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/privacy-and-governance/), and the appropriate Work Order.

1 Service Overview

Microsoft 365 is a suite of cloud-based software-as-a-service (SaaS) productivity, collaboration, security and governance applications and tools that delivers an integrated and seamless user experience to organisations across the world. When organisations introduce Microsoft 365 services into their IT services landscape, it can transform the ways of working and attitude to how technology can be an enabler for working smart from anywhere on any device and on your terms.

The bluesource Managed M365 service, (the "**Service**") provides support and management of the platform ensuring that the Customer' tenant operates smoothly, is secured and that it maximises the investment in Microsoft 365 no matter which license level is deployed. The core of the bluesource service delivers periodic reviews of the platform to ensure continuous optimisation with usage and availability reporting to help the Customer understand how the platform is being utilised. This is combined with inclusive administrative tasks that we perform on the Customer's behalf during the lifecycle of the service, such as out-tasking around:

- Azure Active Directory
- Exchange Online
- SharePoint Online
- OneDrive for Business
- Teams
- Information Governance
- Information Protection
- Intune
- Defender for Endpoint
- Defender for Identity
- Defender for M365
- Defender for Cloud Apps

bluesource's Service Management Centre ("**SMC**") delivers 24x7x365 monitoring and management of applications, devices, and servers for our client environments – be it public cloud, private cloud or on-premises. When an incident, problem, service request, event, or request for change is received, a ticket is logged within our ITIL structured ITSM platform where one of our engineers will review, investigate and action the request. This could be resolving an incident in-house, escalating to a vendor for debugging – where the bluesource "Escalation Support Add-on" service has been purchased or another escalation path is available – or assigning to our managed service team for change requests.

The bluesource Managed M365 service includes the following key features:

- **Reactive support** – for issues arising out of the day-to-day business as usual activities to maintain and optimise the performance and health of the solution.
- **Inclusive standard administration** – to support the business as it grows (see note [2] in section 4, Service Details, below for more details).
- **Secure score recommendations** – ensuring that the security posture is maintained based on the licensing in place.
- **Compliance score recommendations** – ensuring that the environment is well governed based on the licensing in place.
- **Productivity score recommendations & usage reporting** – to help encourage the use of features available based on the licensing in place and to help you plan for future initiatives.
- **Licensing optimisation recommendations** – to ensure the investment in Microsoft is maximised and the right license mix is in place.
- **Annual security posture assessment** – to continually improve the security posture of the Microsoft 365 platform and align to industry best and proven practices frameworks and guidance such as NCSC (National Cyber Security Centre) and NIST (National Institute of Standards and Technology).
- **Service delivery management** – to support and manage service quality, govern relationships with 3rd party IT services organisations and assist with expectations and requirements of the service.

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

"**BaaS**"	"Druva 365 Backup" service provided by bluesource's partner, Harbor (please refer to the appropriate Service Schedule at https://www.harborsolutions.com/service-descriptions). All references to the MSA in the Harbor Service Schedule shall apply to the General Terms and Conditions and not Harbor's MSA.
"Business Day"	08:00 – 18:00 BST/GMT, as appropriate, on a day other than a Saturday, Sunday or a public or bank holiday in England and Wales or Scotland. If the extended escalation hours option is added to the order, the 'Business Day' for escalations to Microsoft refers to the extended hours detailed on the Work Order (either Monday to Friday 08:00 to 23:00 GMT\BST or 24x5, both excluding public holidays).
"Escalation Support Add-on"	a service add-on to facilitate the escalation of an incident on to MS (please see the Escalation Support Add-on service schedule at: a copy of which can be found at https://www.bluesource.co.uk/privacy-and-governance).
"Fair Usage Policy"	the number of inclusive hours logged against the Customer's account in any calendar month that are used for reactive support incident. The number of hours included per calendar month is as detailed in the Work Order.
"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.
"Response Time"	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 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, and in absence of this date, the date the order was placed with bluesource by Customer.
"SMC"	bluesource's global Service Management Centre providing personnel responsible for delivery of the Services.
"Supported Products"	the product/s to be supported under this Service, which includes Microsoft 365 workloads only.
"Target Response Time"	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.
"Ticket"	a ticket raised for bluesource to resolve an Incident for Customer.

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 12-monthly Renewal Terms, unless terminated in advance in accordance with clauses 9.3 or 9.4 of the General Terms and Conditions.

