

This Service Schedule should be read in conjunction with the General Terms and Conditions (a copy of which can be found at <https://www.bluesource.co.uk/about/privacy-governance-terms/>) and the appropriate Work Order.

1 Service Overview

MONITORING is a 24x7x365 monitoring and alerting service which provides the Customer with peace of mind that Incidents within the scope of this Service will be detected and alerted to the Customer. The Service is designed to automatically alert bluesource, based on predefined metrics related to bluesource's experience and industry best practice/industry, to potential issues within the scope of the monitoring.

bluesource will then proactively alert the Customer to the potential issue so that the Customer can then investigate further and resolve the underlying issue. Alternatively where additional services have been purchased from bluesource and relevant to what is being monitored, bluesource may undertake this remedial work on behalf of the Customer.

For the purpose of this Service Schedule, the following definitions apply:

“Incident” a technical issue associated with any related software or hardware that bluesource is supporting for the Customer. The technical issue is opened by bluesource's service desk with a unique case ID and placed in bluesource's Incident management system.

“SMC” bluesource's global service management centers providing personnel responsible for delivery of the Services.

2 Term and Termination

This Service Schedule shall commence on the Service Start Date and shall continue for the Initial Term stated in the Work Order subject to the provisions of clause 9 (Term and Termination) of the General Terms and Conditions. Thereafter this Service Schedule shall automatically renew for additional periods of one (1) year until terminated in accordance with clause 9 of the General Terms and Conditions.

3 Service Availability

The Service is provided 24x7x365.

From time to time it will be necessary for bluesource to schedule maintenance which could cause a disruption to the Services. bluesource will endeavour to provide a minimum of 72 working hour notice before conducting any planned Services affecting maintenance. Where significant changes are planned, bluesource will endeavour to provide a minimum of 28 calendar days' notice.

Where emergency maintenance, updates, or other procedures are required to maintain the Services or prevent a failure, bluesource will review these on a case-by-case basis and may be unable to notify the Customer in advance, based on the urgency and severity of the change.

4 Service Summary

The Service includes:

- Monitoring of applicable applications and operating system (Windows OS only),
- Monitoring of applicable hardware / infrastructure,
- Monitoring of applicable virtual devices,
- Monitoring of applicable servers,
- Proactive alerting to Customer support, and
- Basic alert and Incident reporting.

5 Service Inclusions

SERVICE BREAKDOWN		
1	Monitoring and Alerting	Service Items
1.1	24x7x365 monitoring and alerting	included
1.2	Bespoke threshold management	included
1.3	Prioritisation of alerts	included
1.4	Relaying identified issues to Customer's nominated support	included
1.5	Basic alert and Incident reporting	included
2	Service Management Centre (Support)	Service Items
2.1	24x7x365 support/remediation for Incidents by the Customer	Available as an additional service and not covered under this Service.

6 Service Levels

When an alert is received by bluesource, bluesource will review the alert and based upon our experience, decide whether the alert is a potential issue or not and where it is, raise and log a support ticket, assign a priority to the Incident and communicate with the Designated Contact within the following timescales:

Priority	Target Response Time
P1 – Critical Business Impact	15 minutes
P2 – Severe Business Impact	30 minutes
P3 – Inconvenient Business Impact	4 hours within Business Day
P4 – Minor Business Impact	1 Business Day

Incidents will be advised to Designated Contact/s via email unless otherwise agreed between the Parties.

If the Customer needs to raise the priority of a service ticket for any reason it should contact the SMC who will endeavour to review the assigned priority on a case by case basis.

The Priority definitions are:

<p>P1 - CRITICAL BUSINESS IMPACT with no workaround, where the use of a critical system is impossible in the production environment, or severely risks critical business operations.</p> <p>examples:</p> <ul style="list-style-type: none"> • Complete loss of service • Loss of connectivity in the live environment • Hardware failure in the live environment, causing a major business impact • Server "Out of disk space" in the live environment • Server down and unresponsive, impacting business
--

<p>P2 - SEVERE BUSINESS IMPACT with no workaround, where major functionality is severely affected or restricted, but not causing immediate work stoppage, and operation can continue in a restricted fashion.</p> <p>examples:</p> <ul style="list-style-type: none"> • High server processor utilisation • Issue with server log file size • Journaling not working • Whole Department outage

P3 - INCONVENIENT BUSINESS IMPACT, where there is a moderate loss or degradation of services but work can reasonably continue in an impaired manner.

examples:

- Errors encountered when upgrading supported software which is affecting service, but not crippling the live environment
- Error reported opening vaulted items

P4 - MINOR BUSINESS IMPACT, where there is a minor loss or degradation of services but work can reasonably continue in an impaired manner, or a query regarding a product/service.

examples:

- Minor Changes
- General queries
- Monitoring configuration adjustment
- Upgrades
- Patching

Where necessary, during the Business Day, the SMC may be contacted via **0345 319 2200**, or by emailing: **support@bluesource.co.uk**

7 Customer obligations

The Customer shall:

- Provide reasonable and relevant access necessary for bluesource to troubleshoot and resolve the Incident;
- Provide any relevant documentation reasonably required for bluesource to provide the Service;
- Provide a list and contact details of authorised personnel, who can engage with bluesource support;
- Maintain relevant Third-Party support and maintenance contracts;
- Communicate up to date Customer contact information and ensure that bluesource is informed of any such changes;
- Provide reasonable and relevant access to the items being monitored by the Service and to facilitate bluesource setting up monitoring agents required to operate the Service.
- Be responsible for any necessary firewall configuration changes needed on the Customer's end to establish connectivity between bluesource and the Customer's sites for monitoring.
- Identify and communicate a named point of contact for major Incident escalation and 24x7x365 out of hours contact/s.
- Provide reasonable documentation of any security policies and change management procedures that the Customer require bluesource to adhere to.
- Inform bluesource of scheduled downtime or maintenance.
- Be responsible for investigating alerts escalated to them by bluesource and any subsequent resolution.
- Acknowledge that servers, usually a VM, can enter an "Indeterminate State" where they are able to respond to some network traffic, such as pings, and honour only some work requests. Monitoring services may be unable to detect this state or a failure of a service on a server experiencing this issue. The Customer exempts bluesource, as a service, exclusion under such circumstances and may need to escalate an Incident to the SMC, if they observe an issue. The cause of this state can be varied and can range from faulty hardware to issues within virtual infrastructure.

8 Data Protection

Personal Data provided by the Customer shall, unless otherwise agreed in writing by both Parties, be processed in accordance with bluesource's Data Processing Policy, available at <https://www.bluesource.co.uk/about/privacy-governance-terms/>, and the relevant Agreement, including this Service Schedule.