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

bluesource will deliver a Cloud Application Backup service ("**Service**") (including all Equipment, Software and Systems), to enable:

(i) copies of Backup Data protecting the Data; and
(ii) recovery of Backup Data following Data loss.

## 2 Definitions

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

| | |
|---|---|
| **"Backup Data"** | means the Customer's data located within the Cloud Application (collectively referred to herein as "Data") which is the subject of the Services and which is managed and backed up pursuant to this Service Schedule. This source data or data that is backed up prior to applying any deduplication or compression. |
| **"Backup Data Retention(s)"** | means the period that data is stored within the backup service. |
| **"Backup Schedule(s)"** | means the frequency of the backups. The default schedule is that backup data will be backed up once per day typically after the Business Day has completed. |
| **"Backup Vault"** | means a target for storing backups. |
| **"Cloud Application"** | means the application[s] that are subject for backup. These can include Mailboxes in Office 365, One Drive for Business and SharePoint online. |
| **"Cloud Application[s] Networks"** | means the network over which data is transferred. |
| **"DataShield Cloud Targets"** | is where backup data is stored. |
| **"Equipment"** | includes collectively or individually bluesource's computer and other associated equipment (including any part or parts thereof) for use by either bluesource or Customer at the Site (or any subsequent site agreed in writing by the Parties in the provision of the Services including any third-party hardware and software. |
| **"Media Agents"** | means the compute resource needed to backup, restore and manage content for backup and recovery purposes. |
| **"Site(s)"** | the Customer's premises where the Services are to be delivered as set out in the Work Order. |
| **"Software"** | all computer programs supplied by and/or used by and/or procured by bluesource for the provision of the Services. |
| **"System"** | collectively or individually the Software, computer equipment and associated equipment (including any part or parts thereof) for use by either bluesource or licensed by bluesource to Customer at the Sites for the provision of the Services. |

## 3 Term and Termination

This Service Schedule shall commence on the Commencement Date and shall continue for the Initial Term subject to the provisions of Clause 9 of the General Terms and Conditions and clause 4 below. Upon expiry of the Initial Term, this Service Schedule shall automatically continue until terminated by either party giving to the other not less than 90 days written notice to expire on or after the expiry of the Initial Term, in accordance with the termination provisions of said Clause 9.

## 4 Effects of Termination

In addition to clause 11 (Effects of Termination) of the General Terms and Conditions:

**4.1** On termination of this Service Schedule for any reason:

a) bluesource shall immediately cease provision of the Services but may provide services for a further period in accordance with Clause 4.2;
b) any licence to use the Software, Equipment, Programs or any other licence granted by bluesource to the Customer shall terminate;
c) any licence to use Customer data or Backup Data granted by the Customer to bluesource shall terminate;
d) the Customer shall allow bluesource and its employees and subcontractors reasonable access to the Site to remove the Equipment;
e) The accrued rights of the parties as at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced.

**4.2** The Customer may, no less than three (3) months (or such shorter period as bluesource may agree in writing) prior to the termination of this Agreement request bluesource to offer reasonable assistance in transitioning the Services from bluesource to the Customer or its nominated replacement supplier. bluesource may, subject to agreeing reasonable terms and fees (to be agreed in advance), provide such additional services for a maximum period of three months. bluesource shall use its reasonable endeavours to agree an appropriate plan, co-operate and support the Customer to achieve an orderly transfer.

## 5 Support for Cloud Application/s

Backup and recovery of SaaS (Software as a Service) applications as detailed below:

### 5.1 Cloud Applications

5.1.1 **Exchange Online** – is supported for the protection of Mailbox data using “one pass” technology, this service is delivered purely to DataShield Cloud Targets (bypasses on premise Media Agents if the Customer has them) – Backups are performed on a per mailbox basis (not database level) and data can be restored to the mailbox, or to PST file. In order to protect Exchange Online, the Customer must complete certain Office 365 configuration tasks relating to service accounts, Application and API setup and configuration and permissions management. The steps are detailed in the service onboarding guide.

