DATA PROTECTION & INFORMATION SECURITY REQUIREMENTS FOR SUPPLIERS

Suppliers (and any contractors forming part of services to bluesource or its customers) must comply with this security policy in relation to the performance of services to bluesource and its customers, except as otherwise agreed in writing between the Parties. This includes access to technology and handling of both bluesource and customer information/data in whatever form.

All capitalised terms not defined in this security policy (the "**Security Policy**") will have the meaning assigned to them in the relevant contract, work order or other agreement between the Parties.

1. Definitions

"Agreement" means any written agreement, master service agreement, contract, sow, service schedule or other such document agreed between Bluesource and Supplier, together the Parties.

"Bluesource Data" means, collectively and individually, all data and information including, without limitation, confidential information and Personal Data which is (a) disclosed or furnished, in any form, by bluesource, its customers, associates, agents or employees to Supplier in connection with Supplier's performance of the Services, or (b) collected, stored, processed, transmitted, accessed or used by Supplier in connection with Supplier's performance of the Services.

"Bluesource Personal Data" means Bluesource Data that is considered as Personal Data.

"Bluesource Systems" means collectively and individually, bluesource's, its customers' and associates' information systems, applications, databases, infrastructure, platforms, and networks.

"Customer" means collectively and individually bluesource, its customers and associates.

"Data Protection Law" means all applicable data protection and privacy legislation, regulations and guidance including Regulation (EU) 2016/679 (the "General Data Protection Regulation" or the "GDPR") and Data Protection Act 2018 ("DPA") (or, in the event that the UK leaves the European Union, all legislation enacted in the UK in respect of the protection of personal data) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (all as amended, updated or re-enacted from time to time).

"Data Controller" has the meaning given to it in Data Protection Law.

"Data Processor" has the meaning given to it in Data Protection Law**.**

"Data Privacy Incident" means any: a) Disclosure of Personal Data by Supplier in violation of this Security Policy or applicable laws pertaining to data protection or data security, or b) Other unauthorised, accidental or unlawful access, acquisition, disclosure or use of Personal Data that has occurred or may have occurred, including, without limitation, any unauthorised access of which Supplier is notified or suspects.

"Data Processing Regulator" means the Information Commissioner's Office and any other data protection supervisory authority with jurisdiction over either party and/or their Processing activities, and in each case any successor body from time to time.

"Data Subject" has the meaning given to it in Data Protection Law.

"Information Security Incident" means any: a) Data Privacy Incident, or b) any event, activity or occurrence that threatens or may threaten the confidentiality, integrity and/or availability of the Systems.

"Parties" shall refer to both bluesource and the Supplier, as parties to a contractual arrangement.

"Personal Data" has the meaning given to it in Data Protection Law.

"Policy" means this **"**DATA PROTECTION & INFORMATION SECURITY REQUIREMENTS FOR SUPPLIERS" policy.

"Process", **"Processing"** and **"Processed"** each has the meaning given in Data Protection Law.

"Service" means the service/s provided to bluesource, its customers, or associates.

"Standard Contractual Clauses" shall mean the Standard Contractual Clauses annexed to the European Commission Decision (2010/87/EU

"Supplier" means a supplier of services to bluesource and/or bluesource's customers.

"Supplier Systems" means Supplier's information systems, processes, facilities, applications, databases, infrastructure, platforms, and networks (a) utilised to provide the Services, (b) collecting, storing, processing, transmitting, accessing or using Bluesource Data, and/or (c) with access to, connection to, use of or otherwise interacting with Bluesource Systems.

"Systems" means collectively bluesource Data, bluesource Systems and Supplier Systems.

SECTION 1 - Data Protection Obligations ("Data Protection Policy")

2. Data Protection

2.1 In connection with performing its services, Supplier may process Bluesource Personal Data as Data Processor (or sub-processor, as the case may be) on behalf of Bluesource. The details of the Processing carried out by Supplier on behalf of Bluesource should be set out as per clause 10 (Data Processing Instructions). Each of Bluesource and Supplier will comply with their respective obligations under Data Protection Law, and Bluesource will procure that each Bluesource Customer does so.

