

**Cabinet Office**

**- and -**

**Warwick Economics & Development Ltd**

**ATTACHMENT 5**

**relating to**

**Provision of UK Property Workforce Report**

**CCZZ23A14**

**CONTENTS**

[**ANNEX 1 – TERMS AND CONDITIONS** 6](#_heading=h.30j0zll)

[1](#_heading=h.1fob9te) INTERPRETATION 6

[2](#_heading=h.21od6so) BASIS OF AGREEMENT 7

[3](#_heading=h.2et92p0) SUPPLY OF SERVICES 8

[4](#_heading=h.1t3h5sf) TERM 8

[5](#_heading=h.2s8eyo1) CHARGES, PAYMENT AND RECOVERY OF SUMS DUE 8

[6](#_heading=h.17dp8vu) PREMISES AND EQUIPMENT 9

[7](#_heading=h.gtnh0h) STAFF AND KEY PERSONNEL 10

[8](#_heading=h.z337ya) ASSIGNMENT AND SUB-CONTRACTING 11

[9](#_heading=h.30tazoa) INTELLECTUAL PROPERTY RIGHTS 11

[10](#_heading=h.1fyl9w3) GOVERNANCE AND RECORDS 12

[11](#_heading=h.3zy8sjw) CONFIDENTIALITY, TRANSPARENCY AND PUBLICITY 12

[12](#_heading=h.2f3j2rp) FREEDOM OF INFORMATION 13

[13](#_heading=h.u8tczi) PROTECTION OF PERSONAL DATA AND SECURITY OF DATA 14

[14](#_heading=h.3e8gvnb) LIABILITY 14

[15](#_heading=h.1tdr5v4) FORCE MAJEURE 15

[16](#_heading=h.1v1yuxt) UK PROPERTY WORKFORCE REPORT SECURITY SCHEDULE FINAL V1 15

[17](#_heading=h.4ddeoix) SECURITY TESTING 15

[18](#_heading=h.2sioyqq) TERMINATION 21

[19](#_heading=h.17nz8yj) COMPLIANCE 22

[20](#_heading=h.25b2l0r) PREVENTION OF FRAUD AND CORRUPTION 22

[21](#_heading=h.3rnmrmc) DISPUTE RESOLUTION 23

[22](#_heading=h.2iq8gzs) GENERAL 23

[23](#_heading=h.3hv69ve) NOTICES 24

[24](#_heading=h.4h042r0) GOVERNING LAW AND JURISDICTION 24

[**ANNEX 2 – PRICE SCHEDULE** 25](#_heading=h.2w5ecyt)

[**ANNEX 3 – STATEMENT OF REQUIREMENTS** 26](#_heading=h.1baon6m)

[**ANNEX 4 – SUPPLIERS RESPONSE** 34](#_heading=h.22vxnjd)

[**ANNEX 5 – CLARIFICATIONS** 35](#_heading=h.1h65qms)

[**ANNEX 6 – ADDITIONAL TERMS & CONDITIONS** 36](#_heading=h.26sx1u5)

[**ANNEX 7 – CHANGE CONTROL FORMS** 45](#_heading=h.ly7c1y)

[**ANNEX 8 – UK PROPERTY WORKFORCE REPORT SECUIRTY SCHEDULE FINAL V1** 47](#_heading=h.35xuupr)

**ANNEX 1 – TERMS AND CONDITIONS**

1. **INTERPRETATION**
	1. In these terms and conditions:

|  |  |
| --- | --- |
| “Agreement”  | means the contract between (i) the Customer acting as part of the Crown and (ii) the Supplier constituted by the Supplier’s countersignature of the Award Letter and includes the Award Letter; |
| “Award Letter” | means the letter (including the Annexes thereto) from the Customer to the Supplier via the e-Sourcing Suite at the point of award; |
| “Central Government Body” | means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:1. Government Department;
2. Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);
3. Non-Ministerial Department; or
4. Executive Agency;
 |
| “Charges” | means the charges for the Services as specified in the Award Letter;  |
| “Confidential Information” | means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential; |
| “Customer” | means the Contracting Authority/Customer named in the Award Letter; |
| “DPA” | means the Data Protection Act 2018;  |
| “Expiry Date” | means the date for expiry of the Agreement as set out in the Award Letter;  |
| “FOIA” | means the Freedom of Information Act 2000; |
| “Information” | has the meaning given under section 84 of the FOIA;  |
| “Key Personnel”  | means any persons specified as such in the Award Letter or otherwise notified as such by the Customer to the Supplier in writing;  |
| “Party” | means the Supplier or the Customer (as appropriate) and “Parties” shall mean both of them;  |
| “Personal Data” | means personal data (as defined in the DPA) which is processed by the Supplier or any Staff on behalf of the Customer pursuant to or in connection with this Agreement; |
| “Purchase Order Number” | means the Customer’s unique number relating to the supply of the Services;  |
| “Request for Information” | has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term “request” shall apply);  |
| “Services” | means the services to be supplied by the Supplier to the Customer under the Agreement;  |
| “Specification” | means the specification for the Services (including as to quantity, description and quality) as specified in the Award Letter;  |
| “Start Date” | means the commencement date of the Agreement as set out in the Award Letter; |
| “Staff” | means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any sub-contractor of the Supplier engaged in the performance of the Supplier’s obligations under the Agreement;  |
| “Staff Vetting Procedures” | means vetting procedures that accord with good industry practice or, where requested by the Customer, the Customer’s procedures for the vetting of personnel as provided to the Supplier from time to time;  |
| “Supplier” | means the person named as Supplier in the Award Letter; |
| “Term” | means the period from the Start Date of the Agreement set out in the Award Letter to the Expiry Date as such period may be extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement;  |
| “VAT” | means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and |
| “Working Day” | means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London. |

* 1. In these terms and conditions, unless the context otherwise requires:
		1. references to numbered clauses are references to the relevant clause in these terms and conditions;
		2. any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;
		3. the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Agreement;
		4. any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and
		5. the word ‘including’ shall be understood as meaning ‘including without limitation’.
1. **BASIS OF AGREEMENT**
	1. The Award Letter constitutes an offer by the Customer to purchase the Services subject to and in accordance with the terms and conditions of the Agreement.
	2. The offer comprised in the Award Letter shall be deemed to be accepted by the Supplier on receipt by the Customer, within 2 days of the date of the award letter, of a copy of the Award Letter countersigned by the Supplier.
2. **SUPPLY OF SERVICES**
	1. In consideration of the Customer’s agreement to pay the Charges, the Supplier shall supply the Services to the Customer for the Term subject to and in accordance with the terms and conditions of the Agreement.
	2. In supplying the Services, the Supplier shall:
		1. co-operate with the Customer in all matters relating to the Services and comply with all the Customer’s instructions;
		2. perform the Services with all reasonable care, skill and diligence in accordance with good industry practice in the Supplier’s industry, profession or trade;
		3. use Staff who are suitably skilled and experienced to perform tasks assigned to them, and in sufficient number to ensure that the Supplier’s obligations are fulfilled in accordance with the Agreement;
		4. ensure that the Services shall conform with all descriptions, requirements, service levels and specifications set out in the Specification;
		5. comply with all applicable laws; and
		6. provide all equipment, tools and vehicles and other items as are required to provide the Services.
	3. The Customer may by written notice to the Supplier at any time request a variation to the scope of the Services. In the event that the Supplier agrees to any variation to the scope of the Services, the Charges shall be subject to fair and reasonable adjustment to be agreed in writing between the Customer and the Supplier.
3. **TERM**
	1. The Agreement shall take effect on the Start Date and shall expire on the Expiry Date, unless it is otherwise extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement.
	2. The Customer may extend the Agreement for one period of up to two weeks by giving not less than 10 Working Days’ notice in writing to the Supplier prior to the Expiry Date. The terms and conditions of the Agreement shall apply throughout any such extended period.
4. **CHARGES, PAYMENT AND RECOVERY OF SUMS DUE**
	1. The Charges for the Services shall be as set out in the Award Letter and shall be the full and exclusive remuneration of the Supplier in respect of the supply of the Services. Unless otherwise agreed in writing by the Customer, the Charges shall include every cost and expense of the Supplier directly or indirectly incurred in connection with the performance of the Services.
	2. All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Customer shall, following the receipt of a valid VAT invoice, pay to the Supplier a sum equal to the VAT chargeable in respect of the Services.
	3. The Supplier shall invoice the Customer as specified in the Agreement. Each invoice shall include such supporting information required by the Customer to verify the accuracy of the invoice, including the relevant Purchase Order Number and a breakdown of the Services supplied in the invoice period.
	4. In consideration of the supply of the Services by the Supplier, the Customer shall pay the Supplier the invoiced amounts no later than 30 days after verifying that the invoice is valid and undisputed and includes a valid Purchase Order Number. The Customer may, without prejudice to any other rights and remedies under the Agreement, withhold or reduce payments in the event of unsatisfactory performance.
	5. If the Customer fails to consider and verify an invoice in a timely fashion the invoice shall be regarded as valid and undisputed for the purpose of paragraph 5.4 after a reasonable time has passed.
	6. If there is a dispute between the Parties as to the amount invoiced, the Customer shall pay the undisputed amount. The Supplier shall not suspend the supply of the Services unless the Supplier is entitled to terminate the Agreement for a failure to pay undisputed sums in accordance with clause 16.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 19.
	7. If a payment of an undisputed amount is not made by the Customer by the due date, then the Customer shall pay the Supplier interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.
	8. Where the Supplier enters into a sub-contract, the Supplier shall include in that sub-contract:
		1. provisions having the same effects as clauses 5.3 to 5.7 of this Agreement; and
		2. a provision requiring the counterparty to that sub-contract to include in any sub-contract which it awards provisions having the same effect as 5.3 to 5.8 of this Agreement.
		3. In this clause 5.8, “sub-contract” means a contract between two or more suppliers, at any stage of remoteness from the Customer in a subcontracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Agreement.
	9. If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Customer in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Customer from any sum then due, or which may come due, to the Supplier under the Agreement or under any other agreement or contract with the Customer. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Customer in order to justify withholding payment of any such amount in whole or in part.
5. **PREMISES AND EQUIPMENT**
	1. If necessary, the Customer shall provide the Supplier with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Customer’s premises by the Supplier or the Staff shall be at the Supplier’s risk.
	2. If the Supplier supplies all or any of the Services at or from the Customer’s premises, on completion of the Services or termination or expiry of the Agreement (whichever is the earlier) the Supplier shall vacate the Customer’s premises, remove the Supplier’s plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Customer’s premises in a clean, safe and tidy condition. The Supplier shall be solely responsible for making good any damage to the Customer’s premises or any objects contained on the Customer’s premises which is caused by the Supplier or any Staff, other than fair wear and tear.
	3. If the Supplier supplies all or any of the Services at or from its premises or the premises of a third party, the Customer may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises.
	4. The Customer shall be responsible for maintaining the security of its premises in accordance with its standard security requirements. While on the Customer’s premises the Supplier shall, and shall procure that all Staff shall, comply with all the Customer’s security requirements.
	5. Where all or any of the Services are supplied from the Supplier’s premises, the Supplier shall, at its own cost, comply with all security requirements specified by the Customer in writing.
	6. Without prejudice to clause 3.2.6, any equipment provided by the Customer for the purposes of the Agreement shall remain the property of the Customer and shall be used by the Supplier and the Staff only for the purpose of carrying out the Agreement. Such equipment shall be returned promptly to the Customer on expiry or termination of the Agreement.
	7. The Supplier shall reimburse the Customer for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Supplier or any Staff. Equipment supplied by the Customer shall be deemed to be in a good condition when received by the Supplier or relevant Staff unless the Customer is notified otherwise in writing within 5 Working Days.
6. **STAFF AND KEY PERSONNEL**
	1. If the Customer reasonably believes that any of the Staff are unsuitable to undertake work in respect of the Agreement, it may, by giving written notice to the Supplier:
		1. refuse admission to the relevant person(s) to the Customer’s premises;
		2. direct the Supplier to end the involvement in the provision of the Services of the relevant person(s); and/or
		3. require that the Supplier replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Customer to the person removed is surrendered,

