SERVICE SCHEDULE

PENETRATION TESTING

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 **"Penetration Test"** — A controlled exercise in which the tester uses cyber attacks to attempt to compromise or gain unauthorised access to the target infrastructure, in order to identify any security weaknesses present in that infrastructure.

2 Penetration Testing – Service Scope and Description

2.1 Pulsant's Penetrating Testing Service engages a third-party testing agency to run independent tests on elements of the Customer's infrastructure in order to identify security vulnerabilities.

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 Pulsant's Penetration Testing Service is a one-time, fixed scope engagement in accordance with the terms of the Contract and the Supplier's acceptable use, security, and access policies and procedures.

2.3.1 The scope and duration of the Penetration Testing engagement will be as specified in the Order Form.

2.3.2 The scope of the standard Service is to subject five of the Customer's IP addresses to testing.

2.3.3 Additional testing beyond the agreed scope would constitute a separate Service engagement.

2.4 Pulsant's Penetration Testing Service is subject to payment by the Customer of the Supplier's Charges for the Service, as set out in the Order Form.

2.5 The Supplier will perform the following activities as part of the Service engagement:

2.5.1 Consult the Customer to determine the five IP addresses that will be tested against as part of the standard Service.

2.5.2 Construct a suitable timetable for tests, consulting the Customer to ensure that disruption of the Customer's business operations is minimised.

2.5.3 Commission the agreed penetration test from the Supplier's trusted testing partners.

2.5.4 Supply the Customer with a report detailing the results of the test and recommendations for addressing any vulnerabilities identified by the test.

2.5.5 Discuss the report with the Customer and discuss options for remediation or threat mitigation activities.

2.6 All tests will be conducted in Business Hours, unless specifically agreed in advance between the Supplier and the Customer and so noted on the Order Form.

2.7 The Supplier will perform actions to mitigate or remediate any security vulnerabilities that the tests have identified on infrastructure managed by the Supplier.

2.7.1 This work may be chargeable if outside the scope of contracted managed services, as defined by the relevant Service Contracts and Schedules.

2.7.2 The Customer is responsible for carrying out or commissioning remediation activities on any infrastructure not directly managed by the Supplier.

2.8 The Supplier will not subject a Customer's infrastructure to a penetration test without the Customer's knowledge and explicit agreement.

3 Service Levels

3.1 The Supplier does not offer a guaranteed SLA for the availability of this Service.