Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements – <u>This part is not used for this agreement</u>

1. Definitions

1.1 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 the rewith 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

3.1 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.

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

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

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

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

3.3 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.

3.4 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

4.1 Introduction

4.1.1 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.

4.2 Content of the Security Management Plan

4.2.1 The Security Management Plan shall:

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

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

c) 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;

d) 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;

e) 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;

f) 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

g) 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.

4.3 Development of the Security Management Plan

4.3.1 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.

4.3.2 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.

4.3.3 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.

4.3.4 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.

4.4 Amendment of the Security Management Plan

4.4.1 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;

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

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

d) any new perceived or changed security threats; and

e) any reasonable change in requirements requested by the Buyer.

4.4.2 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;

b) updates to the risk assessments; and

c) suggested improvements in measuring the effectiveness of controls.

4.4.3 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.

4.4.4 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.

5. Security breach

5.1 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.

5.2 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:

5.2.1 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.

5.3 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.

Part B: Long Form Security Requirements

1. Definitions

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

"Breach of Security"	2 means the occurrence of: a) any unauthorised access to or use of the Goods and/or 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, 3 in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;
"ISMS"	4 the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and
"Security Tests"	5 tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Requirements

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 Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security

under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:

2.3.1 Security representative of the Buyer: Information.SECURITY@education.gov.uk

2.3.2 Security representative of the Supplier: [redacted]

2.4 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

2.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

2.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and cooperation between the Parties.

3. Information Security Management System (ISMS)

3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

3.2 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 the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that;

3.3.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

3.4 The ISMS shall:

3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, 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, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) 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;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.3 at all times provide a level of security which:

a) is in accordance with the Law and this Contract;

b) complies with the Baseline Security Requirements;

c) as a minimum demonstrates Good Industry Practice;

d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;

e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)

f) takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk)

g) complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm)

h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

i) addresses issues of incompatibility with the Supplier's own organisational security policies; and

j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

3.4.4 document the security incident management processes and incident response plans;

3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the

potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 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.

3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall 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 the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

3.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4. Security Management Plan

4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which

shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) 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;

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) 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;

4.2.6 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 delivery of the Deliverables and 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 Schedule (including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those

incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

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

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall 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 the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure 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.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5. Amendment of the ISMS and Security Management Plan

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

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;

5.1.5 any new perceived or changed security threats; and

5.1.6 any reasonable change in requirement requested by the Buyer.

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

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or 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.

6. Security Testing

6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in

relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practises of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.

7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practises of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.

7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practises of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. Security Breach

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 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 or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.3 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 ISMS with the Security Policy (where relevant) or the requirements of this

Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

9. Vulnerabilities and fixing them

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat 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 ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 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 http://nvd.nist.gov/cvss.cfm); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 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

9.3.3 The Buyer agrees to a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

9.4.1 where upgrading such COTS Software reduces the level of

mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;

9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 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 ICT Environment); and

9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

1. Handling Classified information

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. End user devices

2.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre (“NCSC”) to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a ‘known good’ state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

3.1 The Supplier and Buyer recognise the need for the Buyer’s information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

3.2 The Supplier shall agree to any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. Security by design

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

6.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used

to manage Government Data except where agreed with the Buyer in writing.

6.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. Restricting and monitoring access

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

8. Audit

8.1 The Supplier shall collect audit records which relate to security events in the systems 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:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 - Security Management Plan

[To be completed by supplier]

Annex 3 – Departmental Security Clauses

1 SUPPLIER OBLIGATIONS

Core requirements

1.1 The Supplier must comply with the core requirements set out in Paragraphs 3 to 9.

1.2 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements relating to that option set out in the relevant Paragraph:

Certifications (see Paragraph 4)		
The Supplier must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	☒
	Cyber Essentials Plus	☐
	Cyber Essentials	☐
	No certification required	☐
Subcontractors that Handle Government Data must have the following Certifications (or equivalent):	ISO/IEC 27001:2022 by a UKAS-recognised Certification Body	☒
	Cyber Essentials Plus	☐
	Cyber Essentials	☐
	No certification required	☐
Locations (see Paragraph 5)		
The Supplier and Subcontractors may store, access or Handle Government Data in:	the United Kingdom only	☒
	a location permitted by and in accordance with any regulations for the time being in force made under 17A of the Data Protection Act	☐

	2018 (adequacy decisions by the Secretary of State)	
	anywhere in the world not prohibited by the Buyer	☐
Staff Vetting Procedure (see Paragraph 6)		
The Buyer requires a Staff Vetting Procedure other than BPSS		☐
Where an alternative Staff Vetting Procedure is required, the procedure is: N/A		

Optional requirements

1.3 Where the Buyer has selected an option in the table below, the Supplier must comply with the requirements of the corresponding Paragraph. Where the Buyer has not selected an option, the corresponding requirement does not apply.

