## 1. INTERPRETATION

Any capitalised terms utilised in this Services Description that are not defined below shall have the definitions provided in the Services Order Form or the General Terms and Conditions.

**"Black Holing"** means discarding packets destined for the Customer's Network so that they do not disrupt the flow of traffic to other IP Addresses;

**"CDR" means Committed Data Rate, which is** the bandwidth over the MT network that the Customer specifies to Manx Telecom at the start of each Calendar month that Manx Telecom applies to the Customer's actual bandwidth utilisation to calculate the bandwidth-related fees payable by the Customer in a particular Calendar month**;**

**"Cleaning & Mitigation Phase"** shall take the meaning provided in clause 2.2(d);

**"Configuration Phase"** shall take the meaning provided in clause 2.2(a);

**"Critical Change"** means a change without which there will be a material impact on the Services and/or Customer's Network;

**"Customer's Network"** means a set of IP Addresses unique to the Customer;

**"DDoS Attack"** means forms of electronic attacks involving repeated requests to a server or application, generating false traffic and rendering it inaccessible to valid users;

**"Emergency Invocation"** means a request for DDoS Protection from a Customer under DDoS Attack, who is not a subscriber of the Services at the time of the DDoS Attack.

**"General Terms and Conditions"** means MT's general terms and conditions, the original version of which was provided to the Customer at the execution of each Services Order Form, as may be amended from time to time by MT, the latest version of which can be obtained at www.manxtelecom.com;

**"IP Address"** means the unique identifying number of any computer or other device that is attached to the Internet;

**"Learning Phase"** shall take the meaning provided in clause 2.2(b);

**"Monitoring & Detection Phase"** shall take the meaning provided in clause 2.2(c);

**"Non-Critical Change"** means a change which has no immediate or significant impact on the running of the Services and/or the Customer's Network;

**"Normal Traffic Pattern"** means the traffic patterns of data packets to each IP address on the Customer's Network during normal operation that is identified from time to time by MT during the Term;

**"Services"** means the DDoS Protection Services, as described in more detail in the Services Order Form the purpose of which is to mitigate the effects of a DDoS Attack on the Customer's Network;

**"Service Level"** means the Service Level provided in Section 3; and

**"Services Order Form"** means each service order form entered into by the Parties.

## 2. SERVICE OVERVIEW

2.1 MT shall provide the Customer with the Services until the expiry of the Term.

2.2 The Services are comprised by the following phases:

(a) **Configuration Phase** – the configuration and updating of MT's equipment and systems in order to enable the provision of the Services to the Customer, which shall include:

(i) the inclusion of the IP addresses that comprise the Customer's Network on the relevant MT equipment and systems that will be involved in the provision of the Services to the Customer;

(ii) the setting and implementation of pre-defined monitoring parameters that will be used during the first Learning Phase;

(b) **Learning Phase –** the passive monitoring of the incoming traffic to the Customer's Network that is undertaken by MT from time to time in order to identify the Customer's Normal Traffic Pattern the results of which are used during the Monitoring & Detection Phase;

(c) **Monitoring & Detection Phase** - the monitoring of traffic flows to the Customer's Network in order to identify deviations from the Normal Traffic Pattern that may constitute a DDoS Attack that is addressed during the Cleaning & Mitigation Phase; and

(d) **Cleaning & Mitigation Phase –** during a potential DDoS Attack all data traffic that is addressed to the Customer's Network is subjected to:

(i) multiple layers of analysis;

(ii) active verification; and

(iii) anomaly recognition,

by comparison to the Customer's most recent Normal Traffic Pattern in order to any identify malicious sources, confirm abnormal behaviour and discard data packets that do not conform to the Customer's Normal Traffic Pattern.

2.3 If the Customer's Network suffers a DDoS Attack, then MT shall:

(a) use its reasonable endeavours to enable all legitimate data packets to be passed to the Customer's Network; and

(b) use its reasonable endeavours to minimise any disruption to the Customer's users or the Customer's Network; and

(c) only use techniques such as Black Holing if MT considers that all other measures have deemed to have failed.

