Advanced Support for M365
SERVICE SCHEDULE

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 Advanced Support for M365 service, (the "**Service**") provides proactive support and management of the platform ensuring that the Customer's tenant operates smoothly, is secured and that the investment in Microsoft 365 is maximised 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 reports to help the Customer understand how the platform is being utilised. This is combined with inclusive out-tasking that Bluesource perform on the Customer's behalf during the lifecycle of the Service.

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 Customer service desk will remain responsible for taking end user calls, performing triage and actioning first-time fixes and will remain responsible for desktop support where face-to-face or 'hands-on' access is required to end user compute devices. The SMC will work alongside, acting as an extension to the Customer's team to receive incident escalations from the level 1 teams, troubleshooting issues, actioning service requests where they pertain to the Microsoft 365 services and managing escalations through to Microsoft, when necessary.

The Service includes the following key features:

- **2nd and 3rd line support** – for issues arising out of the day-to-day business as usual activities to maintain and optimise the performance and health of the service.
- **Standard administration, investigations, and reporting**– to support the business as it grows and ensure that the environment is well governed and maintained.
- **Annual tenant posture assessment with quarterly recommendations updates** – ensuring that the tenant configurations are in line with the Modern Workplace guidelines and strategy along with industry best and proven practices, while maintaining the security posture.
- **Usage reporting and recommendations** – to help encourage the use of features available based on the licensing in place and to help you plan for future initiatives.
- **License reporting and recommendations** – to ensure the investment in Microsoft is maximised and the right license mix is in place.
- **Inclusive hours** – to deliver on-demand activities throughout the contract such as workshops, workload current state assessments and the implementation of non-standard change requests, service requests and remediation activities.
- **Endpoint & application update management** – to maintain the security posture of endpoints and govern the application and operating system environment estate.
- **Service delivery management** – to support and manage service quality, govern relationships, and assist with expectations and requirements of the service.

For this Service Schedule, the following definitions apply:

"**BaaS**"	"Druva Backup as a Service" 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).

"Inclusive Hours"	A bundle of hours to be utilised for ad-hoc engagements to deliver a defined outcome such as engagements defined in the inclusive hours catalogue, technology roadmap sessions or configuration of specific features or policy settings within a Bluesource in-house supported product.
"Inclusive Hours Time Bundle Account"	the Customer's account with Bluesource, which records a running balance of the number of hours the Customer has remaining for use with Chargeable Hours activities. The initial amount of inclusive hours is detailed in the Work Order.
"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.
"Proposal"	quotation document generated on Orderporter or issued by other means for Goods and/or Services from Bluesource.
"Relief Events"	the following events: (a) any failure by the Customer or Bluesource to comply with its obligations under the [General Terms and Conditions / agreements]; (b) any error or malfunction in the Customer's systems or any other software, hardware, or systems for which Bluesource is not responsible or any failure by the Customer, its agents, or contractors (including any existing service provider) to obtain sufficient support and maintenance, as required, for any software, hardware, or systems for which Bluesource is not responsible; or (c) any failure by the Customer or its agents or contractors (including any existing service provider) to provide any information, co-operation, or instructions to Bluesource which is reasonably required by Bluesource for the proper performance of its obligations under this Service Schedule.
"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 Modules"	the modules that are included as part of the Service as detailed on the Work Order. If none are selected, only the 'Standard' module is included.
"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.
"Support Data"	all data, including all text, sound, video, image files, or software, that are provided to Bluesource by or on behalf of Customer under this Agreement or produced during the relationship between the Parties, such as and not limited to support tickets, project documentation, contracts, purchase orders, invoices, and emails.
"Supported Products"	the product/s to be supported under this Service, which includes Microsoft 365 workloads only.
"Target Response Time" ("TRT")	The target time to acknowledge receipt of a ticket that has been logged for the Customer by the SMC.
"Target Time to Action" ("TTA")	The target time for work to begin on a ticket raised under the Service.
"Target Time to Resolution" ("TTR")	The estimated target time to resolve or to provide a Temporary Fix or Workaround where applicable for a ticket that has been raised related to the Service.