Security Management Plan (see Paragraph 10)	
The Supplier must provide the Buyer with a Security Management Plan detailing how the requirements for the options selected in this table have been met.	☒
Buyer Security Policies (see Paragraph 11)	
The Buyer requires the Supplier to comply with the following policies relating to security management: • N/A	☐
Security testing (see Paragraph 12)	
The Supplier must undertake security testing at least once every Contract Year and remediate any vulnerabilities, where it is technically feasible to do so	☒
Cloud Security Principles (see Paragraph 13)	

The Supplier must assess the Supplier System against the Cloud Security Principles	☐
Record keeping (see Paragraph 14)	
The Supplier must keep records relating to Subcontractors, Sites, Third-Party Tools and third parties	☐
Encryption (see Paragraph 15)	
The Supplier must encrypt Government Data while at rest or in transit	☒
Protective Monitoring System (see Paragraph 16)	
The Supplier must implement an effective Protective Monitoring System	☐
Patching (see Paragraph 17)	
The Supplier must patch vulnerabilities in the Supplier System promptly	☐
Malware protection (see Paragraph 18)	
The Supplier must use appropriate Anti-virus Software	☒
End-User Devices (see Paragraph 19)	
The Supplier must manage End-User Devices appropriately	☒
Vulnerability scanning (see Paragraph 20)	
The Supplier must scan the Supplier System monthly for unpatched vulnerabilities	☐
Access control (see Paragraph 21)	
The Supplier must implement effective access control measures for those accessing Government Data and for Privileged Users	☒
Remote Working (see Paragraph 22)	

The Supplier may allow Supplier Staff to undertake Remote Working once an approved Remote Working Policy is in place	☒
Backup and recovery of Government Data (see Paragraph 23)	
The Supplier must have in place systems for the backup and recovery of Government Data	☐
Return and deletion of Government Data (see Paragraph 24)	
The Supplier must return or delete Government Data when requested by the Buyer	☒
Physical security (see Paragraph 25)	
The Supplier must store Government Data in physically secure locations	☐
Security breaches (see Paragraph 26)	
The Supplier must report any Breach of Security to the Buyer promptly	☒

2 DEFINITIONS

"Anti-virus Software" means software that:

(a) protects the Supplier System from the possible introduction of Malicious Software;

(b) scans for and identifies possible Malicious Software in the Supplier System;

(c) if Malicious Software is detected in the Supplier System, so far as possible:

(i) prevents the harmful effects of the Malicious Software; and

(ii) removes the Malicious Software from the Supplier System;

"BPSS" means the employment controls applied to any individual member of the Supplier Staff that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 7.0, June 2024 (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), as that document is updated from time to time;

"Breach of Security" means the occurrence of:

(a) any unauthorised access to or use of the Services, the Sites, the Supplier System and/or the Government Data;

(b) the loss (physical or otherwise), corruption and/or unauthorised disclosure of any Government Data, including copies of such Government Data; and/or

(c) any part of the Supplier System ceasing to be compliant with the required Certifications;

(d) the installation of Malicious Software in the Supplier System:

(e) any loss of operational efficiency or failure to operate to specification as the result of the installation or operation of Malicious Software in the Supplier System; and

(f) includes any attempt to undertake the activities listed in sub-Paragraph (a) where the Supplier has reasonable grounds to suspect that attempt:

(i) was part of a wider effort to access information and communications technology operated by or on behalf of Central Government Bodies; or

(ii) was undertaken, or directed by, a state other than the United Kingdom;

"Buyer Equipment" means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System;

"Buyer Security Policies" means those securities specified by the Buyer in Paragraph 1.3;

"Buyer System" means the Buyer's information and communications technology system, including any software or Buyer Equipment, owned by the Buyer or leased or licenced to it by a third-party, that:

(a) is used by the Buyer or Supplier in connection with this Contract;

(b) interfaces with the Supplier System; and/or

(c) is necessary for the Buyer to receive the Services.

