SERVICE SCHEDULE

DDOS PROTECT

This is a Service Schedule as defined in the Conditions. Where the Services set out in this Service Schedule form part of the Services to be supplied under a Contract (as defined in the Conditions), this Service Schedule forms part of the Contract.

In this Service Schedule, references to Clauses are to Clauses of the Conditions, and references to paragraphs are to the paragraphs of (i) this Service Schedule or (ii) whichever other document is specifically referred to.

1 Additional Definitions

In this Service Schedule the following words and expressions shall have the following meanings:

1.1 **"Client"** — A device on the Customer's network that accepts traffic from the internet and is therefore vulnerable to DDoS attack.

2 DDoS Protect – Service Scope and Description

2.1 The Supplier provides managed volumetric DDoS (Distributed Denial of Service) mitigation, DDoS Protect, which automatically triggers traffic cleaning of Customer internet traffic so as to reduce the risk of disruption to Customer services in the event of malicious activity.

2.2 The Customer confirms that it has considered and accepts full responsibility for all scenarios relating to any failure conditions and functionality of each related or dependent service where those services are not provided by the Supplier.

2.3 The Supplier's DDoS Protect Service is provided to the Customer for so long as the Contract remains in force in accordance with the terms of the Contract and the Supplier's AUP, security and access policies and procedures

2.4 The Supplier's DDoS Protect Service is subject to payment by the Customer of the Supplier's Charges for installation and support services, as set out in the Order Form or as subsequently agreed between the parties from time to time.

2.5 Where diagnostic services are required to identify any issue or potential issue, the Supplier will only provide end-to-end diagnostics if the connectivity, hardware and software is entirely managed by the Supplier. If any elements are shown not to be managed by the Supplier, then any end-to-end diagnostic services will be stopped.

2.6 This service is designed to mitigate against a multitude of DDoS events but does not guarantee there will be no service disruption and the Supplier shall accept no further liability for any service disruption in excess of the fee credits set out in paragraph 4.4 below.

2.7 The Supplier's DDoS Protect Service is designed to minimise the disruption a Client may experience during a DDoS event but due to Client configurations, application and services, there may be a brief period of time as the Service qualifies the threat and instigates mitigation responses where inbound network traffic to a Client service may be disrupted.

2.8 In line with this being a fast but automated, reactive Service, Customers that attract frequent, complex, application or sustained attacks may require additional or bespoke protection and the Supplier may insist on this level of protection being put in place in such circumstances and accordingly the Service Levels shall be suspended until such protection is put in place to the Supplier's satisfaction.

2.9 During an attack event, and once the traffic cleaning service is active, the Customer accepts that traffic passing through the DDoS Protect Service will have increased network latency as a result of the cleaning process. The Customer accepts that this additional latency and any performance degradation associated with it are acceptable during an attack event.

2.10 DDoS Protect uses a combination of analytic approaches to detect malicious traffic however it should not be considered a precise science. DDoS Protect, whilst extremely accurate, may cause some traffic to be blocked as a false positive. The Customer accepts that any degradation of Customer services associated with such occurrences are acceptable during such an attack event and maintains responsibility for ensuring that services are compatible with the DDoS Protect Service. The Supplier accepts no liability for any effect on Customer services as a result of false positives.

3 Customer Responsibilities

3.1 Should the Customer notice a DDoS attack against their services where DDoS Protect does not automatically trigger protection, the Customer should notify the Supplier immediately so that traffic cleaning can be manually enabled and the protection system can be tuned so as to detect similar subsequent events. Should the Customer fail to notify the Supplier and then receive further attacks which also do not trigger protection, service credits will only be issued for the first of those events.

3.2 Any faults or problems detected by the Customer must be reported immediately by the Customer (and in any event within 24 hours of detection by the Customer) to the Supplier using the customer portal ticket system or for critical issues using the telephone number provided to the Customer. The fault or problem will then be logged by the Supplier and the Customer will receive a ticket reference which can be used to track work on the ticket.

4 Service Levels

4.1 The Supplier will use its reasonable endeavours to deliver the following Response Times, Fix Times and Availability as classified in the tables below.

4.2 Incident Response Times

Event Priority	Definition	Service Hours	Response Time
P1	• Total loss of production service; or • A significant revenue, operational, or safety impact on the entire company; or • Service degraded, affecting the entire company	24/7/365	Within 15 minutes
P2	• Partial loss of service affecting the company; or • Service degraded, affecting multiple departments or a single site; or • There is the potential of significant revenue, operational, or safety impact to the company if not resolved quickly	24/7/365	Within 30 minutes
P3	• Service degraded, affecting non-production services; or • Loss of service affecting a single user	Business Hours	Within 1 Hour
P4	• Degraded service affecting a single user	Business Hours	Within 2 Hours
P5	• Request for information	Business Hours	Within 4 Hours

4.3 Service Availability

4.3.1 The Supplier will use its reasonable endeavours to deliver the following Service Levels in respect of the Services as set out in the table below.

Measure	Description	Value	Fee Credits
Service Hours	The hours during which the service and SLA is provided	Monday–Friday, 8am–6pm	
Availability	% of the service hours during which service availability is guaranteed (excluding Planned Maintenance)	100%	Pro rata proportion of the Monthly Charges for any Non-Availability Period
Detection Window	The maximum period of time from the beginning of the attack to enablement of the traffic cleaning service	15 minutes	Pro rata proportion of the Monthly Charges for any Non-Availability Period

4.4 Fee Credits

4.4.1 Any Fee Credits which fall due pursuant to this paragraph 4.4 are payable subject to and in accordance with the Conditions.

4.4.2 A pro rata proportion shall be calculated according to the number of complete minutes in the relevant calendar month and the number of complete minutes of Non-Availability in that calendar month.

4.4.3 "Monthly Charge" means the recurring Charges for the relevant Component for the relevant calendar month, net of VAT.

4.4.4 "Availability" means the percentage of the Service hours during which Service availability is guaranteed, not including Planned Maintenance.

4.4.5 “Non-Availability” means a period of time during which the relevant Service is unavailable in breach of the Availability Service Levels set out in paragraph 4.3 above.