# Description: Cabinet Office logo

**Appendix 1 – Special Terms Schedule**

**FOR**

**Dynamic Marketplace RM6102 - For the Provision of Apprenticeship Training and Related Services**

**CONTRACT REFERENCE NUMBER: CCZP23A11**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CONTENTS**  [**Description: Cabinet Office logo 1**](#_heading=h.gjdgxs)  [**Part A** 6](#_heading=h.3dy6vkm)  [**DEFINITIONS** 6](#_heading=h.1t3h5sf)  [**Part B – Security and Assurance Requirements** 9](#_heading=h.4d34og8)  [**1.**](#_heading=h.2s8eyo1) **ASSURANCE REQUIREMENTS** 9  [**2.**](#_heading=h.4i7ojhp) **SECURITY REQUIREMENTS** 16  [**3.**](#_heading=h.1ci93xb) **SECURITY REQUIREMENTS FOR SUB-CONTRACTORS** 21  [**Annex 1: Security Management Plan Template** 23](#_heading=h.3fwokq0)  [**Part C – Data Processing** 24](#_heading=h.4f1mdlm)  [**Part D – Contract Schedule 7: Processing Person Data and Data Subjects** 26](#_heading=h.206ipza)  [**1.**](#_heading=h.4k668n3) **Processing Data** 26  [**2.**](#_heading=h.2dlolyb) **Independent Controllers of Personal Data** 29  [**3.**](#_heading=h.1opuj5n) **Joint Controllers** 31  [**Part E – Joint Controller Agreement** 32](#_heading=h.2nusc19) **Part A****DEFINITIONS**  |  |  | | --- | --- | | “Anti-Malicious Software” | means software that scans for and identifies possible Malicious Software in the ICT Environment; | | Breach of Security | an event that results, or could result, in: set out in Section 1 Assurance Requirements Paragraph 1.39 to 1.43 : any unauthorised access to or use of the Government Data, the Services and/or the Information Management System; and/or the loss, corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract; | | Certification Requirements | means the information security requirements set out in Section 1 Assurance Requirements Paragraph 1.21 to 1.27; | | CHECK Service Provider | means a company which has been certified by the National Cyber Security Centre, holds "Green Light" status and is authorised to provide the ITHC services required by the Section 1 Assurance Requirements Paragraph 1.11 (a) and 1.28 (a); | | CREST Service Provider | means a company with a SOC Accreditation from CREST International; | | EU GDPR | meansRegulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law; | | Higher Risk Sub-contractor | means a Sub-contractor that Processes Government Data, where that data includes either: the Personal Data of 1000 or more individuals in aggregate during the period between the Contract Start Date and the End Date; or Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned; | | Incident Management Process | is the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse impact on the Government Data, the Buyer, the Services and/or users of the Services and which shall be shall be prepared by the Supplier in accordance with Section 1 Assurance Requirements Paragraph 1.10 to 1.16 using Annex 1 Security Management plan template. | | Independent Controller | meansa party which is Controller of the same Personal Data as the other Party and there is no element of joint control with regards to that Personal Data; | | Information Assurance Assessment | is the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 3 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using Annex 1 Security Management plan template. | | Information Management System | Means; those parts of the Supplier System, and those of the Sites, the Supplier or its Sub-contractors will use to provide the parts of the Services that require Processing Government Data; and the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources. | | Information Security Approval Statement | a notice issued by the Buyer which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that the Buyer: (i) is satisfied that the identified risks have been adequately and appropriately addressed; (ii) the Buyer has accepted the residual risks; and (iii) the Supplier may use the Information Management System to Process Government Data. | | ITHC | has the meaning set out in Section 1 Assurance Requirements Paragraph 1.11 (a). | | Medium Risk Sub-contractor | means a Sub-contractor that Processes Government Data, where that data includes the Personal Data of between 100 and 999 individuals (inclusive) in the period between the Contract Start date and the End Date; and does not include Special Category Personal Data, other than information about the access or dietary requirements of the individuals concerned. | | Personal Data | has the meaning given in the Data Protection Legislation. | | Personal Data Breach | has the meaning given in the Data Protection Legislation. | | Personal Data Processing Statement | sets out: (i) the types of Personal Data which the Supplier and/or its Sub-contractors are Processing on behalf of the Buyer; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Sub-contractors are Processing on behalf of the Buyer; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Government Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Government Data against a Security Breach including a Personal Data Breach, which shall be prepared by the Supplier set out in Section 1 Assurance Requirements Paragraph 1.13 (c) and included in Annex 1 Security Management Plan template. | | Process Government Data | any operation which is performed on Government Data, whether or not by automated means, including adapting, altering, collecting, combining, copying, destroying, erasing, organising, publishing retrieving, storing, structuring, transmitting or otherwise using Government Data. | | Processor Personnel | meansall directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under the Contract; | | Required Changes Register | is the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in Section 1 Assurance Requirements Paragraph 1.13 (b) together with the date by which such change shall be implemented and the date on which such change was implemented. | | Risk Register | is the risk register within the Information Assurance Assessment which is to be prepared and submitted to the Buyer for approval in accordance with set out in Section 1 Assurance Requirements Paragraph 1.13. | | Security Management Plan | comprises: (i) the Information Assurance Assessment; (ii) the Personal Data Processing Statement; (iii) the Required Changes Register; and, (iv) the Incident Management Process, which shall be prepared by the Supplier using Annex 1 Security Management Plan template. | | Sites | comprise: (i) those premises from which the Services are to be provided; (ii) those premises from which Supplier manages, organises or otherwise administers the provision of the Services; and, (iii) those premises at which any Supplier Equipment or any party of the Supplier System is located. | | Special Category Personal Data | means the categories of Personal Data set out in article 9 (1) of the GDPR. | | Supplier System | the information and communications technology system used by the Supplier in implementing and performing the Services, including the Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System). | |