For the avoidance of doubt, the Customer is required to provide at least 90 days' written notice in advance of the end date of any Term in order to terminate the Services on the end date of that Term. The Renewal Term Fee shall be payable in full at the same billing frequency as the Initial Term unless otherwise agreed in advance.

In accordance with clause 11.1 of the General Terms and Conditions, should the Agreement be terminated for any reason, any agreed sums owing, including any remaining balance of the Fee or Renewal Term Fee shall be due for payment in full by the Customer.

At the end of each quarter, bluesource will review the number of hours logged against the agreement and should the average number of hours per month exceed the amount of inclusive hours included in the Fair Usage Policy by more than 10%, bluesource may suspend the provision of Service, pending the purchase of an increase to the Fair Usage Policy hours. bluesource may at its discretion, continue to provide the Service whilst discussions regarding the plan of action for the next quarter takes place with the Customer.

3 Service Availability

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

Priority 2, 3 and 4 Incidents/service requests can be logged and will be actioned 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 Inclusions

Service Component	Description	Service hours	Included?
Incident management[1]	2nd and 3rd line remote technical support for Supported Products with incident activity tracking & reporting. See note[1] below for examples of Incidents covered under the Service.	Business Day	Included
Problem management	Managing identified problems through to resolution and updating the internal knowledgebase for expedited future resolutions.	Business Day	Included
Service Level Agreement (SLA) driven Time-To-Action (TTA)	See section 5 (Service Levels) for SLA details.	Business Day	Included
Monthly service reports	Report of service usage delivered via email.	Once per month	Included
Quarterly service reviews	Meeting delivered by the service delivery manager to review the service delivery, hours used and remaining along with addressing any challenges.	Once per quarter	Included
Standard administration – moves, adds and changes[2]	Well-defined pre-approved changes that do not require change board review. See note [2] below for complete list of changes.	Business Day	Included
Major incident reporting	Service delivery management reporting for any P1 major incidents through to resolution.	Business Day	Included
Secure score reviews	Analyse the tenant secure score and provide recommendations to enhance security where possible within the license level deployed – quarterly activity.	Once per quarter	Included
Compliance score reviews	Analyse the tenant compliance score and provide recommendations to maintain compliance where possible within the license level deployed – quarterly activity.	Once per quarter	Included
Productivity score reviews	Analyse the tenant productivity score and provide recommendations to maximise productivity where possible within the license level deployed – quarterly activity.	Once per quarter	Included
License optimisation review	Analyse the license usage for the tenant and recommend options for optimising costs – annual activity.	Once per annum	Included
Security posture assessment	Analyse the tenant configuration against industry standard benchmarks and best practices for Microsoft 365 security – annual activity.	Once per annum	Included

Notes:

[1] Examples of Incidents that are within the scope of this service include:

- One or more users cannot log into Outlook, One Drive for Business, the Office 365 portal or Teams.
- One or more Teams user profiles have been corrupted or hung.
- One or more users cannot setup their multifactor authentication tokens.
- Azure Active Directory Synchronisation is failing.
- One of more users cannot send an email.
- One or more users cannot receive an email.
- One or more users cannot apply a sensitivity label to document.
- One or more users cannot assign rights management to a document or email.

[2] The following activities are included as standard administration activities:

- Assign or remove a license to or from a user or group.
- Create, modify, or delete a user object.
- Create, modify, or delete an Azure AD group.
- Create, archive, or delete a Team.
- Add, or remove a channel to or from a Team.
- On-board a device to Defender for Endpoint.
- Create a SharePoint site based on a pre-defined standard template.
- Assign or remove an administrative eligible or permanent role.
- Reset a user's authentication method – password or multifactor authentication token.

Examples of non-standard service requests that require a separate “chargeable hours bundle” of time to call off:

- Create or modify and test an M365 policy
  - Teams.
  - DLP.
  - Information protection.
  - Conditional access.
  - Alerts.
  - Defender for Cloud Apps.
  - Defender for Endpoint.
  - Microsoft endpoint manager device configuration or security.
  - Retention.
  - Label.
  - Threat Protection.
- Delete an existing policy.
- Conduct an e-discovery search.
- Rebuild a user PC through Microsoft Endpoint Manager Autopilot.
- Package an application for Microsoft Endpoint Manager (cloud).
- Provision an app registration.
- Configure an access package.
- Create a custom role.
- Publish an application through Azure AD SSO.
- Publish a new domain.
- Provision a message transport rule.