"Certifications" means one or more of the following certifications (or equivalent):

(a) ISO/IEC 27001:2022 by a UKAS- recognised Certification Body in respect of the Supplier System, or in respect of a wider system of which the Supplier System forms part; and

(b) Cyber Essentials Plus; and/or

(c) Cyber Essentials;

"CHECK Scheme" means the NCSC's scheme under which approved companies can conduct authorised penetration tests of public sector and critical national infrastructure systems and networks;

"CHECK Service Provider" means a company which, under the CHECK Scheme:

(a) has been certified by the NCSC;

(b) holds "Green Light" status; and

(c) is authorised to provide the IT Health Check services required by Paragraph 12.2 (*Security Testing*);

"Cloud Security Principles"	means the NCSC's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles;
"Contract Year"	means: 14.9.1 a period of 12 months commencing on the Start Date; 14.9.2 thereafter a period of 12 months commencing on each anniversary of the Start Date; (a) with the final Contract Year ending on the expiry or termination of the Term;
"CREST Service Provider"	means a company with an information security accreditation of a security operations centre qualification from CREST International;
"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme;
"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the NCSC;
"Developed System"	means the software or system that the Supplier is required to develop under this Contract;
"End-User Device"	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic devices used in the provision of the Services;
"Expected Behaviours"	means the expected behaviours set out and updated from time to time in the Government Security Classification Policy, currently found at paragraphs 12

	to 16 and in the table below paragraph 16 of https://www.gov.uk/government/publications/government-security-classifications/guidance-11-working-at-official-html;
“Government Data”	Means any: . (a) data, texts, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; (b) Personal Data for which the Buyer is a, or the, Data Controller; or (c) any meta-data relating to categories of data referred to in Paragraphs (a) or (b); that is: (d) supplied to the Supplier by or on behalf of the Buyer; or (e) that the Supplier is required to generate, Process, Handle, store or transmit under this Contract;
"Government Security Classification Policy"	means the policy, as updated from time to time, establishing an administrative system to protect information assets appropriately against prevalent threats, including classification tiers, protective security controls and baseline behaviours, the current version of which is found at https://www.gov.uk/government/publications/government-security-classifications;
"Handle"	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data;
“IT Health Check”	means the security testing of the Supplier System;

"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations;
"NCSC"	means the National Cyber Security Centre, or any successor body performing the functions of the National Cyber Security Centre;
"NCSC Device Guidance"	means the NCSC's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance;
"Privileged User"	means a user with system administration access to the Supplier System, or substantially similar access privileges;
"Prohibition Notice"	means the meaning given to that term by Paragraph 5.4.
"Protective Monitoring System"	has the meaning given to that term by Paragraph 16.1;
"Relevant Conviction"	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences) or any other offences relevant to Services as the Buyer may specify;
"Remote Location"	means [**insert** the relevant Supplier Staff's permanent home address authorised by the Supplier or Sub-contractor (as applicable) for Remote Working OR a location other than a Supplier's or a Sub-contractor's Site];
"Remote Working"	means the provision or management of the Services by Supplier Staff from a location other than a Supplier's or a Sub-contractor's Site;
"Remote Working Policy"	the policy prepared and approved under Paragraph 22 under which Supplier Staff are permitted to undertake Remote Working;
"Security Controls"	means the security controls set out and updated from time to time in the Government Security Classification Policy, currently found at Paragraph 12 of

https://www.gov.uk/government/publications/government-security-classifications/guidance-15-considerations-for-security-advisors-html;

"Sites" means any premises (including the Buyer's Premises, the Supplier's premises or third party premises):

(a) from, to or at which:

(i) the Services are (or are to be) provided; or

(ii) the Supplier manages, organises or otherwise directs the provision or the use of the Services; or

(b) where:

(i) any part of the Supplier System is situated; or

(ii) any physical interface with the Buyer System takes place;

"Staff Vetting Procedure" means the procedure for vetting Supplier Staff set out in Paragraph 6;

"Subcontractor Staff" means:

(a) any individual engaged, directly or indirectly, or employed, by any Subcontractor; and

(b) engaged in or likely to be engaged in:

(i) the performance or management of the Services; or

(ii) the provision of facilities or services that are necessary for the provision of the Services;

"Supplier System" means

(a) any:

