SERVICE SCHEDULE

PULSANT CLOUD 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 **"Pulsant Service Description – Cloud Protect"** – the document which sets out the scope and description of the Services being provided by the Supplier.

1.2 **"Armor"** – a third-party company which the Supplier partners with. The Cloud Protect Service is powered by Armor tools and technology.

1.3 **"Agent"** – a software application installed on a protected device, required for the Service to function.

2 Pulsant Cloud Protect – Service Scope and Description

2.1 Pulsant Cloud Protect Service (as described in the Pulsant Service Description – Cloud Protect document) is a full-stack security and compliance solution that provides vulnerability and configuration assessment, log management, network intrusion detection and out-of-band web application protection with 24x7x365 threat monitoring.

2.2 The management scope of the Services being provided by the Supplier is illustrated in the Pulsant Service Description – Cloud Protect 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 Cloud Protect 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 Cloud 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 The Supplier will perform the following activities as part of this Service:

2.5.1 Install and configure Service Agents on all servers identified on the Order Form, where the Supplier is responsible for managing those Servers.

2.5.1.1 Provide the Customer with instructions on how to deploy the Service Agent on any servers not managed by the Supplier.

2.5.2 Monitor the Service Agents to ensure they continue to function correctly, including applying any required upgrades or patches to the Agent, on servers which the Supplier is responsible for managing.

2.5.3 Configure the environment managed by the Supplier to enable Agent communication and secure forwarding of data to the Service.

2.5.4 Grant Customer access to the Service management portal on request.

2.5.5 Review vulnerability scan reports and, where vulnerabilities are identified in infrastructure managed by the Supplier, recommend remediation measures and apply those measures on the Customer's confirmation, within the scope of the Supplier's managed service.

2.5.6 Validate the Customer's security patch status and, where missing security patches are identified in infrastructure managed by the Supplier, apply the patches in accordance with the contracted managed service.

2.5.7 Respond to any threat alerts raised by the Service, within the Service SLA.

2.6 Armor can remotely access the Customer's virtual machine via the Armor Agent with the Customer's permission, to provide full incident response and forensics capability during a Critical incident.

2.6.1 Remote support will only be provided with the Customer's permission.

2.6.2 Remote support will be restricted, secured, and audited to protect the Customer's systems and data, by the use of jump hosts, multi-factor authentication, privileged access management (PAM) systems.

2.6.3 The Supplier will monitor any use of remote support and report to the Customer.

2.6.4 Remote Support sessions will be recorded; these recordings are available upon Customer request.

2.7 The Supplier will disable Armor's ability to perform remote support at the Customer's request; this must be requested prior to deployment of the service.

2.7.1 The Customer accepts that doing this will limit the level of support available in response to a critical security incident.

2.8 The Supplier only guarantees a maximum of two hours support time in response on any single incident; support time beyond this limit may, at Supplier's discretion and on agreement from the Customer, be chargeable.

2.9 The Supplier will not:

2.9.1 Install, configure, or support Agents on infrastructure not managed by the Supplier.

2.9.2 Perform any remediation on infrastructure that is not managed by the Supplier, unless explicitly agreed.

2.9.3 Perform any patching on infrastructure that is not managed by the Supplier, unless explicitly agreed.

2.9.4 Guarantee that all attacks against the server will be detected and/or blocked by the Service, or accept liability for damage caused by any attacks that are not blocked by the service.

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
Critical	24/7/365	Within 15 minutes
Service Affecting	24/7/365	Within 30 minutes
Routine	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 Cloud Protect Service.

Measure	Description	Value
Service Hours	The hours during which the service and SLA is provided	24/7/365
Availability	% of the service hours during which service availability is guaranteed (excluding planned maintenance in Clause 5 below)	99.9%

3.2.2 Availability here specifically refers to availability of the Pulsant Protect Service and not the availability of the server which it protects.

4 Fee Credits

4.1 Any Fee Credits which fall due pursuant to this Clause 4 are payable subject to and in accordance with Clause 5 of the Conditions.

	Service Hours	Target Availability	Fee Credits
Cloud Protect	24/7/365	99.9%	Pro rata proposition of the Monthly Charges for any Non-Availability Period

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.

"Non-Availability" means a period of time during which the relevant Service is unavailable in breach of the Availability Service Levels set out in Clause 3.2 above.

5 Planned Maintenance

5.1 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.

5.2 During the period of Planned Maintenance, the SLAs will not apply.