OFFICIAL

ATTACHMENT 15-3 SPECIAL TERMS

PSN CONNECTIVITY

CALL-OFF TERMS

SCHEDULE 2.2

SECURITY REQUIREMENTS AND PLAN

1 INTRODUCTION

1.1 The Parties acknowledge that the purpose of the ISMS and Security Plan is to ensure an efficient and effective organisational approach under which the specific Service Requirements of this Agreement relating to security will be met. This approach shall ensure compliance with the Customer Authority's obligations to the Security Policy Framework (and all relevant subordinate policies and best practice guidance) and support wider security requirements of the Customer Authority such as those required for PSN connectivity.

1.2 The Parties shall each appoint a member of the Services Board to be responsible for security. The initial member of the Services Board appointed by the Contractor for such purpose shall be the Contractor's Service Delivery Manager as named as such in Appendix 2 (Information Required for Call-Off Terms) and the provisions of Clauses 26.5 to 26.11 of the Call-Off Terms (Key Personnel) shall apply in relation to such person.

1.3 The Contractor shall ensure that the ISMS, Security related activity and any mitigation measures meet all Security Requirements set out in Annex 2 and take into account the sensitivity of the Customer Authority Data. Data on the Customer Authority network will be up to the Government Security Classification tier of 'OFFICIAL' with much of it OFFICIAL-SENSITIVE.

1.4 Each Party shall provide a reasonable level of access to any members of the other party's personnel and to any Customer Authority Sites as required for the purposes of designing, implementing and managing security.

1.5 The Contractor shall ensure that the Customer Authority Data remains under the control of the Contractor at all times.

1.6 The Contractor shall ensure that its Security Policy relating to the operation of its own organisation and systems is kept up-to-date and, on request by the Customer Authority, shall supply evidence of this (such as an appropriately scoped ISO27001 registration/certificate) to the Customer Authority.

1.7 The Customer Authority and the Contractor acknowledge that information security risks are shared between the Parties and that a compromise of either the Contractor's or the Customer Authority's security provisions represents an

unacceptable risk to the Customer Authority and shall require immediate communication and co-operation between the Parties to resolve or mitigate such risk.

1.8 On the Effective Date the Contractor shall supply to the Customer Authority a SAL which has been duly signed and executed for and on behalf of the Contractor and the terms and conditions of such SAL are hereby incorporated into this Call-Off Contract.

2 ISMS

2.1 During Transition, and in any event prior to the first Operational Service Commencement Date (or such other period as specified in the Implementation Plan or as otherwise agreed by the Parties in writing, the Contractor shall develop and submit to the Customer Authority for the Customer Authority's approval (in accordance with Paragraph 2.6 below) an ISMS for the purposes of this Agreement, which, at the date of submission:

(a) shall have been tested in accordance with Schedule 4.2 (Testing Procedures); and

(b) shall comply with the requirements of Paragraphs 1 to 17 of Annex 1, and all Security Requirements set out in Annex 2.

2.2 The Contractor acknowledges that the Customer Authority places great emphasis, reliance and importance on the reliability of the Services and the confidentiality, integrity and availability of Information and consequently on the security provided by the ISMS, and that the Contractor acknowledges that it shall be solely responsible for the effective performance of the ISMS, to the satisfaction of the Customer Authority.

2.3 The ISMS shall:

(a) unless otherwise specified by the Customer Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Customer Authority Sites, the Contractor System, the Customer Authority System (to the extent that it is under the control of the Contractor), connectivity to secure services (e.g. PSN) and any IT, information and data (including Sensitive Information as defined by the Government Security Classification Policy and the Customer Authority Data) to the extent used by the Customer Authority or the Contractor in connection with this Agreement;

(b) achieve certification to ISO 27001 within a timescale agreed by the Customer Authority and in accordance with Paragraph 2.3(a); and

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

(i) is in accordance with Law and this Agreement;

(ii) complies with Good Industry Practice;

(iii) complies with the Security Policy Framework obligations and Baseline Security Requirements ensuring all accreditation and secure connectivity objectives are fulfilled;

(iv) addresses and resolves any issues of incompatibility with the Contractor's own organisational security policies;

(v) meets any specific security threats of immediate relevance to the Services and/or Customer Authority Data;

(vi) complies with the Security Requirements as set out in Annex 2 to this Schedule 2.2 (Security Requirements and Plan));

(vii) complies with the Customer Authority's IT policies; and

(viii) is to the satisfaction of the Customer Authority;

(d) documents the security Incident management processes and Incident response plans;

(e) 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 Authority approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

(f) be certified by a Contractor's Service Board representative (or by a person with the direct delegated authority of such 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 Authority and Contractor in advance of issue of the relevant Security Plan).