## **Part B – Security and Assurance Requirements**

## **ASSURANCE REQUIREMENTS**

**Introduction**

* 1. The reference to ‘Attachment 6 of this Contract’ in paragraph 16.1 of Contract Schedule 2: Goods and/or Services, shall be read as a reference to this Part B of Appendix 1.
  2. This Part B of Appendix 1 sets out:
     + 1. the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Contract to ensure the security of the Government Data and the Information Management System;
       2. the Certification Requirements applicable to the Supplier and each of those Subcontractors which Processes Government Data;
       3. The security requirements in Section 2 of this Schedule with which the Supplier must comply;
       4. the tests which the Supplier shall conduct on the Information Management System during the Term;
       5. the Supplier's obligations to:
          1. return or destroy Government Data on the expiry or earlier termination of this Contract; and
          2. prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in Paragraph 1.36; and
          3. report Breaches of Security to the Buyer.

**Principles of Security**

* 1. The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Government Data and, consequently on the security of:
     + 1. the Sites;
       2. the Supplier System;
       3. the Information Management System; and
       4. the Services.
  2. Notwithstanding the involvement of the Buyer in assessing the arrangements which the Supplier shall implement in order to ensure the security of the Government Data and the Information Management System, the Supplier shall be, and shall remain, responsible for:
     + 1. the security, confidentiality, integrity and availability of the Government Data whilst that Government Data is under the control of the Supplier or any of its Subcontractors; and
       2. the security of the Information Management System.
  3. The Supplier shall:
     + 1. comply with the security requirements in Section 2; and
       2. ensure that each Sub-contractor that Processes Government Data complies with the security requirements in Section 3.
  4. The Supplier shall provide the Buyer with access Supplier Personnel responsible for information assurance to facilitate the Buyer's assessment of the Supplier's compliance with its obligations set out in this Section 3 at reasonable times on reasonable notice.

