OFFICIAL

APPLICATIONS AND HOSTING SERVICES

CALL OFF SCHEDULE 8

SECURITY

1 OVERVIEW

1.1 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure an effective approach to security under which the specific requirements of this Call Off Contract will be met. This approach should ensure compliance with the Customer's obligations in relation to the Security Policy Framework and all subordinate best practice policies and guidance and also support wider security requirements such as those required for PSN connectivity.

2 INTRODUCTION

2.1 The Parties shall each appoint named individuals to be responsible for security in connection with this Call Off Contract. The initial member of the Implementation Governance Board (or other implementation or transition mechanism) appointed by the Supplier for such purpose shall be the person named as such in Call Off Schedule 4 (Implementation Plan, Customer Responsibilities and Key Personnel) Part E and the provisions of Clause 26 (Key Personnel) of the Call Off Contract shall apply in relation to such person.

2.2 The Customer shall articulate its high level security requirements driven by the sensitivity of Customer Data which shall be identified at the Government Security Classification of 'OFFICIAL' so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs. It should be noted that casework data is identified as 'OFFICIAL-SENSITIVE and the Supplier shall apply any necessary additional controls that are required to handle.

2.3 Each Party shall provide a reasonable level of access to any members of its Customer Personnel or Supplier Personnel (as applicable) and to any premises as required for the purposes of designing, implementing and managing security.

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

2.5 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 evidence of this (e.g. appropriately scoped ISO27001 registration/certificate) as soon as practicable to the Customer.

2.6 The Customer and the Supplier acknowledge that a compromise of either the Supplier or the Customer's security provisions represents an unacceptable risk to the Customer, requiring immediate communication and co-operation between the Parties.

3 ISMS

3.1 By the date specified in the Implementation Plan, the Supplier shall develop and submit to the Customer for the Customer's Approval in accordance with Paragraph 3.6 of this Call Off Schedule, an ISMS (Information Security Management System) for the purposes of this Call Off Contract, which:

(a) shall have been tested in accordance with this Call Off Schedule; and

(b) shall comply with the requirements of Paragraphs 3.3 to 3.5 of this Call Off Schedule.

3.2 The Supplier acknowledges that the Customer places great emphasis on the reliability of the Services and 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 ISMS shall:

(a) unless otherwise specified by the Customer in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Customer Premises, the Sites, the Supplier System, the Customer System (to the extent that it is under the control of the Supplier), connectivity to secure services (e.g. PSN) and any IT, information and data (including Sensitive Information and the Customer Data) to the extent used by the Customer or the Supplier in connection with this Call Off Contract;

(b) achieve certification to the extant version of ISO 27001 within a timescale agreed by the Customer and in accordance with Paragraph 7 of this Call Off Schedule;

(c) comply with any other relevant security standard that may be appropriate to the proposed solution or technology arrangement as identified by the Customer from time to time;

(d) at all times provide a level of security which:

(i) is in accordance with Law and this Call Off Contract;
(ii) demonstrates Good Industry Practice;
(iii) complies with extant national security and criminal justice specific obligations and Baseline Security Requirements, ensuring all accreditation and secure connectivity objectives are fulfilled;
(iv) complies with the requirements referred to in Annex 2 of this Call Off Schedule;
(v) addresses issues of incompatibility with the Supplier's own organisational security policies;
(vi) meets any specific security threats of immediate relevance to the Services and/or Customer Data;
(vii) complies with the security requirements as set out in Call Off Schedule 2 (Services); and
(viii) comply with the Customer security PPPs;

(e) document the security incident management processes and incident response plans and cooperate with the Customer and/or its nominated agent to deliver an integrated incident management process;

(f) 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, prioritisation of security patches, testing of security patches, application of security patches, a process for

Customer Approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy;

(g) 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 Customer in advance of issue of the relevant Security Management Plan); and

(h) be supported by the Supplier's attendance of scheduled and ad-hoc security working group meetings as determined by the Customer.

3.4 All references to standards, guidance and policies set out in Paragraph 3.3 of this Call Off Schedule 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. Where reference is made to the Security Policy Framework, the Supplier shall take account of the range of policy and guidance information that has been drafted by organisations such as Cabinet Office and the National Cyber Security Centre (formerly CESG) to support compliance with this framework.