2.2 Where Supplier processes Bluesource Personal Data as Data Processor on behalf of Bluesource (or a Bluesource Customer, as the case may be) Supplier shall:

2.2.1 Process Bluesource Personal Data only on behalf of Bluesource and only as necessary to provide the relevant Services to Bluesource for the benefit of the relevant Bluesource Customer (as specified in an Agreement) (the "**Instructions**");

2.2.2 Prior to carrying out any Instruction from Bluesource, notify Bluesource if in the Supplier's reasonable opinion, such Instruction is likely to result in a breach of Data Protection Law, provided that Bluesource acknowledges and agrees that Supplier is not a law firm or data privacy consultancy, and that advice on data privacy compliance is not within the scope of its Services, and that consequently Supplier will have no liability whatsoever to any person whosoever for the giving or not giving, or the content or accuracy of, any such notification;

2.2.3 Assist Bluesource from time to time, as the relevant Bluesource Customer may reasonably request, having regard to Supplier's role and the information available to it, and at Bluesource's cost, with:

a) completing and reviewing data protection impact assessments and prior consultations of relevant supervisory authorities;

b) so far as practicable given Supplier's levels of access to and knowledge of the relevant Bluesource Personal Data, responding to requests by data subjects to exercise their rights over that Bluesource Personal Data, it being acknowledged and agreed that such assistance will be available to Bluesource only where the tools accessible to it as part of the relevant Service do not enable it or the relevant Bluesource Customer to identify or extract relevant data without Supplier's assistance, and where Supplier is technically able to do so;

2.2.4 Implement measures to mitigate against any data protection risks that could affect Bluesource Personal Data;

2.2.5 Not transfer Bluesource Personal Data outside of the UK or European Economic Area ("EEA") without Bluesource's prior written consent. Where Bluesource provides such consent, Parties shall agree an appropriate mechanism as permitted under Data Protection Laws to protect the rights and freedoms of the data subjects affected by that transfer.

2.3 The Company shall notify Bluesource without undue delay should it:

2.3.1 receive notice of any investigation or adverse finding by a Data Protection Regulator in relation to its Processing of Personal Data which could pose a risk to Bluesource Personal Data;

2.3.2 be under a legal obligation to Process Bluesource Personal Data, other than under the Instructions, in which case it shall inform Bluesource of the legal obligation, except to the extent the law prohibits it from doing so;

2.3.3 receive any request from or on behalf of a Data Subject exercising their rights under the Data Protection Law in respect of Bluesource Personal Data under the exclusive control of Supplier.

2.4 The Company is not permitted to use Bluesource Personal Data in a test environment unless Bluesource has provided prior written consent. Such use shall be in accordance with written instructions given by Bluesource from time to time.

2.5 When Processing live Bluesource Personal Data in a test environment, the Supplier's obligations under this Policy shall continue to apply.

3. Security

3.1 When Processing Bluesource Personal Data, Supplier shall take the Information Security Requirements for Suppliers detailed in Section 2 below (the "**Security Measures**"). Supplier hereby warrants and undertakes that it is fully compliant with the Security Measures save for any exceptions authorised by Bluesource in writing.

3.2 The Supplier shall test:

3.2.1 the Security Measures regularly (and, in any event, at least annually) to assess the effectiveness of the measures in ensuring the security, confidentiality, integrity, availability and resilience of Bluesource Personal Data;

3.2.2 the disaster recovery and business continuity plans regularly (and in any event, at least annually) to assess the effectiveness of such plans; and

3.2.3 all back up facilities containing Bluesource Personal Data regularly (and, in any event, at least quarterly).

3.3 The Supplier shall maintain written records of all testing carried out in accordance with Clause 3.1 and make non confidential extracts of such records available to Bluesource on request.

3.4 The Supplier shall not combine or aggregate Bluesource Personal Data with any third-party data unless approved in writing by Bluesource. The storage of Bluesource Personal Data shall be logically separated from all other third-party data unless such aggregation of data is authorised within the Services specification or, otherwise by written agreement between the Parties.

4. Records of Processing

4.1 In order for Bluesource to fulfil its obligations to record the processing of Bluesource Personal Data under Data Protection Law, it requires its suppliers to comply with their obligations under Article 30, as a Data Processor, and to provide bluesource with details of:

4.1.1 its data protection officer (“DPO”) or person responsible for data protection, where a DPO is not required under Data Protection Law, so that bluesource can engage on data protection maters; and

4.1.2 a summary of the data processing carried out on Bluesource Personal Data as per clause 10.1

5. Security breach notification

5.1 Supplier shall notify Bluesource without undue delay and within 24 hours of Supplier confirming a security breach (as defined by Data Protection Laws) has occurred involving Bluesource Personal Data.