"Temporary Fix" or "Workaround"	A change advised by Bluesource in the procedures to be followed by Customer to minimise any disruption caused by an Incident.
"Ticket"	a ticket raised for Bluesource to resolve an Incident for Customer.
"Work Order"	the document detailing an order for Services and/or Goods agreed in writing by the Parties, including but not limited to: the Customer accepting a Proposal; issuing a purchase order to Bluesource; placing an order via an order form, email, or other means; or receiving a document labelled 'work order' from Bluesource.

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 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.

Fair Usage Policy

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 number of inclusive hours included in the Fair Usage Policy by more than 10%, Bluesource may require the purchase of an increase to the Fair Usage Policy hours to guarantee the continuity of the Service. 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. Bluesource may at its discretion suspend the service if, after 1 (one) quarter, an agreement between the Parties has not been formalised, by means of a purchase order and signing the related quote.

Inclusive Hours Time Bundle

The Inclusive Hours Time Bundle Account hours can only be used within twelve (12) months of the Service Start Date and after this time, any unused time will expire and may no longer be used. The Customer will be contacted prior to the expiry of the Service to discuss renewing the Service for another term.

The Inclusive Hours Time Bundle Account hours are drawn down in hourly increments where activities are ad-hoc requests based on the number of hours used for the Inclusive Hours Activity. Where a defined workshop, assessment, regular activity or defined outcome is selected, the number of hours that the activity will consume will be communicated to the Customer before the activity takes place and will be drawn down from the bundle on the completion of each activity. When the Customer's Inclusive Hours Time Bundle Account exceeds 90% utilisation, Bluesource will contact the Customer to discuss the purchase of additional time. At any time, should the Customer's Inclusive Hours Time Bundle Account record a negative number, Bluesource may suspend the provision of Service, pending the purchase of additional hours.

A minimum of 40 hours may be purchased as a Work Order to 'top up' the Customer's Inclusive Hours Time Bundle Account. Additional time purchased is co-termed with the existing agreement and as such will expire at the anniversary of the main agreement. Should the agreement be renewed, Bluesource may – at their discretion – roll the unused hours forward to the next contracted year.

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 Service. Bluesource will endeavour to provide a minimum of 72 working hours notice before conducting any planned Service 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. Bluesource shall advise Customer at the earliest opportunity where such activities have impacted

Service. By the nature of emergency application of such activities, it is not possible to advise customers in advance, to prevent failure or timely resolution.

4 Service Inclusions

Service Component	Description	Hours of Service / Frequency	Service Modules inclusion
Incident management	2nd and 3rd line remote technical support for Supported Products with incident activity tracking & reporting. See section 12 for examples of Incidents covered under the Service.	Business Day	Standard
Problem management	Managing identified problems through to resolution and updating the internal knowledgebase for expedited future resolutions.	Business Day	Standard
Service Level Agreement (SLA) driven TRT & TTA	See section 6 (Service Levels) for SLA details.	n/a	Standard
Major incident reporting	Service delivery management reporting for any P1 major incidents through to resolution.	Business Day	Standard
Monthly service reports	Report detailing service and time bundle usage - delivered via email.	Once per month	Standard
Monthly 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 month	Standard
Standard administration	Daily monitoring activities and advisory notifications to the tech team. Well-defined pre-approved changes that do not require change board review. See section 12 for included activities.	Business Day	Standard
Message centre management	Message centre management with weekly investigations and monthly reporting.	Once per month	Standard
Inactive object discovery	Discovery of inactive objects to utilise for quarterly reporting (users, Teams, Viva communities, sites, mailboxes, devices).	Once per month	Standard
Inactive license management	Identification of inactive Microsoft 365 licenses.	Once per month	Standard
Quarterly recommendations interim update report	Analyse the tenant secure score and adoption score and provide recommendations to enhance security and compliance where possible within the license level deployed. Report on technology usage and trends. Analyse monthly discovery data collected to report on trends and identify opportunities to optimise the tenant configuration.	Once per quarter	Standard
License optimisation review	Analyse the license usage for the tenant and recommend options for optimising costs – annual activity.	Once per annum	Standard