and the Supplier shall comply with any such notice.

* 1. The Supplier shall:
		1. ensure that all Staff are vetted in accordance with the Staff Vetting Procedures;
		2. if requested, provide the Customer with a list of the names and addresses (and any other relevant information) of all persons who may require admission to the Customer’s premises in connection with the Agreement; and
		3. procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Customer.
	2. Any Key Personnel shall not be released from supplying the Services without the agreement of the Customer, except by reason of long-term sickness, parental leave and termination of employment or other extenuating circumstances.
	3. Any replacements to the Key Personnel shall be subject to the prior written agreement of the Customer (not to be unreasonably withheld). Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.
1. **ASSIGNMENT AND SUB-CONTRACTING**
	1. The Supplier shall not without the written consent of the Customer assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the Agreement or any part of the Agreement. The Customer may, in the granting of such consent, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Supplier shall be responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.
	2. Where the Customer has consented to the placing of sub-contracts, the Supplier shall, at the request of the Customer, send copies of each sub-contract, to the Customer as soon as is reasonably practicable.
	3. The Customer may assign, novate, or otherwise dispose of its rights and obligations under the Agreement without the consent of the Supplier provided that such assignment, novation or disposal shall not increase the burden of the Supplier’s obligations under the Agreement.
2. **INTELLECTUAL PROPERTY RIGHTS**
	1. All intellectual property rights in any materials provided by the Customer to the Supplier for the purposes of this Agreement shall remain the property of the Customer or the respective owner of such intellectual property rights but the Customer hereby grants the Supplier a royalty-free, non-exclusive and non-transferable licence to use such materials as required until termination or expiry of the Agreement for the sole purpose of enabling the Supplier to perform its obligations under the Agreement.
	2. All intellectual property rights in any materials created or developed by the Supplier pursuant to the Agreement or arising as a result of the provision of the Services shall vest in the Supplier. If, and to the extent, that any intellectual property rights in such materials vest in the Customer by operation of law, the Customer hereby assigns to the Supplier by way of a present assignment of future rights that shall take place immediately on the coming into existence of any such intellectual property rights all its intellectual property rights in such materials (with full title guarantee and free from all third party rights).
	3. The Supplier hereby grants the Customer:
		1. a perpetual, royalty-free, irrevocable, non-exclusive licence (with a right to sub-license) to use all intellectual property rights in the materials created or developed pursuant to the Agreement and any intellectual property rights arising as a result of the provision of the Services; and
		2. a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:
			* 1. any intellectual property rights vested in or licensed to the Supplier on the date of the Agreement; and
				2. any intellectual property rights created during the Term but which are neither created or developed pursuant to the Agreement nor arise as a result of the provision of the Services,

including any modifications to or derivative versions of any such intellectual property rights, which the Customer reasonably requires in order to exercise its rights and take the benefit of the Agreement including the Services provided.

* 1. The Supplier shall indemnify, and keep indemnified, the Customer in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded against or incurred or paid by the Customer as a result of or in connection with any claim made against the Customer for actual or alleged infringement of a third party’s intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of the Supplier or any Staff.
1. **GOVERNANCE AND RECORDS**
	1. The Supplier shall:
		1. attend progress meetings with the Customer at the frequency and times specified by the Customer and shall ensure that its representatives are suitably qualified to attend such meetings; and
		2. submit progress reports to the Customer at the times and in the format specified by the Customer.
	2. The Supplier shall keep and maintain until 6 years after the end of the Agreement, or as long a period as may be agreed between the Parties, full and accurate records of the Agreement including the Services supplied under it and all payments made by the Customer. The Supplier shall on request afford the Customer or the Customer’s representatives such access to those records as may be reasonably requested by the Customer in connection with the Agreement.
2. **CONFIDENTIALITY, TRANSPARENCY AND PUBLICITY**
	1. Subject to clause 11.2, each Party shall:
		1. treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and
		2. not use or exploit the disclosing Party’s Confidential Information in any way except for the purposes anticipated under the Agreement.
	2. Notwithstanding clause 11.1, a Party may disclose Confidential Information which it receives from the other Party:
		1. where disclosure is required by applicable law or by a court of competent jurisdiction;
		2. to its auditors or for the purposes of regulatory requirements;
		3. on a confidential basis, to its professional advisers;
		4. to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;
		5. where the receiving Party is the Supplier, to the Staff on a need to know basis to enable performance of the Supplier’s obligations under the Agreement provided that the Supplier shall procure that any Staff to whom it discloses Confidential Information pursuant to this clause 11.2.5 shall observe the Supplier’s confidentiality obligations under the Agreement; and
		6. where the receiving Party is the Customer:
			* 1. on a confidential basis to the employees, agents, consultants and contractors of the Customer;
				2. on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company to which the Customer transfers or proposes to transfer all or any part of its business;
				3. to the extent that the Customer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or
				4. in accordance with clause 12 and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the customer under this clause 11.