5.2 The notification in Clause 5.1 shall include, where practicable given the stage of Supplier’s investigation, reasonable details of the:

5.2.1 nature of the data breach, including where possible, the categories and approximate number of Data Subjects and records concerned;

5.2.2 contact at the Supplier who will liaise with Bluesource concerning the Security Incident; and

5.2.3 remediation measures being taken or proposed to be taken to mitigate and contain the breach.

5.3 In the event of a breach:

5.3.1 the Supplier shall provide reasonable updates if requested by Bluesource; and

5.3.2 the Supplier shall comply with any remediation actions reasonably required by Bluesource to protect their Personal Data.

5.4 All notifications should be sent to:

- Nick Jaggers
  Head of Operations
  020 7940 6220
  nick.jaggers@bluesource.co.uk; and
- Privacy@bluesource.co.uk

5.5 All emails should be followed up by a telephone call after 2 hours of sending to confirm receipt.

5.6 In relation to any effected Bluesource Personal Data, Bluesource shall at its sole discretion determine whether and in what form to provide notification to the Data Subject, any third party or Data Protection Regulator and Supplier shall not notify the Data Subject, any third party or Data Protection Regulator unless such disclosure by Supplier is required by law or is otherwise approved by Bluesource.

6. Sub-contracting

6.1 Supplier may engage sub-processors to process Bluesource Personal Data on its behalf (each, a "**Sub-Processor**") provided that it: (i) identifies those Sub-Processors to Bluesource; (ii) binds those Sub-Processors by a written agreement complying with the requirements of article 28 of GDPR (as it applies to that Sub-Processor's processing activities); and (iii) it remains liable to Bluesource for the acts and omissions of those Sub-Processors as if they were the acts or omissions of Supplier itself (and subject therefore to the limitations and exclusions of liability set out in the Agreement. Supplier's Sub-Processors relevant to a Service must be set out in the relevant Agreement. Where Supplier wishes to engage a different or an additional Sub-Processor, it shall first inform Bluesource of the identity of the proposed Sub-Processor and provide Bluesource with a reasonable opportunity to object to that Sub-Processor's engagement. If Bluesource does so object it will inform Supplier within 14 days of being so informed, giving reasons for the objection, and if Supplier cannot within 30 days of that objection address the reasons for it to Bluesource's reasonable satisfaction then Supplier may choose not to appoint that Sub-Processor, or it may choose to appoint that Sub-Processor regardless, in which case Bluesource will be entitled to terminate the affected Agreements by notice to Supplier.

7. Personnel

7.1 The Supplier shall:

7.1.1 take reasonable steps to ensure the reliability of any of its employees, agents and sub-contractors (including Approved Sub-contractors) who have access to Bluesource Personal Data;

7.1.2 ensure that only those of its employees, agents and sub-contractors (including Approved Sub-contractors) who need to have access to Bluesource Personal Data are granted such access to the Bluesource Personal Data and only for the purposes of performing its obligations under Agreement; and

7.1.3 ensure that the employees, agents and sub-contractors (including Approved Sub-contractors) who, in accordance with clause 7.1.2, have access to Bluesource Personal Data:

7.1.3.1 are informed of the confidential nature of Bluesource Personal Data and are subject to appropriate contractual obligations of confidentiality;

7.1.3.2 undergo training in Data Protection Law and in the care and handling of Personal Data; and

7.1.3.3 comply with the obligations set out in this Policy including the obligations set out as Security Measures.

8. Audit

8.1 Supplier shall allow the Data Controller (i.e. Bluesource Customer, or Bluesource where it is the Data Controller), or its external auditor (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit Supplier's data processing activities insofar as they relate to the Bluesource Personal Data, to enable the Data Controller to verify that Supplier is in compliance with this schedule, provided that Bluesource shall procure that: (i) the Bluesource Customer may exercise that inspection and audit right no more frequently than once per calendar year, unless required by a supervisory authority of competent jurisdiction; (ii) the Bluesource Customer will meet Supplier's reasonable costs incurred as a result of any such inspection or audit, unless that inspection or audit shows Supplier to be in breach of this schedule; (iii) the Bluesource Customer (or its auditor, as the case may be) will not thereby be entitled to access to personal data or confidential information of any other Supplier customer (including but not limited to any other Bluesource Customer), nor to direct access to any computer or storage system of Supplier or its Sub-Processors unless explicitly required by a supervisory authority of competent jurisdiction; (iv) the Bluesource Customer (or its auditor, as the case may be) complies with Supplier's reasonable policies while onsite, including its safety and security policies; and (v) any information coming into Bluesource's or the Bluesource Customer's possession (or that of its auditor, as the case may be) as a result of such inspection or audit will be and remain the Confidential Information of Supplier for the purposes of the Agreement, and Bluesource and the Bluesource Customer will (and will procure that its auditor will, as the case may be) treat it accordingly.