**Information Security Approval Statement**

* 1. The Supplier must ensure that its Implementation Plan sets out in sufficient detail how it will ensure compliance with the requirements of Section 2 Security Requirements, including any requirements imposed on Sub-contractors set out in Section 3 of this Schedule, from the Contract Start Date.
  2. The Supplier may not use the Information Management System to Process Government Data unless and until:
     + 1. the Supplier has procured the conduct of an ITHC of the Supplier System by a CHECK Service Provider or a CREST Service Provider in accordance with Paragraph 1.25; and
       2. the Buyer has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this section.
  3. The Supplier shall document in the Security Management Plan how the Supplier and its Subcontractors shall comply with the requirements set out in this section and the contract in order to ensure the security of the Government Data and the Information Management System.
  4. The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this contract, the Security Management Plan, which comprises:
     + 1. an Information Assurance Assessment;
       2. the Required Changes Register;
       3. the Personal Data Processing Statement; and
       4. the Incident Management Process.
  5. The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:
     + 1. an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Government Data; or
       2. a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.
  6. If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Authority's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Buyer for review within 10 Working Days or such other timescale as agreed with the Buyer.
  7. The Buyer may require and the Supplier shall provide the Buyer and its authorised representatives with:
     + 1. access to the Supplier Personnel;
       2. access to the Information Management System to audit the Supplier and its Subcontractors’ compliance with this Contract; and
       3. such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,
       4. to assist the Buyer to establish whether the arrangements which the Supplier and its Subcontractors have implemented in order to ensure the security of the Government Data and the Information Management System are consistent with the representations in the Security Management Plan. The Supplier shall provide the access required by the Buyer in accordance with this Paragraph within 10 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.

**Compliance Reviews**

* 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.
  2. The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:
     + 1. a significant change to the components or architecture of the Information Management System;
       2. a new risk to the components or architecture of the Service;
       3. a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out Section 2 Security Requirements Paragraph 2.19;
       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.
  3. Within 10 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 Required Changes Register and submit the updated Required Changes Register the Buyer for review and approval.
  4. Where the Supplier is required to implement a change, including any change to the Information Management System the Supplier shall effect such change at its own cost and expense.

**Certification Requirements**

* 1. The Supplier shall be certified as compliant with:
     + 1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and
       2. Cyber Essentials PLUS
       3. and shall provide the Buyer with a copy of each such certificate of compliance before the Supplier shall be permitted to receive, store or Process Government Data.
  2. The Supplier shall ensure that each Higher Risk Sub-contractor is certified as compliant with either:
     + 1. ISO/IEC 27001:2013 by a United Kingdom Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; or
       2. Cyber Essentials PLUS,
       3. and shall provide the Buyer with a copy of each such certificate of compliance before the Higher-Risk Subcontractor shall be permitted to receive, store or Process Government Data.
  3. The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with Cyber Essentials.
  4. The Supplier shall ensure that the Supplier and each Sub-contractor who is responsible for the secure destruction of Government Data:
     + 1. securely destroys Government Data only on Sites which are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013; and
       2. are certified as compliant with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard or an alternative standard as agreed by the Buyer.
  5. The Supplier shall provide the Buyer with evidence of its and its Sub-contractor's compliance with the requirements set out in this Paragraph before the Supplier or the relevant Sub-contractor (as applicable) may carry out the secure destruction of any Government Data.
  6. The Supplier shall notify the Buyer as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Subcontractor ceases to be compliant with the Certification Requirements and, on request from the Buyer, shall or shall procure that the relevant Sub-contractor shall:
     + 1. immediately ceases using the Government Data; and
       2. procure that the relevant Sub-contractor promptly returns, destroys and/or erases the Government Data in accordance with the requirements set out in this Paragraph.
  7. The Buyer may agree to exempt, in whole or part, the Supplier or any Sub-contractor from the requirements of this Section. Any exemption must be in writing to be effective. The Supplier must include the exemption in the Security Management Plan.