* 1. The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of the Agreement is not Confidential Information and the Supplier hereby gives its consent for the Customer to publish this Agreement in its entirety to the general public (but with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the Agreement agreed from time to time. The Customer may consult with the Supplier to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the provisions of the FOIA.
	2. The Supplier shall not, and shall take reasonable steps to ensure that the Staff shall not, make any press announcement or publicise the Agreement or any part of the Agreement in any way, except with the prior written consent of the Customer.
1. **FREEDOM OF INFORMATION**
	1. The Supplier acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall:
		1. provide all necessary assistance and cooperation as reasonably requested by the Customer to enable the Customer to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;
		2. transfer to the Customer all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 2 Working Days of receipt;
		3. provide the Customer with a copy of all Information belonging to the Customer requested in the Request for Information which is in its possession or control in the form that the Customer requires within 5 Working Days (or such other period as the Customer may reasonably specify) of the Customer's request for such Information; and
		4. not respond directly to a Request for Information unless authorised in writing to do so by the Customer.
	2. The Supplier acknowledges that the Customer may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Supplier or the Services (including commercially sensitive information) without consulting or obtaining consent from the Supplier. In these circumstances the Customer shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the Supplier advance notice, or failing that, to draw the disclosure to the Supplier’s attention after any such disclosure.
	3. Notwithstanding any other provision in the Agreement, the Customer shall be responsible for determining in its absolute discretion whether any Information relating to the Supplier or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.
2. **PROTECTION OF PERSONAL DATA AND SECURITY OF DATA**
	1. The Supplier shall, and shall procure that all Staff shall, comply with any notification requirements under Data Protection Legislation and both Parties shall duly observe all their obligations under Data Protection Legislation which arise in connection with the Agreement.
	2. REPLACED BY ANNEX 6 IN RELATION TO PROTECTION OF PERSONAL DATA
	3. When handling Customer data (whether or not Personal Data), the Supplier shall ensure the security of the data is maintained in line with the security requirements of the Customer as notified to the Supplier from time to time.
3. **LIABILITY**
	1. The Supplier shall not be responsible for any injury, loss, damage, cost or expense suffered by the Customer if and to the extent that it is caused by the negligence or wilful misconduct of the Customer or by breach by the Customer of its obligations under the Agreement.
	2. Subject always to clauses 14.3 and 14.4:
		1. the aggregate liability of the Supplier in respect of all defaults, claims, losses or damages howsoever caused, whether arising from breach of the Agreement, the supply or failure to supply of the Services, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed a sum equal to 125% of the Charges paid or payable to the Supplier; and
		2. except in the case of claims arising under clauses 9.4 and 18.3, in no event shall the Supplier be liable to the Customer for any:
			* 1. loss of profits;
				2. loss of business;
				3. loss of revenue;
				4. loss of or damage to goodwill;
				5. loss of savings (whether anticipated or otherwise); and/or
				6. any indirect, special or consequential loss or damage.
	3. Nothing in the Agreement shall be construed to limit or exclude either Party's liability for:
		1. death or personal injury caused by its negligence or that of its Staff;
		2. fraud or fraudulent misrepresentation by it or that of its Staff; or
		3. any other matter which, by law, may not be excluded or limited.
	4. The Supplier’s liability under the indemnity in clause 9.4 and 18.3 shall be unlimited.
4. **FORCE MAJEURE**
	1. Neither Party shall have any liability under or be deemed to be in breach of the Agreement for any delays or failures in performance of the Agreement which result from circumstances beyond the reasonable control of the Party affected. Each Party shall promptly notify the other Party in writing when such circumstances cause a delay or failure in performance and when they cease to do so. If such circumstances continue for a continuous period of more than two months, either Party may terminate the Agreement by written notice to the other Party.
5. **UK PROPERTY WORKFORCE REPORT SECURITY SCHEDULE FINAL V1**
	1. UK Property Workforce Report Security Schedule Final V1 - Annex 8 –
6. **SECURITY TESTING**
	1. This paragraph applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
	2. **Note:** the definition of Supplier Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Supplier providing the Services.
	3. The Supplier must, at the Buyer’s option, before providing the Services and when reasonably requested by the Buyer, either:
		1. conduct security testing of the Supplier Information Management System by:
			1. engaging a CHECK Service Provider or a CREST Service Provider;
			2. designing and implementing the testing so as to minimise its impact on the Supplier Information Management System and the delivery of the Services; and
			3. providing the Buyer with a full, unedited and unredacted copy of the testing report without delay and in any event within ten Working Days of its receipt by the Supplier; or
		2. Provide details of any security testing undertaken by a CHECK Service Provider or a CREST Service Provider in respect of the Supplier Information Management System in the calendar year immediately preceding the Buyer’s request or the Effective Date (as appropriate), including:
			1. the parts of the Supplier Information Management System tested;
			2. a full, unedited and unredacted copy of the testing report; and
			3. the remediation plan prepared by the Supplier to address any vulnerabilities disclosed by the security testing; and
			4. the Supplier’s progress in implementing that remediation plan.
	4. The Supplier must remediate any vulnerabilities classified as “medium” or above in the security testing:
		1. before Processing Buyer data where the vulnerability is discovered before the Supplier begins to process Authority Data;
		2. where the vulnerability is discovered when the Supplier has begun to Process Buyer Data:
			1. by the date agreed with the Buyer; or
			2. where no such agreement is reached:
				1. within five Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;
				2. within one month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and
				3. within three months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.
7. End-user Devices
	1. The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data is stored or processed in accordance the following requirements:
		1. the operating system and any applications that store, process or have access to Buyer Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
		2. users must authenticate before gaining access;
		3. all Buyer Data must be encrypted using a encryption tool agreed to by the Buyer;
		4. the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
		5. the End-user Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data;
		6. the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data on the device and prevent any user or group of users from accessing the device;
		7. all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001:2018 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
	2. The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.
	3. Where there any conflict between the requirements of this Schedule [x] (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.
8. Encryption
	1. Unless paragraph 5.2 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:
		1. when stored at any time when no operation is being performed on it; and
		2. when transmitted.
	2. Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.1, the Supplier must:
		1. immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
		2. provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
		3. provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.
	3. The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.
	4. This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
	5. Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
		1. the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;
		2. the protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Buyer Data.
	6. Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to be determined by an expert in accordance with the Dispute Resolution Procedure.
9. Access Control
	1. The Supplier must, and must ensure that all Sub-contractors:
		1. identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
		2. require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;
		3. allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
		4. maintain records detailing each person’s access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.
	2. The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:
		1. are accessible only from dedicated End-user Devices;
		2. are configured so that those accounts can only be used for system administration tasks;
		3. require passwords with high complexity that are changed regularly;
		4. automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.
	3. The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Supplier Information Management System.
	4. The Supplier must, and must ensure that all Sub-contractors:
		1. configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
		2. change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.
10. Malicious Software
	1. The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.
	2. The Supplier shall ensure that such Anti-virus Software:
		1. is configured to perform automatic software and definition updates;
		2. performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
		3. where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
	3. If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
	4. Any cost arising out of the actions of the parties taken in compliance with the provisions of paragraph 7.3 shall be borne by the parties as follows:
		1. by the Supplier where the Malicious Software originates from the Supplier Software, any third-party software licenced by the Supplier or the Buyer Data (whilst the Buyer Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
		2. by the Buyer, in any other circumstance.
11. Breach of Security
	1. If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.
	2. The Supplier must, upon becoming aware of a Breach of Security or attempted Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other reasonably steps necessary to:
		1. minimise the extent of actual or potential harm caused by such Breach of Security;
		2. remedy such Breach of Security to the extent possible;
		3. apply a tested mitigation against any such Breach of Security; and
		4. prevent a further Breach of Security in the future which exploits the same root cause failure.
	3. As soon as reasonably practicable and, in any event, within five Working Days, or such other period agreed with the Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.
	4. The Supplier must take the steps required by paragraph 8.2 at its own cost and expense.
12. Sub-contractors
	1. The Supplier must assess the parts of the information and communications technology system and the Sites that its Subcontractors will use to provide the Services against the NCSC Cloud Security Principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Buyer at the Buyer’s request.
13. Third-party Software
	1. The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Progress the Buyer Data greater than those rights strictly necessary for the use of the software.
14. Deletion of Buyer Data
	1. The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor when requested to do so by the Buyer using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