9. General

9.1 In the event of any conflict between the provisions and/or Schedules of this Policy, and the provisions and/or Schedules of an Agreement in respect of the subject matter of this Policy, save where otherwise agreed in writing between the Parties or as otherwise expressly provided for in this Policy, the order of precedence shall be: 1) clauses of this Policy; 2) Schedules of this Policy; and unless otherwise defined in an Agreement to the contrary; 3) Schedules of an Agreement; and finally 4) the clauses of an Agreement.

9.2 A breach of the provisions of this Policy shall be deemed a material breach of the Agreement.

10. Data Processing Instruction

10.1 Unless otherwise agreed in writing by the Parties, the following Data Processing Instruction shall be updated/completed by the Supplier and incorporated into relevant Agreements as a "Data Processing Summary", as required by Article 28 of GDPR:

SUPPLIER DETAILS	
Company Name	[to be updated by the Supplier]
Address	[to be updated by the Supplier]

SUPPLIER CONTACT	
Contact Name	[to be updated by the Supplier]
Contact Title / Job Role	[to be updated by the Supplier]
Department	[to be updated by the Supplier]
Phone Number	[to be updated by the Supplier]
Email	[to be updated by the Supplier]

DATA PROCESSING SUMMARY / INSTRUCTION FOR PROCESSING

In respect of services, application and/or systems containing Bluesource Personal Data:

	Response
Purpose for which the Personal Data shall be processed and its legal basis, and nature of consent.	For example: The legal basis for processing PII related to providing Information Technology related services to Bluesource and/or its customers, and maintain a contractual relationship [GDPR, Article 6,1 (b)]. Without the appropriate Personal Data, the services and Agreement/s could not be maintained. [to be updated by the Supplier and agreed between the Parties]
Nature of processing	For example: Storing, accessing and reviewing Personal Data in accordance with the terms of the Agreement and any applicable statement of work or services specification form. [to be updated by the Supplier and agreed between the Parties]
Description of the categories of the Data Subjects	For example: The Data Subjects, who's appropriate Personal Data may be processed during the provision of services under Agreement include: • Bluesource employees, subcontractors or associates; • Bluesource customer employees, associates, contractors and subcontractors; using a service provided by Supplier under Agreement; • Supplier employees necessary to procure and provide services to Bluesource. [to be updated by the Supplier and agreed between the Parties]
Description of the categories of Personal Data	For example: Personal Data includes but not limited to: • Names; • Job titles; • Departments; • Address; • Email addresses; • Telephone numbers. Certain Services, and access to websites and portals, may also capture necessary login details, cookies and IP addresses for authentication, security and customisation purposes. Further details can be found in Supplier's privacy and cookie policies, which may be updated from time to time. [to be updated by the Supplier and agreed between the Parties]

Categories of Special Category Data	For example: Through the normal course of providing this type of services, Supplier would not normally process Special Categories of Personal Data, as defined by Data Protection Laws. [to be updated by the Supplier and agreed between the Parties]
Description of transfers of Personal Data to a country outside of the EEA.	For example: Supplier will not transfer or process Bluesource Personal Data outside of the EEA without the prior written authorisation of Bluesource. [to be updated by the Supplier and agreed between the Parties]
Duration of Processing	For example: Supplier will retain Personal Data for as long as necessary to deliver services under Agreement and relevant for their operations or to comply with relevant laws. In addition, Supplier may need to retain certain Personal Data after termination of the relationship to comply with laws or legislation, prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with any investigation, enforce our policies and agreements and take other actions permitted or required by applicable laws. [to be updated by the Supplier and agreed between the Parties]
General description of technical and organisational security measures	For example: Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the severity of the risks to the rights and freedoms of natural persons, take and maintain appropriate technical and organisational measures (including, where applicable, complying with Bluesource's policies and procedures relating to data protection) in relation to the Personal Data to ensure a level of security appropriate to the level of risk (and in assessing risk shall take account, in particular, of the risks that are presented by processing in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the personal data). Such measures shall include inter alia as appropriate: • Access control on a "who needs to know, minimum rights" basis for both electronic and paper-based data, • Maintaining an information security management system to ISO27001, • Minimising the processing of Personal Data, • The pseudonymisation and encryption of Personal Data, • Transparency with regards to the functions and processing of Personal Data, • The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, • The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and • A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;". These measure/controls may be updated from time to time. [to be updated by the Supplier and agreed between the Parties]
Authorised Sub-Processors	For example: The Supplier shall not engage subcontractors, except Authorised Subcontractors, without the prior written authorisation of Bluesource senior management. [to be updated by the Supplier and agreed between the Parties]

