Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

1. Definitions

In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	the occurrence of: (a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or (b) the loss 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, in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time.

2. Complying with security requirements and updates to them

2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

2.6 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

2.7 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

2.7.1 is in accordance with the Law and this Contract;

2.7.2 as a minimum demonstrates Good Industry Practice;

2.7.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

2.7.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

2.8 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

2.9 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

2.10 Introduction

2.10.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

2.11 Content of the Security Management Plan

2.11.1 The Security Management Plan shall:

comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to

ensure that the Deliverables comply with the provisions of this Contract;

set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and

be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

2.12 **Development of the Security Management Plan**

2.12.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

2.12.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved,

the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

2.12.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However, a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

2.12.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

2.13 **Amendment of the Security Management Plan**

2.13.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

a) emerging changes in Good Industry Practice;

any change or proposed change to the Deliverables and/or associated processes;

where necessary in accordance with paragraph 2.2, any change to the Security Policy;

any new perceived or changed security threats; and

any reasonable change in requirements requested by the Buyer.

2.13.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

a) suggested improvements to the effectiveness of the Security Management Plan;

updates to the risk assessments; and

suggested improvements in measuring the effectiveness of controls.

2.13.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

2.13.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice

to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

2.14 **Security breach**

2.14.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

2.14.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

2.14.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

a) minimise the extent of actual or potential harm caused by any Breach of Security;

b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

c) prevent an equivalent breach in the future exploiting the same cause failure; and

d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

2.14.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

3 The Authorities security clauses have been included below in Annex A and supersede any above materials.

Part A – Annex 1 – Department for Education security clauses

1. Project Outputs

1.1. Unless otherwise agreed between the Parties, the Deliverables shall be published by the Buyer on its research website. The Buyer shall not use the Supplier's name in any advertising or public communications unless agreed in writing in advance with the Supplier (such agreement not to be unreasonably withheld or delayed).

1.2. The Supplier shall ensure that all outputs for publication by the Buyer adhere to the Buyer's style guide and MS Word template, available to download from: https://www.gov.uk/government/publications/eoi-guide.

1.3. Unless otherwise agreed between the Parties, the Supplier shall supply the Buyer with a draft for comment at least eight weeks before the intended publication date, for interim reports, and eight weeks before the expiry date of the Contract for final reports.

1.4. The Supplier shall consider revisions to the drafts with the Buyer in the light of any comments pursuant to clause 1.3. The Supplier shall provide final, signed off interim reports and other outputs planned within the lifetime of the Contract to the Buyer by no later than four weeks before the intended publication date, and final, signed off Deliverables by no later than the contracted expiry date of the Contract.

1.5. Until the date of publication, findings from all Contract shall be treated as confidential. The Supplier shall not release findings to the press or disseminate them in any way or at any time prior to publication without approval of the Buyer.

1.6. Where the Supplier wishes to issue a press notice or other publicity material containing findings from the Contract it may only do so with the prior written agreement of the Buyer and notification of plans, including timing and drafts of planned releases, shall be submitted by the Supplier to the Buyer at least

three weeks before the intended date of release and before any agreement is made with press or other external audiences, to allow the Buyer time to review. All press notices released by the Parties shall state the full title of the research report, and include a hyperlink to the Buyer's research web pages, and any other web pages as relevant, to access the publication/s. This clause applies at all times prior to publication of the final report.

1.7. Where the Supplier wishes to present findings from the Contract in the public domain, for example at conferences, seminars, or in journal articles, it may only do so with the prior written agreement of the Buyer and the Supplier shall notify the Buyer before any agreement is made with external audiences, to allow the Buyer time to consider the request. The Supplier shall only present findings that are already be in the public domain at the time of presentation, unless otherwise agreed with the Buyer. This clause applies at all times prior to publication of the final report.

2. Publicity and Branding

2.1. Each Party acknowledges to the other that nothing in this Contract either expressly or by implication constitutes an endorsement of any products or services of the other Party (including the Deliverables) and each Party agrees not to conduct itself in such a way as to imply or express any such approval or endorsement.

2.2. The Buyer may disclose, copy, and otherwise distribute to the public, including but not limited to, by way of the Open Government Licence, any information arising out of the Deliverables or comprised in any work relating to the Deliverables.