1. **TERMINATION**
	1. The Customer may terminate the Agreement at any time by notice in writing to the Supplier to take effect on any date falling at least 1 month (or, if the Agreement is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.
	2. Without prejudice to any other right or remedy it might have, the Customer may terminate the Agreement by written notice to the Supplier with immediate effect if the Supplier:
		1. (without prejudice to clause 16.2.5), is in material breach of any obligation under the Agreement which is not capable of remedy;
		2. repeatedly breaches any of the terms and conditions of the Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Agreement;
		3. is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier receiving notice specifying the breach and requiring it to be remedied;
		4. undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;
		5. breaches any of the provisions of clauses 7.2, 11, 12, 13 and 17;
		6. becomes insolvent, or if an order is made or a resolution is passed for the winding up of the Supplier (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Supplier’s assets or business, or if the Supplier makes any composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 16.2.6) in consequence of debt in any jurisdiction; or
		7. fails to comply with legal obligations in the fields of environmental, social or labour law.
	3. The Supplier shall notify the Customer as soon as practicable of any change of control as referred to in clause 16.2.4 or any potential such change of control.
	4. The Supplier may terminate the Agreement by written notice to the Customer if the Customer has not paid any undisputed amounts within 90 days of them falling due.
	5. Termination or expiry of the Agreement shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and clauses 2, 3.2, 6.1, 6.2, 6.6, 6.7, 7, 9, 10.2, 11, 12, 13, 14, 16.6, 17.4, 18.3, 19 and 20.7 or any other provision of the Agreement that either expressly or by implication has effect after termination.
	6. Upon termination or expiry of the Agreement, the Supplier shall:
		1. give all reasonable assistance to the Customer and any incoming supplier of the Services; and
		2. return all requested documents, information and data to the Customer as soon as reasonably practicable.
2. **COMPLIANCE**
	1. The Supplier shall promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Agreement. The Customer shall promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer’s premises and which may affect the Supplier in the performance of its obligations under the Agreement.
	2. The Supplier shall:
		1. comply with all the Customer’s health and safety measures while on the Customer’s premises; and
		2. notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Agreement on the Customer’s premises where that incident causes any personal injury or damage to property which could give rise to personal injury.
	3. The Supplier shall:
		1. perform its obligations under the Agreement in accordance with all applicable equality Law and the Customer’s equality and diversity policy as provided to the Supplier from time to time; and
		2. take all reasonable steps to secure the observance of clause 17.3.1 by all Staff.
	4. The Supplier shall supply the Services in accordance with the Customer’s environmental policy as provided to the Supplier from time to time.
	5. The Supplier shall comply with, and shall ensure that its Staff shall comply with, the provisions of:
		1. the Official Secrets Acts 1911 to 1989; and
		2. section 182 of the Finance Act 1989.
3. **PREVENTION OF FRAUD AND CORRUPTION**
	1. The Supplier shall not offer, give, or agree to give anything, to any person an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Agreement or for showing or refraining from showing favour or disfavour to any person in relation to the Agreement.
	2. The Supplier shall take all reasonable steps, in accordance with good industry practice, to prevent fraud by the Staff and the Supplier (including its shareholders, members and directors) in connection with the Agreement and shall notify the Customer immediately if it has reason to suspect that any fraud has occurred or is occurring or is likely to occur.
	3. If the Supplier or the Staff engages in conduct prohibited by clause 18.1 or commits fraud in relation to the Agreement or any other contract with the Crown (including the Customer) the Customer may:
		1. terminate the Agreement and recover from the Supplier the amount of any loss suffered by the Customer resulting from the termination, including the cost reasonably incurred by the Customer of making other arrangements for the supply of the Services and any additional expenditure incurred by the Customer throughout the remainder of the Agreement; or
		2. recover in full from the Supplier any other loss sustained by the Customer in consequence of any breach of this clause.
4. **DISPUTE RESOLUTION**
	1. The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Agreement and such efforts shall involve the escalation of the dispute to an appropriately senior representative of each Party.
	2. If the dispute cannot be resolved by the Parties within one month of being escalated as referred to in clause 19.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the “**Mediator**”) chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.
	3. If the Parties fail to appoint a Mediator within one month, or fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, either Party may exercise any remedy it has under applicable law.
5. **GENERAL**
	1. Each of the Parties represents and warrants to the other that it has full capacity and Customer, and all necessary consents, licences and permissions to enter into and perform its obligations under the Agreement, and that the Agreement is executed by its duly authorised representative.
	2. A person who is not a party to the Agreement shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of the Parties.
	3. The Agreement cannot be varied except in writing signed by a duly authorised representative of both the Parties.
	4. The Agreement contains the whole agreement between the Parties and supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Agreement on the basis of any representation that is not expressly incorporated into the Agreement. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.
	5. Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Agreement shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Agreement.
	6. The Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Agreement. Neither Party shall have, nor represent that it has, any Customer to make any commitments on the other Party’s behalf.
	7. Except as otherwise expressly provided by the Agreement, all remedies available to either Party for breach of the Agreement (whether under the Agreement, statute or common law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.
	8. If any provision of the Agreement is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Agreement and rendered ineffective as far as possible without modifying the remaining provisions of the Agreement, and shall not in any way affect any other circumstances of or the validity or enforcement of the Agreement.
6. **NOTICES**
	1. Any notice to be given under the Agreement shall be in writing and may be served by personal delivery, first class recorded or, subject to clause 21.3, e-mail to the address of the relevant Party set out in the Award Letter, or such other address as that Party may from time to time notify to the other Party in accordance with this clause:
	2. Notices served as above shall be deemed served on the Working Day of delivery provided delivery is before 5.00pm on a Working Day. Otherwise delivery shall be deemed to occur on the next Working Day. An email shall be deemed delivered when sent unless an error message is received.
	3. Notices under clauses 15 (Force Majeure) and 16 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in clause 21.1.
7. **GOVERNING LAW AND JURISDICTION**

The validity, construction and performance of the Agreement, and all contractual and non-contractual matters arising out of it, shall be governed by English law and shall be subject to the exclusive jurisdiction of the English courts to which the Parties submit.

**ANNEX 2 – PRICE SCHEDULE**

The total contract charges are £50,000.00 excluding VAT. Including option to extend for one period of six weeks subject to further approval.

Late completion: fee will be reduced by 2.5% of the agreed price for every working week beyond the deadline that the work remains undelivered.

**ANNEX 3 – STATEMENT OF REQUIREMENTS**

1. **PURPOSE**

* 1. A UK Property Workforce Insights Report will enable the Profession Team to take an evidence-based approach to developing the Government Property Profession (GPP) Capability Programme.
	+ Identifying and evidencing current and projected workforce trends in property and construction to 2025 will support the Programme in ensuring that attraction, retention and capability development activity is sustainable, future-focused and effective, proactively mitigating skills gaps.
	1. The purpose will be achieved by meeting the following objectives:
* Support Strategic Workforce Planning, by identifying projected capability gaps between 2022-25
* Inform a strategic approach to attraction and retention, i to increase and diversify candidate pools
* Introduce Build, Buy, Borrow solutions to address property capability requirements
* An evidence-based approach to talent development and learning so that we are developing capabilities in the right areas for the long term, putting Government Property at the leading edge of resourcing the top industry talent.

1. **BACKGROUND TO THE CONTRACTING AUTHORITY**

* 1. The Property Profession Team was established to build the capability of c.6,000 property professionals across government.
	2. The team is responsible for the GPP Capability programme. The programme was launched in 2019 to increase property capability across government through developing and delivering initiatives and services in Learning & Development, Leadership, Talent, Community, Brand, Resourcing and Reward.
	3. The GPP Capability Programme objectives ensure that Departments are suitably equipped with an industry-leading property profession that can deliver key ministerial priorities and government ambitions, including: Levelling Up (which includes the creation of Government Hubs across the UK); Civil Service reform (driving professionalisation and deep, area-specific knowledge); and the Declaration for a Modern Civil Service (including investing in skills and championing true expertise); and the Government Estate Strategy (building back better and greener);
	4. Departments have been set clear property deliverables as priorities in the latest Spending Review, focused on providing crucial public services, including the building of new schools (DfE), prisons and courts (MoJ), and hospitals (DHSC). Meeting requirements such as these will rely on departments having the right levels of capability, skill and expertise in property teams up to and beyond 2025 - which the Profession Team will be integral to enabling.
	+
1. **BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT**

* 1. To progress the GPP Capability Programme we require insights beyond government so we can move towards a forward-looking, sustainable and strategic approach to capability building. The requirement is for a Property Labour Market Insights Report which outlines current and predicted future property workforce trends and challenges between 2022-2025, and highlights case studies and recommendations for best practice.
	2. There are property skills which are significantly challenging to attract and retain as they are highly sought after cross-industry with limited supply. We need credible projections of where roles may become difficult to fill or capabilities may grow or reduce in demand, based on predicted changes in the property landscape over the coming years.
	3. Government departments increasingly rely on the Profession Team’s insight and context of wider government to develop business cases for higher pay, develop new advertising approaches for example. The report will provide market-intelligent insights so the Profession Team can better support Departments, and ensure GPP Capability Programme o invests in the right places.
	4. This work will enable the Government Property Profession to provide an evidence-based projection of where Departments will need to recruit, develop and retain talent, ensuring:
* The Profession is suitably equipped to deliver the government’s plans
* The Workforce is built and developed in line with the challenges and opportunities in the wider sector
* We have a deeper understanding of where to build, buy and borrow skills from, moving so we are equipped to proactively mitigate projected skills gaps now and up to 2025.
	+
	1. The report will enable the Profession Team to enhance support and services to Departments from the centre which will enable efficiencies. For example, ensuring:
* money is spent only on recruitment that satisfies the strategic needs, and not when short term solutions would be more appropriate
* talent development schemes and learning programmes are investing in developing skills in tune with the future landscape of the sector, and not wasted developing current skills that won’t be required
* time and money is spent on attracting and recruiting the right skills in the right way (including approaching recruitment differently where intelligent labour market insight tells us particular roles will be more challenging)

1. **DEFINITIONS**

|  |  |
| --- | --- |
| Expression or Acronym | Definition |
| GPS | Means Government Property Service |
| GPP | Means Government Property Profession |
| SR21 | Means Spending Review 2021, referring to 3 year budget (and spend) settlement from 2022-2025. |

1. **SCOPE OF REQUIREMENT**
	1. In scope are data and/or case studies for:
* All job roles and related skills in the UK property and construction sectors, including roles aligned to, the [Government Property Career Framework](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1083390/GPP_Career_Framework.pdf)
* Private sector organisations and their employee offer (e.g. their core employee benefits)
* Public Sector and Civil service organisations (as described on [gov.uk](https://www.gov.uk/government/organisations/civil-service/about#who-we-are))

* 1. Out of scope are data and/or case studies for:
* Non-UK organisations
* Organisations whose workforce are not responsible for property or construction activities in the UK (e.g. project management firms managing work in Australia)