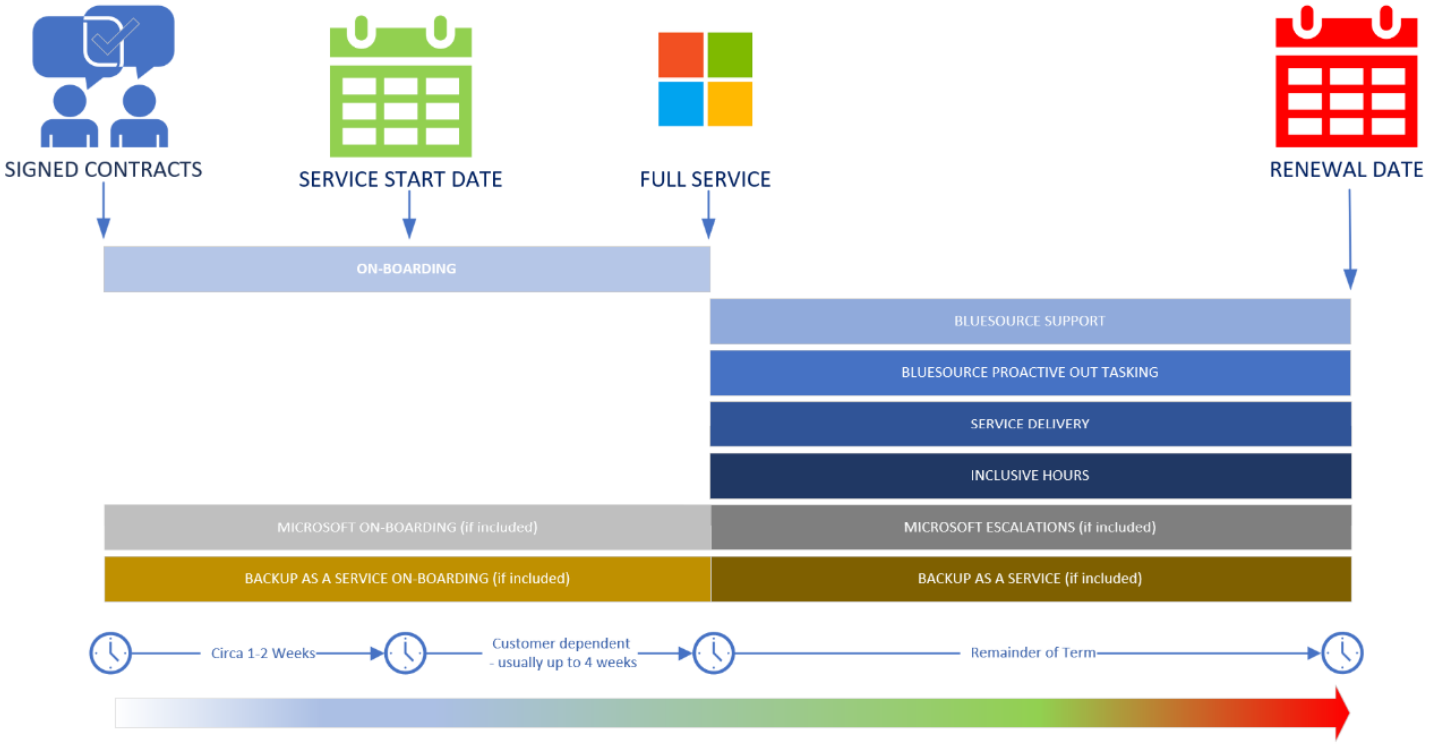
Tenant posture assessment	Analyse the tenant configuration against industry standard security benchmarks and best practices for Microsoft 365 security – annual activity.	Once per annum	Standard
Inclusive Hours Bundle	Bundle of time to call off for actioning ad-hoc requests such as workshops, probable root cause analysis, workload current state assessments and the implementation of non-standard change requests, service requests and remediation activities. **Note:** this is not to be used for projects or rollout of new services. These types of requests will be treated a separate project workstreams that will be quoted for and governed by a dedicated statement of work.	Business Day	Standard
Standard administration – endpoints	Device compliance monitoring & notifications to the tech team.	Daily	Endpoint management
Windows 11 update compliance management	Executing the 3-tier ring group updates rollout to Windows 11 endpoints managed via Intune.	Once per month	Endpoint management
Windows 11 advanced analytics report	Monthly reporting on Windows device health *Dependant on Intune suite licenses being assigned to all users.	Once per month	Endpoint management
Windows 11 driver management	Updating Windows 11 device drivers using Intune driver management.	Twice per annum	Endpoint management
Windows 11 app update management	Packaging in-band updates to applications. See limits in the notes below.	Once per month	Endpoint management

