Annex 3 - SERVICE SPECIFICATION: SECURITY

Security accreditation, Information management system, Security proceedings and markings

	Requirement	Description
R3.1-01	HMG Security Policy Framework	The Supplier shall ensure that the Service is provided and operated in a manner which supports Home Office compliance with the HMG Security Policy Framework (SPF) at current and future versions. The HMG Security Policy Framework is located at http://www.gov.uk/government/publications/security-policy-framework and updated periodically. It includes by reference HMG IA Standards, Good Practice Guides and other guidance produced by CESG. It is the responsibility of the Supplier to ensure that they understand these standards and guidance and employ resources (e.g. Cyber Security Consultancy) to interpret them.
R3.1-02	HMG Security Policy Framework	The Supplier shall review changes to the HMG Security Policy Framework as they occur, shall immediately inform UKVI as to whether or not compliance can be maintained, and shall then negotiate any changes to the Service with UKVI.
R3.1-03	Legislation	The Supplier shall at all times comply with relevant legislation, in particular the Official Secrets Act and the Data Protection Act (when handling personal data).
R3.1-04	Encryption	The Supplier shall apply correct levels of encryption to personal data being processed, handled, transmitted and stored which does not affect the receipt of data to the rightful recipient/Customer.
R3.1-05	Accreditation Scope	The entire Service shall be covered by Accreditation in accordance with the SPF to a specified level and scope to be agreed with UKVI.

R3.1-06	Obtain Accreditation	The Supplier shall obtain Accreditation or Approval to Operate of the entire Service by UKVI's Accreditor prior to live operation of the Service. In obtaining this Accreditation, the Supplier shall fully consult the Accreditor and UKVI representatives throughout the design, build and Accreditation process. The Accreditor will want to see a technical and logical description of the system and data, showing where the data is held and transported and describing who has access and from where etc. This should also describe the processes for incident management, change management, leavers joiners and movers and also name the Information Asset Owner, Senior Responsible Owner and both the supplier's and HO's Security Managers plus any ISO27001 certification, including the scope and an IT Health Check report that tested the system and any interconnects and resultant Remediation Action Plan.
R3.1.07	Provide an accreditable Service	The Supplier shall ensure that the Service is accreditable within the scope defined with the Home Office and the Security Classifications as detailed in the Security Aspects Letter (SAL).
R3.1-08	ISO/IEC 27001 Certification	The Supplier shall ensure that all parts of the Service shall be covered at all times by Certification to ISO/IEC 27001:2013 (or later versions thereof).
R3.1-09	ISMS under ISO/IEC 27001	The Supplier shall have and operate an Information Security Management System (ISMS) that complies with ISO 27001, and addresses the Service against the scope approved by UKVI.
R3.1-10	CESG approval of encryption	The Supplier shall ensure that any component of the Service requiring CESG approved cryptographic capabilities shall have been formally evaluated under a CESG evaluation scheme as agreed with UKVI.
R3.1-11	Appoint Crypto Custodian	If any cryptographic materials are required as part of the Service then the Supplier shall appoint trained and vetted personnel to carry out handling and management of such materials.
R3.1-12	HADRIAN	The Supplier shall submit to a HADRIAN assessment to be carried out by the Home Office and shall provide such information as the Home Office sees fit in order to complete such assessment.
R3.1-13	Cyber Essentials	Your organisation should aim towards achieving Cyber Essentials or Cyber Essentials Plus certification. The Cyber Essential scheme demonstrates that an organisation has taken essential precautions to mitigate the risk from common internet based threats. Further information on Cyber Essentials is available at: https://www.cyberstreetwise.com/cyberessentials/

