Terms and Conditions for Anti-Distributed Denial of Service ("DDoS Service"):

1. Definitions

"**Alerts**" means notification via email of IP Traffic Anomalies or IP Threats that, in HGC opinion, requires immediate action by Customer, to mitigate or to monitor possible defensive action.

"**Attack Mitigation Equipment**" means the denial of service detection equipment and the data scrubbing equipment located at HGC premises and used in connection with the DDoS Services provided to Customer by HGC.

"**Attack Mitigation Capability**" is the level of scrubbing capacity purchased by Customer from HGC. HGC will use its commercially reasonable efforts to provide adequate scrubbing or mitigation capacity to support the defined attack size.

"**DDoS Services**" means the DDoS Attack Mitigation service platform(s) comprising the management and operation of the multilayer DDoS solution to Customer. The DDoS Services are managed and operated by Service Operation Center (SOC) and Network Operation Center (NOC) of HGC.

"**Denial** of **Service**" Attacks (**DoS**) is traffic based attacks which, if not scrubbed are likely to materially disrupt Internet access.

Example of attacks:

Attack Type	Description
Amplification	Amplification attack makes a request that generates a larger response
Application	An application-level attack (layer 7) that overloads an application server, such as by making excessive log-in, database-lookup or search requests
Brute-force	Sending packets that exceed defined flow rates of threshold
Flood	Sending large amounts of legitimately formed packet
Fragmented	Sending fragment packets that will never be completed
Malformed	Sending packets with abnormal bits or flags set
Null	Sending packets with no content or illegitimate protocol
Spoofed	Sending packets with a forged source address

"**Distributed Denial of Service**" Attack (**DDoS**) is a type of DDoS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system attack Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

"**IP Traffic Anomaly**" means data traffic across HGC network has a pattern or characteristic recognized by HGC as warranting investigation.

"**IP Threat**" refers to data traffic across HGC's network such as viruses, buffer overloads. DDoS attack or other traffic, that may potentially disable, interrupt or degrade single or multiple connections to HGC network.

"**Right**" refers to HGC right to black-hole the victim IP as last resort in case the attack volume is significantly degrading the backbone network and/or exceeded the support defined attack size.

"**Scrubbing Device**" refers to the equipment used by HGC to isolate and mitigate a DDoS attack.

"**Traffic Data**" means a sample of Customer data traffic on HGC backbone used to identify and mitigate DDoS Attack(s).

2. Compatibility with the DDoS Services

Customer agrees to the following for use of the DDoS Services:

(a) Subscribe for DIA Premium Service for a Fixed Contract Period as determined by HGC from time to time;

(b) Subscribe for DDoS Services for a Fixed Contract Period as determined by HGC from time to time; and

(c) Provide HGC with requisite information to enable HGC to provide the DDoS Services.

3. Use of DDoS Services

(a) Customer shall ensure the applications, equipment, hardware, software and networks meet the DDoS Services' minimum system requirements as determined by HGC from time to time, and that they are compatible and may properly function and inter-operate with the DDoS Services and in accordance with the following :-

(i) All applicable instructions, safety and security procedures applicable to the use of such applications (or as the case may be, equipment hardware, software or networks) are complied with; and

(ii) All instructions, notices and directions as may be determined by HGC from time to time are complied with and followed.

(b) HGC reserves the right to immediately stop any ongoing mitigation initiated by Customer, if any, with or without notice to Customer, if HGC considers that such mitigation will or may affect the infrastructure, or the backbone network of the DDoS Services.

(c) HGC may, at any time and without any notice to Customer, temporarily suspend the DDoS Services for operational reasons such as repair, maintenance, upgrade or improvement of the DDoS Services or in case of emergency. DDoS Services will be resumed as soon as reasonably practicable. HGC may also modify any part of the DDoS Services in order to keep pace with the prevailing standards and technological developments, at any time without any notice to Customer.

(d) HGC may at any time without notice to Customer, trigger a 'black-hole' if necessary to prevent any potential harm or imminent harm (such as interruption, disruption, congestion, signal leakage and/or any unauthorized act) to the network of any third party.

(e) HGC reserves the right to implement Access Control List (ACL) filtering or black-hole the victim IP as a last resort in case the attack volume is significantly degrading the backbone network.

(f) HGC will not be liable to Customer or any third party for any loss or damage arising under this paragraph c). (Use of DDoS Services).

4. Responsibility of Customer

Customer shall be obliged to:-

(a) Provide accurate and complete particulars/information to HGC and such particulars/information will be set out in the order/supplement form issued by HGC.

(b) Be solely responsible for initiating the mitigation of any and all attacks via the DDoS Services.

(c) Be solely responsible for determining the severity of the attack, including how and when to use the DDoS Services to address it.

(d) Acknowledges that auto-trigger email alerts on detected anomalies are subjected to Customer internet connectivity and network condition (e.g.: router processing capability, etc.)

(e) Cooperate with HGC in respect of any fault investigation pertaining to the DDoS Services or relevant attacks.

(f) Cooperate with HGC in all aspects of the DDoS Services, including but not limited to, providing HGC with information regarding any changes to Customer network, in order to assist HGC in the analysis and examination of Customer traffic data.

(g) Provide HGC with a list of Customer IP addresses to be connected to HGC network which will be subject to the DDoS option, and immediately notify HGC of any changes to such list throughout the term of this offer.

5. The amount of clean traffic generated (maximum up to port size) depends on the outcome of Customer mitigation efforts made via the DDoS Services. HGC will not be liable to Customer or any third party for any loss or damage arises from any event occurred under paragraphs 4(a) to (e) above.

6. Provision of DDoS Service is conditional upon subscription of the DIA Premium Service. Unless otherwise specified, the terms and conditions of DIA Premium Service which by their nature or otherwise should be applicable to the DDoS Service shall also apply upon subscription of the DDoS Service.

7. Unless otherwise specified, DDoS Services will be charged at the special price as set out in this offer during the Fixed Contract Period.

8. Termination of the DIA Premium Service will automatically lead to termination of the DDoS Service as well as any value-added service subscribed for. However, the DDoS Service could be terminated on its own by giving one month's prior written notice to HGC.

9. Expiration date of the Fixed Contract Periods of both the DIA Premium Service and DDoS Service will be aligned irrespective of whether both services are applied on the same date unless otherwise agreed between HGC and Customer.