10.2 If any part of Bluesource Personal Data is no longer needed by the Supplier for the purposes of performing its obligations under Agreement or where the Agreement has been terminated or expired for whatever reason, Bluesource shall have the option to direct the Supplier to:

10.2.1 securely return Bluesource Personal Data to Bluesource; and/or

10.2.2 securely delete such Bluesource Personal Data from all of the Supplier's software and/or hardware systems; and/or

10.2.3 procure that Bluesource Personal Data is securely deleted from all of the software and/or hardware systems of the Supplier's employees, agents or sub-contractors (as applicable).

10.3 If the Supplier s unable is to comply with Clause 10.2 because it is required by law or an applicable regulator to retain a copy of Bluesource Personal Data, or required for reasonable Supplier operational needs (such as compliance with HMRC, FSA, accounting, fraud and audit), shall provide written details of Bluesource Personal Data it is retaining and the reason for such retention.

SECTION 2 – Security Measures ("Security Policy")

1. Governance and Risk

The Supplier shall:

1.1 Implement and maintain an information security policy covering the Services provided to Customer, in line with industry standards such as ISO 27001/2.
1.2 Provide Bluesource with copies of its certifications in information security, such as ISO27001, and maintain them during the term of Services.
1.3 Establish clear roles and responsibilities for information security.
1.4 Provide bluesource with a named single point of contact who holds overall responsibility for information security at the Supplier.
1.5 Conduct an independent review of information security controls and processes annually.
1.6 Conduct risk assessments for the Services provided to Customer.
1.7 Not subcontract any part of the Services, including hosted or cloud-based technology services, without the prior written consent of bluesource. Furthermore the Supplier is responsible for ensuring the requirements within this security policy are included within contractor agreements.
1.8 Maintain an inventory of all IT assets supporting the services.
1.9 Maintain a policy that requires information to be classified, handled and disposed of according to its sensitivity.
1.10 Inform Bluesource of any material changes to the Service provision or the Supplier's operations, including but not limited to: change of IT strategy or geographical operations, mergers and acquisitions, change of third party support or hosting, security breach that could affect the Customer's data.
1.11 Promptly correct any vulnerability or security issue discovered in the Supplier's Systems.

2. Confidentially and Bluesource Data

2.1 The provisions in this Paragraph 13 are in addition to, and without limitation to, the confidentiality requirements set forth in Agreement between Bluesource and the Supplier. Bluesource Data will be considered Confidential Information as that term is defined in this Security Policy and will be treated in accordance with the terms of this Security Policy.
2.2 Upon termination of an Agreement for any reason or if requested by Bluesource, Supplier in accordance with clause 10.2 of the Data Protection Policy above, will promptly rectify, amend, erase, block, destroy or return, in each case in a sufficiently secure manner as approved and directed by Bluesource, all Bluesource Data in its possession and shall not retain any copies of Bluesource Data. If destruction is requested, Supplier will:
(i) destroy the Bluesource Data in accordance with applicable laws, Bluesource's directions (if any) and taking into account available technology so that the Bluesource Data cannot be read or reconstructed, and
(ii) promptly provide Bluesource with a declaration in a form satisfactory to Bluesource, duly executed by an officer of Supplier, verifying that such Bluesource Data has been destroyed. Supplier will keep all system generated security logs created as part of standard operational security procedures associated with the protection of Bluesource for a period of seven (7) years.
2.3 Supplier will ensure the integrity of Bluesource Data and protect it from unlawful, accidental or improper alteration, corruption, or destruction.