3.5 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.3 of this Call Off Schedule, the Supplier shall immediately notify the Customer Representative of such inconsistency and the Customer Representative shall, as soon as practicable, notify the Supplier which provision the Supplier shall comply with.

3.6 If the ISMS submitted to the Customer pursuant to Paragraph 3.1 of this Call Off Schedule is Approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Call Off Schedule. If the ISMS submitted to the Customer pursuant to Paragraph 3.1 of this Call Off Schedule is not Approved by the Customer, the Supplier shall amend it within 10 Working Days of a notice of non-Approval from the Customer and re-submit it to the Customer for Approval. Any related technical work to be implemented by the Supplier shall be agreed in accordance with Call Off Schedule 14 (Change Control Procedure). 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 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Customer. If the Customer 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 Customer 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 3.3 to 3.5 of this Call Off Schedule shall be deemed to be reasonable.

3.7 Approval by the Customer of the ISMS pursuant to Paragraph 3.6 of this Call Off Schedule or of any change to the ISMS shall not relieve the Supplier of its obligations under this Call Off Schedule.

4 SECURITY MANAGEMENT PLAN

4.1 Within 40 Working Days after the Call Off Commencement Date, the Supplier shall prepare and submit to the Customer for Approval in accordance with Paragraph 4.3

of this Call Off Schedule a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2 of this Call Off Schedule.

4.2 The Security Management Plan shall:

(a) be based on the initial Security Management Plan that will have been provided as part of the original Tender response;

(b) comply with any Baseline Security Requirements, and the requirements referred to in Annex 2 of this Call Off Schedule, and support compliance with the organisational Security Policy obligations;

(c) identify the necessary delegated organisational roles defined for those responsible for ensuring this Call Off Schedule is complied with by the Supplier;

(d) detail the process for managing any security risks from Sub-Contractors and third parties authorised by the Customer with access to the Services, processes associated with the delivery of the Services, the Customer Premises, the Sites, the Supplier System, the Customer System (to extent that it is under the control of the Supplier) and any IT, information and data (including Sensitive Information and the Customer Data) and any system that could directly or indirectly have an impact on that information, data and/or the Services;

(e) unless otherwise specified by the Customer in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Customer Premises, the Sites, Supplier's Sites, the Supplier System, the Customer System (to the extent that it is under the control of the Supplier) and any IT, information and data (including Sensitive Information and the Customer Data) to the extent used by the Customer or the Supplier in connection with this Call Off Contract or in connection with any system that could directly or indirectly have an impact on that information, data and/or the Services;

(f) 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 Call Off Schedule (including the requirements set out in Paragraph 3.3 of this Call Off Schedule);

(g) demonstrate that the Supplier Solution has minimised the Customer and Supplier effort required to comply with this Call Off Schedule through consideration of available, appropriate and practicable pan-government accredited or pre-assured services;

(h) set out the plans for transiting all security arrangements and responsibilities from those in place at the Call Off Commencement Date to those incorporated in the ISMS by the date set out in Call Off Schedule 4 (Implementation Plan, Customer Responsibilities and Key

Personnel) for the Supplier to meet the full obligations of the security requirements set out in Clause 35.7 of the Call Off Contract, Call Off Schedule 2 (Services) and this Call Off Schedule;

(i) set out the scope of the Customer System that is under the control of the Supplier;

(j) be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other Call Off Schedules which cover specific areas included within those standards (e.g. business continuity management/DR); and

(k) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Customer 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 Call Off Schedule.

4.3 If the Security Management Plan submitted to the Customer pursuant to Paragraph 4.1 of this Call Off Schedule is Approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Call Off Schedule. If the Security Management Plan is not Approved by the Customer, the Supplier shall amend it within 10 Working Days of a notice of non-Approval from the Customer and re-submit it to the Customer for Approval. Any related technical work to be implemented by the Supplier shall be agreed in accordance with the Change Control Procedure. 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 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Customer. If the Customer 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 Customer pursuant to this Paragraph 4.3 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 of this Call Off Schedule shall be deemed to be reasonable.