3. Safeguarding Children and Vulnerable Adults

Regulated Activity	(a) in relation to children as defined in Part 1 of Schedule 4 to the

Safeguarding Vulnerable Groups Act 2006; and

(b) in relation to vulnerable adults as defined in Part 2 of Schedule 4 to the Safeguarding Vulnerable Groups Act 2006;

3.1. The Parties acknowledge that the Supplier is carrying out a Regulated Activity with ultimate responsibility for the management and control of the Regulated Activity provided under this Contract and for the purposes of the Safeguarding Vulnerable Groups Act 2006.

3.2. The Supplier shall put in place safeguards to protect children and/or vulnerable adults from any risk of significant harm which could arise from the performance of this Contract. The Supplier shall agree these safeguards, including procedures for dealing with allegations against staff with the Buyer before commencing work on the Contract.

3.3. In addition, the Supplier shall carry out checks with the Disclosure and Barring Service (DBS checks) on all Supplier Staff carrying out Regulated Activity. The Supplier must carry out a DBS check for each relevant member of Supplier Staff and shall renew the DBS check every three years for as long as this Contract is in force. The DBS check must be completed before any of the Supplier Staff work with children and/or vulnerable adults, as applicable, in Regulated Activity.

3.4. The Supplier shall monitor the level and validity of the checks under this Clause for each member of the Supplier Staff.

3.5. The Supplier shall immediately notify the Buyer of any information that it reasonably requests to enable it to be satisfied that the obligations of the Supplier under this Clause have been met.

3.6. The Supplier shall not employ or use the services of any person who is barred from, or whose previous conduct or records indicate that such person would not be suitable to carry out, Regulated Activity or who may otherwise present a risk to children or vulnerable adults.

3.7. The Supplier shall refer information about any person carrying out the Deliverables to the Disclosure and Barring Service where it removes permission for such person to carry out the Services (or would have, if such person had not otherwise ceased to carry out the Services) because, in its opinion, such person has harmed or poses a risk of harm to children or vulnerable adults.

3.8. The Supplier represents, warrants, and undertakes that at all times for the purposes of this Contract it has no reason to believe that any member of the Supplier Staff is barred from performance of the Services in accordance with the provisions of the Safeguarding Vulnerable Groups Act 2006 and any regulations made thereunder, as amended from time to time.

3.9. Both Parties will comply with all applicable requirements of Data Protection Legislation in relation to the requirements of this Clause. The Parties acknowledge that, for the purposes of the Data Protection Legislation, the Supplier is the Controller in respect of DBS Checks carried out on Supplier Staff. The Supplier will ensure that it has all necessary appropriate consents and notices in place to obtain the DBS Checks and to enable lawful disclosure of the DBS certificates and any other relevant Personal Data to the Supplier for the duration and purposes of this Contract.

4. Security Terms

"BPSS" "Baseline Personnel Security Standard"	the Government's HMG Baseline Personal Security Standard. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard

"CCSC" "Certified Cyber Security Consultancy"	is the National Cyber Security Centre's (NCSC) approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
"CCP" "Certified Professional"	is a NCSC scheme in consultation with government, industry, and academia to address the growing need for specialists in the cyber security profession. See website: https://www.ncsc.gov.uk/information/about-certified-professional-scheme
"Cyber Essentials" "Cyber Essentials Plus"	Cyber Essentials is the government backed; industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. There are a number of certification bodies that can be approached for further advice on the scheme, the link below points to these providers: https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body
"Data" "Data Controller" "Data Protection Officer" "Data Processor" "Personal Data"	shall have the meanings given to those terms by the Data Protection Legislation

"Personal Data requiring Sensitive Processing" "Data Subject", "Process" and "Processing"	
"Buyer's Data" "Buyer's Information"	is any data or information owned or retained to meet departmental business objectives and tasks, including: (a) any data, text, drawings, diagrams, images, or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical, or tangible media, and which are: (i) supplied to the Supplier by or on behalf of the Buyer; or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; or (b) any Personal Data for which the Buyer is the Data Controller;
"Departmental Security Requirements"	the Buyer's security policy or any standards, procedures, process, or specification for security that the Supplier is required to deliver.
"Digital Marketplace / G-Cloud"	the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects.
"End User Devices"	the personal computer or consumer devices that store or process information.

