attack. While Traffic Cleaning is in progress, an increase in latency may be experienced and this shall be excluded from any Service Level calculations. Mitigation will be provided for up to 72 consecutive hours at no additional charge. Should the Partner request mitigation be continued past this point, additional charges will apply. Mitigation will be provided on up to 12 separate occasions in any calendar year commencing from the Service Commencement Date. Should the Partner require additional mitigations, then this will constitute a non-standard service for the Partner and the Partner will be required to contract with Exponential-e for a bespoke DDoS solution. During the first thirty (30) days after the Service Commencement Date, the Partner may request Minor Changes. After the initial 30 days, up to three (3) Minor Changes per calendar month can be requested by the Partner at no additional charge. Additional Minor Changes can be made at additional charge. Exponential-e will use all reasonable endeavours to ensure that non-attack traffic is received as normally as possible during a DDoS attack. Blackholing of traffic will only be used by Exponential-e if Exponential-e determines that all other measures have failed or are likely to fail. Where the Partner has a Diverse Internet Solution and requires Exponential-e to provision the DDoS Mitigation Service on that Diverse Internet Solution which requires specific configuration work to be carried out, then additional charges will apply.

Exponential-e does not warrant or guarantee that the DDoS Mitigation Service will prevent or mitigate all DDoS attacks.

2. Target Service Commencement Date

DDoS Mitigation Service	5 Working Days*

** From order acceptance if provisioned in respect of an existing Internet Service / from date of provision of any new Internet Service required.*

3. DDoS Service Level Agreement

No Service Level Agreement is offered in respect of this Service.

4. Additional Terms applicable to DDoS Mitigation Service

The following terms apply to the provision of the DDoS Mitigation Service by Exponential-e in addition to the General Terms.

4.1 Additional Partner Responsibilities

4.1.1 The Partner shall:

4.1.1.1 notify the Exponential-e Service Desk in advance of any impending activity that can reasonably be expected to result in or encourage additional traffic to the Partner / End User website that may or may not be malicious in nature, including but not limited to marketing campaigns, moral hacktivist attacks and other traffic outside of the normal traffic profile for the Internet Service; and

4.1.1.2 immediately inform Exponential-e if any threats is made, whether publicly, privately, intimated, inferred or directly, of any intention to initiate a DDoS or DoS attack at any time.

5. Definitions

5.1 In this Service Definition, the following terms below shall have the meaning given below.

“Blackholing” discarding all data destined for a particular IP address;

“DDoS” Distributed Denial of Service; an electronic attack involving multiple computers sending repeated requests to a web-site generating false traffic with the aim of rendering it inaccessible;

“Diverse Internet Solution” an internet solution comprised of an internet service from Exponential-e and one or more internet service(s) from third parties;

“Minor Change” changes to fine tune the Service to function better and changes to IP addresses;

“Traffic Cleaning” Statistical analysis, active verification, anomaly recognition and the discarding of packets that do not conform to the Partner’s / End User’s “normal” traffic profile.