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

5 AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN

5.1 The ISMS and 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) on-going ISO 27001 certification requirements;

(c) on-going Customer Accreditation / Assurance Strategy and obligations;

(d) any change or proposed change to the Customer System, Supplier System, the Services and/or associated processes;

(e) any new perceived or changed security threats; and

(f) any reasonable change in requirements requested by the Customer.

5.2 The Supplier shall provide the Customer 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 Customer. The results of the review shall include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS (e.g. corrective actions identified by an external accredited certification body);
(b) updates to the risk assessments;
(c) proposed modifications to respond to events that may impact on the ISMS including the security incident management process, incident response plans and general procedures and controls that affect information security; and
(d) suggested improvements in measuring the effectiveness of controls and improved performance measures and targets (e.g. *x*% reduction in incidents in the next 12 months).

5.3 Subject to Clause 22.2 of the Call Off Terms and Paragraph 5.4 of this Call Off Schedule, 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 of this Call Off Schedule, a Customer request, a Change to Call Off Schedule 2 (Services) or otherwise) shall be subject to the Change Control Procedure detailed in Call Off Schedule 14 (Change Control Procedure) and shall not be implemented until Approved in writing by the Customer.

5.4 The Customer may, where it is reasonable to do so, 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 for the purposes of this Call Off Contract.

6 SECURITY TESTING

6.1 The Supplier shall conduct relevant Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally security testing should be conducted as part of any change that is applied to the technical environment or 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 Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Customer. The Supplier will produce a 'Security Testing Scope' document that will be reviewed and Approved by the Customer to ensure that all relevant service aspects are covered.

6.2 The Customer shall be entitled to send a Representative to witness the conduct of the Security Tests. The Supplier shall provide the Customer with the results of such

tests (in a form Approved by the Customer 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 Customer pursuant to this Call Off Contract, the Customer and/or its authorised representatives shall be entitled, at its own cost, 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 Customer may notify the Supplier of the results of such tests after completion of each such test. Any penetration testing carried out under this Paragraph 6.3 shall only be undertaken by an approved service provider from the then-current NCSC list (https://www.ncsc.gov.uk/scheme/penetration-testing).

6.4 Where any Security Test carried out pursuant to Paragraphs 6.1 or 6.3 of this Call Off Schedule 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 Customer 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 Customer's prior 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 Customer or, otherwise, as soon as reasonably possible. Where the change to the ISMS or Security Management Plan is to address a non-compliance with the Baseline Security Requirements, requirements referred to in Annex 2 of this Call Off Schedule, requirements under the **Customer Accreditation / Assurance Strategy**, secure service connectivity obligations or the requirements of this Call Off Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Customer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 of this Call Off Schedule reveals an actual or potential Breach of Security exploiting the same Root Cause failure, such circumstance shall constitute a material Default for the purposes of this Call Off Contract.

6.6 At its own cost, the Supplier shall carry out penetration testing to check the Supplier's compliance with the ISMS and the Security Management Plan. Such penetrating testing shall only be undertaken by an approved service provider from the then-current NCSC list (https://www.ncsc.gov.uk/scheme/penetration-testing).

7 ISMS COMPLIANCE

7.1 The Customer 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 all Security Policy and system accreditation/assurance objectives including under the **Customer Accreditation / Assurance Strategy**, and the specific security requirements set out or referred to in Call Off Schedule 2 (Services), this Call Off Schedule and/or the Baseline Security Requirements.

7.2 ISO 27001 certification/registration shall be confirmed by an external accredited certification body on an annual basis at the cost of the Supplier.

7.3 If, on the basis of evidence provided by such audits, it is the Customer's reasonable opinion that compliance with identified security principles and practices, the specific security requirements set out or referred to in Call Off Schedule 2 (Services) this Call Off Schedule and/or the Baseline Security Requirements is not being achieved by the Supplier, then the Customer 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 any necessary remedy. If the Supplier does not become compliant within the required time then the Customer shall have the right to obtain an independent audit against these standards in whole or in part.

7.4 If, as a result of any such independent audit as described in Paragraph 7.3 of this Call Off Schedule the Supplier is found to be in material Default of the identified security principles and practices, the specific security requirements set out or referred to in Call Off Schedule 2 (Services), this Call Off Schedule and/or the Baseline Security Requirements then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance shall reimburse the Customer for all reasonable costs incurred by the Customer in the course of the audit.