R3.1-14	IT Health Check	The Supplier shall be responsible for carrying out IT Health Checks (ITHCs) to be performed by a CESG CHECK "Green Light" approved company on all the Supplier's infrastructure and systems used to provide the Service. The first ITHC shall be carried out prior to Live operation of the service, and further ITHCs shall be carried out annually or after major changes as directed by the UKVI's Accreditor.
R3.1-15	ITHC Scope	The Scope of all ITHCs shall be at the sole discretion of the UKVI's Accreditor. The Scoping Document shall be prepared by the Supplier and submitted to the UKVI's Accreditor for approval. No ITHC shall be carried out without first gaining the Accreditor's approval.
R3.1-16	ITHC Reports	The Supplier shall make IT Health Check reports available in full to UKVI, a Draft being supplied immediately upon completion of each ITHC with the final report following as soon as it is made available by the CHECK company and in any case within a maximum of 10 working days.
R3.1-17	Issues & Vulnerabilities	The Supplier shall ensure that any findings, issues or vulnerabilities highlighted in IT Health Checks are rectified to the reasonable satisfaction of UKVI's Accreditor. A Remedial Action Plan (RAP) or Risk Treatment Plan (RTP) provided and actioned by the Supplier shall be the vehicle for recording, agreeing and controlling these rectification activities.
R3.1-18	Security and system architecture	The Supplier shall produce and maintain detailed security and system architecture documentation as part of the design process and following any changes to the systems used to provide the Service and shall submit same to UKVI.
R3.1-19	RMADS	The Supplier shall develop, maintain and comply with, and ensure that all Subcontractors will comply with, and shall assist UKVI in complying with a Risk Management and Accreditation Document Set (RMADS) in accordance with the HMG Security Policy Framework and UKVI's security and business requirements. RMADS shall: a) comply with current CESG Standards & Guidance b) include a full Technical Risk Assessment c) be owned by UKVI d) comply with UKVI Security Policy e) be kept up to date in accordance with the Accreditation Strategy f) be verified through the Security Working Group.
R3.1-20	Security Aspects Letter	The Supplier shall ensure that all information it handles or processes is correctly classified in accordance with the Security Aspects Letter (SAL) which will be supplied by the UKVI. The Supplier must ensure that any 3rd party to whom it supplies information is aware of, and complies with, the requirements in the SAL.

R3.1-21	Remote access	No remote maintenance and/or diagnostics in relation to the Service shall be allowed without prior approval by the UKVI Security Manager and/or Accreditor. Mechanisms shall be in place to prevent any remote access unless authorised.
R3.1-22	Security Tests carried out by UKVI	Without prejudice to any other access granted to any other Customer of the Supplier, UKVI shall be entitled at any time and without giving notice to the Supplier to carry out such Security Tests (including penetration tests) as it may deem necessary in relation to the Security Management Plan and the Supplier's compliance with and implementation of the Security Management Plan. UKVI may notify the Supplier of the results of such tests after completion of each such test. UKVI's Security Tests shall be designed and implemented so as to minimise the impact on the Service. If any UKVI Security Test impacts adversely on the Supplier's ability to deliver the Service to the agreed Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Test, and for such other period beyond the period of the Security Test, provided the Supplier is able to demonstrate to UKVI's satisfaction that the adverse impact has continued beyond the period of the Security Test. The security test must be at least an annual test and no 'live' data may be stored or manipulated on the system before an ITHC has been carried out and a Remediation Action Plan for any vulnerabilities found agreed with the customer. If there are any substantial changes to the system, number of users or amount/type of data being used further testing may be required.
R3.1-23	Security failures and weaknesses	Where any Security Test carried out by UKVI or the Supplier, whether under an ITHC or not, reveals any actual or potential security failure or weakness, the Supplier shall promptly notify UKVI of any changes to the Security Management Plan (and the implementation thereof within the Service) which the Supplier proposes to make in order to correct such failure or weakness. Subject to UKVI's agreement, the Supplier shall implement such changes to the Security Management Plan and/or Service in accordance with the timetable agreed with UKVI or, otherwise, as soon as reasonably possible. Where as a result of Supplier Default there is a change to the Security Management Plan or the Service to address a non-compliance with the Security Management Plan or Security Requirements, the change(s) shall be made by the Supplier at no additional cost to UKVI. In cases where there is no such Supplier Default, changes to the Security Management Plan shall be subject to the Change Control Procedure. For the purposes of this paragraph, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Management Plan or Security Requirements