2.4 Where reference is made in this Agreement to the Security Policy Framework, such reference shall also include the range of policy and guidance information that has been drafted by organisations such as Cabinet Office and CESG to support such compliance. The Contractor shall be familiar with and take account of such guidance.

2.5 In the event that the Contractor becomes aware of any inconsistency in, or conflict between, the provisions of the standards, guidance and policies referred to in paragraphs 2.3 and 2.4 above, the Contractor shall immediately notify the Customer Authority Representative of such inconsistency, and provide expert advice at its own cost. The Customer Authority Representative shall, as soon as practicable, notify the Contractor as to which of the conflicting provision the Contractor shall comply with.

2.6 If the ISMS submitted to the Customer Authority pursuant to Paragraph 2.1 is approved in writing by the Customer Authority, it shall be adopted by the Contractor immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not approved by the Customer Authority, the Contractor

shall amend and re-submit it to the Customer Authority within 10 Working Days of the date of notice of non-approval from the Customer Authority. The Parties shall use all reasonable endeavours to ensure that the approval process in relation to the ISMS takes as little time as possible from the date of the first submission of the ISMS by the Contractor to the Customer Authority. If the Customer Authority does not approve the ISMS following its resubmission, the matter of the Customer Authority's approval of the ISMS shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Customer Authority pursuant to this Paragraph 2.6 may be unreasonably withheld or delayed. However any failure by the Customer Authority to approve the ISMS on the basis that the ISMS does not, in the opinion of the Customer Authority, comply with all of the requirements set out in this Paragraph 2 shall be deemed to be reasonable.

2.7 Approval by the Customer Authority of the ISMS pursuant to Paragraph 2.6 or of any change to the ISMS shall not relieve the Contractor of its obligations under this Schedule.

3 SECURITY PLAN

3.1 No later than forty (40) Working Days after the LOI 1 Date (or such other period as specified in the Implementation Plan or as otherwise agreed by the Parties in writing, the Contractor shall have prepared and submit to the Customer Authority for approval in accordance with Paragraph 3.3, a fully developed, detailed, complete and up-to-date Security Plan which shall comply with the requirements of Paragraph 3.2.

3.2 The Security Plan shall:

(a) unless otherwise agreed in writing between the Parties, be based on the initial Security Plan that was provided as part of the original tender response;

(b) comply with the Baseline Control Set and support compliance with the Security Policy Framework;

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

(d) detail the process for managing any security risks from Subcontractors and third parties authorised by the Customer Authority with access to the Services, processes associated with the delivery of the Services, the Customer Authority Premises, the Sites, the Contractor System, the Customer Authority System (to extent that it is under the control of the Contractor) and any IT, Information and data (including Sensitive Information as defined by the Government Security Classification Policy and the Customer Authority 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 Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Customer Authority Premises, the Sites, the Contractor System, the Customer Authority System (to the extent that it is under the control of the Contractor) and any IT, Information and data (including Sensitive Information as defined by the Government Security Classification Policy and the Customer Authority Data) to the extent used by the Customer Authority or the Contractor in connection with this Agreement 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 Contractor 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 Schedule;

(g) demonstrate that the Contractor Solution has minimised the efforts required by the Customer Authority and the Contractor to comply with this Schedule through careful consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offerings from the G-Cloud catalogue);

(h) set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those incorporated in the ISMS at the date set out in the (Implementation Plan for the Contractor to meet the full obligations of the security requirements set out in Annex 2 of this Schedule 2.2 (Security Requirements and Plan) and this Schedule;

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

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

(k) be written in plain English in language which is relevant to the Customer Authority's business and readily comprehensible to the staff of the Contractor and the Customer Authority that are engaged in the provision and use of the Services; and

(l) shall reference only documents which are in the possession of both of the Parties or whose location is otherwise specified in this Schedule.