3. Access Control

3.1 Logical and physical access to Bluesource Data and Bluesource Systems shall be on a least-privilege basis and only at a level required for the performance of a function or role.
3.2 All actions on IT systems shall be attributable to an individual.
3.3 Prompt removal of logical and physical access to information where Supplier personnel no longer require this.
3.4 Immediate removal of logical and physical access to information where employment is terminated.
3.5 Regular review of user accounts and system privileges, in particular privileges of IT personnel.

3.6 Use of strong passwords on all systems processing Bluesource Data in accordance with the following minimum standard: seven characters, complexity enabled, not reused with 6 months, valid for a maximum age of 90 days, lockout threshold of three invalid logon attempts, reset lockout counter after 30 minutes.

3.7 Secure procedures for the management and distribution of passwords to personnel.

3.8 Bluesource Data shall be physically or logically segregated from other data.

3.9 End user devices, including mobile devices, shall be password/pin protected when left unattended.

3.10 Remote access to systems shall use two-factor authentication and only be provided on a needs basis and with automatic time out enabled.

3.11 Equipment accessing Bluesource Data and Bluesource Systems shall have password protected screensavers and automatic locking enabled for 5 minutes of inactivity and where left unattended.

4. Device and Media Controls

4.1 Supplier will ensure that all media containing Bluesource Data sent outside its facilities is logged, authorised by management, and sent via secured courier or other delivery method that can be tracked.

4.2 The Service Provider shall ensure that no Bluesource Data is stored on any portable medium or device except where such storage is strictly required for the performance of the Services.

4.3 Where Bluesource Data is stored in accordance with 4.2 or transmitted across a network or stored on any portable medium or device, the level of protection that the Supplier is obliged to adopt pursuant to 5.1 shall be consistent both with the data security classification of the data in question and with the additional risk posed by its transmission and/or its storage on a portable medium or device.

5. Data Security and Personal Data

5.1 Supplier will implement and maintain physical and technical controls designed to:

(i) Guard against unauthorised access to or disruption or altering or copying or removal of the Supplier Systems and Bluesource Data (including when Bluesource Data is transmitted over an electronic communications network or while being recorded onto data carriers), and

(ii) Implement no less than industry standard encryption with respect to all records and files containing Bluesource Data either at rest or in transit including, without limitation, all Bluesource Data to be transmitted across public networks or wirelessly, and all Bluesource Data stored on laptops, servers or removable media.

5.2 Supplier will process Personal Data in accordance with Data Protection Laws

5.3 Supplier agrees not to transfer Bluesource Data out of the UK or EEA, without the prior written consent of Bluesource in accordance with clause 2.2.5 of the Data Protection Policy above.

6. Cloud Hosting (where appropriate)

6.1 Supplier will not utilize “public cloud” computing services as part of any hosted solution or service or otherwise connect Bluesource Systems to, or allow Bluesource Data to be collected, transmitted, processed or stored on a “public cloud” service without first obtaining written consent from Bluesource.

6.2 Where any part of the Services is supported by cloud hosting, the following additional requirements apply:

6.2.1 Compliance with the latest version of the Cloud Security Alliance Cloud Controls Matrix https://cloudsecurityalliance.org/ or other substantially similar assurance agreed with Bluesource and where necessary the Customer.

6.2.2 Penetration test of internet-facing services by an independent CREST-certified provider and all outstanding findings remediated or mitigated within 30 days of the test report.

6.2.3 Encryption of Bluesource Data at rest.

6.2.4 Logical isolation of Bluesource Data from other customers of the Supplier.

6.2.5 Physical or logical isolation or encapsulation of Supplier's service from other cloud tenants.

7. Personnel security

7.1 Supplier shall screen all personnel prior to providing access to Bluesource Data to the following minimum standard:

7.1.1 Identity check

7.1.2 Criminal record check
7.1.3 Eligibility to work check
7.1.4 Qualification check (where applicable)
7.1.5 Reference validation

7.2 Bluesource may require reasonable additional levels of screening where Supplier has access to information of a particularly sensitive nature as agreed in a specific Agreement such as the requirement for credit checks to be able to work on FSA regulated customers, or relevant security clearance for government and police forces, etc.

