

CALL OFF SCHEDULE 13: SECURITY REQUIREMENTS

PART A – SHORT FORM SECURITY REQUIREMENTS

Not used

PART B – LONG FORM SECURITY REQUIREMENTS

1 DEFINITIONS

In this Part B (Long Form Security Requirements) of this Call Off Schedule 13 (Security Requirements), the following definitions shall apply:

"CHECK Scheme"	means the term for the National Cyber Security Centre (NCSC) approved penetration test companies and the methodology used to conduct a penetration test. More information can be found in the below hyperlink: https://www.ncsc.gov.uk/information/check-penetration-testing ;
"Baseline Security Requirements"	the baseline security requirements set out in Annex 1 of this Part B of Call Off Schedule 13 (Security Requirements);
"ISMS"	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 Part B of Call Off Schedule 13 (Security Requirements);
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Part B of Call Off Schedule 13 (Security Requirements), a draft of which has been provided by the Supplier to the Buyer and is set out in the Order Form and as updated from time to time; and
"Security Tests"	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 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.
- 2.2 The Parties shall each appoint a security representative to be responsible for security. As at the Commencement Date, the initial security representatives of the Parties are:

For the Buyer:

Name:
Role:
Email:



For the Supplier:

Name:



Role:
Email:
Tel:



- 2.3 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.
- 2.4 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.
- 2.5 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Buyer Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Buyer Data remains under the effective control of the Supplier at all times.
- 2.6 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.
- 2.7 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 co-operation 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 Commencement 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 Services, 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 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 Services and all processes associated with the provision of the associated with the delivery of the Services, 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 IT, information and data (including the Buyer's Confidential Information and the Buyer 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) 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 (<https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>);
 - (f) takes account of guidance issued by the National Protective Security Authority (NPSA) (<https://www.npsa.gov.uk>);
 - (g) complies with HMG GovS007: Security Functional Standard (<https://www.gov.uk/government/publications/government-functional-standard-govs-007-security>);
 - (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 3.12;
- 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 Services 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 Part B of Call Off Schedule 13 (Security Requirements). 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 3.7 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 Part B of Call Off Schedule 13 (Security Requirements).

4 SECURITY MANAGEMENT PLAN

- 4.1 Within twenty (20) Working Days after the Commencement 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 the Order Form;
 - 4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with Paragraph 3.4.5, the Security Policy;
 - 4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Part B of Call Off Schedule 13 (Security Requirements) is complied with by the Supplier;
 - 4.2.4 detail the process for managing any security risks from Sub-Contractors 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 IT, Information and data (including the Buyer's Confidential Information and the Buyer Data) and any system that could directly or indirectly have an impact on that information, data and/or the Services;
 - 4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, 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 IT, Information and data

(including the Buyer's Confidential Information and the Buyer 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 Services;

- 4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Part B of Call Off Schedule 13 (Security Requirements) (including the requirements set out in Paragraph 3.4);
 - 4.2.7 demonstrate that the Supplier's approach to delivery of the Services has minimised the Buyer and Supplier effort required to comply with this Part B of Call Off Schedule 13 (Security Requirements) 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 Commencement 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 of this Contract 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 Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Part B of Call Off Schedule 13 (Security Requirements).
- 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 Part B of Call Off Schedule 13 (Security Requirements). 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 Part B of Call Off Schedule 13 (Security Requirements).

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 Services and/or associated processes;
- 5.1.3 any new perceived or changed security threats;
- 5.1.4 where required in accordance with Paragraph 3.5.4, 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 the Baseline Security Requirements or otherwise) shall be subject to the Change Control 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 Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control 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:

- 6.1.1 carried out by CREST (Council of Registered Ethical Security Testers) or CHECK Scheme registered professionals; and

- 6.1.2 designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer.
- 6.2 Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
- 6.3 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.
- 6.4 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 Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.
- 6.5 Where any Security Test carried out pursuant to Paragraphs 6.1.1 or 6.1.2 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 Baseline Security Requirements or the requirements of this Part B of Call Off Schedule 13 (Security Requirements), the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.
- 6.6 If any repeat Security Test carried out pursuant to Paragraph 6.2 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.
- 6.7 If a 'High' vulnerability (as defined by Paragraph 9.2.1) or 'Critical' vulnerability (as defined by Paragraph 9.2.2) is identified during any Security Test, then the Supplier shall notify the Buyer immediately of such vulnerability, and shall then provide the Buyer with the full results of the Security Test in accordance with Paragraph 6.3. Where the full test results include information relating to a third party which could reasonably be determined as being commercially sensitive and the Supplier is unable for contractual reasons, and having used reasonable endeavours to obtain permission from the relevant third party, to disclose such information to the Buyer, the Supplier may redact such third party commercially sensitive information contained within the full results of the Security Test, provided that the Supplier shall not redact information which would make it impossible for the Buyer to reasonably understand the results of the Security Test.