Notes:

- Tickets can be raised by one of up to 10 designated contacts by calling the SMC on 0345 319 2200, or by emailing: support@bluesource.co.uk
- P1 classified Incidents must be reported by telephone to receive the appropriate response.
- P2, P3 and P4 classified Incidents may be reported by either telephone, or email.
- Where necessary to troubleshoot and resolve an Incident, Bluesource may, with the Customer's permission and supervision, need to remote on to the Customer environment using appropriate remote-control software.
- The following activities only are included as standard administration activities:

a. Daily advisories monitoring & reporting.
b. Message centre management with weekly investigations and monthly reporting.
c. Assign or remove a license to or from a user or group – typically this would be automated where possible.
d. Create, modify, or delete a user object.
e. Create, modify, or delete an Azure AD group.
f. Create, archive, or delete a Team.
g. On-board a device to Defender for Endpoint – typically this would be automated where possible.
h. Assign or remove an administrative eligible or permanent role.
i. Reset a user's authentication method – password or multifactor authentication token.
j. Publish a packaged application to users\groups\devices via Intune.
k. Perform an Autopilot reset for an end user Windows device.
l. Provision a new end user Windows device through Autopilot.
m. Update Intune packaged applications to the latest version – limited to once per month and up to 50 packaged applications that are available in the Bluesource app management catalogue. Apps that fall outside these limits could be addressed through service requests that call time off the Inclusive Hours Time Bundle Account.

5 Service On-boarding and Lifecycle



From signing contracts, the Service will be setup and transition through various phases in its lifecycle:

On-boarding:

The first main milestone is the Service Start Date, from which the Service shall commence, as agreed between the Parties, and usually detailed on the Work Order. Typically, this phase commences around one (1) to two (2) weeks after signing contracts and the order being placed. After the order has been placed, Bluesource will start to setup the Service in readiness and make contact to gather any necessary information ahead of the Service Start Date.

The main on-boarding tasks before the Service can go live are:

- Holding an on-boarding call,
- Creating and circulating the Service Operations Manual,
- Provisioning Bluesource named accounts for the SMC and managed service consultants,
- Assigning Bluesource any necessary rights (as per section 11 below),
- Provisioning the Bluesource reporting app, and
- On-boarding to the Bluesource monitoring platform,

During this on-boarding phase, Bluesource will be unable to provide support, conduct any out-tasking or escalate any Incidents to Microsoft for assistance. It is therefore advisable that the Customer completes all its obligations in a timely manner, so that the Full Service Date can coincide with the Service Start Date as closely as possible.

Full Service Date:

The Service can only commence once Onboarding has been completed and the following elements of service become live:

Bluesource Support:

The Bluesource Support element of the Service is available from the Full Service Start Date, for the Term of the Service.

