

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 Azure Virtual Desktop is Microsoft's platform as a service (PaaS) based remote desktop and application virtualisation solution hosted through the Azure regional datacentres. It delivers a flexible and scalable managed virtual desktop infrastructure leveraging Microsoft 365 Enterprise licensing and exploiting Windows 10\11 Enterprise multi-session support to reduce the number of virtual machines required to support the user-base whilst enhancing the user experience and keeping control of costs.

Part of managing an Azure Virtual Desktop estate is ensuring standardisation of session hosts through the use of master images. These images are typically locked down to ensure the configuration remains standardised across all session hosts in the pool and this means that updates need to be carefully planned and controlled so as to minimise the risk of configuration drift, ensuring that no matter which session host users connect to in the pool, they receive the same level of performance, application stack and patch levels.

This approach to managing locked down images poses a challenge, as the usual patch management tools and cycles are not best placed or designed to support this.

bluesource addresses this challenge with our managed virtual desktop service. Our experts will keep the Azure Virtual Desktop master image(s) up to date with the latest operating system and application patches to ensure an evergreen and up to date service. We will – on a monthly basis – roll out the updated master image(s) across the session host pool(s), move users onto the new session hosts and ensure the old session hosts are cleaned up from the pool and Active Directory.

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 enhanced support service has been purchased or another escalation path is available – or assigning to our managed service team for change requests.

The bluesource Managed Virtual Desktop service includes the following key features:

- **2<sup>nd</sup> & 3<sup>rd</sup> line reactive support** – for issues arising out of the day-to-day business as usual activities to maintain the health of the solution. An unlimited number of tickets can be logged with bluesource under the Agreement although a time-based Fair Usage Policy applies.
- **Proactive monitoring and management** – delivering automated alerting for monitoring threshold breaches and service to maintain and optimise the performance and health of the Azure Virtual Desktop infrastructure.
- **Master image update management** – monthly patching of Azure Virtual Desktop master images operating systems and applications to ensure the platform remains up to date and protected as patches are released as well as ensuring session host standardisation and predictable user experience by tightly controlling session host configuration.
- **Inclusive standard administration** – to support clients as the platform grows.
- Service delivery management – to support and manage service quality, govern relations 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:

<b>"Business Day"</b>	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.
<b>"Fair Usage Policy"</b>	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 as detailed in the Work Order.
<b>"Incident"</b>	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.
<b>"Images"</b>	the number of distinct Azure Virtual Desktop master images that are managed under this agreement is limited to one (1) unless otherwise detailed in the Work Order.

<b>“Pools”</b>	the number of distinct Azure Virtual Desktop host pools that are managed under this agreement is limited to one (1) unless otherwise detailed in the Work Order.
<b>“Update Rollout”</b>	the number of image updates included under this agreement is limited to twelve (12) per annum unless otherwise detailed in the Work Order.
<b>“Service Level Agreement (SLA)”</b>	the Service level obligations set out in this Service Schedule.
<b>“Service Start Date”</b>	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.
<b>“SMC”</b>	bluesource’s global Service Management Centre providing personnel responsible for delivery of the Services.
<b>“Target Response Time”</b>	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.
<b>“Ticket”</b>	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 Service is provided 24x7x365 for monitoring and proactive management.

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

Priority 2, 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 Inclusions

Service Component	Description	Service hours	Service level
Incident management <sup>1</sup>	2 <sup>nd</sup> and 3 <sup>rd</sup> line remote technical support with incident activity tracking & reporting.	24x7	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 3.3 for SLA details.	Business Day	Included
Service availability & resource health monitoring <sup>2</sup>	Proactive monitoring and management of the Azure Virtual Desktop platform.	24x7	Included
Standard administration <sup>3</sup>	Well-defined pre-approved activities that do not require change board review.	Business Day	Included
Master image Update Rollout <sup>4</sup>	Twelve (12) master image updates per annum (one per month).	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, hours used along with addressing any challenges.	Once per quarter	Included
Major incident reporting	Service delivery management reporting for any P1 major incidents through to resolution.	Business Day	Included

### Notes:

<sup>1</sup> Examples of Incidents that are within the scope of this service include:

- One or more session hosts are not available.
- One or more user profiles have been corrupted, hung or are ghosting.
- Monthly patching has affected an application and requires rollback.
- One or more users are unable to login to Azure Virtual Desktop.

<sup>2</sup>The following activities only are included as part of the monitoring service:

- Azure Virtual Desktop availability, capacity & performance monitoring & dashboard.
- User profile storage capacity monitoring.
- Resource health monitoring and alerting.
- Automated ticket logging.

<sup>3</sup>The following activities only are included as standard administration:

- Installation of a new app to one of the in-scope master images to be rolled out during the monthly pool re-roll.
- Removal of an app from one of the in-scope master images to be removed as part of the monthly pool re-roll.
- Scaling up or down the master image and session hosts to a different virtual machine size.
- Scaling out or in the number of session hosts for a given host pool.
- User assignment changes.
- Azure Virtual Desktop policy changes.
- Publishing applications to users.

<sup>4</sup>Patch updates are limited to the following unless otherwise detailed in the Work Order:

- Windows operating system patches.
- Microsoft Office application patches where appropriate.
- Browser updates where appropriate.

## 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](mailto: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](mailto: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:

- Customer network diagnosis – both local area networks and wide area networks.
- End user desktop support incidents.
- Support or remediation of Azure Virtual Desktop dependencies such as Active Directory Domain Services and networks.
- Support monitoring or remediation of the wider Azure services.
- Documentation of any infrastructure.
- Support for published applications.
- Onsite response to any incidents, service requests or change requests.
- Implementation of new workloads and features – bluesource can deliver these through discrete project engagements via our consultancy service.
- Availability of Microsoft 365 applications.
- Patching and management of end user compute hardware or software applications and packages.
- 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's Customer's purchase the bluesource enhanced support add-on, we will escalate incidents to Microsoft via the Customer's enhanced support agreement with bluesource.

## 7 Customer obligations

The Customer shall:

- Provide sufficient available bandwidth on the Customer network to support the Azure Virtual Desktop 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 reasonable and relevant access and permissions necessary for bluesource to monitor the service and provision Azure Monitor workbooks
- Provide contact details of authorised personnel, who can engage with bluesource support.
- Provide reasonable and relevant access and permissions necessary for bluesource to action change requests.
- Maintain suitable licensing to support the Azure Virtual Desktop service – should the Customer wish bluesource to manage licensing then we can quote for licenses through the Microsoft Cloud Solution Provider (CSP) program.
- Maintain relevant Third-Party support and maintenance contracts for published applications.
- 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" and "granular delegated admin roles" for the tenant/s.
- Be responsible for all Azure hosting costs.

## 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.