5.1.2 **Mailbox Archiving**.

5.1.3 **OneDrive for Business** – is supported for the protection of One Drive folder data. This service is delivered purely to DataShield Cloud Targets (bypasses on premise Media Agents if the customer has them) – Backups are performed on a per OneDrive folder basis (individually selected OneDrive accounts) and data can be restored in or out of place. The Customer must complete certain Office 365 configuration tasks relating to service accounts, Application and API setup and configuration and permissions management. The steps are detailed in the service onboarding guide.

5.1.4 **SharePoint Online** – is supported for the protection of SharePoint site data (not databases) for the recovery of site level and document level information. This service is delivered purely to DataShield Cloud Targets (bypasses on premise Media Agents if the customer has them) – Backups are performed on a per SharePoint site basis with the capability to restore individual items in or out of place. The Customer must complete certain Office 365 configuration tasks relating to service accounts, Application and API setup and configuration and permissions management, An Azure Storage account is required for SharePoint recoveries.

5.1.5 **Microsoft Teams**.

### 5.2 Self-service portal

The portal is secured with a CA signed certificate for security and enables the Customer to perform certain administrative tasks without the need to log service tickets.

5.2.1 **Tenant Users** – Designated Customer accounts that can administer resources within their tenancy.

A customer registered as a **“Tenant User”** is typically able to:

a. Browse & restore protected files (including files within Supported VM’s), virtual machines, databases, and Cloud App backups on-demand on behalf of their end users for resources against which they have been assigned ownership.
b. Perform on-demand backup jobs for data, Supported VMs, or database and applications
c. View data protection and restore job history for all data types

d. View data protection configurations
e. View data protection/restore reports.

## 6 Back up schedule

The Service provides a default backup schedule once per day, to which writes the Backup Data to a Media Agent[s]. Subject to Change Management (see section 8 below), the Customer may request an alternative backup schedule or Data Retention to meet specific industry, legal, regulatory, audit or best practice demands; this may incur additional costs. The contract may deploy data retention service tiers which will be identified in the Service Pricing and the table below indicates the frequency of backups within each Service tier:

| | Daily Backups (Qty) | Weekly Full Backup (Qty) | Monthly Full Backup (Qty) | Yearly Full Backup (Qty) | Maximum Data Retention |
|---|---|---|---|---|---|
| **Standard (Default)** | **7** | **4** | | | **30 Days** |
| **Silver** | **7** | **4** | **3** | | **90 Days** |
| **Gold** | **7** | **4** | **12** | | **1 year** |
| **Platinum** | **7** | **4** | | **1** | **7 Years** |

bluesource shall use all reasonable endeavours to respond to Data restoration requests promptly and it is anticipated that the majority of individual files can be rapidly recovered from the backup information held on the backup master server, with the recovery process being initiated as soon is reasonably practicable after bluesource has become aware of the need to do the same.

## 7 Network

The Service is dependent on the Customer's own computer systems, network and data communication links. The Customer may also be reliant on Cloud Application/s Networks that provide Customer access to the backup data. If required, bluesource will advise Customer prior to commencement of the Services as to the performance characteristics required including, without limitation, the size of the networks to enable the transmission of Backup Data to meet the agreed Backup Schedule. For the avoidance of doubt, Customer shall be responsible, without limitation, for ensuring that Customer has arranged any necessary firewall and network setup, way-leave, landlord permission, and associated planning requirements or similar upon which it needs to be able to use the Service.