R3.1-24	Service change control	The Supplier shall ensure that the Accreditor has approved any significant Change to the Service, including to the configuration or functionality of any systems used to provide the Service, before any such Change is implemented and subsequently Accredited. Where Emergency Changes to the Service are required for whatever reason, the Supplier shall ensure that the changes are implemented in a secure manner. The Supplier shall ensure that the Accreditor is informed about any Emergency Changes at the earliest possible opportunity. If the Accreditor does not approve the Emergency Changes, the Supplier must rectify the changes at its cost, at the earliest possible opportunity.
R3.1-25	Personal devices	The Supplier (including sub-contractors) shall not use their own personal devices for handling UKVI information without prior agreement from the Authority.
R3.1-26	Offshoring	The Supplier (including sub-contractors) shall not process or otherwise transfer any Personal Data outside of the UK. If, after the Commencement Date, the Supplier (or any Sub-Contractor) wishes to Process and/or transfer any Personal Data outside of the UK, prior approval must be sought from UKVI.
R3.1-27	Information - software/ hardware	The Supplier shall proactively monitor relevant briefings and alerts for information pertaining to emerging threats and/or vulnerabilities associated with software and hardware used by the Supplier in the provision of the Services to UKVI and shall propose corrective measures to UKVI.
R3.1-28	Supplier Relations	The Supplier shall inform UKVI of any new relations with foreign entities that could have a direct influence on the Supplier Service provision to UKVI or allow direct or indirect access to UKVI information or cause embarrassment to UKVI.
R3.1-29	Site Access & Inspection	The Supplier shall ensure that UKVI is allowed reasonable access, on request, to all relevant premises to conduct on site inspections for the purpose of fraud prevention, security policy and security requirements and compliance monitoring.
R3.1-30	Compliance	The Supplier shall comply with relevant RMADS, codes of connection and other requirements in respect of services, systems and business processes the Supplier's systems will interface with for the provisions of the contracted Service to UKVI. (Example services/systems include the Public Sector Network (PSN) and the Government Secure Intranet (GSi).)

R3.1-31	Data retention and disposal	The Supplier shall comply with the UKVI's policy on data retention, and disposal and decommission of UKVI's data shall be in accordance with HMG SPF and IAS5. This must be described within the RMADS and/or the Security Management Plan be in line with UKVI's retention & disposal standards. Audit data (where the scope of audit data is agreed with the UKVI) shall be kept for the lifetime of the contract. Data must be stored in the UK. If you cannot comply with this arrangement, you will need to notify UKVI immediately.
R3.1-32	Access control	The Supplier shall produce and maintain an Access Control Policy (detailing who is allowed access and how it is controlled) that covers the Service. The Access Control Policy must be finalised before the contract commences.
R3.1-33	Unauthorised user access	The Supplier shall ensure that unattended servers, workstations, laptops, network devices and any other equipment that form any part of the Service are protected against use or abuse by unauthorised persons. An agreed leavers and joiners policy must be put in place before the contract commences to ensure only authorised users have access to the system.
R3.1-34	Incident Investigation	The Supplier shall maintain adequate records and facilitate inspections to enable the investigation of any security incidents by UKVI or their authorised representatives.
R3.1-35	Records	The Supplier shall keep formal records, or audit logs, including without limitation dispatch and receipt information, as specified in the Security Management Plan, where any data is sent to, or received from, other organisations in relation to the Service
R3.1-36	Audit	The Supplier shall provide a Service which ensures that all system activity is auditable. This may include but is not limited to, read-only accesses, manual searches, automated searches, changes made to Application data, addition of new system users, suspension of user accounts, removal of system users, amendment of decisions made by the system or an UKVI Authorised Staff member etc.
R3.1-37	Logs	The Supplier shall create, store and make available to the UKVI all audit logs and audit reports in a format agreed with the UKVI.
R3.1-38	Monitoring	The Supplier shall ensure that robust access, auditing, monitoring controls and capabilities in line with CSEG's Good Practice Guide 13 (GPG13) are in place to ensure the prevention and identification of attempts at and actual unauthorised access, be it physical or logical (electronic).