7.3 Supplier shall review status of screened individuals for changes at regular intervals.

7.4 Where applicable, specific information security training shall be provided to all Supplier staff.

7.5 Security awareness shall be provided to all Supplier staff on an ongoing basis and at least every twelve months.

7.6 Supplier maintains the right to invoke the disciplinary process, up to and including staff dismissal, for a breach of Supplier's security policy.

7.7 Training and awareness shall provide instructions and guidance on at least the following:

7.7.1 Reporting suspected or confirmed security incidents, including lost devices.
7.7.2 Secure handling and disposal of hard-copy information.
7.7.3 Consequences of non-compliance with security policy.
7.7.4 General cyber threats and common contemporary attack methods such as phishing and social engineering.
7.7.5 Staying secure when out of the office and travelling.
7.7.6 Keeping authentication credentials confidential.
7.7.7 Prohibition on the use of personal messaging, email and collaboration services for work purposes
7.7.8 Use of unauthorised software.
7.7.9 Locking work stations and other devices when unattended.

8. Physical Security

8.1 Supplier shall employ appropriate controls to restrict physical access to Bluesource Data, including but not limited to: physical barriers on entry, visitor and contractor access controls, video recording, alarm systems or guarded entry.

8.2 Areas requiring additional physical security, such as those housing IT equipment, shall employ enhanced or additional controls such as restricted access control, access logging, two-factor authentication.

8.3 Hard copy Bluesource Data and other media must be disposed of securely and where stored, held securely with appropriate access controls in place.

9. Change and incident management

9.1 All IT system changes shall be reviewed, tested and deployed using a formal change management process.

9.2 Supplier shall operate a formal security incident management process and one that includes response plans and procedures for forensic analysis that legally preserve evidence.

9.3 Supplier shall report to Bluesource any incident that has, or is likely to have, a material adverse effect on the Customer.

10. Resilience and business continuity

10.1 In the event of a failure or disruption to the services, Supplier shall ensure that normal services are available in the shortest practicable time.

10.2 Supplier shall have in place business continuity plans and procedures for the Service that are tested annually.

11. Operations security

11.1 Where Supplier develops software:

11.1.1 this shall be in accordance with a secure development lifecycle that employs secure coding practices. Software found to have security vulnerabilities will not be accepted by Bluesource.
11.1.2 Supplier shall respond to software vulnerabilities identified by Bluesource with a remediation plan with agreed remediation timescales.
11.1.3 Software development shall be performed using segregated development/test and live environments.

11.2 No Bluesource Data shall be used for testing purposes without the prior consent of Bluesource.

11.3 Supplier shall operate a formal patch management process with expedited application off critical security patches.

11.4 Supplier shall maintain standardised and hardened builds for systems and end-user devices, that are patched for known vulnerabilities prior to use.

11.5 Supplier shall install and maintain robust malware protection software on systems and end-user devices.

11.6 Supplier shall implement and maintain appropriately configured firewalls, intrusion detection/prevention technologies and other network security measures to protect Customer data.

12. Logging and monitoring

12.1 Supplier shall collect and store logs such that access to Bluesource Data can be determined. These logs shall be made available to Bluesource on request.

12.2 Supplier shall monitor security logs and devices to detect malicious activity.

12.3 Supplier shall implement monitoring and detection processes to protect Bluesource Data against disclosure, in accordance with applicable privacy legislation.

13. Incident Response Plan; Notification of Information Security Incident; Remedial Action

13.1 Supplier will implement policies and procedures designed to detect, respond to, and otherwise address Information Security Incidents.

13.2 Supplier will notify Bluesource of any Information Security Incident within one (1) hour of Supplier's knowledge or suspicion thereof via telephone and electronic mail. In addition, within twelve (12) hours of the Information Security Incident, Supplier will provide a written report via secure email describing in sufficient detail the Information Security Incident, the Bluesource Data concerned, the Suppliers response and corrective actions. This written report will include relevant information needed for Bluesource to assess the impact of the Information Security Incident.