3.3 If the Security Plan submitted to the Customer Authority pursuant to Paragraph 3.1 is approved by the Customer Authority, it shall be adopted by the Contractor immediately and thereafter operated and maintained in accordance with this

Schedule. If the Security Plan is not approved by the Customer Authority, the Contractor shall amend and re-submit it within 10 Working Days of the date of notice of non-approval from the Customer Authority. The Parties shall use all reasonable endeavours to ensure that the approval process in relation to the Security Plan takes as little time as possible from the date of the first submission of the Security Plan by the Contractor to the Customer Authority. If the Customer Authority does not approve the Security Plan following its resubmission, the matter of the Customer Authority's approval of the Security Plan shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Customer Authority pursuant to this Paragraph 3.3 may be unreasonably withheld or delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in Paragraph 3.2 above shall be deemed to be reasonable.

3.4 Approval by the Customer Authority of the Security Plan pursuant to Paragraph 3.3 or of any change or amendment to the Security Plan shall not relieve the Contractor of its obligations under this Schedule.

4 AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN

4.1 The ISMS and Security Plan shall be fully reviewed and updated by the Contractor on an annual basis, to reflect:

(a) emerging changes in Good Industry Practice;

(b) on-going ISO27001 certification requirements;

(c) on-going Customer Authority system accreditation obligations;

(d) any change or proposed change to the ICT Environment, the Services and/or associated processes;

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

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

4.2 The Contractor shall provide the Customer Authority with the results of such review as soon as reasonably practicable after its completion and shall amend the ISMS and Security Plan at no additional cost to the Customer Authority. The results of the review shall include, without limitation:

(a) improvements suggested regarding 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, lessons learnt; 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), emerging best practice.

4.3 Subject to Paragraph 4.2, any change which the Contractor proposes to make to the ISMS or Security Plan (as a result of a review carried out pursuant to Paragraph 4.1, a Customer Authority request, a change to Appendix 3 (Service Requirements and Contractor Service Descriptions) or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Customer Authority.

4.4 The Customer Authority may, where it is reasonable to do so, approve and require changes or amendments to the ISMS or Security 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 Agreement.

5 SECURITY TESTING

5.1 Unless the Customer Authority notifies the Contractor otherwise, the Contractor shall conduct relevant Security Tests from time to time (and at least annually across the scope of the ISMS) and after any architectural changes to the ICT Environment or after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Plan. Security Tests shall be designed and implemented by the Contractor so as to avoid any impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in writing in advance with the Customer Authority.

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

5.3 Without prejudice to any other right of audit or access granted to the Customer Authority pursuant to this Agreement, the Customer Authority and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Contractor, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Contractor's compliance with the ISMS and the Security Plan. The Customer Authority may notify the Contractor of the results of such tests after completion of each test. If the Contractor proves, to the Customer Authority's satisfaction, that any such Customer Authority test adversely affects the Contractor's ability to deliver the Services so as to meet the Service Level Targets, the Contractor may be granted relief against any resultant under-performance for the period of such Customer Authority test.

5.4 Where any Security Test carried out pursuant to Paragraph 5.1 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Contractor shall promptly notify the Customer Authority of any suggested changes to the ISMS and to the Security Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to the Customer Authority's prior written approval, the Contractor shall implement such changes to the ISMS and the Security Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Customer Authority or, otherwise, as soon as possible. For the avoidance of doubt, where the change to the ISMS or Security Plan is to address an issue of non-compliance with the Baseline Security Requirements, accreditation requirements, secure service connectivity obligations or security requirements (as set out in Appendix 3 (Service Requirements and Contractor Service Descriptions) or the requirements of this Schedule 2.2 (Security Requirements and Plan), the change to the ISMS or Security Plan shall be at no cost to the Customer Authority.

5.5 If any repeat Security Test carried out pursuant to Paragraph 5.4 reveals an actual or potential Breach of Security exploiting the same Root Cause failure, such circumstance shall constitute a material Default.

5.6 Any penetration testing of the Customer Authority systems shall only be undertaken by a CESG approved CHECK Green Contractor, or as directed by the Customer Authority.

6 ISMS COMPLIANCE

6.1 The Customer Authority shall be entitled to carry out such security audits as it may deem necessary in order to ensure that the ISMS maintains compliance with the Security Policy Framework and system accreditation objectives, the specific security requirements set out in Annex 2 to this Schedule 2.2 (Security Requirements and Plan) and the Baseline Security Requirements.

6.2 ISO27001 certification/registration shall be confirmed by an external accredited certification body on an annual basis at the cost of the Contractor, or as directed otherwise by the Customer Authority.