* 1. Note - this work should **not** be:
* Salary benchmarking in isolation
* An observation or comparison of differing property team structures or operating models. (These should be referenced where they result in differences between, or are relevant to, attraction and development activity, and/or employee benefits).
	+
1. **THE REQUIREMENT**
	1. A “UK Property Workforce Report” which outlines research and analysis of the current labour market position, and a longer term projection to 2025, including information and insight relating to:
* Supply / Demand of job roles and related skills and how this is projected to change
* Identifying critical roles/skills in the context of the GPS and the Government Property Career Framework, and the projected changes to this (i.e. which will become more critical, examples might include BIM, MMC and Sustainability)
* Identifying emerging roles and skills not yet covered by the Career Framework but may be required by 2025
* Diversity profile of wider sector’s workforce, predictions of how this may shift, and successful methods of sourcing talent from diverse backgrounds (considering characteristics such as ethnicity, disability, socio-economic, religion, sexual orientation, etc.)
* Talent pool/source - locations, training providers, universities (Who is training the talent in the skills areas that will be critical in the future?)
* Direct competitors and industry leading employers (who is hiring the people with these key skills)
* Employee benefit trends and attraction methods in property (including best practice case studies), and a projection of how this might change as capability requirements and demographics change across industry e.g. flexible working, training offer
	+
1. **KEY MILESTONES AND DELIVERABLES**
	1. Key deliverables:
		1. Production of a report as set out in section 6 in both “final” PDF (or similar) format and an editable version (e.g. PowerPoint, Word).
			1. Report should visually conform to GPP branding guidelines - to be agreed at scoping.
		2. Outlining of sources of data for reference and assurance
		3. Presentation of report and recommendations to GPP (including senior property leaders)
			1. Structure / format of report & presentation workshop to be agreed during scoping
			2. Report must be easy to read, present data clearly, and be aesthetically professional, appropriate for a senior executive level audience

* 1. Key milestone is delivery of report **no later than 28th April 2023**. Interim milestones will be set during regular contract review meetings set out in section 18, but will include at least:
		1. Work should begin **no later than w/c 13th March 2023**, with the contract anticipated to last 6 weeks.
		2. Presentation of headline findings to the Profession team, and to Senior Property Leaders **11th April 2023**.
		3. Scoping exercise at commencement **(day one from contract award)** for supplier to clarify requirements, finalise approach and confirm timescales for interim milestones below
		4. **Interim Milestone 1**: completion of research stage, and outline of interim findings to the Government Head of Profession.
		5. **Interim Milestone 2**: presentation of findings & draft report to the GPP team and Senior Property Leaders (as deemed appropriate by GPP), allowing opportunity for question and challenge, and to feedback any amendments required
		6. **Final milestone:** production of summary and detailed report suitable for senior leaders, plus handover of data and findings to Profession Team
		7. Timescales and deadlines for interim milestones to be discussed at first contract review meeting
*
1. **MANAGEMENT INFORMATION/REPORTING**
	1. Report should include referencing all data sources

1. **VOLUMES**
	1. For the supplier’s reference, an example report produced for the Project Delivery Profession enclosed with bid pack for illustrative purposes.
2. **CONTINUOUS IMPROVEMENT**
	1. The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.
	2. If the Supplier has additional services/insights that are within the maximum budget the supplier shall propose these as a way of adding value to the piece of work
	3. The Supplier should present new ways of working to the Authority during weekly Contract Review meetings.
	4. Changes to the way in which the Services are to be delivered must be brought to the Authority’s attention and agreed prior to any changes being implemented.
3. **QUALITY**
	1. Report must be of a suitable quality to be presented at senior executive level (e.g. contain a suitable executive summary and include concise presentation of information through graphics)
4. **PRICE**
	1. Price to be itemised to outline level of consultant, tasks and time taken.
	2. Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.
5. **STAFF AND CUSTOMER SERVICE**
	1. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.
	2. The Supplier’s staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
	3. The Supplier shall ensure that staff understand the Authority’s vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.
6. **SERVICE LEVELS AND PERFORMANCE**
	1. The Authority will measure the quality of the Supplier’s delivery by:
		1. Breadth, reputation and influence of research sources:
			1. Seniority and influence of contacts
			2. Reputation of organisations (including engaging with UK top 10 firms in property management, surveying, construction, facilities management and engineering, and design/architecture)
			3. Breadth of different organisations/sectors engaged with e.g.
				1. Private sector design, project management & sureying (e.g. BDP, CBRE)
				2. Private sector construction (e.g. Balfour Beatty, Laing O’Rourke)
				3. public & charity sector property & construction (e.g. NHS property services, social housing)
				4. relevant professional bodies (e.g. CIPD, or property bodies outlined in the GPP Career Framework)
			4. Number of regions represented in the research, analysis and recommendations i.e. not simply presenting a national picture, but addressing regional differences
			5. Influence and value-added by the additional networks / contacts / data sources within the supplier’s reach
		2. Practical usability of recommendations in developing attraction, retention, development advice and Strategic Workforce Plan
		3. Quality of communication and updates from the supplier showing a full understanding of the requirements and objectives
		4. Timeliness - 100% in line with the defined timescales

* 1. Late completion: fee will be reduced by 2.5% of the agreed price for every working week beyond the deadline that the work remains undelivered.
	2. Poor performance:
		1. The Contracting Authority will provide written notice of poor performance to the Supplier’s Project Manager, at which point the Supplier will produce an action plan for improvement within 1 working day
		2. Unsatisfactory improvement will lead to termination of the contract. The Contracting Authority will provide 1 working week’s written notice

1. **SECURITY AND CONFIDENTIALITY REQUIREMENTS**
	1. Any government data or context shared or obtained during conversations during the procurement or delivery of services must be treated as confidential unless it is already available in the public domain, or unless express permission from the customer is granted.
	*
2. **PAYMENT AND INVOICING**
	1. Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.
	2. Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.
	3. Invoices should be submitted to:
	* **REDACTED TEXT under FOIA Section 40, Personal Information** **REDACTED TEXT under FOIA Section 40, Personal Information**
	* **REDACTED TEXT under FOIA Section 40, Personal Information** **REDACTED TEXT under FOIA Section 40, Personal Information**
	* **REDACTED TEXT under FOIA Section 40, Personal Information** **REDACTED TEXT under FOIA Section 40, Personal Information**
	* Emailed to: **REDACTED TEXT under FOIA Section 40, Personal Information**
	1. Any Invoices received that do not include a Purchase Order number and

payment will be rejected by the Authority.

1. **CONTRACT MANAGEMENT**

Contract review meetings will take place virtually, via Google Meet or Microsoft Teams. The supplier’s project lead will be expected to attend all review meetings, and must obtain permission from the customer project lead if a colleague is to deputise.

* 1. Attendance at Contract Review meetings shall be at the Supplier’s own expense.
1. **LOCATION**
	1. The location of the Services will be carried out at supplier premises, and engagement with the contracting authority will be via email to the project team and video link (Google Meet or Microsoft Teams) where required (for example for Contact Review Meetings).

**ANNEX 4 – SUPPLIERS RESPONSE**

From the Supplier’s Bid 28/02/2023

****

 **ANNEX 5 – CLARIFICATIONS**

Not Applicable

**ANNEX 6 – ADDITIONAL TERMS & CONDITIONS**

1. Data Protection

* 1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor. The only processing that the Supplier is authorised to do is listed in Annex 1 to this Schedule (Processing Personal Data) by the Customer and may not be determined by the Supplier.
	2. The Supplier shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.
	3. The Supplier shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:
		1. a systematic description of the envisaged processing operations and the purpose of the processing;
		2. an assessment of the necessity and proportionality of the processing operations in relation to the Services;
		3. an assessment of the risks to the rights and freedoms of Data Subjects; and
		4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.4. The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Framework Agreement:

* + 1. process that Personal Data only in accordance with Annex 1 (Processing Personal Data), unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;
		2. ensure that it has in place Protective Measures which have been reviewed and approved by the Customer as appropriate to protect against a Data Loss Event having taken account of the:
			1. nature of the data to be protected;
			2. harm that might result from a Data Loss Event;
			3. state of technological development; and
			4. cost of implementing any measures;
		3. ensure that :
			1. the Supplier Personnel do not process Personal Data except in accordance with this Framework Agreement (and in particular Annex 1 (Processing Personal Data));
			2. it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:
				1. are aware of and comply with the Supplier’s duties under this Clause;
				2. are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;
				3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this Contact; and
				4. have undergone adequate training in the use, care, protection and handling of Personal Data;
		4. not transfer Personal Data outside of the EU unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:
			1. the Customer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer;
			2. the Data Subject has enforceable rights and effective legal remedies;
			3. the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Customer in meeting its obligations); and
			4. the Supplier complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;
		5. at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of the this Contract unless the Supplier is required by Law to retain the Personal Data.

1.5 Subject to Clause 1.7, the Supplier shall notify the Customer immediately if it:

* + 1. receives a Data Subject Access Request (or purported Data Subject Access Request);
		2. receives a request to rectify, block or erase any Personal Data;
		3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
		4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
		5. receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
		6. becomes aware of a Data Loss Event.

1.6 The Supplier’s obligation to notify under Clause 1.5 shall include the provision of further information to the Customer in phases, as details become available.

