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 & MANAGE is a proactive support, maintenance & management solution which adheres to industry best practice and processes. It analyses the health of technical infrastructures whilst proactively resolving incidents, reducing risk and optimising the day to day running of business critical systems. This end to end service means that optimal system performance is assured 24/7 and downtime is minimised ensuring business critical information is not compromised.

The service offers 99.9% Application Availability and Service Credits for SLA breaches, with a highly skilled support team and service delivery management.

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

"Account Manager"	bluesource's account manager responsible for the management of sales, and relationships with Customer. The Account Manager does not manage the daily running of the account itself.
"Application Availability"	the proportion of time, measured on a monthly basis, during which the application and all associated services are available, excluding 'Planned Downtime'.
"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.
"MACDs"	Moves, Adds, Changes and Deletions.
"Operational Phase"	the operational phase of the Service which commences once the service has been set up, configured and the service has been transitioned to an operational state.
"Operations Manual"	An operational framework agreed by both Parties, which defines how the Service is delivered and utilised by the Customer;
"Planned Downtime"	any pre-announced and agreed system outage resulting from planned maintenance such as upgrades, patch installs and pro-active re-boots (if and when needed).
"Response Time"	is the total time for bluesource to respond to an Incident once it has been created into bluesource's incident management system. The response time is measured from the time stamp when the Incident ticket is created, and the time stamp when an SMC engineer is assigned to work on the ticket and commences investigative work.
"Service Credits"	the value placed for each SLA breach by bluesource, used by way of financial recompense and credit towards future services rendered.

"Service Level Agreement ("SLA")" the Service level obligations set out in this Service Schedule.

"Service Start Date"	is the date that remote connectivity is established and bluesource begins to deliver the Service.
"SLA Adherence Date"	the commencement of the Operational Phase and the date when SLAs become effective for bluesource and the date upon which bluesource becomes liable for Service Credits.
"SMC"	bluesource's global Service Management Centers providing personnel responsible for delivery of the Services.
"Unplanned Downtime"	any system related outage to bluesource or the Customer's systems and infrastructure that was not pre-announced and/or scheduled in advance.

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 for monitoring and procative support.

The SMC will be available 24x7x365 for logging of Priority 1 and 2 Incidents.

Priority 3 and 4 Incidents/service requests can be logged during the Business Day and outside of these hours, logged the next Business Day.

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,
- Incident resolution,
- Problem management relating to Incidents where necessary,
- Change management relevant to supported systems,
- OS patching where included as part of the Service (See Service Inclusions and relevant Work Order), and
- Service reporting.

5 Service Inclusions

SERVICE BREAKDOWN		
1	**Monitoring and Alerting**	**Service Terms**
1.1	24x7x365 monitoring and alerting	included
1.2	24x7x365 event prioritisation and classification	included
1.3	Bespoke threshold management	included
2	**Service Management Centre (Support)**	**Service Items**
2.1	24x7x365 automatic support/remediation of Monitoring Alerts	included
2.2	24x7x365 support/remediation for escalated Incidents by the Customer	included
2.3	Incident prioritisation and classification	included
2.4	Problem Management (Correlation of Incidents for Root Cause)	included
2.5	Change Management (Customer Compliant)	included
2.6	99.9% Applcation Availability with Service Credits for Breach	Included

2.7	MACDs (Up to 20 per Month)	Included
2.8	Quarterly Windows O/S Patching	Included
3	**Service Delivery Management**	**Service Items**
3.1	Service Delivery Management	Included
3.2	Monthly Service Reports	Included
3.3	Quarterly Service Review	Included
3.3	Incident Reporting for P1 Service Outages (as requested)	included
4	**Account Management**	**Service Items**
4.1	Named Account Manager	Included
4.2	Quarterly Account Management Review	Included

6 Service Levels

When an Incident is escalated to bluesource it is received and logged as a support ticket, assessed and then assigned a priority based on bluesource's experience. An engineer will be assigned to start working on the ticket within the following time scales.

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

Where P1 and P2 classified incidents, problems and service requests are identified by the Customer, they need to be escalated to the SMC via telephone, **0345 319 2200,** in order to receive the appropriate Target Response Time which applies 24x7x365.