## 8 Change Management

bluesource will install any Software and Equipment required for the Service usually within the Business Day. All reconfiguration, rescheduling and performance tuning of the Equipment and/or Software will be agreed by both Parties and carried out by bluesource upon receipt of written notification from the Customer

## 9 Service Availability

bluesource's Service Management Centre ("SMC") will be available 24x7 for Priority 1 and 2 incidents/problems and for Priority 3 and 4 incidents/problems/service requests, available during the Business Day. Outside of these hours, Priority 3 and 4 incidents/problems/service requests will be logged the next Business Day.

bluesource does not warrant that the Customer's use of the Service will be uninterrupted or error free.

## 10 Service Levels

### 10.1 Support

bluesource offers SLAs for the time to start working on issues raised to its service management centre ("**SMC**").

When an incident, problem or service request is received and logged as a service ticket, they are assigned a priority based on bluesource 's experience, which has a targeted response time ("target Response Time"), as below:

| Priority | Target Response Time |
|---|---|
| P1 – Critical Business Impact | 15 minutes |
| P2 – Severe Business Impact | 60 minutes |
| P3 – Inconvenient Business Impact | 1 Business Day (within 10 hrs) |
| P4 – Minor Business Impact | Next Business Day (within 20 hrs) |

Where P1 and P2 classified incidents, problems and service requests are identified by the Customer, they need to be escalated to the bluesource SMC via telephone, **0345 319 2200,** in order to receive the appropriate response. The target Response Time for P1 and P2 classified incidents applies 24x7.

P3 and P4 classified incidents, problems and service requests 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.

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

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.

### 10.2 Target Service Levels

The estimated target for provision of the Service is that at least 97% of submitted and active backup data will successfully complete to the Media Agents according to the agreed Backup Schedule but excluding failure and/or non-availability of the Customer's own computer networks, equipment (including desktops) and data communications links.

## 11 Security

Bluesource does not access the Backup Data, apart from to automatically index individual filenames and the directory structure to aid identification and recovery of files by the Customer. The Customer is therefore responsible for undertaking appropriate virus detection and prevention actions to secure their Data against corruption.

Customer shall ensure that any encryption keys associated with bluesource's optional encryption service are securely retained by the Customer. Unless explicitly stated otherwise, if the Customer loses its encryption key, it will not be able to access its data and (as between Bluesource and Customer) Customer is solely responsible for the Customer's confidentiality and use of encryption keys. In no event will bluesource be liable for any loss of Data or other claims arising in connection with unauthorized access caused by the act or omission of Customer.

## 12 Monitoring

bluesource monitors the Equipment (and Software) against the Target Service Levels. This monitoring is undertaken within the Vault server/s by bluesource. The monitoring includes critical components of the Equipment, interpreting error logs in order to seek to ensure that Data is backed up in accordance with this Service Schedule.

## 13 Reporting

bluesource will provide exception reports, notifying Customer any Service failures. In addition, bluesource will provide Customer with monthly service reports detailing achievement against Target Service Levels, Customer's protected mailboxes, service and usage characteristics.

## 14 bluesource Responsibilities

As necessary for the performance of the Service bluesource will:

- Install Software on to Customer's agreed nominated servers and desktops to meet the reasonable operational requirements of the Services.
- Integrate and configure the Equipment and Software including testing to demonstrate to a nominated Customer representative that bluesource is capable of providing the Service.
- Remotely monitor the Services using automated processes.
- Undertake regular health checks of all backup servers and related components.
- Provide regular patch updates and upgrades to the Software and Equipment.
- Provide the opportunity for quarterly onsite meetings with a nominated Customer representative to discuss the performance of the Service against the Target Service Levels.