1.7 Taking into account the nature of the processing, the Supplier shall provide the Customer with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.5 (and insofar as possible within the timescales reasonably required by the Customer) including by promptly providing:

* + 1. the Customer with full details and copies of the complaint, communication or request;
		2. such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
		3. the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;
		4. assistance as requested by the Customer following any Data Loss Event;
		5. assistance as requested by the Customer with respect to any request from the Information Commissioner’s Office, or any consultation by the Customer with the Information Commissioner's Office.

1.8 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

* + 1. the Customer determines that the processing is not occasional;
		2. the Customer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
		3. the Customer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Supplier shall allow for audits of its Data Processing activity by the Customer or the Customer’s designated auditor.

1.10 The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Supplier must:

* + 1. notify the Customer in writing of the intended Sub-processor and processing;
		2. obtain the written consent of the Customer;
		3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this Clause 1.11 such that they apply to the Sub-processor; and
		4. provide the Customer with such information regarding the Sub-processor as the Customer may reasonably require.

1.12. The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The Supplier may, at any time on not less than 30 Working Days’ notice, revise this Clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Customer may on not less than 30 Working Days’ notice to the Supplier amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner’s Office.

* 1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor. The only processing that the Supplier is authorised to do is listed in Annex 1 (Processing Personal Data) by the Customer and may not be determined by the Supplier.
	2. The Supplier shall notify the Customer immediately if it considers that any of the Customer’s instructions infringe the Data Protection Legislation.
	3. The Supplier shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer, include:
		1. a systematic description of the envisaged processing operations and the purpose of the processing;
		2. an assessment of the necessity and proportionality of the processing operations in relation to the Services;
		3. an assessment of the risks to the rights and freedoms of Data Subjects; and
		4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.18 The Supplier shall, in relation to any Personal Data processed in connection with its obligations under this Call Off Contract:

* + 1. process that Personal Data only in accordance with Annex 1 (Processing Personal Data), unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;
		2. ensure that it has in place Protective Measures which have been reviewed and approved by the Customer as appropriate to protect against a Data Loss Event having taken account of the:
			1. nature of the data to be protected;
			2. harm that might result from a Data Loss Event;
			3. state of technological development; and
			4. cost of implementing any measures;
		3. ensure that :
			1. the Supplier Personnel do not process Personal Data except in accordance with this Call Off Contract (and in particular Annex 1 (Processing Personal Data));
			2. it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:
				1. are aware of and comply with the Supplier’s duties under this Clause;
				2. are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;
				3. are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this Call Off Contract; and
				4. have undergone adequate training in the use, care, protection and handling of Personal Data;
		4. not transfer Personal Data outside of the EU unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:
			1. the Customer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer;
			2. the Data Subject has enforceable rights and effective legal remedies;
			3. the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Customer in meeting its obligations); and
			4. the Supplier complies with any reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;
		5. at the written direction of the Customer, delete or return Personal Data (and any copies of it) to the Customer on termination of the Call Off Contract unless the Supplier is required by Law to retain the Personal Data.

1.19 Subject to Clause 1.21, the Supplier shall notify the Customer immediately if it:

* + 1. receives a Data Subject Access Request (or purported Data Subject Access Request);
		2. receives a request to rectify, block or erase any Personal Data;
		3. receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
		4. receives any communication from the Information Commissioner or any other regulatory Customer in connection with Personal Data processed under this Call Off Contract;
		5. receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
		6. becomes aware of a Data Loss Event.

1.20 The Supplier’s obligation to notify under Clause 1.19 shall include the provision of further information to the Customer in phases, as details become available.

1.21 Taking into account the nature of the processing, the Supplier shall provide the Customer with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.19 (and insofar as possible within the timescales reasonably required by the Customer) including by promptly providing:

* + 1. the Customer with full details and copies of the complaint, communication or request;
		2. such assistance as is reasonably requested by the Customer to enable the Customer to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
		3. the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;
		4. assistance as requested by the Customer following any Data Loss Event;
		5. assistance as requested by the Customer with respect to any request from the Information Commissioner’s Office, or any consultation by the Customer with the Information Commissioner's Office.

1.22 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

* + 1. the Customer determines that the processing is not occasional;
		2. the Customer determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
		3. the Customer determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.23 The Supplier shall allow for audits of its Data Processing activity by the Customer or the Customer’s designated auditor.

1.24 The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.25 Before allowing any Sub-processor to process any Personal Data related to this Call Off Contract, the Supplier must:

* + 1. notify the Customer in writing of the intended Sub-processor and processing;
		2. obtain the written consent of the Customer;
		3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this Clause 1.25 such that they apply to the Sub-processor; and
		4. provide the Customer with such information regarding the Sub-processor as the Customer may reasonably require.

1.26 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

1.27 The Supplier may, at any time on not less than 30 Working Days’ notice, revise this Clause by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Call Off Contract).

1.28 The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Customer may on not less than 30 Working Days’ notice to the Supplier amend this Call Off Contract to ensure that it complies with any guidance issued by the Information Commissioner’s Office.

**Annex 1 –Processing Personal Data**

**Authorised Processing Template**

* + 1. The contact details of the Customer’s Data Protection Officer is:

**REDACTED TEXT under FOIA Section 40, Personal Information**

* + 1. The contract details of the Supplier Data Protection Officer is:

**REDACTED TEXT under FOIA Section 40, Personal Information**

* + 1. The Processor shall comply with any further written instructions with respect to processing by the Controller.
		2. Any such further instructions shall be incorporated into this Annex.

|  |  |
| --- | --- |
| **Contract Reference:** | CCZZ23A14 |
| **Date:**  | **08/03/2023** |
| **Description Of Authorised Processing** | **Details** |
| Identity of the Controller and Processor | * 1. **OPTION A:** *Customer as Controller*

The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor in accordance with Clause 1.1.]Legislation:* + 1. The Customer is the Controller and the Supplier is the Processor for the following Personal Data under this Contract:

Scope: Data to be processed and those individuals in scope is articulated in this annex. |
| Subject matter of the processing | Individual's perceptions of trends in the UK property labour market.  |
| Duration of the processing | Initial Term 09th March 2023 – 03rd May 2023Extension subject to budgetary approval04th May 2023 – 14th June 2023 |
| Nature and purposes of the processing | Obtain professional opinions as to the supply & demand of property skills in the UK labour market, to feed into a wider report (which will include factual data) outlining the current and projected supply and demand of these skills. |
| Type of Personal Data | Full name Work email addressOrganisation worked forMembership organisation (e.g. RICS) if applicableOpinions / perceptions of the market based on experience |
| Categories of Data Subject | Members of the public who work for property organisations. Possibly civil servants from within the property profession.  |

**ANNEX 7 – CHANGE CONTROL FORMS**

|  |
| --- |
|  **CHANGE CONTROL NOTICE (CCN)** |
| **Contract Title:** | Contract for the Provision of **Insert title of requirement** (The Contract) |
| **Contract Reference:** |  | **Contract Change Number:** |  |
| **Date CCN issued:** |  | **Date Change Effective from:** |  |
| **Between**: The **Insert Name of Contracting Authority** (The Customer) and **Insert name of Supplier** (The Supplier)1. The Contract is varied as follows:

1.1. **Insert details of changes to the original contract.**1. Words and expressions in this Change Control Notice shall have the meanings given to them in the Contract.
2. The Contract, including any previous Contract changes, authorised in writing by both Parties, shall remain effective and unaltered except as amended by this Change Control Notice.
 |
|  Change authorised to proceed by: (Customer’s representative):   Signature Print Name and Job Title Date |
| Authorised for and on behalf of the Supplier:Signature Print Name and Job Title Date |
| Authorised for and on behalf of the Customer: Signature Print Name and Job Title Date |

**ANNEX 8 – UK Property Workforce Report Security Schedule 16 Final V1**

1. **BUYER OPTIONS**

**Risk assessment**

|  |  |  |
| --- | --- | --- |
| The Buyer has assessed this Agreement as | a standard consultancy agreement | ☒ |
| a higher-risk consultancy agreement | ☐ |

**Relevant Certifications**

|  |  |  |
| --- | --- | --- |
| Where the Buyer has assessed this Agreement as a standard consultancy agreement, it requires the Supplier to be certified as compliant with: | Cyber Essentials | ☒ |
| Cyber Essentials Plus | ☐ |