**Security Testing**

* 1. The Supplier shall, at its own cost and expense procure and conduct:
     + 1. testing of the Information Management System by a CHECK Service Provider or a CREST Service Provider (“ITHC”); and
       2. such other security tests as may be required by the Buyer,
       3. The Supplier shall complete all of the above security tests before the Supplier submits the Security Management Plan to the Buyer for review in accordance within section 1.10; and it shall repeat the ITHC not less than once every 12 months during the Term and submit the results of each such test to the Buyer for review in accordance with this Paragraph.
  2. In relation to each ITHC, the Supplier shall:
     + 1. agree with the Buyer the aim and scope of the ITHC;
       2. promptly, and no later than 10 working days, following the receipt of each ITHC report, provide the Buyer with a copy of the full report;
  3. in the event that the IT Health Check report identifies any vulnerabilities, the Supplier shall:
     + 1. prepare a remedial plan for approval by the Buyer (each a "**Vulnerability Correction Plan**") which sets out in respect of each vulnerability identified in the ITHC report:
          1. how the vulnerability will be remedied;
          2. the date by which the vulnerability will be remedied;
          3. the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Buyer, include a further IT Health Check) to confirm that the vulnerability has been remedied;
       2. comply with the Vulnerability Correction Plan; and
       3. conduct such further tests on the Service as are required by the Vulnerability Correction Plan to confirm that the Vulnerability Correction Plan has been complied with.
  4. The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Buyer.
  5. If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information Management System, the Supplier shall within days of becoming aware of such risk, threat, vulnerability or exploitation technique provide the Buyer with a copy of the test report and:
     + 1. propose interim mitigation measures to vulnerabilities in the Information System known to be exploitable where a security patch is not immediately available; and
       2. where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Buyer.
  6. The Supplier shall conduct such further tests of the Supplier System as may be required by the Buyer from time to time to demonstrate compliance with its obligations set out this Schedule and the Contract.
  7. The Supplier shall notify the Buyer immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in set out in Section 2 of this Schedule.

**Security Monitoring and Reporting**

* 1. The Supplier shall:
     + 1. monitor the delivery of assurance activities;
       2. maintain and update the Security Management Plan in accordance with Section 1 Assurance Requirements Paragraph 1.10 (b);
       3. agree a document which presents the residual security risks to inform the Buyer’s decision to give approval to the Supplier to Process, store and transit the Government Data;
       4. monitor security risk impacting upon the operation of the Service;
       5. report Breaches of Security in accordance with the approved Incident Management Process;
       6. agree with the Buyer the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Buyer within 30 days of the date of this Contract.

**Malicious Software**

* 1. The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Government Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.
  2. 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 Government Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.
  3. Any cost arising out of the actions of the parties taken in compliance with the provisions of Paragraph 1.34 shall be borne by the parties as follows:
     + 1. by the Supplier where the Malicious Software originates from the Supplier Software, the Third Party Software supplied by the Supplier or the Government Data (whilst the Government 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.

**Breach of Security**

* 1. If either party becomes aware of a Breach of Security it shall notify the other in accordance with the Incident Management Process.
  2. The Incident Management Process shall, as a minimum, require the Supplier to do the following upon it becoming aware of a Breach of Security or attempted Breach of Security:
  3. Immediately take all reasonable 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;
  4. as soon as reasonably practicable and, in any event, within 2 Working Days, 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.
  5. In the event that any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Subcontractors and/or all or any part of the Information Management System with this Contract, then such remedial action shall be completed at no additional cost to the Buyer.

## **SECURITY REQUIREMENTS**

**Security Classification of Information**

* 1. If the provision of the Services requires the Supplier to Process Government Data, which is classified as OFFICIAL-SENSITIVE, the Supplier shall implement such additional measures as agreed with the Buyer from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

**End User Devices**

* 1. The Supplier shall ensure that any Government Data, which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Buyer except where the Buyer has given its prior written consent to an alternative arrangement.
  2. The Supplier shall ensure that any device which is used to Process Government Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/collection/end-user-device-security>

**Networking**

* 1. The Supplier shall ensure that any Government Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