## 15 Customer Responsibilities

Customer will:

- **Account Administration** -
  - keep account details and any associated passwords secure and confidential at all times;
  - acknowledge that anyone accessing the Customer account or Services using the Customer's password is assumed by bluesource to be doing so with the Customer's authority; and
  - be responsible for the administration for user accounts and services.
  - the configuration of Service Accounts, API integration, Permissions and other configuration items required specifically for the protection of Cloud Applications
- **Security** –
  - be solely responsible for determining whether the security is sufficient for their purposes and for implementing any other security measures deemed appropriate. bluesource only provides the security features that are expressly stated to be part of the Service.
  - responsible for implementing reasonable security and environmental precautions to ensure a high level of system availability and data protection and recovery
  - responsible for securing any passwords and encryption keys for the Service
- **System Change**
  - Inform bluesource of any Cloud Application[s] that no longer require the backup service, any new Cloud Application[s] or any increase in Data exceeding 30% of current month Data to be submitted for backup;

- **Communications Links**
  - provide communication links between the edge point of the Service the Customer's network as required to use the Service.
  - provide VPN access where required, between the Site and the Service. Delay or failure to setup suitable access could affect bluesource's ability to provide the Service.
  - perform and/or arrange all firewall configuration changes needed on the Customer's end to establish connectivity between bluesource and the Sites at its own expense.
  - responsible for all Internet, communication and other costs associated with the use of the Services.
- **Support**
  - if required, provide a secure, monitored and protected rack space/data centre space to install onsite Equipment at the nominated Sites and provide necessary data communications network links for the Services to be provided;
  - reasonably alert bluesource to potential issues that may affect the performance of the Services including non-availability of Cloud Applications environmental failures in their data centre, network or internet connectivity, or external security threats that may be caused, but not limited to, virus or persistent system intrusion events;
  - provide access to the Sites (by prior arrangement) as required to provide the Service including desk, computer, telephony, stationery and any other equipment reasonably required to meet the requirements of the assignment;
  - acknowledge that bluesource's ability to provide support may be severely affected if an appointed Customer contact lacks the necessary technical and product knowledge to assist with the timely resolution of a fault. Accordingly, bluesource shall have no liability to Customer in this regard.
  - provide bluesource with a list of personnel (including contact details), who are authorised to engage with bluesource support on behalf of the Customer, this list being updated from time to time and communicated to bluesource.
  - provide a dedicated point of contact for major incident escalation and 24/7 out of hours contact/s, as frequently communicated to bluesource and updated.
  - provide details and reasonable documentation of any security policies and change management procedures that bluesource has agreed to adhere to in the applicable Work Order.
  - notify bluesource of any Customer planned changes, downtime and maintenance windows, and include bluesource in CAB and ECAB meetings where Services are likely to be affected.
  - be responsible for patching, hot fix and vulnerability application within their environment;
  - respond to and resolve escalations relating to issues not covered by bluesource under this Service Description.
  - be responsible for arranging any third-party support and maintenance contracts for applications and hardware outside the scope of the Service.
  - be responsible for the support of applications and hardware, including that of third parties, not referenced in the Service Description has being bluesource's responsibility.

## 16 Backup Data Security

**16.1** Bluesource shall establish and maintain such security measures and procedures as are reasonable to provide for the safe custody of the System, the Software and the Backup Data and to seek to reasonably prevent unauthorised access to or use thereof.

**16.2** Security copies and reconstruction of the System:

a) During the term of the applicable Service, bluesource shall keep such Backup Data copies until Customer requests in writing for the Backup Data to be destroyed or returned. Within 14 days of termination or expiry of the applicable Service, bluesource shall at the request and cost of Customer, destroy (and where required certify), or return the Backup Data;
b) In the event of any breakdown of or fault in the System with consequential loss or spoiling of the Backup Data or any part thereof, bluesource shall provide such Backup Data copies as to Customer to enable Customer to reconstitute the Backup Data.

**16.3** Loss of the Backup Data: If the Backup Data or any part thereof shall be lost, destroyed or damaged whilst in bluesource's possession prior to inputting, then bluesource shall notify Customer, who shall, if available, promptly provide bluesource with copies of the Backup Data or other records held by Customer, whereupon bluesource shall use such copy to resubmit for Backup Data generation.

## 17 Data Protection

**17.1** 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

**17.2** 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.

**17.3** 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.

**17.4** 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.