(i) information assets,

(ii) IT systems,

(iii) IT services; or

(iv) Sites,

that the Supplier or any Subcontractor will use to Handle, or support the Handling of, Government Data and provide, or support the provision of, the Services; and

(b) the associated information management system, including all relevant:

(i) organisational structure diagrams;

(ii) controls;

(iii) policies;

(iv) practices;

(v) procedures;

(vi) processes; and

(vii) resources;

"Third-party Tool"	means any software used by the Supplier by which the Government Data is accessed, analysed or modified, or some form of operation is performed on it;
"UKAS-recognised Certification Body"	means: (a) an organisation accredited by UKAS to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022; or (b) an organisation accredited to provide certification of ISO/IEC27001:2013 and/or ISO/IEC27001:2022 by a body with the equivalent functions as UKAS in a state with which the UK has a mutual

recognition agreement recognising the technical equivalence of accredited conformity assessment.

Part One: Core Requirements

3 HANDLING GOVERNMENT DATA

3.1 The Supplier acknowledges that it:

(a) must only Handle Government Data that is classified as OFFICIAL; and

(b) must not Handle Government Data that is classified as SECRET or TOP SECRET.

3.2 The Supplier must:

(a) not alter the classification of any Government Data.

(b) if it becomes aware that it has Handled any Government Data classified as SECRET or TOP SECRET the Supplier must:

i. immediately inform the Buyer; and

ii. follow any instructions from the Buyer concerning the Government Data.

3.3 The Supplier must, and must ensure that Sub-contractors and Supplier Staff, when Handling Government Data, comply with:

(a) the Expected Behaviours; and

(b) the Security Controls.

4 CERTIFICATION REQUIREMENTS

4.1 Where the Buyer has not specified Certifications under Paragraph 1, the Supplier must ensure that it and any Subcontractors that Handle Government Data are certified as compliant with Cyber Essentials (or equivalent).

4.2 Where the Buyer has specified Certifications under Paragraph 1, the Supplier must ensure that both:

(a) it; and

(b) any Subcontractor that Processes Government Data,

are certified as compliant with the Certifications specified by the Buyer in Paragraph 1 (or equivalent certifications):

4.3 The Supplier must ensure that the specified Certifications (or their equivalent) are in place for it and any relevant Subcontractor:

(a) before the Supplier or any Subcontractor Handles Government Data; and

(b) throughout the Term.

5 LOCATION

5.1 Where the Buyer has not specified any locations or territories in Paragraph 1, the Supplier must not, and ensure that Subcontractors do not store, access or Handle Government Data outside:

(a) the United Kingdom; or

(b) a location permitted by and in accordance with any regulations for the time being in force made under section 17A of the Data Protection Act 2018 (adequacy decisions by the Secretary of State).

5.2 Where the Buyer has specified locations or territories in Paragraph 1, the Supplier must, and ensure that all Subcontractors, at all times store, access or Handle Government Data only in or from the geographic areas specified by the Buyer.

5.3 The Supplier must, and must ensure that its Subcontractors store, access or Handle Government Data in a facility operated by an entity where:

(a) the entity has entered into a binding agreement with the Supplier or Subcontractor (as applicable);(b) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Subcontractors in this Annex;

(c) the Supplier or Subcontractor has taken reasonable steps to assure itself that:

(i) the entity complies with the binding agreement; and

(ii) the Subcontractor's system has in place appropriate technical and organisational measures to ensure that the Subcontractor will store, access, manage and/or Process the Government Data as required by this Annex;

5.3.1 the Buyer has not given the Supplier a Prohibition Notice under Paragraph 5.4.

5.4 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Subcontractors must not undertake or permit to be undertaken the storage, accessing or Processing of Government Data in one or more countries or territories (a "**Prohibition Notice**").

5.5 Where the Supplier must and must ensure Subcontractors comply with the requirements of a Prohibition Notice within 40 Working Days of the date of the notice.

6 STAFF VETTING

6.1 The Supplier must not allow Supplier Staff, and must ensure that Subcontractors do not allow Subcontractor Staff, to access or Handle Government Data, if that person:

(a) has not completed the Staff Vetting Procedure; or

(b) where no Staff Vetting Procedure is specified in the Order Form:

i. has not undergone the checks required for the BPSS to verify:

A. the individual's identity;

B. where that individual will work in the United Kingdom, the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom; and

C. the individual's previous employment history; and

D. that the individual has no Relevant Convictions; and

ii. national security vetting clearance to the level specified by the Authority for such individuals or such roles as the Authority may specify.