P3 and P4 classified incidents, problems and service requests may be reported by either telephone, **0845 319 2200** or email **support@bluesource.co.uk**. The Target Response Time for P3 and P4 classified incidents is based on the Business Day.

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:

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.

examples:

- 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

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.

examples:

- High server processer 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

7 Service Credits

7.1 In the event that bluesource fails to meet the Application Availability SLA for a given application in any given calendar month, bluesource will credit the Customer as follows against the provision of future services:

Application Availability	Unplanned Downtime Per Month	Credit
> 99.9%	Less than (<) 43.8 minutes	0 (in SLA)
> 99.8% to 99.9%	Between 86.23 & 43.8 minutes	1 Service Credit
> 99.5% to 99.8%	Between 3.6 hours & 86.23 minutes	3 Service Credits
< 99.5%	Greater than (>) 3.6 hours	5 Service Credits

Service Credits are capped at a maximum of 5 Service Credits for any given calendar month. A Service Credit is the equivalent of 5% of the monthly Fee for the Service in the calendar month in which the Application Availability Service Level was breached.

Any failure by bluesource to meet the monthly Application Availability SLA will be reviewed by Customer and bluesource at the quarterly service review meetings, prior to any potential Service Credit(s) allocation.

7.2 Exclusions

The following are excluded from the monthly Application Availability SLA and percentage availability statistics:

- Planned Downtime involving scheduled maintenance activities such as proactive reboots, patch installs and so forth.
- Unplanned Downtime that results from activities by Customer personnel or a decision by the Customer not to adopt best-practice configuration measures that promote high availability and which were recommended by bluesource to the Customer.
- Incidents that indicate a failure due to a lack of bandwidth or availability of the Customer's network (Local Area Network or Wide Area Network).
- Incidents or Unplanned Downtime that results from the misconfiguration, downtime or service failure of interdependent applications including but not limited to Microsoft Active Directory, Microsoft Exchange Server, Microsoft SharePoint, Microsoft Windows file systems, Microsoft Internet Information Services, not under the Service remit of bluesource.
- Incidents that indicate a Service failure due to availability of the Customer's Storage Area Network or Direct Attached Storage.
- Unplanned Downtime that arises as a result of failure by Customer personnel to follow change control measures agreed between the Customer and bluesource caused by the Customer.
- Unplanned Downtime that results from a lack of best-practice highly available server infrastructure, not provided by bluesource as part of the Services.

- Unplanned Downtime that results from a lack of best-practice highly available Storage architecture, not provided by bluesource as part of the Services.
- Unplanned Downtime that results from a lack of best-practice highly available network solution, not provided by bluesource as part of the Services.
- Unplanned Downtime that results from the lack of best practice in the physical environment including physical infrastructure security, power and cooling redundancy, not provided by bluesource as part of the Services.
- Unplanned Downtime or data loss that results from the lack of a best-practice highly available technical and process driven backup solution, not provided by bluesource as part of the Services.
- Unplanned Downtime that results from the manual intervention of Customer staff in any services hosted by bluesource.
- Unplanned Downtime that results from the actions of a third party vendor or warranty support provider directly engaged by the Customer.

7.3 Service Credit Exemption Period:

Service Levels set forth in this Agreement apply to bluesource at the SLA Adherence Date when bluesource begins to deliver the Service to the Customer.

All SLA breaches may be discussed between Customer and bluesource and will be recorded in minutes prior to imposing any potential Service Credits. For the avoidance of doubt, such discussion shall not delay or impact bluesource's issuance of a Service Credit.

8 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 Service Management Centre (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.

9 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.

Additionally, if the Work Order related to this Service Schedule includes the management and/or support of Veritas NetBackup, the following subcontractor may assist in the resolution of software related Incidents:

- **Harbor Solutions**
  bluesource partner located at Hamilton House, Mabledon Place, Bloomsbury, London WC1H 9BB, providing managed backup services and support on behalf of bluesource.
  Purpose of processing: providing 24/7/365 support, monitoring and managed services. Personal Data relating to contacts and support issues may be processed to provide the services and raise service tickets and process Backup Data.