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 practices 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 practices 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 7.1, the Supplier is found to be non-compliant with the principles and practices 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 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 Services so as to meet the relevant Service Levels, 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 National Cyber Security Centre) 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

8.2.2 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 Part B of Call Off Schedule 13 (Security Requirements), 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 IT 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 the Supplier COTS Software and/or Third Party 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 7 days of release, 'Important' within 14 days of release and all 'Other' within 60 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 a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Services Specification and Implementation Plan (if applicable) shall include provisions for major version upgrades of all Supplier COTS Software and/or Third Party 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 Supplier COTS Software and/or Third Party 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 IT Environment (to the extent that the IT 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 IT Environment by actively monitoring the threat landscape during the Contract Period;
 - 9.5.4 using a SCAP compliant vulnerability scanning tool (<https://csrc.nist.gov/projects/scap-validation-program/validated-products-and-modules>), pro-actively scan the IT Environment (to the extent that the IT 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 3.4.5;
 - 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 IT Environment (to the extent that the IT 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 IT 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 IT 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 IT 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.

ANNEX 1 TO PART B – 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 Buyer 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 Buyer 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 Buyer Data will be subject to at all times.
- 3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with the Change Control Procedure.
- 3.3 The Supplier shall:
- 3.3.1 provide the Buyer with all Buyer Data on demand in an agreed open format;
 - 3.3.2 have documented processes to guarantee availability of Buyer Data in the event of the Supplier ceasing to trade;
 - 3.3.3 securely destroy all media that has held Buyer Data at the end of life of that media in line with NCSC Data Sanitisation guidance (<https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>) and Good Industry Practice;
 - 3.3.4 securely erase any or all Buyer Data held by the Supplier when requested to do so by the Buyer; and
 - 3.3.5 without prejudice to Clauses 26.4 to 26.10 (inclusive), implement all appropriate technical and organisational measures to detect any
 - 3.3.6 loss, corruption or degradation of the Buyer Data and if at any time the Supplier suspects or has reason to believe that the Buyer Data is corrupted, lost or sufficiently

degraded in any way for any reason, then the Supplier shall notify the Buyer immediately and inform the Buyer of the remedial action the Supplier proposes to take including to restore such Buyer Data to the state it would have been in had it not been lost or corrupted.

- 3.4 The Supplier shall not and shall ensure that no third party appointed by the Supplier to assist in the provisions of the Services shall, dispose, re-assign or re-use any equipment or any electronic, magnetic or other medium which is or has been used to store Buyer Data or any other data that has been generated, obtained, held, used or stored for the purposes of this Contract without ensuring that such data has been entirely removed, or otherwise obliterated.

4. ENSURING SECURE COMMUNICATIONS

- 4.1 The Buyer requires that any Buyer 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, 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 Buyer Data.
- 5.2 When designing and configuring the IT Environment (to the extent that the IT 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 IT Environment (to the extent that the IT Environment is within the control of the Supplier).

6. SECURITY OF SUPPLIER PERSONNEL

- 6.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity, employment history (covering the last three (3) years as a minimum), unspent criminal convictions and right to work.
- 6.2 The Supplier shall agree on a case by case basis Supplier Personnel roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Buyer Data.
- 6.3 The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Buyer Data except where agreed with the Buyer in writing.
- 6.4 All Supplier Personnel that have the ability to access Buyer Data or systems holding Buyer 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 Sub-Contractors grants increased IT privileges or access rights to Supplier Personnel, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When Supplier Personnel no longer need elevated privileges or leave the organisation, their access rights shall be revoked within twenty four (24) hours.

7. RESTRICTING AND MONITORING ACCESS

- 7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the IT Environment (to the extent that the IT 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 IT 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 IT Environment (to the extent that the IT Environment is within the control of the Supplier). To the extent the design of the Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.
 - 8.1.2 Security events generated in the IT Environment (to the extent that the IT 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 IT Environment.
- 8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least two (2) years.