5 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 (Business Day)	Target Response Time (Outside Business Day)
P1 – Critical	1 hour	1 hour
P2 – Urgent	4 hours within business day	N/A
P3 – High	1 business day (within 10 hours)	N/A
P4 – Low	Next business day (within 20 hours)	N/A

Tickets can be raised by one of up to 5 designated contacts by calling the SMC on 0345 319 2200, or by emailing: support@bluesource.co.uk.

Where P1 classified Incidents 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.

P2, P3 and P4 classified Incidents may be reported by either telephone, **0345 319 2200** or email **support@bluesource.co.uk**. The Target Response Time for P3 and P4 classified incidents is based on the Business Day.

Where necessary to troubleshoot and resolve an Incident, bluesource may, with the Customer's permission and supervision, need to remote on to the Customer's environment using appropriate remote-control software.

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:

Priority	Description
P1 – Critical	No workaround available, where the use of a critical system is impossible in the production environment, or severely risks critical business operations.
P2 – Urgent	No workaround available, where major functionality is severely affected or restricted, but not causing immediate work stoppage, and operation can continue in a restricted fashion.
P3 – High	There is a moderate loss or degradation of services, but work can reasonably continue in an impaired manner.
P4 – Low	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. Service requests and change requests.

The priority will be assigned by bluesource based on the information provided by the Customer when the ticket is logged. The Customer is expected to provide, at a minimum, the following information when logging an incident to enable Bluesource to assign the most appropriate priority service level:

- Description of the incident including detailed error messages.
- How the issue is impacting the business.
- How many systems are affected by the issue (where relevant).
- Details of any deadlines at jeopardy that may be faced due to the issue.
- Details of if the issue is causing work stoppage, or a business down scenario.
- How many users are being affected by the issue (estimate).
- Date and time the issue was first experienced.
- Details of any recent changes to the environment.
- Additional relevant information.

6 Exclusions

Any component not explicitly defined in the service inclusions section is deemed out of scope of the service such as but not limited to:

- Implementation of new workloads and features – bluesource can deliver these through discrete project engagements via our M365 consultancy service.
- Implementation of updates to workloads, apps and features – bluesource can deliver these through discrete project engagements via our M365 consultancy service.
- Troubleshooting or remediation of networking equipment, LAN, WAN, firewall and proxy services.
- Designing, building or troubleshooting custom developed workflows. This can be delivered by bluesource via discrete projects via our professional services team.
- Migration of data into or out of the Microsoft 365 platform.
- Custom development.
- End user desktop support incidents.
- Documentation of any infrastructure.
- Onsite response to any incident requests, service requests or change requests.
- Availability of Microsoft 365 applications.
- Monitoring, management, or support of any 3rd party applications.
- Proactive maintenance except for where specified in the service inclusions.

- Where incidents are deemed to be platform related and require escalation to Microsoft, we will escalate incidents via the Customer's existing cloud solution provider (CSP) or direct support agreement. Where Customer has purchased the Enhanced Support Add-on, we will escalate incidents to Microsoft directly.

7 Customer obligations

The Customer shall:

- Provide sufficient available bandwidth on the Customer network to support the Microsoft 365 workloads deployed.
- 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.
- 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.
- Provide reasonable and relevant access and permissions necessary for bluesource to action change requests.
- Designate bluesource as "Partner of Record" with Microsoft.
- Grant bluesource "delegated admin role" or "granular delegated admin role" for the tenant/s.
- Subscribe to Microsoft 365 under a separate agreement. This service does not include supply of licenses.
- When logging an incident provide, as a minimum, the information detailed in clause 5 above, in order for bluesource to assign the most appropriate priority service level to an incident.

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/privacy-and-governance/, and the relevant Agreement, including this Service Schedule.

Where BaaS has been included as part of the Service, the following shall also apply:

- The following subcontractor is used in the delivery of the Service:
    - **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.
- Customer acknowledges that information processed in the course of performing the Services may contain personally identifiable information of individuals and associated metadata and that the processing of such information may therefore involve the processing of personal data. With respect to any and all data, including, but not limited to, third party data, personally identifiable information and associated metadata obtained by bluesource or its subcontractors pursuant to Customer's use of the Services, Customer shall take all necessary measures to ensure that it, and all its employees, are aware that their personal data may be processed as part of the Services and that they have given their consent to such processing as well as complied with their responsibilities as data controller or data subjects, as applicable, in accordance with applicable Data Protection Laws.
- Customer understands and agrees that bluesource and its subcontractors have no control or influence over the content of the backup data processed by Service, which they perform on behalf of Customer.