8 BREACH OF SECURITY AND PERSONAL DATA BREACHES

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 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 of this Call Off Schedule, the Supplier shall:

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

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

(ii) remedy such Breach of Security to the extent possible and protect the integrity of the Service technical environment to the extent within its control against any such Breach of Security or attempted Breach of Security;

(iii) providing that reasonable testing has been undertaken by the Supplier, apply a mitigation against any such Breach of Security or attempted Breach of Security. If the mitigation 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 such period as the Customer, acting reasonably, may specify by written notice to the Supplier;

(iv) prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same Root Cause failure; and

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

(b) as soon as reasonably practicable provide to the Customer 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 Customer.

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 Baseline Security Requirements or security requirements set out or referred to in Call Off Schedule 2 (Services), this Call Off Schedule, or the Breach of Security results from any non-compliance with this Call Off Schedule, then any required change to the ISMS shall be at no cost to the Customer.

8.4 Either Party becoming aware of a Personal Data Breach affecting the other Party's Data Protection responsibilities shall notify the other Party. The Supplier shall ensure that the Customer is notified without undue delay in accordance with the requirements of Paragraph 2 of Annex 3 to Call Off Schedule 15 (Data Protection).

9 VULNERABILITES AND CORRECTIVE ACTION

9.1 The severity of threat vulnerabilities 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:

(a) 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

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

(c) Vulnerability information provided by Oracle on critical patches and security alerts at https://www.oracle.com/technetwork/topics/security/alerts-086861.html

The Supplier shall revise promptly any categorisation that it makes pursuant to this Paragraph 9.1 as requested by the Customer from time to time.

9.2 Subject to Approval from the Customer, the Supplier shall procure the application of security patches (including public release patches) to vulnerabilities categorised as 'Critical' within 4 hours of such Approval, 'Important' within 10 Working Days of Approval and all 'Other' within 40 Working Days of Approval, except where:

(a) the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a Component of the Software 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;

(b) the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the

Customer may (in its absolute discretion) grant the Supplier an extension to such timescales , provided the Supplier had followed and continues to follow the security patch test plan agreed with the Customer;

(c) the Customer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS; or

(d) the relevant information technology vendor recommends the application of security patches to vulnerabilities within a shorter time period in which case the patches will be applied in accordance with the vendor's recommendations.

9.3 The Supplier Solution and the Detailed Implementation Plan shall include provisions for major version upgrades of all Software to be promptly upgraded following release of the latest version in accordance with the provisions of Clause 7.1.4 of the Call Off Terms and Paragraphs 6.2 and 6.3 of Call Off Schedule 9 (Software and Assets), 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:

(a) upgrading such 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

(b) an alternative approach is agreed with the Customer in writing.

9.4 The Supplier shall:

(a) implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent public sector organisation;

(b) ensure that the Service technical environment is monitored in accordance with the requirements of CESG Good Practice Guide 13 – Protective Monitoring for HMG ICT systems (or its successor) to facilitate the detection of anomalous behaviour that would be indicative of system compromise and report to the Customer such behaviour;

(c) ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the Service technical environment by actively monitoring the threat landscape;

(d) pro-actively scan the Service technical environment for vulnerable Components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3 of this Call Off Schedule;

(e) from the date specified in the Security Management Plan (and before the First Operational Services Commencement Date) provide a report to the Customer within 5 Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the Service technical environment (to the extent that such 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;

(f) propose interim mitigation measures to vulnerabilities in the Service technical environment known to be exploitable where a security patch is not immediately available;

(g) remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier Solution and Service technical environment); and

(h) inform the Customer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the Service technical environment and provide initial indications of possible mitigations.

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

9.6 A failure to comply with Paragraph 9.2 shall constitute a material Default, and the Supplier shall comply with the Rectification Plan Process.

10 SYSTEM SAFETY

10.1 The Parties acknowledge that "System Safety" is about *the management of risks related to systems whose anomalous behaviour could affect the physical safety or security of its users or the general public.* It is separate from health and safety which deals more with physical risks associated with the use of equipment or the local environment or infrastructure.

10.2 The Parties agree that System Safety is out of scope and not part of this Call Off Contract. During the Implementation Period the Parties will work together in good faith to discuss a solution for System Safety including the possibility of following the approach previously used under COMPASS.