6.2 Where the Supplier considers it cannot ensure that a Sub-contractor will undertake the relevant security checks on any Sub-contractor Staff, it must:

(a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Buyer;

(b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected Sub-contractor staff will perform as the Buyer reasonably requires; and

(c) comply, at the Supplier's cost, with all directions the Buyer may provide concerning the vetting of the affected Sub-contractor Staff and the management of the Sub-contract.

7 SUPPLIER ASSURANCE LETTER

7.1 The Supplier must, no later than the last day of each Contract Year, provide to the Buyer a letter from its [**insert** chief technology officer] (or equivalent officer) confirming that, having made due and careful enquiry:

(a) the Supplier has in the previous year carried out all tests and has in place all procedures required in relation to security matters required by this Contract;

(b) it has fully complied with all requirements of this Annex; and

(c) all Subcontractors have complied with the requirements of this Annex with which the Supplier is required to ensure they comply;

(d) the Supplier considers that its security and risk mitigation procedures remain effective.

8 ASSURANCE

8.1 The Supplier must provide such information and documents as the Buyer may request in order to demonstrate the Supplier's and any Subcontractors' compliance with this Annex.

8.2 The Supplier must provide that information and those documents:

(a) at no cost to the Buyer;

(b) within 10 Working Days of a request by the Buyer;

(a) except in the case of original document, in the format and with the content and information required by the Buyer; and

(b) in the case of original document, as a full, unedited and unredacted copy.

9 USE OF SUBCONTRACTORS AND THIRD PARTIES

9.1 The Supplier must ensure that Subcontractors and any other third parties that store, have access to or Handle Government Data comply with the requirements of this Annex.

Part Two: Additional Requirements

10 SECURITY MANAGEMENT PLAN

10.1 This Paragraph 10 applies only where the Buyer has selected this option in Paragraph 1.3.

Preparation of Security Management Plan

10.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Annex and the Contract in order to ensure the security of the Supplier solution and the Buyer data.

10.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Contract, the Security Management Plan, which must include a description of how all the options selected in this Annex are being met along with evidence of the required certifications for the Supplier and any Subcontractors specified in Paragraph 3.

Approval of Security Management Plan

10.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

(a) an information security approval statement, which shall confirm that the Supplier may operate the service and process Buyer data; or

(b) a rejection notice, which shall set out the Buyer's reasons for rejection the Security Management Plan.

10.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within 10 Working Days of the date of the rejection, or such other period agreed with the Buyer.

10.6 The process set out in Paragraph 10.5 shall be repeated until such time as the Authority issues a Risk Management Approval Statement to the Supplier or terminates this Contract.

10.7 The rejection by the Buyer of a second revised Security Management Plan is a material Default of this Contract.

Updating Security Management Plan

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

Monitoring

10.9 The Supplier shall notify the Buyer within 2 Working Days after becoming aware of:

(a) a significant change to the components or architecture of the Supplier System;

(b) a new risk to the components or architecture of the Supplier System;

(c) a vulnerability to the components or architecture of the Supplier System using an industry standard vulnerability scoring mechanism;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

(g) a proposal to change any of the Sites from which any part of the Services are provided; and/or

(h) an ISO27001 audit report produced in connection with the Certification indicates significant concerns.

10.10 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 Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

11 BUYER SECURITY POLICIES

11.1 The Supplier must comply, when it provides the Services and operates and manages the Supplier System, with all Buyer Security Policies identified in the relevant option in Paragraph 1.3.

11.2 If there is an inconsistency between the Buyer Security Policies and the requirement of this Annex, then the requirements of this Annex will prevail to the extent of that inconsistency.

12 SECURITY TESTING

12.1 The Supplier must:

(a) before Handling Government Data;

(b) at least once during each Contract Year; and

undertake the following activities:

(c) conduct security testing of the Supplier System (an "**IT Health Check**") in accordance with Paragraph 12.2; and

(d) implement any findings, and remedy any vulnerabilities identified by the IT Health Check in accordance with Paragraph 12.3.