**Personnel Security**

* 1. All Supplier Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record.
  2. The Buyer and the Supplier shall review the roles and responsibilities of the Supplier Personnel who will be involved in the management and/or provision of the Services in order to enable the Buyer to determine which roles require additional vetting and a specific national security vetting clearance (e.g. a Counter Terrorist Check; a Security Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to IT systems which Process Government Data or data which is classified as OFFICIAL-SENSITIVE.
  3. The Supplier shall not permit Supplier Personnel who fail the security checks required by Paragraphs 2.5 and 2.6 to be involved in the management and/or provision of the Services except where the Buyer has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services.
  4. The Supplier shall ensure that Supplier Personnel are only granted such access to Government Data as is necessary to enable the Supplier Personnel to perform their role and to fulfil their responsibilities.
  5. The Supplier shall ensure that Supplier Personnel who no longer require access to the Government Data (e.g. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Government Data revoked within 1 Working Day.

**Identity, Authentication and Access Control**

* 1. The Supplier shall operate an access control regime to ensure:
     + 1. all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and
       2. all persons who access the Sites are identified and authenticated before they are allowed access to the Sites.
  2. The Supplier shall apply the ‘principle of least privilege’ when allowing persons access to the Supplier System and Sites so that such persons are allowed access only to those parts of the Sites and the Supplier System they require.
  3. The Supplier shall retain records of access to the Sites and to the Supplier System and shall make such record available to the Buyer on request.

**Data Destruction or Deletion**

* 1. The Supplier shall:
     + 1. prior to securely sanitising any Government data or when requested the Supplier shall provide the Government with all Government Data in an agreed open format;
       2. have documented processes to ensure the availability of Government Data in the event of the Supplier ceasing to trade;
       3. securely erase in a manner agreed with the Buyer any or all Government Data held by the Supplier when requested to do so by the Buyer;
       4. securely destroy in a manner agreed with the Buyer all media that has held Government Data at the end of life of that media in accordance with any specific requirements in this Contract and, in the absence of any such requirements, as agreed by the Buyer; and
       5. implement processes which address the CPNI and NCSC guidance on secure sanitisation.

**Audit and Protective Monitoring**

* 1. The Supplier shall collect audit records which relate to security events in the Information Management System or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Government Data.
  2. The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the Information Management System.
  3. The retention periods for audit records and event logs must be agreed with the Buyer and documented in the Security Management Plan.

**Location of Government Data**

* 1. The Supplier and any of its Sub-contractors must not process any Government Data outside the EEA without the prior written consent of the Buyer, which may be subject to conditions of which the Supplier and any of its Sub-contractors must comply. Any permission must be in writing to be effective.

**Vulnerabilities and Corrective Action**

* 1. The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the Information Management System will be discovered which unless mitigated will present an unacceptable risk to the Government Data.
  2. The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as ‘Critical’, ‘Important’ and ‘Other’ by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:
     + 1. the ‘National Vulnerability Database’ ‘Vulnerability Severity Ratings’: ‘High’, ‘Medium’ and ‘Low’ respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and
       2. Microsoft’s ‘Security Bulletin Severity Rating System’ ratings ‘Critical’, ‘Important’, and the two remaining levels (‘Moderate’ and ‘Low’) respectively.
  3. Subject to Paragraph 1.25, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:
     + 1. 7 days after the public release of patches for those vulnerabilities categorised as ‘Critical’;
       2. 30 days after the public release of patches for those vulnerabilities categorised as ‘Important’; and
       3. 60 days after the public release of patches for those vulnerabilities categorised as ‘Other’.
  4. The timescales for applying patches to vulnerabilities in the Information Management System set out in Paragraph 2.16 shall be extended where:
     + 1. the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (e.g. because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in Paragraph 2.16 if the vulnerability becomes exploitable within the context of the Services;
       2. the application of a ‘Critical’ or ‘Important’ security patch adversely affects the Supplier’s ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or
       3. the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.
  5. The Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Buyer in writing. All COTS Software should be no more than N-1 versions behind the latest software release.