R3.1-39	Audit Data	The Supplier shall provide UKVI Authorised Staff with access to all Security audit data. Such access shall be unlimited and may be required without prior notice.
R3.1-40	Security Working Groups	The Supplier shall participate in joint Security Working Group (SWG) meetings with UKVI which occur at an agreed interval, initially once per month at an UKVI-agreed location. The Supplier shall resource the Security Working Groups with their Information Assurance, Technical, Commercial, Service Management and Project Management stakeholders as noted in the SWG Terms of Reference (which shall be agreed during the first twenty days of the service provision operation).
R3.1-41	Remedial Action Plan	The Supplier shall provide updates (at a rate to be agreed with UKVI but fortnightly by default) on the progress against any agreed Remedial Action Plan and also at the Security Working Group meetings if applicable.
R3.1-42	Patching Plan	The Supplier shall agree a Patching Plan with UKVI. (This may be part of the Supplier's Security Management Plan)
R3.1-43	Patching of systems	The Supplier shall ensure that all systems used to provide the Service are kept up-to-date in accordance with the Patching Plan. Details of patching and anti-virus software updates should be provided on a monthly basis to the members of the SWG at least two days before each SWG.
R3.1-44	Employee Vetting	The Supplier, in conjunction with UKVI, shall establish employee vetting procedures to establish and maintain security clearances for both existing and newly hired staff. The cost of such vetting will be met by the Supplier.
R3.1-45	Terms and conditions	The Supplier shall ensure that their Terms and Conditions of employment include the employee's responsibility for information security, and that all staff sign a Non-Disclosure Agreement (NDA). These shall include, but not be limited to, obligations under the Official Secrets Act.
R3.1-46	Appoint Security Manager	Supplier shall appoint a nominated Security Manager security manager should have, at least, formal security qualifications (CISM/CISSP/CISA/CCP) and have experience of VMware, SQL server, Windows server, IIS, firewalls and PaaS security issues.

R3.1-47	Baseline Personnel Security Standard (BPSS) – Pre-employment process	The Supplier shall ensure that their designated employees (including any sub-contractors) meet, and continue to meet, the required level of security checks defined by UKVI before they start work on the UKVI contract. The minimum standard is Baseline Personnel Security Standard (BPSS) - but additional National Security Vetting (NSV) clearances are required for staff requiring access to UKVI information, systems, hardware or infrastructure that comprise any part of the service. Details of NSV clearances against roles will be given in the Security Aspects Letter (SAL). The level of security clearance for this contract is Security Check (SC).
R3.1-48	Immigration status/right to work	The Supplier shall ensure that all staff who work directly on provision of the Service have a valid immigration status and the right to work in the UK.
R3.1-49	Identification document	The Supplier shall ensure that their designated employees, agents and contractors present a valid and legal UK identification document when required to do so by UKVI Security staff.
R3.1-50	Security questionnaire	In respect of any personnel that the Supplier proposes to employ on UKVI accommodation for the purpose of providing the Service, the Supplier shall obtain from UKVI, a security questionnaire for completion by such personnel. Completed questionnaires shall be returned to the UKVI's representative at least thirteen (13) weeks before security clearance is required.
R3.1-51	Personnel details	The Supplier shall provide a list of names and addresses of all persons who may require admission in connection with the provision of the Service to any UKVI premises specifying the capacities in which they are concerned with the Service and giving such other particulars as UKVI may require. The Supplier shall comply with any directions issued by the designated representative of the UKVI as to which persons may be admitted to such premises and at what times.
R3.1-52	Security Criminal Records Declaration	In respect of any personnel that the Supplier proposes to employ on UKVI accommodation for the purpose of providing the Service, the Supplier shall obtain from UKVI a Criminal Records Declaration form for completion by such personnel. Completed Criminal Records Declaration forms shall be retained by the Supplier for the duration of the contract and be made available within three (3) Working Days to UKVI/Home Office Security on request.

R3.1-53	National Security Vetting (NSV)	The Supplier shall ensure that any member of Supplier Personnel (including sub-contractors) who does not have the correct level of NSV clearance does not gain access to any Security Classified information, systems, hardware or infrastructure that comprise any part of the Service.
R3.1-54	Physical Security	The Supplier shall ensure that all cabling includes physical security to maintain compliance with the applicable RMADS and/or Security Management Plan and any installation of equipment is carried out by vetted staff.
R3.1-55	Physical Security	The Supplier shall ensure that the physical security of locations used to provide the Services meets the protective marking of the information stored or processed at those locations.
R3.1-56	Physical locations	The Supplier shall ensure that unless agreed otherwise by the UKVI all physical locations storing or accessing HMG Information (including Personal Data) shall be UK based (HMG Policy (CESG Good Practice Guide 6) refers)
R3.1-57	Layered physical security	The Supplier shall provide a layered approach to physical security and shall provide floor plans and CCTV overlays for all locations annually to the UKVI.
R3.1-58	Security environment and implementation	The Supplier shall accommodate site surveys conducted by UKVI in accordance with HMG Security Policy Framework to determine Security Environments. The Supplier shall implement, within the scope of the HMG Security Policy Framework, any recommendations made by the UKVI following the survey (e.g. CCTV, secure cages, fences, access controls, SEAP locks, doors, PIR).
R3.1-59	Security Management Plan	The Supplier shall within 10 days of the start of service provision produce for approval by UKVI a Security Management Plan to detail how IA activities and deliverables will be delivered during the service provision period, and the Supplier shall conform to the agreed Security Management Plan at all times. (Security Management Plan may be synonymous with the ISMS.)
R3.1-60	Security Management Plan	The Security Management Plan shall be written in plain English in language which is readily comprehensible to the Supplier Personnel and all employees, agents, consultants and individual contractors who are wholly or mainly assigned to work on the Services and shall not reference any other documents which are not either in the possession of UKVI or otherwise specified in this Appendix.