12.2 In arranging an IT Health Check, the Supplier must:

(a) use only a CHECK Service Provider or CREST Service Provider to perform the IT Health Check;

(b) design and plan for the IT Health Check so as to minimise the impact of the IT Health Check on the Supplier System and the delivery of the Services;

(c) ensure that the scope of the IT Health Check encompasses the components of the Supplier System used to access, store, Process or manage Government Data; and

(d) ensure that the IT Health Check provides for effective penetration testing of the Supplier System.

12.3 The Supplier treat any vulnerabilities as follows:

(a) the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

i. if it is technically feasible to do so, within 5 Working Days of becoming aware of the vulnerability and its classification; or

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3i, then as soon as

reasonably practicable after becoming aware of the vulnerability and its classification;

(b) the Supplier must remedy any vulnerabilities classified as high in the IT Health Check report:

i. if it is technically feasible to do so, within 1 month of becoming aware of the vulnerability and its classification; or

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3(b)(i), then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

(c) the Supplier must remedy any vulnerabilities classified as medium in the IT Heath Check report:

iii. if it is technically feasible to do so, within 3 months of becoming aware of the vulnerability and its classification; or

iv. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 12.3iii, then as soon as reasonably practicable after becoming aware of the vulnerability and its classification;

12.3.2 where it is not technically feasible to remedy the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

13 CLOUD SECURITY PRINCIPLES

13.1 The Supplier must ensure that the Supplier System complies with the Cloud Security Principles.

13.2 The Supplier must assess the Supplier System against the Cloud Security Principles to assure itself that it complies with Paragraph 13.1:

13.2.1 before Handling Government Data;

13.2.2 at least once each Contract Year; and

13.2.3 when required by the Buyer.

13.3 Where the Cloud Security Principles provide for various options, the Supplier must document the option it has chosen to implement and its reasons for doing do.

13.4 The Supplier must:

(a) keep records of any assessment that it makes under Paragraph 13.2; and

(b) provide copies of those records to the Buyer within 10 Working Days of any request by the Buyer.

14 INFORMATION ABOUT SUBCONTRACTORS, SITES AND THIRD-PARTY TOOLS

14.1 The Supplier must keep the following records:

(a) for Subcontractors or third parties that store, have access to or Handle Government Data:

i. the Subcontractor or third party's name:

A. legal name;

B. trading name (if any); and

C. registration details (where the Subcontractor is not an individual), including:

(A) country of registration;

(B) registration number (if applicable); and

(C) registered address;

D. the Certifications held by the Subcontractor or third party;

E. the Sites used by the Subcontractor or third party;

F. the Services provided or activities undertaken by the Subcontractor or third party;

G. the access the Subcontractor or third party has to the Supplier System;

H. the Government Data Handled by the Subcontractor or third party; and

I. the measures the Subcontractor or third party has in place to comply with the requirements of this Annex;

ii. for Sites from or at which Government Data is accessed or Handled:

A. the location of the Site;

B. the operator of the Site, including the operator's:

(A) legal name;

(B) trading name (if any); and

(C) registration details (where the Subcontractor is not an individual);

C. the Certifications that apply to the Site;

D. the Government Data stored at, or Handled from, the site; and

iii. for Third-party Tools:

A. the name of the Third-Party Tool;

iv. the nature of the activity or operation performed by the Third-Party Tool on the Government Data; and

A. in respect of the entity providing the Third-Party Tool, its:

(A) full legal name;

(B) trading name (if any)

(C) country of registration;

(D) registration number (if applicable); and

(E) registered address.

14.2 The Supplier must update the records it keeps in accordance with Paragraph 14.1:

(a) at least four times each Contract Year;

(b) whenever a Subcontractor, third party that accesses or Handles Government Data, Third-party Tool or Site changes; or

(c) whenever required to go so by the Buyer.

14.3 The Supplier must provide copies of the records it keeps in accordance with Paragraph 14.1 to the Buyer within 10 Working Days of any request by the Buyer.

15 ENCRYPTION

15.1 The Supplier must, and must ensure that all Subcontractors, encrypt Government Data:

15.1.1 when stored at any time when no operation is being performed on it, including when stored on any portable storage media; and

15.1.2 when transmitted.

16 PROTECTIVE MONITORING SYSTEM

16.1 The Supplier must, and must ensure that Subcontractors, implement an effective system of monitoring and reports, analysing access to and use of the Supplier System and the Government Data to:

(a) identify and prevent any potential Breach of Security;

(b) respond effectively and in a timely manner to any Breach of Security that does;

(c) identify and implement changes to the Supplier System to prevent future any Breach of Security; and

(d) help detect and prevent any potential criminal offence relating to fraud, bribery or corruption using the Supplier System,

(the "Protective Monitoring System").

