

## SERVICE SCHEDULE

### PULSANT ENDPOINT PROTECTION

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 **“Agent”** – a software application installed on a protected device, required for the Service to function.
- 1.2 **“Endpoint”** – a physical computing device, such as a desktop or laptop computer, used to access a network or the Internet.
- 1.3 **“Pulsant Service Description - Endpoint Protection”** - the document which sets out the scope and description of the Services being provided by the Supplier.
- 1.4 **“Webroot”** – a third-party company which the Supplier partners with. The Endpoint Protection Service is powered by Webroot tools and technology.

#### 2 Pulsant Endpoint Protection – Service Scope and Description

- 2.1 Pulsant Endpoint Protection Service (as described in the “Pulsant Service Description – Endpoint Protection” document) is a Cloud-based solution providing anti-virus and web filtering protection.
- 2.2 The management scope of the Services being provided by the Supplier is illustrated in the “Pulsant Service Description – Endpoint Protection” document, which also contains recommended specific considerations under the section “Service Dependencies and/or Related Services”. 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 Endpoint Protection Services are 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 acceptable use, security and access policies and procedures.
- 2.4 Pulsant Endpoint Protection 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 The Service consists of two options, either or both of which may be provided to the Customer, as stated on the Order Form. The two options are:
  - 2.5.1 Anti-Virus
  - 2.5.2 Web Filtering
- 2.6 If the Service is used to protect infrastructure that is not directly managed by the Supplier, the Supplier will not be responsible for remediation of malware infection or security vulnerabilities identified in that infrastructure.
- 2.7 The Customer will follow the Supplier’s recommendations in the remediation of security vulnerabilities.
- 2.8 The Customer will ensure that Customer-owned networks, systems, and applications within the scope of the Service are maintained and functioning properly.
  - 2.8.1 The Supplier shall not be responsible for any failure of the Service due to issues in any Customer-owned networks, systems, or applications.
- 2.9 If the Order Form includes “Anti-Virus”, the Supplier will perform the following activities as part of this Service:

- 2.9.1 Supply a method for the customer to deploy the Service Agent (for example, a link in an email).
  - 2.9.2 Monitor the Agents to ensure they continue to function correctly, including applying any required upgrades or patches to the Agent software.
  - 2.9.3 Provide support to the Customer's IT department on the use of the Service.
  - 2.9.4 Provide reports detailing any infection found within the Customer's network.
  - 2.9.5 Grant Customer access to the Service management portal on request.
  - 2.9.6 Where virus infections are detected in infrastructure managed by the Supplier, implement any recommended remediation measures, within the scope of the Pulsant managed service.
- 2.10 If the Order Form includes "Web Filtering", the Supplier will perform the following activities as part of this Service:
- 2.10.1 Where the Supplier manages the Customer's network, configure the DNS to enable the Service.
  - 2.10.2 Provide support to the Customer's IT department on the use of the Service.
  - 2.10.3 Grant Customer access to the Service management portal on request.
- 2.11 The Supplier will not:
- 2.11.1 Perform any remediation on infrastructure that is not managed by the Supplier, unless explicitly agreed.
  - 2.11.2 Configure the DNS on any network not managed by the Supplier, unless explicitly agreed.

### 3 Service Levels

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

| Event Type               | Service Hours  | Response Time                                     |
|--------------------------|----------------|---|
| <b>Critical</b>          | 24/7/365       | Within 15 minutes                                 |
| <b>Service Affecting</b> | 24/7/365       | Within 30 minutes                                 |
| <b>Routine</b>           | Business Hours | Within 30 minutes, measured during Business Hours |

- 3.2 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.

- 3.2.1 The below table defines the SLA for the Endpoint Protection Service.

| Measure              | Description  | Value    |
|----------------------|--|----------|
| <b>Service Hours</b> | The hours during which the service and SLA is provided   | 24/7/365 |
| <b>Availability</b>  | % of the service hours during which service availability is guaranteed (excluding planned maintenance in Clause 4 below) | N/A      |

### 4 Planned Maintenance

- 4.1 Save in situation which is an Event of Force Majeure or in the case of an emergency, where the Supplier considers (in its sole discretion) that it is necessary to carry out maintenance activities that will affect or can reasonably be expected to affect the Customer's operations, the Supplier shall notify the Customer at least 48 hours in advance of the commencement of the works detailing the nature of the work to be carried out and the timetable for completion of the works. These works will be carried out in accordance with the Supplier's standard procedures which are available upon request by the Customer. In the case of an Event of Force Majeure or an emergency, no advance notice is required.
- 4.2 During the period of Planned Maintenance, the SLAs will not apply.