ANNEX 1
Baseline Security Requirements

Higher Classifications

1. The Supplier shall not handle Customer Data 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 Customer.

End User Computing

2. When Customer Data is held by or is in the control of the Supplier which is accessible by a mobile, removable or physically uncontrolled device such Customer Data must be stored encrypted using a Component of any product or system which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA"). It should be noted that CESG is now referred to as the National Cyber Security Centre. Any references made in this document are relevant to CESG in its new form. If no CESG standard is applicable an assurance strategy will be agreed with the Customer.

3. All Supplier devices accessing Customer Data are expected to meet the set of security requirements set out in the CESG End User Devices Platform 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 Customer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG/NCSC guidance, then this should be agreed in writing on a case by case basis with the Customer. The Parties will work together to agree the detailed compliance in relation to this Paragraph 3 as part of its Detailed Implementation Plan and separately Approved Security Management Plan.

Data Processing, Storage, Management and Destruction

4. The Supplier and Customer recognise the need for the Customer's information to be safeguarded under the applicable Data Protection Legislation and taking full account of the relevant obligations identified by the Data Protection Legislation in accordance with this Call Off Contract.

5. The Supplier must be able to state to the Customer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Customer Data will be subject to at all times.

6. The Supplier shall agree any change in location of data storage, Processing and administration with the Customer in advance where the proposed location is outside the UK.

7. The Supplier shall:

    (a) provide the Customer with all Customer Data on demand in an agreed open format;
    (b) have documented processes to guarantee availability of Customer Data in the event of the Supplier ceasing to trade;

(c) securely destroy all media that has held Customer Data at the end of life of that media in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor); and

(d) securely erase any or all Customer Data held by the Supplier when requested to do so by the Customer in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor).

Networking

8. Any Customer 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 Component of any product or system which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under Commercial Product Assurance ("CPA") or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products). If no CESG standard is applicable an assurance strategy will be agreed with the Customer.

9. The Customer 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 CESG guidance and Good Industry Practice.

Encryption

10. Data at rest both within the database environment (including archive data and data logs save for those data logs agreed with the Customer by exception as not requiring encryption) and that which is stored as 'back up' shall be encrypted using a Component of any product of system which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA"). In the event that a Supplier determines that the risk which this level of encryption mitigates against is managed by some other means, then this must be formally recorded and notified to the Customer. In such circumstances, the Customer will, taking account of 'residual risk,' determine acceptability. If no CESG standard is applicable an assurance strategy will be agreed with the Customer.

Security Architectures

11. 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 Customer information.

12. When designing and configuring the Supplier Solution the Supplier shall comply with CESG (or other relevant HMG body) stated good practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification or from a Certified Cyber Security Consultancy https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy If no CESG standard is applicable an assurance strategy will be agreed with the Customer.

Personnel Security

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

14. 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 Customer Data.

15. 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 Customer Data except where agreed with the Customer in writing.

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

17. 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 and be subject to appropriate monitoring in accordance with CESG Good Practice Guide 13 - Protective Monitoring for HMG ICT systems. When Supplier Personnel no longer need elevated privileges or leave the organisation, their access rights shall be revoked within 1 Working Day.

Identity, Authentication and Access Control

18. The Supplier shall operate an access control regime to ensure all users and administrators of the Supplier Solution 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 Supplier Solution they require. The Supplier shall retain an audit record of accesses in accordance with CESG Good Practice Guide 13 - Protective Monitoring for HMG ICT systems.

Audit and Monitoring

19. In accordance with CESG Good Practice Guide 13 - Protective Monitoring for HMG ICT systems 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:

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

    b. Security events generated in the Supplier Solution (to the extent that the Supplier Solution is within the control of the Supplier) and shall include: privileged account logon and logoff 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.

20. The Supplier and the Customer shall work together to establish any additional audit and monitoring requirements for the Supplier Solution.

21. The Supplier shall retain audit records collected in compliance with Paragraph 19 of this Annex to this Call Off Schedule for a period of at least 6 Months. Forensic data shall be supplied as required by the Customer, based upon the Supplier's obligation to be compliant with CESG Good Practice Guide 18 – Forensic Readiness.

ANNEX 2

Security Requirements

As set out in Call Off Schedule 2 – Part E