16.2 The Protective Monitoring System must provide for:

(a) event logs and audit records of access to the Supplier System; and

(b) regular reports and alerts to identify:

i. changing access trends;

ii. unusual usage patterns; or

iii. the access of greater than usual volumes of Government Data; and

iv. the detection and prevention of any attack on the Supplier System using common cyber-attack techniques.

17 PATCHING

17.1 The Supplier must, and must ensure that Subcontractors, treat any public releases of patches for vulnerabilities as follows:

(a) the Supplier must patch any vulnerabilities classified as "**critical**":

i. if it is technically feasible to do so, within 5 Working Days of the public release; or

ii. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1(a)(i), then as soon as reasonably practicable after the public release;

(b) the Supplier must patch any vulnerabilities classified as "**important**":

i. if it is technically feasible to do so, within 1 month of the public release; or

ii. if it is technical feasible to patch the vulnerability but not technically feasible to do so as required by Paragraph 17.1i, then as soon as reasonably practicable after the public release;

(c) the Supplier must remedy any vulnerabilities classified as "**other**" in the public release:

i. if it is technically feasible to do so, within 2 months of the public release; or

ii. if it is technical feasible to remedy the vulnerability but not technically feasible to do so as required by Paragraph 17.1(c)(i), then as soon as reasonably practicable after the public release;

(d) where it is not technically feasible to patch the vulnerability, the Supplier must implement appropriate technical and organisational measures to mitigate the risk posed by the vulnerability.

18 MALWARE PROTECTION

18.1 The Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier System.

18.2 The Supplier must ensure that such Anti-virus Software:

(a) prevents the installation of the most common forms of Malicious Software in the Supplier System;

(b) performs regular scans of the Supplier System to check for Malicious Software; and

(c) where Malicious Software has been introduced into the Supplier System, so far as practicable

i. prevents the harmful effects from the Malicious Software; and

ii. removes the Malicious Software from the Supplier System.

19 END-USER DEVICES

19.1 The Supplier must, and must ensure that all Subcontractors, manage all End-User Devices on which Government Data is stored or Handled in accordance with the following requirements:

(a) the operating system and any applications that store, Handle or have access to Government Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Government Data must be encrypted using a suitable encryption tool;

(d) the End-User Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-User Device is inactive;

(e) the End-User Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Government Data to ensure the security of that Government Data;

(f) the Supplier or Subcontractor, as applicable, can, without physical access to the End-User Device, remove or make inaccessible all Government Data stored on the device and prevent any user or group of users from accessing the device;

(g) all End-User Devices are within the scope of any required Certification.

19.2 The Supplier must comply, and ensure that all Subcontractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Contract.

20 VULNERABILITY SCANNING

20.1 The Supplier must:

(a) scan the Supplier System at least once every month to identify any unpatched vulnerabilities; and

(b) if the scan identifies any unpatched vulnerabilities, ensure they are patched in accordance with Paragraph 17.

21 ACCESS CONTROL

21.1 The Supplier must, and must ensure that all Subcontractors:

(a) identify and authenticate all persons who access the Supplier System before they do so;

(b) require multi-factor authentication for all user accounts that have access to Government Data or that are Privileged Users;

(c) allow access only to those parts of the Supplier System and Sites that those persons require;

(d) maintain records detailing each person's access to the Supplier System.

21.2 The Supplier must ensure, and must ensure that all Subcontractors ensure, that the user accounts for Privileged Users of the Supplier System:

(a) are allocated to a single, individual user;

(b) are accessible only from dedicated End-User Devices;

(c) are configured so that those accounts can only be used for system administration tasks;

(d) require passwords with high complexity that are changed regularly;

(e) automatically log the user out of the Supplier System after a period of time that is proportionate to the risk environment during which the account is inactive; and

(f) are:

i. restricted to a single role or small number of roles;

ii. time limited; and

iii. restrict the Privileged User's access to the internet.

22 REMOTE WORKING

22.1 The Supplier must ensure, and ensure that Sub-contractors ensure, that:

(a) unless in writing by the Authority, Privileged Users do not undertake Remote Working;

(b) where the Authority permits Remote Working by Privileged Users, the Supplier ensures, and ensures that Sub-contractors ensure, that such Remote Working takes place only in accordance with any conditions imposed by the Authority.