6.3 If, on the basis of evidence provided by such audits, it is the Customer Authority's opinion that compliance with identified security principles and practices, the specific security requirements set out in Annex 2 to this Schedule 2.2 (Security Requirements and Plan) and/or the Baseline Security Requirements is not being achieved by the Contractor, then the Customer Authority shall notify the Contractor of the same and give the Contractor 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 Contractor does not become compliant within the required time then the Customer Authority shall have the right to obtain an independent audit against these standards in whole or in part, and at the cost of the Contractor.

6.4 If, as a result of any such independent audit as described in Paragraph 6.3 the Contractor is found to be non-compliant with identified security principles and practices, the specific security requirements set out in Annex 2 to this Schedule 2.2

(Security Requirements and Plan) and/or the Baseline Security Requirements then the Contractor 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 Customer Authority in obtaining such audit.

6.5 The provisions of Paragraphs 6.3 and 6.4 are without prejudice to the Customer Authority's other rights and remedies set out in this Agreement.

7 BREACH OF SECURITY

7.1 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 or potential Breach of Security.

7.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 7.1, the Contractor shall:

(a) immediately take all reasonable steps (which shall include any action or changes required by the Customer Authority) 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 ICT Environment to the extent within its control against any such Breach of Security or attempted Breach of Security;

(iii) 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 Contractor, if the mitigation adversely affects the Contractor's ability to deliver the Services so as to meet the Service Level Targets, the Contractor shall be granted relief against any resultant under-performance for such period as the Customer Authority, acting reasonably, may specify by written notice to the Contractor;

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

(v) supply any requested data to the Customer Authority and, on the Customer Authority's request, to the Computer Emergency Response Team for UK Government ("GovCertUK") 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 Authority full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted or potential Breach of Security,

including a root cause analysis and lessons learnt where required by the Customer Authority.

7.3 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 the security requirements in Annex 2 to this Schedule 2.2 (Security Requirements and Plan) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Customer Authority.

8 VULNERABILITES AND CORRECTIVE ACTION

8.1 The Customer Authority and the Contractor acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Customer Authority's information.

8.2 The severity of threat vulnerabilities shall be categorised by the Contractor 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.

8.3 The Contractor shall procure the application of security patches to vulnerabilities with appropriate urgency but at least within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 calendar days of release, 'Important' within 30 calendar days of release and all 'Other' within 60 Working Days of release, except where:

(a) the Contractor 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 Contractor asserts cannot be exploited within the context of a Service must be remedied by the Contractor 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 Contractor's ability to deliver the Services in which case the Contractor shall be granted an extension to such timescales of 5 calendar days, provided the Contractor had followed and continues to follow the security patch test plan agreed with the Customer Authority; or

(c) the Customer Authority agrees a different maximum period after a case-by-case consultation with the Contractor under the processes defined in the ISMS.

The Contractor Solution shall include provisions for major version upgrades of all 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: where 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 is agreed with the Customer Authority in writing.

8.4 The Contractor shall:

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

(b) ensure that the ICT 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 Authority such behaviour, and ensure appropriate data is preserved to enable forensics;

(c) ensure it is fully aware of the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Term;

(d) pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 2);

(e) from the relevant date set out in paragraph 8.3 above and specified in the Security Plan (and before the first Operational Service Commencement Date or such other period as specified in the Implementation Plan or as otherwise agreed by the Parties in writing) provide a written report to the Customer Authority within 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 Contractor)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, and when agreed, implement, interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;

(g) proactively review, and if agreed, 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 Contractor Solution and ICT Environment); and

(h) inform the Customer Authority 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 implement controls compliant with the ISMS.

8.5 If the Contractor is unlikely to be able to mitigate the vulnerability within the timescales under Paragraph 8.3, the Contractor shall immediately notify the Customer Authority.

8.6 A failure to comply with Paragraph 8.3 shall constitute a Service Failure, and, without prejudice to any other rights and obligations under this Agreement the Contractor shall comply with the provisions of Clauses 10.2 and 10.3 of the Call-Off Terms.

ANNEX 1

Baseline Security Requirements

Higher Classifications

The Contractor shall not use, transfer, store or process Customer Authority information classified SECRET or TOP SECRET except if there is a specific requirement and, if such specific requirement exists, then prior to receipt of such information by Contractor,, Customer Authority shall inform Contractor that information is SECRET or TOP SECRET and the Contractor shall seek additional specific guidance from the Customer Authority.

End User and Network Devices

1. When Customer Authority 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 UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA"), or as otherwise agreed by the Customer Authority.