**Secure Architecture**

* 1. The Supplier shall design the Information Management System in accordance with:
     + 1. the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main>;
       2. the NCSC "Bulk Data Principles", a copy of which can be found at https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and
       3. the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:
       4. "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;
       5. "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;
       6. "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;
       7. "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;
       8. "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;
       9. "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Government Data and/or the Buyer System that those personnel be subject to appropriate security screening and regular security training;
       10. "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;
       11. "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;
       12. "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Buyer to securely manage the Buyer's use of the Service;
       13. "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;
       14. "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted interfaces with the Services should be identified and appropriately defended;
       15. "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;
       16. "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Buyer with the audit records it needs to monitor access to the Service and the Government Data held by the Supplier and/or its Sub-contractors; and
       17. "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

## **SECURITY REQUIREMENTS FOR SUB-CONTRACTORS**

**Application of Annex**

## This Annex applies to all Sub-contractors that Process Government Data.

## The Supplier must:

* + - 1. ensure that those Sub-contractors comply with the provisions of this Annex;
      2. keep sufficient records to demonstrate that compliance to the Buyer; and
      3. ensure that its Implementation Plan includes Deliverable Items, Milestones and Milestone Dates that relate to the design, implementation and management of any systems used by Sub-contractors to Process Government Data.

**Designing and managing secure solutions**

## The Sub-contractor shall implement their solution(s) to mitigate the security risks in accordance with the NCSC’s Cyber Security Design Principles <https://www.ncsc.gov.uk/collection/cyber-security-design-principles>.

## The Sub-contractor must assess their systems against the NCSC Cloud Security Principles: [https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles](https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles%20) 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 on the Buyer’s request.

**Data Processing, Storage, Management and Destruction**

## The Sub-contractor must not Process any Government Data outside the EEA without the prior written consent of the Buyer, which may be subject to conditions of which the Sub-contractor must comply. Any permission must be in writing to be effective.

## The Sub-contractor must securely erase any or all Government Data held by the Sub-contractor when requested to do so by the Buyer; and securely destroy all media that has held Government Data at the end of life of that media in accordance with the NCSC Assured Service (CAS) Service Requirement Sanitisation Standard, or an alternative agreed in writing by the Buyer.

**Personnel Security**

## The Sub-contractor must perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all pre-employment checks required by the HMG Baseline Personnel Security Standard including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The HMG Baseline Personnel Security Standard is at https://www.gov.uk/government/publications/government-baseline-personnel-security-standard.

## The Sub-contractor must, if the Buyer requires, at any time, ensure that one or more of the Sub-contractor’s staff obtains Security Check clearance in order to Process Government Data containing Personal Data above certain volumes specified by the Buyer, or containing Special Category Personal Data.

## Any Sub-contractor staff who will, when performing the Services, have access to a person under the age of 18 years must undergo DBS checks.

**End User Devices**

## The Sub-contractor shall ensure that any Government Data stored (for any period of time) on a mobile, removable or physically uncontrolled device is encrypted. The Sub-contractor must follow the Information Commissioner’s Office guidance on implementing encryption, which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/.

## The Supplier shall ensure that any device used to Process Government Data meets all the security requirements set out in the NCSC End User Devices Platform Security Guidance, which can be found at <https://www.ncsc.gov.uk/guidance/end-user-device-security>.

**Networking**

## The Supplier shall ensure that any Government Data which it causes to be transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.

**Patching and Vulnerability Scanning**

## The Sub-contractor must proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.

**Third Party Subcontractors**

## The Sub-contractor must not transmit or disseminate the Government Data to any other person unless specifically authorised by the Buyer. Such authorisation must be in writing to be effective and may be subject to conditions.

## The Sub-contractor must not, when performing any part of the Services, use any software to Process the Government Data where the licence terms of that software purport to grant the licensor rights to Progress the Government Data greater than those rights strictly necessary for the use of the software.

## 

## **Annex 1: Security Management Plan Template**

****

## **Part C – Data Processing**

## **General Provisions**

## The provisions in Part D of this Schedule shall constitute Contract Schedule 7 of the Call-off Terms.

## Where the table in Part D of this Schedule specifies that the Parties are Joint Controllers of Personal Data, the Parties shall use the Joint Controller Agreement in Part E of this Schedule at Schedule 8 to the Contract.