22.2 Where the Supplier or a Sub-contractor wishes to permit Supplier Staff to undertake Remote Working, it must:

(a) prepare and have approved by the Buyer in the Remote Working Policy in accordance with this Paragraph;

(b) undertake and, where applicable, ensure that any relevant Sub-contractors undertake, all steps required by the Remote Working Policy;

(c) ensure that Supplier Staff undertake Remote Working only in accordance with the Remote Working Policy;

(d) may not permit any Supplier Staff or the Supplier or any Sub-contractor to undertake Remote Working until the Remote Working Policy is approved by the Buyer.

22.3 The Remote Working Policy must include or make provision for the following matters:

(a) restricting or prohibiting Supplier Staff from printing documents in any Remote Location;

(b) restricting or prohibiting Supplier Staff from downloading any Government Data to any End-User Device other than an End User Device that:

i. is provided by the Supplier or Sub-contractor (as appropriate); and

ii. complies with the requirements set out in Paragraph 3 (*End-User Devices*);

(c) ensuring that Supplier Staff comply with the Expected Behaviours (so far as they are applicable);

(d) giving effect to the Security Controls (so far as they are applicable); and

(e) for each different category of Supplier Staff subject to the proposed Remote Working Policy:

i. the types and volumes of Government Data that the Supplier Staff can Handle in a Remote Location and the Handling that those Supplier Staff will undertake;

ii. any identified security risks arising from the proposed Handling in a Remote Location;

iii. the mitigations, controls and security measures the Supplier or Sub-contractor (as applicable) will implement to mitigate the identified risks; and

iv. the business rules with which the Supplier Staff must comply.

22.4 The Supplier may submit a proposed Remote Working Policy for consideration at any time.

23 BACKUP AND RECOVERY OF GOVERNMENT DATA

23.1 The Supplier must ensure that the Supplier System:

(a) backs up and allows for the recovery of Government Data to achieve the recovery point and recovery time objectives specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified; and

(b) retains backups of the Government Data for the period specified by the Buyer, or in accordance with Good Industry Practice where the Buyer has not specified.

23.2 The Supplier must ensure the Supplier System:

(a) uses backup location for Government Data that are physically and logically separate from the rest of the Supplier System;

(b) the backup system monitors backups of Government Data to:

i. identify any backup failure; and

ii. confirm the integrity of the Government Data backed up;

(c) any backup failure is remedied properly;

(d) the backup system monitors backups of Government Data to:

i. identify any recovery failure; and

ii. confirm the integrity of Government Data recovered; and

(e) any recovery failure is promptly remedied.

24 RETURN AND DELETION OF GOVERNMENT DATA

24.1 Subject to Paragraph 24.2, when requested to do so by the Buyer, the Supplier must, and must ensure that all Subcontractors:

(a) securely erase any or all Government Data held by the Supplier or Subcontractor using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted; or

(b) provide the Buyer with copies of any or all Government Data held by the Supplier or Subcontractor using the method specified by the Buyer.

24.2 Paragraph 24.1 does not apply to Government Data:

(a) that is Personal Data in respect of which the Supplier is a Controller;

(b) to which the Supplier has rights to Handle independently from this Contract; or

(c) in respect of which, the Supplier is under an obligation imposed by Law to retain.

24.3 The Supplier must, and must ensure that all Sub-contractors, provide the Buyer with copies of any or all Buyer Data held by the Supplier or Sub-contractor:

(a) when requested to do so by the Buyer; and

(b) using the method specified by the Buyer.

25 PHYSICAL SECURITY

25.1 The Supplier must, and must ensure that Subcontractors, store the Government Data on servers housed in physically secure locations.

26 BREACH OF SECURITY

26.1 If the Supplier becomes aware of a Breach of Security that impacts or has the potential to impact the Government Data, it shall:

(a) notify the Buyer as soon as reasonably practicable after becoming aware of the breach, and in any event within [24] hours;

(b) provide such assistance to the Buyer as the Buyer requires until the Breach of Security and any impacts or potential impacts on the Buyer are resolved to the Buyer's satisfaction;

(c) where the Law requires the Buyer to report a Breach of Security to the appropriate regulator provide such information and other input as the Buyer requires within the timescales specified by the Buyer.