1. **SUPPLIER OBLIGATIONS**
	1. Where the Buyer has assessed this Agreement as a higher-risk consultancy agreement, the Supplier must comply with all requirements in this Schedule 16 (Security Management).
	2. Where the Buyer has assessed this Agreement as a standard consultancy agreement, the Supplier must comply with this Schedule 16 (Security Management), other than:
		1. the requirement to be certified as compliant with ISO/IEC 27001:2013 under Paragraph 7.1(b);
		2. the requirement to undertake security testing of the Supplier Information Management System in accordance with paragraph 3 of Appendix 1;
		3. the requirement to produce a Security Management Plan in accordance with Paragraph 8
		4. the requirement to document unencrypted Buyer Data in the Security Management Plan in accordance with paragraph 5.4 of Appendix 1
2. **DEFINITIONS**
	1. In this Schedule 16 (Security Management):

|  |  |
| --- | --- |
| * 1. **“Anti-virus Software”**
 | means software that:* + 1. protects the Supplier Information Management System from the possible introduction of Malicious Software;
		2. scans for and identifies possible Malicious Software in the Supplier Information Management System;
		3. if Malicious Software is detected in the Supplier Information Management System, so far as possible:
			1. prevents the harmful effects of the Malicious Software; and
			2. removes the Malicious Software from the Supplier Information Management System.
 |
| * 1. **“Breach of Security”**
 | * 1. means the occurrence of:
		1. any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement;
		2. the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Buyer, the Supplier or any Sub-contractor in connection with this Agreement; and/or
		3. any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements.
 |
| * 1. **“Buyer Data”**
 | * 1. means any:
		1. data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; or
		2. Personal Data for which the Buyer is a, or the, Data Controller,
	2. that is:
		+ 1. supplied to the Supplier by or on behalf of the Buyer; or
			2. that the Supplier generates, processes, stores or transmits under this Agreement.
 |
| * 1. **“Buyer Equipment”**
 | * 1. means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System.
 |
| * 1. **“Buyer System”**
 | * 1. means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer receives the Services.
 |
| * 1. **“Certification Default”**
 | * 1. means the occurrence of one or more of the circumstances listed in paragraph 7.4.
 |
| * 1. **“Certification Rectification Plan”**
 | * 1. means the plan referred to in paragraph 7.5(a).
 |
| * 1. **“Certification Requirements”**
 | * 1. means the information security requirements set out in paragraph 7.
 |
| * 1. **“Cyber Essentials”**
 | * 1. means the Cyber Essentials certificate issued under the Cyber Essentials Scheme.
 |
| * 1. **“Cyber Essentials Plus”**
 | * 1. means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme.
 |
| * 1. **“Cyber Essentials Scheme”**
 | * 1. means the Cyber Essentials scheme operated by the National Cyber Security Centre.
 |
| * 1. **“End-user Device”**
 | * 1. means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
 |
| * 1. **“HMG Baseline Personnel Security Standard”**
 | * 1. means the employment controls applied to any individual member of the Supplier Personnel that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel Standard”, Version 6.0, May 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/714002/HMG\_Baseline\_Personnel\_Security\_Standard\_-\_May\_2018.pdf), as that document is updated from time to time.
 |
| * 1. **“Malicious Software”**
 | * 1. means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations.
 |
| * 1. **“NCSC Cloud Security Principles”**
 | * 1. means the National Cyber Security Centre’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles.
 |
| * 1. **“NCSC Device Guidance”**
 | * 1. means the National Cyber Security Centre’s document “Device Security Guidance”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance.
 |
| * 1. **“Privileged User”**
 | * 1. means a user with system administration access to the Supplier Information Management System, or substantially similar access privileges.
 |
| * 1. **“Process”**
 | * 1. means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data.
 |
| * 1. **“Prohibited Activity”**
 | * 1. means the storage, access or Processing of Buyer Data prohibited by a Prohibition Notice.
 |
| * 1. **“Prohibition Notice”**
 | * 1. means a notice issued under paragraph 1.3 of Appendix 1.
 |
| * 1. **“Relevant Certifications”**
 | * 1. means those certifications specified in paragraph 7.1.
 |
| * 1. **“Relevant Convictions”**
 | * 1. means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Buyer may specify.
 |
| * 1. **“Security Management Plan”**
 | * 1. means the document prepared in accordance with the requirements of paragraph 8.
 |
| * 1. **“Sites”**
 | * 1. means any premises:
		1. from or at which:
			1. the Services are (or are to be) provided; or
			2. the Supplier manages, organises or otherwise directs the provision or the use of the Services; or
		2. where:
			1. any part of the Supplier Information Management System is situated; or
			2. any physical interface with the Buyer System takes place.
 |
| * 1. **“Standard Contractual Clauses”**
 | * 1. means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area.
 |
| * 1. **“Supplier Information Management System”**
 | * 1. means:
		1. those parts of the information and communications technology system and the Sites that the Supplier or its Sub-contractors will use to provide the Services; and
		2. the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);
 |
| * 1. **“Sub-contractor Personnel”**
 | * 1. means:
		1. any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and
		2. engaged in or likely to be engaged in:
			1. the performance or management of the Services;
			2. or the provision of facilities or services that are necessary for the provision of the Services.
 |
| * 1. **“Supplier Personnel”**
 | * 1. means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier’s obligations under this Agreement.
 |
| * 1. **“UKAS”**
 | * 1. means the United Kingdom Accreditation Service.
 |

1. **INTRODUCTION**
	1. This Schedule 16 (Security Management) sets out:
		1. the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Buyer Data, the Services and the Supplier Information Management System;
		2. the assessment of this Agreement as either a:
			1. standard consultancy agreement; or
			2. higher-risk consultancy agreement,

in paragraph 1;

* + 1. the Buyer’s access to the Supplier Personnel and Supplier Information Management System, in paragraph 6;
		2. the Certification Requirements, in paragraph 7;
		3. the requirements for a Security Management Plan in the case of higher-risk consultancy agreements, in paragraph 8; and
		4. the security requirements with which the Supplier and Sub-contractors must comply in Appendix 1.
1. **PRINCIPLES OF SECURITY**
	1. The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data and, consequently on the security of:
		1. the Sites;
		2. the Services; and
		3. the Supplier’s Information Management System.
	2. The Supplier is responsible for:
		1. the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Sub-contractors; and
		2. the security of the Supplier Information Management System.
	3. The Supplier:
		1. comply with the security requirements in Appendix 1; and
		2. ensure that each Sub-contractor that Processes Buyer Data complies with the security requirements in Appendix 1.
	4. Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Subcontractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.
2. **ACCESS TO SUPPLIER PERSONNEL AND SUPPLIER INFORMATION MANAGEMENT SYSTEM**
	1. The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:
		1. access to the Supplier Personnel;
		2. access to the Supplier Information Management System to audit the Supplier and its Sub-contractors’ compliance with this Agreement; and
		3. such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,
	2. to assist the Buyer to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Buyer Data and the Supplier Information Management System are consistent with the representations in the Security Management Plan.
	3. The Supplier must provide the access required by the Buyer in accordance with paragraph 6.1 within ten Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.
3. **CERTIFICATION REQUIREMENTS**
	1. The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:
		1. in the case of a standard consultancy agreement the option chosen by the Buyer in Paragraph 1; or
		2. in the case of a higher-risk consultancy agreement:
			1. ISO/IEC 27001:2013 by a UKAS-approved certification body in respect of the Supplier Information Management System, or the Supplier Information Management System is included within the scope of a wider certification of compliance with ISO/IEC 27001:2018; and
			2. Cyber Essentials Plus (“**Relevant Certifications”**).
	2. Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.
	3. The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:
		1. currently in effect;
		2. relate to the full scope of the Supplier Information System; and
		3. are not subject to any condition that may impact the provision of the Services.
	4. The Supplier must notify the Buyer promptly, any in any event within three Working Days of becoming aware that:
		1. a Relevant Certification has been revoked or cancelled by the body that awarded it;
		2. a Relevant Certification expired and has not been renewed by the Supplier;
		3. a Relevant Certification no longer applies to the full scope of the Supplier Information Management System or
		4. the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a “**Certification Default**”).
	5. Where the Supplier has notified the Buyer of a Certification Default under paragraph 7.4:
		1. the Supplier must, within ten working Days of the date in which the Supplier provided notice under paragraph 7.4 (or such other period as the Parties may agree) provide a draft plan (a “**Certification Rectification Plan**”) to the Supplier setting out:
			1. full details of the Certification Default, including a root cause analysis;
			2. the actual and anticipated effects of the Certification Default;
			3. the steps the Supplier will take to remedy the Certification Default;
		2. the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;
		3. if the Buyer rejects the Certification Rectification Plan, the Buyer must within five Working Days of the date of the rejection submit a revised Certification Rectification Plan and paragraph 7.5(b) will apply to the re-submitted plan;
		4. the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;
		5. if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.
4. **SECURITY MANAGEMENT PLAN**
	1. This paragraph 8 applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

**Preparation of Security Management Plan**

* 1. The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this Schedule 16 (Security Management) and the Agreement in order to ensure the security of the Buyer Data and the Supplier Information Management System.
	2. The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:
		1. an assessment of the Supplier Information Management System against the requirements of this Schedule 16 (Security Management), including Appendix 1
		2. the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Buyer Data, the Buyer, the Services and/or users of the Services; and
		3. the following information in respect of each Sub-contractor:
			1. the Sub-contractor’s:
				1. legal name;
				2. trading name (if any);
				3. registration details (where the Sub-contractor is not an individual);
			2. the Sites used by the Sub-contractor;
			3. the Buyer Data Processed by the Subcontractor;
			4. the Processing that the Sub-contractor will undertake in respect of the Buyer Data;
			5. the measures the Sub-contractor has in place to comply with the requirements of this Schedule 16 (Security Management).
	3. The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:
		1. an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Process Buyer Data; or
		2. a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.
	4. If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within ten Working Days of the date of the rejection, or such other period agreed with the Buyer.

**Updating Security Management Plan**

* 1. The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this paragraph.