## The definition of “GDPR” used in the Contract shall be read as a reference to “UK GDPR” which means: “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.”

## The defined term “Protected Measures” in Contract Schedule 1 (Definitions) shall be read as the defined term being “Protective Measures.”

## Clause 23.28(d) is deleted and replaced with the following:

* + 1. not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
       1. the transfer is in accordance with Article 45 of the UK GDPR (or section 73 of DPA 2018); or
       2. the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) as determined by the Controller which could include relevant parties entering into the International Data Transfer Agreement (the “**IDTA**”), or International Data Transfer Agreement Addendum to the European Commission’s SCCs (**the “Addendum”),** as published by the Information Commissioner’s Office from time to time, as well as any additional measures determined by the Controller;
       3. the Data Subject has enforceable rights and effective legal remedies;
       4. the Processor 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 Controller in meeting its obligations); and
       5. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data;

## New clause 23.28(f) is added as follows:

* + 1. where the Personal Data is subject to EU GDPR, not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

1. the transfer is in accordance with Article 45 of the EU GDPR; or
2. the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission’s decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by the non-transferring Party;
3. the Data Subject has enforceable rights and effective legal remedies;
4. the transferring Party 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 non-transferring Party in meeting its obligations); and
5. the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

## **Part D – Contract Schedule 7: Processing Person Data and Data Subjects**

## **Processing Data**

## This Schedule shall be completed by the Controllers.

## The contact details of the Customer’s Data Protection Officer are: **REDACTED TEXT under FOIA Section 40, Personal Information**.

## The contact details of the Supplier’s Data Protection Officer are:

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

|  |  |
| --- | --- |
| **Description** | **Details** |
| Identity of the Controller and Processor | The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer and the Supplier are both independent Controllers for the data processed to provide the Services. | |
| Subject matter of the processing | The delivery of a training offer to 29 Cyber Security Degree apprentices. | |
| Duration of the processing | For the duration of the Contract, and thereafter in accordance with the parties’ retention policies | |
| Nature and purposes of the processing | Collection, holding, disclosure and deletion of data.  For the purpose of delivery of a training offer to Cyber Security apprentices. | |
| Type of Personal Data being Processed | Name, address, email address, job title, employer, learning outcomes, reasonable adjustments/health, learning data, candidate progress and assignment portfolios. | |
| Categories of Data Subject | Civil Service Apprentices | |
| Plan for return and destruction of the data once the processing is complete  UNLESS requirement under union or member state law to preserve that type of data | All data to be To be destroyed in line with the parties’ retention policies. | |
|  |  | |

## **Independent Controllers of Personal Data**

## With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller and with the following clauses of Paragraph 2 of this Part D of Appendix 1.

## Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

## Where a Party has provided Personal Data to the other Party in accordance with Paragraph 2.2 of this Part D of Appendix 1 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

## The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

## The Parties shall only provide Personal Data to each other:

## to the extent necessary to perform their respective obligations under the Contract;

## in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

## where it has recorded it in the table in Paragraph 1 of this Part D of Appendix 1.

## Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

## A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

## Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (“Request Recipient”):

## the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

## where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

## promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

## provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

## Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

## do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

## implement any measures necessary to restore the security of any compromised Personal Data;

## work with the other Party to make any required notifications to the Information Commissioner’s Office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

## not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

## Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in this Part D of Appendix 1.

## Personal Data shall not be retained or processed for longer than is necessary to perform each Party’s respective obligations under the Contract which is specified in this Part D of Appendix 1.

## Notwithstanding the general application of Clauses 23.25 to 23.39 of this Contract to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 2.1 to 2.12 of this Part D of Appendix 1.

## **Joint Controllers**

## NOT USED

## **Part E – Joint Controller Agreement**

**SCHEDULE 8**

**JOINT CONTROLLER AGREEMENT**

1. **NOT USED**