2. Devices used to access or manage Customer Authority Data and Services must be under the management control of the Customer Authority or Contractor and shall 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 ICT Environment. Unless otherwise agreed with the Customer Authority in writing, all Contractor devices shall meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.gov.uk/government/collections/end-user-devices-security-guidance--2). Where the guidance highlights any material deficiency in a particular platform the Contractor may wish to use, the Contractor shall make detailed recommendations to the Customer Authority (informed by the Contractor's detailed knowledge of security technology and Government security regulation requirements), and the Customer Authority will decide whether the residual risks are acceptable. Where the Contractor wishes to deviate from the CESG guidance, this shall only be permitted when agreed in writing on a case by case basis with the Customer Authority.

Data Processing, Storage, Management and Destruction

3. The Contractor and Customer Authority recognise the need for the Customer Authority's information to be safeguarded under the UK Data Protection regime. To that end, the Contractor must be able to state at all times to the Customer Authority the physical locations where Customer Authority Data may be stored, processed and managed from, and to confirm that all legal and regulatory frameworks relevant to Customer Authority are complied with.

4. The Contractor shall agree any change in location of Customer Authority Data storage, processing and administration with the Customer Authority in advance, where the proposed new location is outside the UK. The Contractor shall be aware of, and comply with, all Law and Government requirements regarding the storage, transfer and processing of data in and to location outside of the UK.

5. The Contractor shall:

    (a) provide the Customer Authority with all Customer Authority Data on demand in an agreed open format;

    (b) have, and follow, documented processes to guarantee availability of Customer Authority Data in the event of the Contractor ceasing to trade;

    (c) securely destroy all media that has held Customer Authority 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 Authority Data held by the Contractor when requested to do so by the Customer Authority in line with HMG Information Assurance Standard No5. – Secure Sanitisation of Protectively Marked or Sensitive Information (or its successor).

Networking

6. The Customer Authority requires that any Customer Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device, and data held on mobile devices, must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade (as defined in the CESG End User Devices Platform Security Guidance) , for example, under 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), or otherwise as agreed with the Customer Authority.

Security Architectures

7. The Contractor 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 Authority Information.

8. When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Contractor) the Contractor shall comply with PSN and CESG (and other relevant Government bodies) stated best practice, and obtain guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx) for all bespoke or complex components of the Contractor Solution.

Personnel Security

9. Contractor Personnel shall be subject to pre-employment checks that include, as a minimum a full DBS (Disclosure and Barring Service). The Contractor acknowledges that the CPS is exempt from the terms of the Rehabilitation of Offenders Act.

10. The Contractor shall agree with the Customer Authority, on a case by case basis, Contractor Personnel roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Customer Authority Data.

11. The Contractor shall prevent Contractor Personnel who are unable to obtain the required security clearances from accessing, or potentially accessing, Customer Authority Data except where agreed with the Customer Authority in writing.

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

13. Where the Contractor or Sub-Contractors grants increased IT privileges or access rights to Contractor Personnel, those Contractor Personnel shall be granted only those permissions necessary for them to carry out their duties and shall be subject to appropriate monitoring in accordance with CESG Good Practice Guide 13 - Protective Monitoring for HMG ICT systems. When staff no longer needs elevated privileges or leave the organisation, their access rights shall be revoked within 1 Working Day.

Identity, Authentication and Access Control

14. The Contractor shall operate an access control regime to ensure all users and administrators of the Contractor 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 Contractor Solution they require. The Contractor shall retain an audit record of accesses in accordance with CESG Good Practice Guide 13 - Protective Monitoring for HMG ICT Systems, and user acceptance of policies. Appropriate good industry practise must be followed, e.g. strong passwords used for all accounts.

Audit and Monitoring

15. In accordance with CESG Good Practice Guide 13 - Protective Monitoring for HMG ICT systems the Contractor 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 Contractor 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 ICT Environment (to the extent that the ICT Environment is within the control of the Contractor). To the extent the design of the Contractor 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 ICT environment (to the extent that the ICT Environment is within the control of the Contractor) 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, e.g. from third party software, security or otherwise.

c. Ensure such arrangements are compatible with the Data Protection Legislation and Cabinet Office requirements for handling personal data.

16. The Contractor and the Customer Authority shall work together to establish any additional audit and monitoring requirements for the ICT environment.

17. The Contractor shall retain, and store appropriately, audit records collected in compliance with Paragraph 15 for a period of at least six (6) months, or longer as required by the Customer Authority.

OFFICIAL

ANNEX 2

Service Requirements – Security

NONE