2.4 During the calendar month following the Service Commencement Date, MT shall permit what it considers to be reasonable changes to the Services as may be requested by the Customer. Thereafter, any amendments to the Services will be handled in accordance with the Change Management Procedure.

2.5 In the event of failure of any of its equipment that is relevant to the delivery of the Services, MT shall use its reasonable endeavours to repair or replace such the equipment within one business day.

2.6 The Customer agrees and acknowledges that:

(a) due to the unpredictable nature of DDoS Attacks:

(i) MT cannot guarantee that the Services will always or fully mitigate any DDoS Attack to which the Customer's Network may become subject;

(ii) the failure of the Services to fully mitigate a DDoS Attack that is targeted at the Customer's Network shall not, absent negligence on the part of MT, constitute a breach of the provision of the Services by MT that will

entitle the Customer to terminate the Services Order Form and/or seek damages from MT;

(iv) MT's capacity to mitigate a DDoS Attack for any given Customer is dependent on the number of Customers under attack and the method of attack used at any given time

(v) MT's liability to the Customer for any losses that the Customer may face as a result of a DDoS Attack shall at all times be limited as provided in the General Terms & Conditions.

(b) the Services do not include:

(i) load balancing of traffic or of the Services;

(ii) permanent archival and storage of log files;

(iii) incident response, forensics and investigations;

(iv) legal case preparation and PR incident support;

(v) security consulting services (e.g. security policy design, security auditing, penetration testing, contingency/disaster recovery planning or other services);

(vi) security reporting and analysis; or

(vii) permanent filtering or cleaning of traffic.

(c) while the Cleaning & Mitigation Phase is operational the Customer's Network may exhibit increased latency;

(d) MT reserves the right to vary the technical specification of the Services at any time provided that such variation does not have a material adverse effect on the Services being provided by MT to the Customer;

(e) if MT determines, in its sole discretion, that a Non-Critical Change is necessary, then both parties will agree a time to carry-out such change within five business days of MT's request to make such change, otherwise such change shall become a Critical Change; and

(f) MT shall be permitted to implement such Critical Change at a time it considers to be most convenient to the Customer. MT shall use its reasonable endeavours to contact the Customer's technical contract prior to making any Critical Change.

2.7 The monthly subscription charge per Megabit of protected bandwidth shall be equal to the total CDR associated with the Customer's Network. An Emergency Invocation will be charged at eighteen (18) times the total CDR associated with the Customer's Network being protected.

## 3. SERVICE LEVEL

3.1 The Service Levels are detailed in the table below:

3.2

| DDoS Protection Subscription | DDos Protection Emergency Invocation |
|---|---|
| Customer's Network will be placed in Learning Phase within three working days of receiving a completed Service Order Form. | Not applicable |
| Customer's Network will be placed in Monitoring and Detection Phase following seven Learning Phase days (or sooner if required).<br><br>Monitoring & Detection Phase is the normal state of the DDoS Protection Service. | Not applicable |
| Customer's network will be placed in Cleaning and Mitigation Phase within ninety (90) minutes after MT has confirmed nature of DDoS attack with the Customer. | Customer's network will be placed in Cleaning and Mitigation Phase, following confirmation of acceptance of terms, on a best endeavours basis. It should be noted that due to lack of Normal Traffic Pattern information the time taken to provide clean traffic only may be significantly impacted. |
| Customer's Network can be placed in Cleaning and Mitigation Phase an unlimited number of times and removed only when the DDoS Attack is confirmed over by MT. | Customer's Network is placed in Cleaning and Mitigation Phase for the duration of the DDoS Attack and removed only when the DDoS Attack is confirmed over by MT. |
| Non-urgent Customer change requests agreed with MT will be implemented within seven working days | Not applicable |