**Monitoring**

* 1. The Supplier shall notify the Buyer within two Working Days after becoming aware of:
		1. a significant change to the components or architecture of the Supplier Information Management System;
		2. a new risk to the components or architecture of the Supplier Information Management System;
		3. a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;
		4. a change in the threat profile;
		5. a significant change to any risk component;
		6. a significant change in the quantity of Personal Data held within the Service;
		7. a proposal to change any of the Sites from which any part of the Services are provided; and/or
		8. an ISO27001 audit report produced in connection with the Certification Requirements indicates significant concerns.
	2. Within ten Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

**APPENDIX 1: SECURITY REQUIREMENTS**

1. Location
	1. Unless otherwise agreed with the Buyer, the Supplier must, and must ensure that its Subcontractors must, at all times, store, access or process Buyer Data either:
		1. in the United Kingdom;
		2. the European Economic Area; or
		3. in a facility operated by an entity where:
			1. the entity has entered into a binding agreement with the Supplier or Sub-contractor (as applicable);
			2. that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Sub-contractors in this Schedule 16 (Security Management);
			3. the Supplier or Sub-contractor has taken reasonable steps to assure itself that
				1. the entity complies with the binding agreement;
				2. any system operated by the Supplier or Sub-contractor has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Process the Government Data as required by this Schedule 16 (*Security Management*); and
			4. the Supplier has provided the Buyer with such information as the Buyer requires concerning:
				1. the entity;
				2. the arrangements with the entity; and
				3. the entity’s compliance with the binding agreement; and
			5. the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.3.
	2. Where the Supplier cannot comply with one or more of the requirements of paragraph 1.1:
		1. it must provide the Buyer with such information as the Buyer requests concerning the security controls in places at the relevant location or locations; and
		2. the Buyer may grant approval to use that location or those locations, and that approval may include conditions; and
		3. if the Buyer does not grant permission to use that location or those locations, the Supplier must cease to store, access or process Buyer Data at that location or those locations within such period as the Buyer may specify.
	3. The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not undertake or permit to be undertaken, the storage, access or Processing Buyer Data as specified in the notice (a “**Prohibited Activity**”).
		1. in any particular country or group of countries;
		2. in or using facilities operated by any particular entity or group of entities; or
		3. in or using any particular facility or group of facilities, whether operated by the Supplier, a Sub-contractor or a third-party entity (a “**Prohibition Notice**”).
	4. Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities affected by the notice, the Supplier must, and must procure that Sub-contractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.
2. Vetting, Training and Staff Access

**Vetting before performing or managing Services**

* 1. The Supplier must not engage Supplier Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel, in any activity relating to the performance and management of the Services unless:
		1. That individual has passed the security checks listed in paragraph 2.2; or
		2. The Buyer has given prior written permission for a named individual to perform a specific role.
	2. For the purposes of paragraph 2.1, the security checks are:
		1. the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:
			1. the individual’s identity;
			2. the individual’s nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;
			3. the individual’s previous employment history; and
			4. that the individual has no Relevant Convictions;
		2. national security vetting clearance to the level specified by the Buyer for such individuals or such roles as the Buyer may specify; or
		3. such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

**Annual training**

* 1. The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier Personnel, complete and pass security training at least once every calendar year that covers:
		1. general training concerning security and data handling; and
		2. phishing, including the dangers from ransomware and other malware.

**Staff access**

* 1. The Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.
	2. The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.
	3. Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel’s access to the Buyer Data or part of that Buyer Data specified by the Buyer as soon as practicable and in any event within 24 hours of the request.

**Exception for certain Sub-contractors**

* 1. Where the Supplier considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:
		1. as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;
		2. provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Supplier Personnel will perform as the Buyer reasonably requires; and
		3. comply, at the Supplier’s cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.
1. Security Testing
	1. This paragraph applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
	2. **Note:** the definition of Supplier Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the Supplier providing the Services.
	3. The Supplier must, at the Buyer’s option, before providing the Services and when reasonably requested by the Buyer, either:
		1. conduct security testing of the Supplier Information Management System by:
			1. engaging a CHECK Service Provider or a CREST Service Provider;
			2. designing and implementing the testing so as to minimise its impact on the Supplier Information Management System and the delivery of the Services; and
			3. providing the Buyer with a full, unedited and unredacted copy of the testing report without delay and in any event within ten Working Days of its receipt by the Supplier; or
		2. Provide details of any security testing undertaken by a CHECK Service Provider or a CREST Service Provider in respect of the Supplier Information Management System in the calendar year immediately preceding the Buyer’s request or the Effective Date (as appropriate), including:
			1. the parts of the Supplier Information Management System tested;
			2. a full, unedited and unredacted copy of the testing report; and
			3. the remediation plan prepared by the Supplier to address any vulnerabilities disclosed by the security testing; and
			4. the Supplier’s progress in implementing that remediation plan.
	4. The Supplier must remediate any vulnerabilities classified as “medium” or above in the security testing:
		1. before Processing Buyer data where the vulnerability is discovered before the Supplier begins to process Authority Data;
		2. where the vulnerability is discovered when the Supplier has begun to Process Buyer Data:
			1. by the date agreed with the Buyer; or
			2. where no such agreement is reached:
				1. within five Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;
				2. within one month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and
				3. within three months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.
2. End-user Devices
	1. The Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data is stored or processed in accordance the following requirements:
		1. the operating system and any applications that store, process or have access to Buyer Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;
		2. users must authenticate before gaining access;
		3. all Buyer Data must be encrypted using a encryption tool agreed to by the Buyer;
		4. the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;
		5. the End-user Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Buyer Data;
		6. the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer Data on the device and prevent any user or group of users from accessing the device;
		7. all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001:2018 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.
	2. The Supplier must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.
	3. Where there any conflict between the requirements of this Schedule 16 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.
3. Encryption
	1. Unless paragraph 5.2 applies, the Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer Data is encrypted:
		1. when stored at any time when no operation is being performed on it; and
		2. when transmitted.
	2. Where the Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.1, the Supplier must:
		1. immediately inform the Buyer of the subset or subsets of Buyer Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;
		2. provide details of the protective measures the Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;
		3. provide the Buyer with such information relating to the Buyer Data concerned, the reasons why that Buyer Data cannot be encrypted and the proposed protective measures as the Buyer may require.
	3. The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.
	4. This paragraph applies where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.
	5. Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:
		1. the subset or subsets of Buyer Data not encrypted and the circumstances in which that will occur;
		2. the protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Buyer Data.
	6. Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer Data, either party may refer the matter to be determined by an expert in accordance with the Dispute Resolution Procedure.
4. Access Control
	1. The Supplier must, and must ensure that all Sub-contractors:
		1. identify and authenticate all persons who access the Supplier Information Management System and Sites before they do so;
		2. require multi-factor authentication for all user accounts that have access to Buyer Data or that are Privileged Users;
		3. allow access only to those parts of the Supplier Information Management System and Sites that those persons require;
		4. maintain records detailing each person’s access to the Supplier Information Management System and Sites, and make those records available to the Buyer on request.
	2. The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier Information Management System:
		1. are accessible only from dedicated End-user Devices;
		2. are configured so that those accounts can only be used for system administration tasks;
		3. require passwords with high complexity that are changed regularly;
		4. automatically log the user out of the Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.
	3. The Supplier must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the Supplier Information Management System.
	4. The Supplier must, and must ensure that all Sub-contractors:
		1. configure any hardware that forms part of the Supplier Information Management System that is capable of requiring a password before it is accessed to require a password; and
		2. change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.
5. Malicious Software
	1. The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.
	2. The Supplier shall ensure that such Anti-virus Software:
		1. is configured to perform automatic software and definition updates;
		2. performs regular scans of the Supplier Information Management System to check for and prevent the introduction of Malicious Software; and
		3. where Malicious Software has been introduced into the Supplier Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.
	3. If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Buyer Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
	4. Any cost arising out of the actions of the parties taken in compliance with the provisions of paragraph 7.3 shall be borne by the parties as follows:
		1. by the Supplier where the Malicious Software originates from the Supplier Software, any third-party software licenced by the Supplier or the Buyer Data (whilst the Buyer Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
		2. by the Buyer, in any other circumstance.
6. Breach of Security
	1. If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.
	2. The Supplier must, upon becoming aware of a Breach of Security or attempted Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other reasonably steps necessary to:
		1. minimise the extent of actual or potential harm caused by such Breach of Security;
		2. remedy such Breach of Security to the extent possible;
		3. apply a tested mitigation against any such Breach of Security; and
		4. prevent a further Breach of Security in the future which exploits the same root cause failure.
	3. As soon as reasonably practicable and, in any event, within five Working Days, or such other period agreed with the Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.
	4. The Supplier must take the steps required by paragraph 8.2 at its own cost and expense.
7. Sub-contractors
	1. The Supplier must assess the parts of the information and communications technology system and the Sites that its Subcontractors will use to provide the Services against the NCSC Cloud Security Principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Buyer at the Buyer’s request.
8. Third-party Software
	1. The Supplier must not, and must ensure that Sub-contractors do not, use any software to Process Buyer Data where the licence terms of that software purport to grant the licensor rights to Progress the Buyer Data greater than those rights strictly necessary for the use of the software.
9. Deletion of Buyer Data
	1. The Supplier must, and must ensure that all Sub-contractors, securely erase any or all Buyer Data held by the Supplier or Sub-contractor when requested to do so by the Buyer using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.