"Good Industry Standard" "Industry Good Standard"	the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight, and timeliness as would be expected from a leading company within the relevant industry or business sector.
"GSC" "GSCP"	the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
"HMG"	Her Majesty's Government
"ICT"	Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
"ISO/IEC 27001" "ISO 27001"	is the International Standard for Information Security Management Systems Requirements
"ISO/IEC 27002" "ISO 27002"	is the International Standard describing the Code of Practice for Information Security Controls.
"ISO 22301"	is the International Standard describing for Business Continuity
"IT Security Health Check (ITSHC)" "IT Health Check (ITHC)" "Penetration Testing"	an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that ICT system.

"Need-to-Know"	the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear 'need to know' in order to carry out their duties.
"NCSC"	the National Cyber Security Centre (NCSC) is the UK government's National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk
"OFFICIAL" "OFFICIAL-SENSITIVE"	the term 'OFFICIAL' is used to describe the baseline level of 'security classification' described within the Government Security Classification Policy (GSCP). the term 'OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen, or published in the media, as described in the GSCP.
"RBAC" "Role Based Access Control"	Role Based Access Control, a method of restricting a person's or process' access to information depending on the role or functions assigned to them.
"Storage Area Network" "SAN"	an information storage system typically presenting block-based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage.
"Secure Sanitisation"	the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. NCSC Guidance can be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

	The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction-0
"Security and Information Risk Advisor" "CCP SIRA" "SIRA"	the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme
"Senior Information Risk Owner" "SIRO"	the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arm's length bodies (ALBs), non-departmental public bodies (NDPBs) and devolved information held by third parties.
"SPF" "HMG Security Policy Framework"	the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government's Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently, and securely. https://www.gov.uk/government/publications/security-policy-framework
"Supplier Staff"	all directors, officers, employees, agents, consultants, and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under the Contract.

Operative Provisions

4.1. The Supplier shall be aware of and comply with the relevant HMG security policy framework, NCSC guidelines and where applicable these Departmental

Security Requirements which include but are not constrained to the following paragraphs.

4.2. Where the Supplier will provide products or Services or otherwise handle information at OFFICIAL for the Buyer, the requirements of Procurement Policy Note: Updates to the Cyber Essentials Scheme (PDF) - Action Note 09/23 dated September 2023, or any subsequent updated document, are mandated, namely that contractors supplying products or services to HMG shall have achieved and will retain Cyber Essentials certification at the appropriate level for the duration of the contract. The certification scope shall be relevant to the Services supplied to, or on behalf of, the Buyer.

4.3. Where paragraph 4.2 above has not been met, the Supplier shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements). The ISO/IEC 27001 certification must have a scope relevant to the Services supplied to, or on behalf of, the Buyer. The scope of certification and the statement of applicability must be acceptable, following review, to the Buyer, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

4.4. The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Buyer's Data being handled in the course of providing the Services and will handle all data in accordance with its security classification. (In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Buyer's Data).

4.5. Buyer's Data being handled while providing an ICT solution or service must be separated from all other data on the Supplier's or sub-contractor's own IT equipment to protect the Buyer's Data and enable the data to be identified and securely deleted when required in line with paragraph 4.14. For information stored digitally, this must be at a minimum logically separated. Physical information (e.g., paper) must be physically separated.

4.6. The Supplier shall have in place and maintain physical security to premises and sensitive areas used in relation to the delivery of the products or Services, and that store or process Buyer's Data, in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g., door access), CCTV, alarm systems, etc.

4.6.1. Where remote working is allowed, the Supplier shall have an appropriate remote working policy in place for any Supplier staff that will have access to the Buyer's data and/or systems.

4.7. The Supplier shall have in place, implement, and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Buyer's Data. This policy should include appropriate segregation of duties and if applicable role-based access controls (RBAC). User credentials that give access to Buyer's Data or systems shall be considered to be sensitive data and must be protected accordingly.