Bluesource Proactive Out-tasking:

The Bluesource Proactive Out-tasking element of the Service is available from the Full Service Start Date, for the Term of the Service.

Service Delivery Management:

The Service Delivery Management element of the Service is available from the Full Service Start Date, for the Term of the Service.

Inclusive Hours:

The Inclusive Hours element of the Service, subject to this having been purchased in the Work Order, is available from the Full Service Start Date, for the Term of the Service.

Microsoft Escalations:

The final element of the Service, subject to this having been purchased in the Work Order, the ability for Bluesource to be able to escalate Incidents to Microsoft on the Customer's behalf, will be available when the full service comes in to affect, once the on-boarding phase has been fully completed.

Renewal:

Towards the end of the Term, the Parties will discuss any renewal requirements and upon renewing, unless any changes are required, the on-boarding phase will not be required.

For the avoidance of doubt the Fee for the Service applies from the Service Start Date and not when all elements of the Service become available to the Customer.

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 (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
Service Requests	48 hours	N/A

Monthly reports will be delivered within 7 working days of the start of the month.

Quarterly reports will be delivered within 14 working days of the start of the quarter.

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.

7 Raising Tickets

Tickets can be raised by one of the Customer's 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,** 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.

8 Key Performance Indicators (KPI) for endpoint and application update management

The following key performance indicators will be used to measure the effectiveness of service delivery where not covered by measurements of service level discussed previously in this Service Schedule. These KPIs only apply to the Endpoint Management Service Module, if taken out under the Agreement.

Windows Monthly Quality Updates

Windows 10 and 11 operating system updates, defined as 'quality updates' including security, non-security, critical and updates provided to address a zero-day vulnerability, that are published by Microsoft on the second Tuesday of each month, known as 'Patch Tuesday', will be released to the pilot and production ring groups within the following defined timescales:

Endpoint Ring Group (as defined in Intune)	Deferral Period (#days)	Notes	Reporting
Ring Group 0	0	These are test and pilot devices that are used to validate the efficacy of updates.	Included in monthly report pack.
Ring Group 1	1	Updates will be automatically released if no issues are reported to Bluesource for endpoints impacted through the previous phase.	Included in monthly report pack.
Ring Group 2	3	Updates will be automatically released if no issues are reported to Bluesource for endpoints impacted through the previous phase.	Included in monthly report pack.

The term 'released' means that the in-scope update or updates will be made available to the group but does not guarantee when or if the endpoint will successfully install the in-scope update or updates.

The 'Deferral Period' is the length of time, in days, after Microsoft has published the update or updates that the update or updates are released[1] to the endpoint ring group if no intervening action occurs and notwithstanding any additional deferral period that applies as part of a selected servicing channel.

Only Intune-enrolled, fully managed Windows 10 and 11 operating system versions that are within the Microsoft published support lifecycle are considered in-scope of this KPI, any other operating system version is considered out of scope.

Bluesource expects that these types of updates are considered 'standard changes' and will not require formal change board approval to meet the defined schedule.

Windows Out-of-Band Quality Updates

When Microsoft publishes an out-of-band quality update or updates to address an active zero-day vulnerability for Windows 10 and 11 operating systems, the update or updates will be released using the following expedited schedule:

Endpoint Ring Group (as defined in Intune)	Expedited Deferral Period (#days)	Notes	Reporting
Ring Group 0	0	These are test and pilot devices that are used to validate the efficacy of updates.	Daily for one week following release and the rolled up into monthly report pack.
Ring Group 1	0	Updates will be automatically released if no issues are reported to Bluesource for endpoints impacted through the previous phase.	Daily for one week following release and the rolled up into monthly report pack.
Ring Group 2	1	Updates will be automatically released if no issues are reported to Bluesource for endpoints impacted through the previous phase.	Daily for one week following release and the rolled up into monthly report pack.