R3.1-61	Security Management Plan	The Security Management Plan and any supporting documentation shall be compliant with the Security Policy Framework HMG Information Security Standards.
R3.1-62	Security Management Plan assurance	UKVI and the Supplier shall ensure that the Assurance Procedures in respect of the Security Management Plan take as little time as possible and no longer than fifteen (15) Working Days (or such other period as UKVI and the Supplier may agree in writing) from the receipt of the plan.
R3.1-63	Security Management Plan	The Security Management Plan shall be fully reviewed and updated by the Supplier at least every six (6) months and as may be requested by UKVI from time to time to reflect: (a) emerging changes and Industry Best Practice; (b) any change or proposed change to the Service and/or associated systems and processes; (c) any new perceived or changed threats to the Service or changes in risk for UKVI; and (d) any reasonable request by UKVI. The Supplier shall provide UKVI with the results of any such reviews within twenty (20) Working Days of completion of the review or as otherwise agreed in writing with UKVI.
R3.1-64	Business Continuity/ Disaster Recovery/Contingency Planning	The Security Management Plan shall detail how the Supplier will produce a Business Continuity, Disaster Recovery and Contingency Plan to UKVI for UKVI's approval.
R3.1-65	Incident Monitoring	The Security Management Plan shall detail how the Supplier will produce detailed procedures for Security Incident monitoring to the satisfaction of UKVI.
R3.1-66	Incident Reporting	The Security Management Plan shall detail how the Supplier will ensure all Security Incidents are recorded, investigated and immediately reported to UKVI.
R3.1-67	Change Control	The Security Management Plan shall detail how the Supplier will maintain the Accreditation of the Supplier's Solution at all times by submitting details of relevant proposed changes to UKVI's Security Manager and/or Accreditor for approval.
R3.1-68	Maintenance of Accreditation	The Security Management Plan shall detail how the Service shall maintain accreditation. The Service shall be formally re-accredited at least annually.

R3.1-69	Security Management Plan	The Security Management Plan shall detail how the Supplier will obtain and maintain independent certification to ISO/IEC 27001 against a scope approved by UKVI within the Security Management Plan.
R3.1-70	Security Management Plan	Any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of an UKVI request or change to UKVI Requirements or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by UKVI.
R3.1-71	Security controls	The Supplier shall ensure the security controls provided within the Service or its systems are demonstrably correlated to a risk assessment contained in the Security Management Plan.
R3.1-72	Information security policy	The Supplier will have a Supplier Information Security Policy which will be reviewed at least annually by both UKVI and Supplier. (This may be part of the Supplier's ISO/IEC 27001 documentation and/or the Security Management Plan.)
R3.1-73	Transport plan	If any physical movement is required of any UKVI or Supplier assets that form part of the Service then the Supplier shall provide a Transport Plan for such movement which describes in detail the delivery operations, processes, procedures, types of vehicles used and detailed description of the end to end collection, sorting and delivery of such assets. The Transport plan shall be maintained and reviewed at least annually.
R3.1-74	Supply Chain Security & Anonymity	The Supplier shall ensure the security and anonymity of the supply chain; software and hardware for the systems used to provide the Service must be procured in such a manner that the use in relation to the UKVI is not apparent to the Supplier’s source. The Supplier will not use UKVI or Home Office logos without the written consent of UKVI.
R3.1-75	Information security and access	The Supplier shall record and securely store all inbound and outbound Customer contacts for audit, training, quality control and security purposes for a period of 24 months with access on request by UKVI within 24 hours.