4.8. The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer's Data, including but not limited to:

4.8.1. physical security controls;

4.8.2. good industry standard policies and processes;

4.8.3. malware protection;

4.8.4. boundary access controls including firewalls, application gateways, etc;

4.8.5. maintenance and use of fully supported software packages in accordance with vendor recommendations;

4.8.6. use of secure device configuration and builds;

4.8.7. software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;

4.8.8. user identity and access controls, including the use of multi-factor authentication for sensitive data and privileged account accesses;

4.8.9. any services provided to the Buyer must capture audit logs for security events in an electronic format at the application, service and system level to meet the Buyer's logging and auditing requirements, plus logs shall be:

4.8.9.1. retained and protected from tampering for a minimum period of six months;

4.8.9.2. made available to the Buyer on request.

4.9. The Supplier shall ensure that any Buyer's Data (including email) transmitted over any public network (including the Internet, mobile networks, or unprotected enterprise network) or to a mobile device shall be encrypted when transmitted.

4.10. The Supplier shall ensure that any Buyer's 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.

4.11. The Supplier shall ensure that any device which is used to process Buyer's 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/guidance/end-user-device-security and https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles.

4.12. Whilst in the Supplier's care all removable media and hardcopy paper documents containing Buyer's Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

The term ‘lock and key’ is defined as: “securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user’s sole control and to which they hold the keys”.

4.13. When necessary to hand carry removable media and/or hardcopy paper documents containing Buyer’s Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This paragraph shall apply equally regardless of whether the material is being carried inside or outside of company premises.

The term ‘under cover’ means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

4.14. In the event of termination of Contract due to expiry, as a result of an Insolvency Event or for breach by the Supplier, all information assets provided, created or resulting from provision of the Services shall not be considered as the Supplier’s assets and must be returned to the Buyer and written assurance obtained from an appropriate officer of the Supplier that these assets regardless of location and format have been fully sanitised throughout the Supplier’s organisation in line with paragraph 4.15.

4.15. In the event of termination, equipment failure or obsolescence, all Buyer’s Data and Buyer’s Information, in either hardcopy or electronic format, that is physically held or logically stored by the Supplier must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC-approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Supplier shall protect (and ensure that any sub-contractor protects) the Buyer’s Information and Buyer’s Data until such time, which may be long after termination or expiry of the Contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

4.16. Access by Supplier Staff to Buyer's Data, including user credentials, shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Buyer. All Supplier Staff must complete this process before access to Buyer's Data is permitted. [Any Supplier Staff who will be in contact with children or vulnerable adults must, in addition to any security clearance, have successfully undergone an Enhanced DBS (Disclosure and Barring Service) check prior to any contact].

4.17. Notwithstanding any other provisions as to business continuity and disaster recovery in the Contract, the Supplier shall, as a minimum, have in place robust business continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the Contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency, or crisis to the Services delivered. If an ISO 22301 certificate is not available, the supplier will provide evidence of the effectiveness of their ISO 22301 conformant business continuity arrangements and processes including IT disaster recovery plans and procedures. This must include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.

4.18. Any suspected or actual breach of the confidentiality, integrity, or availability of Buyer's Data, including user credentials, used, or handled while providing the Services shall be recorded as a Security Incident. This includes any non-compliance with the Departmental Security Requirements and these provisions, or other security standards pertaining to the solution.

Security Incidents shall be reported to the Buyer immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery and followed up in writing. If Security Incident reporting has been delayed by more than 24 hours,

the Supplier should provide an explanation about the delay. Regular updates on the Security Incident shall be provided to the Buyer in writing until the incident is resolved.

Security Incidents shall be reported through the Buyer's nominated system or service owner.

Security Incidents shall be investigated by the Supplier with outcomes being notified to the Buyer.

4.19. The Supplier shall ensure that any Supplier ICT systems and hosting environments that are used to handle, store or process Buyer's Data, including Supplier ICT connected to Supplier ICT systems used to handle, store or process Buyer's Data, shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. On request by the Buyer, the findings of the ITHC relevant to the Services being provided are to be shared with the Buyer in full without modification or redaction and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required, to be determined by the Buyer upon review of the ITHC findings.

4.20. The Supplier or sub-contractors providing the Services will provide the Buyer with full details of any actual or future intent to develop, manage, support, process, or store Buyer's Data outside of the UK mainland. The Supplier or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Buyer.