Bluesource expects that the Customer security operations centre (SOC) will be responsible for raising tickets with Bluesource for out-of-band update or updates that require deploying to address a zero-day vulnerability or vulnerabilities.

Bluesource expects that these types of updates are considered 'standard changes' and will not require formal change board approval to meet the defined schedule.

Only Intune-enrolled, fully managed Windows 10 and 11 operating system versions that are within the Microsoft published support lifecycle are considered in-scope of this KPI, any other operating system version is considered out of scope.

Application Out-of-Band Updates

When application vendors for in-scope applications publish an out-of-band update or updates to address an active zero-day vulnerability for the in-scope application, the update or updates will be released to all scoped endpoints within 72 hours of Bluesource being notified of the update availability and being supplied the update package installers. Bluesource expects that the Customer security operations centre (SOC) will be responsible for raising tickets with Bluesource for out-of-band update or updates that require deploying to address a zero-day vulnerability or vulnerabilities.

Applications that are considered in-scope for this KPI are limited to those listed in the Bluesource app management catalogue.

Bluesource expects that these types of updates are considered 'standard changes' and will not require formal change board approval to meet the defined schedule.

Windows Annual Feature Updates

Windows 10 and 11 operating system feature updates will be delivered through the 'General Availability' servicing channel, released once per annum for operating system versions that are within the Microsoft published support lifecycle. Any operating system version that is not within the Microsoft published support lifecycle is considered out of scope.

9 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, remediation of networking equipment, LAN, WAN, firewall and proxy services and Customer network diagnosis.
- 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 call logging (level 1 support) – this service is not designed for end user support; the service is available to named callers and is considered a service desk to service desk offering.
- 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.
- Supply of license subscriptions.
- Realtime security alert reporting or threat hunting.
- Realtime analysis of Microsoft 365 alerts.
- Customer network diagnosis – both local area networks and wide area networks.
- 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.

10 Supported Products

For the purposes of this services agreement, the supported products that are covered are limited to:

Microsoft 365	On-premises
Microsoft Defender suite of products, tools & services Microsoft Intune suite Microsoft Entra ID suite of products, tools & services Microsoft Exchange Online Microsoft OneDrive for Business Microsoft Power Platform suite of products, tools & services Microsoft Purview suite of products, tools & services Microsoft SharePoint Online Microsoft Teams Microsoft Viva suite including Yammer Microsoft 365 Apps for Enterprise	Windows 10\11

Bluesource shall only support Microsoft operating systems (Windows 10 and 11) and applications (Microsoft 365 Apps for Enterprise) that are within the Microsoft support lifecycle. Products that have reached end of servicing or end of support are considered out of scope of the Service.

11 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 "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, for Bluesource to assign the most appropriate priority service level to an incident.
- Maintain an active Microsoft Support agreement throughout the lifecycle of this agreement unless the Escalation Support Add-on has been purchased through Bluesource.
- Maintain stable and available WAN, LAN, firewall and proxy services.
- Agree that if Customer restricts access to the Office 365 admin portal then the Bluesource public IP address range will be added as a trusted location to access the Customer's Office 365 admin portal so that we are able to log tickets on behalf of Customer and carry out the necessary management tasks.
- Ensure all in-scope users are correctly licensed.

- Where the Customer has not purchased a computer system backup service from Bluesource, the Customer shall remain responsible and liable for such backup and hold Bluesource harmless for any liability arising out of any computer system backup or failure to provide any computer system backup.

12 Example Incidents & Service Requests

Examples of Incidents that are within the scope of this service include but are not limited to:

- 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.
- Entra ID 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.
- Monthly patching has affected an application and requires rollback.

Examples of non-standard service requests that require a separate “Inclusive hours bundle” of time to call off include but are not limited to:

- Create or modify and test an M365 policy including:
  - 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.
- Package a new application for Intune.
- 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.
- Investigate an alert raised by the Customer SOC.

13 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 while 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.