13.3 Supplier will provide Bluesource with a daily Information Security Incident status update and a final written report once the Information Security Incident has been resolved. Supplier will:

(i) fully assist Bluesource and any regulator or other governmental body with oversight over the Information Security Incident in investigating, remedying and taking any other action Bluesource deems necessary regarding the Information Security Incident (including providing Bluesource with all on-going information related to the Information Security Incident requested by Bluesource, including raw logs for forensic investigations) and any dispute, inquiry or claim that concerns the Information Security Incident;

(ii) indemnify Bluesource for any and all damages, penalties, fines, losses, fees or costs (whether direct, indirect, special or consequential) incurred as a result of such incident, and remedy any harm or potential harm caused by such incident;

(iii) promptly correct any deficiencies that resulted in the Information Security Incident at no additional charge to Bluesource or Customer;

(iv) unless prohibited by an applicable statute or court order, notify Bluesource of any third-party legal process relating to the Information Security Incident; and

(v) provide Bluesource with satisfactory assurance that such Information Security Incident or potential Information Security Incident will not recur. In addition, if Bluesource's investigation of the Information Security Incident is not commercially practicable, Supplier will engage, at its sole cost, a mutually agreeable third party to conduct the investigation.

13.4 Except as required by law, in no event will Supplier serve any notice of, inform a third party of, or otherwise publicise the Information Security Incident, without the prior written consent of Bluesource.

13.5 Bluesource Security Official:

Name: Nick Jaggers
Title: Head of Operations and DPO
Phone: +44 (0)20 7940 6200
Email: nick.jaggers@bluesource.co.uk

14. Compliance, testing and right to audit

The Supplier shall:

14.1 At Bluesource's request and with reasonable notice, permit Bluesource, or its designee, to enter any premises at which the Services, or any part thereof, are performed, for the purpose of inspecting, auditing, and determining whether the Supplier's information security program is consistent with terms herein, and whether the information security program has been adequately implemented to ensure the security of Bluesource Data.

14.2 Where necessary, perform an independent penetration test of all internet-facing systems at least annually.

14.3 Allow Bluesource to conduct penetration testing upon request and where reasonable notice is provided.

14.4 Protect its infrastructure, laptops, pcs and other equipment against virus and malware attacks using suitable endpoint protection solutions.

14.5 Conduct regular vulnerability scans of internal networks and systems and promptly remediate or mitigate findings.

14.6 Monitor the effectiveness of security policy and controls and continuously improve these as appropriate.

14.7 Where applicable, agree data hosting locations with Customer prior to the commencement of services. Changes to the jurisdiction in which data is stored and processed by the Supplier must be agreed in advance with Customer.

15. Acceptable Use Policy

15.1 If Supplier personnel will have access to Customer's internal information technology systems, the terms and conditions of Bluesource's Access Control and Acceptable Use Policies (and, as amended by Bluesource from time-to-time in its sole discretion) which shall be supplied to the Supplier on request, as well as the terms and conditions set forth in this Security Policy, will apply to Supplier and each of its personnel having such access.

16. Subcontractors

16.1 If, consistent with and subject to the terms of this Security Policy, supplier intends to (i) provide access to any Bluesource Data or Bluesource Systems to any subcontractors or other third parties, or (ii) use any subcontractors or other third parties to fulfill information technology or security functions then it must notify Bluesource in advance in writing (such notice to reasonably provide the identity of such party and its functions) and obtain written approval from Bluesource.

16.2 Supplier will execute formal written agreements with each approved subcontractor that require appropriate confidentiality requirements and security controls employed by any such approved subcontractor.

16.3 Supplier will maintain a list of all its subcontractors with details of the date, time and form of approval by Bluesource and a list of locations where Bluesource Data is processed.

16.4 Supplier must pass down the requirements of this Security Policy to the subcontractor and all times be responsible, accountable and liable for the subcontractor's actions and compliance against these Security Policy terms.

17. PCI

17.1 To the extent that Supplier collects, stores, transfers or processes any Payment Data, Supplier acknowledges and agrees that it is responsible for the security of such Payment Data and will comply and maintain compliance with the most current PCI Standards as well as this Security Policy. Upon Bluesource's reasonable request, Supplier will provide attestations of such compliance.

17.2 For the purposes of this Schedule, "Payment Data" means a credit or debit card holder's credit or debit card account number, bank account number, name, service code, security code, card validation code or value (e.g., CVV number), expiration date, magnetic stripe data, PIN, PIN block, and/or password, which is (a) disclosed or furnished, in any form, by Bluesource, its associates, agents or employees to Supplier in connection with Supplier's performance of the Services, or (b) collected, stored, processed, transmitted, accessed or used by Supplier in connection with Supplier's performance of the Services.

18. Survival

18.1 The provisions of this Security Policy will survive the expiration or earlier termination of an Agreement and will only cease once Supplier ceases to process or hold any Bluesource Data.