ANNEX C: DATA AND PERSONNEL SECURITY MANDATORY REQUIREMENTS

1. SECURITY MANAGEMENT

1.1 This Annex C describes the mandatory requirements that the Supplier shall fulfil in their entirety as part of the delivery of the Services.

1.2 The Supplier is also referred to Framework Schedule 2 paragraphs 3.16 and 3.17 with regard to the mandatory requirements in respect of Data Security and Personnel Security respectively.

1.3 The Supplier shall ensure that the capacity, availability and security of the Services is assured throughout the Framework Period.

1.4 The Supplier shall comply with the following requirements to ensure that the processes and procedures set out below meet the system requirements throughout the Framework Period and while any Call Off Agreements remain in force as follows:

(a) Service and Security Principle Requirements (paragraph 1.5);

(b) Security Documentation Requirements (paragraph 1.6);

(c) Service and Security Management Governance Requirements (paragraph 1.7 to 1.12).

1.5 **Service and Security Principle Requirements**

1.5.1 The Service and Security Principle Requirements Matrix at 1.5.4 below defines the main service and security characteristics required in the delivery of the Services under the Framework.

1.5.2 The Supplier shall provide the Authority with the assurance that the System and Security risks are being managed appropriately, and shall provide evidence of compliance with the Service and Security Principles requirements.

1.5.3 Additional Service and Security requirements may be added to the matrix, as required by the Authority, in line with government security policy and Framework Agreement Schedule 2: Services and Key Performance Indicators.

1.5.4 **Service and Security Principle Requirements Matrix**

Serial	Service and Security Principle	Service and Security Requirements
1.	Asset Protection and Resilience	Prior to April 2014 a security process called accreditation was mandated by the HMG Security Policy Framework (SPF) for all Government departments processing classified information. The process of accreditation provided for the assessment of a system against its security requirement using HMG IA Standards 1&2 and the Risk Management Accreditation Document set (RMADS). Approval was required from an accreditor as a pre-requisite for operation. This process was removed as a mandatory requirement for systems operating at Official Level from the April 2014 version of the SPF. However there is still requirement to demonstrate the sustainability of systems to process HMG owned data. This is

		done to provide confidence that the technology and information is secure enough to meet user's business needs. To provide this assurance the Supplier shall provide evidence to the Authority, as requested. Contracting Authority approval is required for any proposed hosting off shore. Some functions may be off-shored as long as independently assured evidence can be provided that no access to user information can be obtained from off-shore locations.
2.	Service Transition and Continuity	The Supplier shall provide to the Authority, on request, a Technology Roadmap of their current system(s) and how it/they will be supported throughout the Framework Period and while any Call Off Agreements remain in force, whichever is the later.
3.	IT Service and System Management Process	The Supplier shall have documented best practice procedures and processes as noted in paragraph 1.9 System Access Management below
4.	Security Accreditation Documentation	• Cyber Essentials and Cyber Essentials Plus certification is a mandatory requirement • ISO 27001 or equivalent is required • Should a Contracting Authority require a change in the Government Security Classification, the Supplier shall provide a plan which documents any changes required, any associated risks and their mitigation. The Supplier shall provide any further documentation required by the Authority and/or Contracting Authority for the change in Impact Level.
5.	Sub-Contractors' Security	The Supplier shall ensure that its Sub-Contractors satisfactorily support all of the security principles that the Services must deliver. The Supplier shall specify: • The specific data that will be shared with Sub-Contractors and/or third parties • Who (names) roles (e.g. system administrator) and level of security vetting in place for Sub-Contractors and/or third parties • Documented minimum relevant security requirements • Risk to the Supplier and/or Services from Sub-Contractors is regularly assessed, with appropriate controls in place • On termination all Sub-Contractor access rights to systems or information are removed The Supplier is also referred to paragraph 1.13 Information Exchange Policies below
6.	Operational Security	The Supplier shall have processes and procedures in place to ensure the operational security of the Services including, but not limited to: • Configuration and change management • Vulnerability management • Protective monitoring • Incident management

7.	Capacity	The Supplier shall provide evidence and results of capacity testing and processes, including plans for expansion as Call Off Agreements are awarded, handling peaks and troughs and concurrent user capacity.
8.	Personal Data Security	The Supplier shall provide evidence of robust handling processes throughout the lifecycle of all information held on the system which conforms to the definition of personal data defined within the Data Protection Act 1998. The robust handling procedures will need to include the provision of a Privacy Impact Assessment that will specify the procedural measures implemented to ensure: • There are clearly defined roles associated with any access to customer data. • Where a role is identified as having access to customer data there shall be defined responsibilities which detail any actions which can be performed in support of maintaining Services delivery. • There is a defined process which authorises Supplier staff to be able access to customer data for the purposes of delivering the Services. • Any individual being given access to customer data is aware of the HMG requirements for data protection. • The Supplier nominates an individual, as noted in paragraph 1.6.1, within its organisation who is independent from the delivery team for the Services and who is responsible for ensuring the enforcement of the measures defined above.

1.6 **Security Documentation**

1.6.1 The Supplier shall produce and maintain the following Data Security documentation in support of the Contracting Authority's security risk management of the Services.

(a) Data Security Context – This shall enable the Supplier to complete and maintain a record throughout the lifetime of the Framework, to document the technical Implementation context against which the Supplier shall state compliance with the Contracting Authority's data security principles. The document shall provide a breakdown of the service implementation which includes:

(i) a description of each different type of user;

(ii) a description of the Information Exchange with each external entity from both a service implementation and a management perspective; and

(iii) a breakdown of the key technical aspects of the Services implementation to a level that shall enable the Contracting Authority to assure comprehensive and consistent application coverage of the principles across the solution.

(b) Data Security Compliance Statement – This shall enable the Supplier to complete and maintain a record throughout the Framework Period to describe the security aspects

of their Service delivery and to provide evidence in support of assurance of their security controls.

(c) Data Security Risk Register – This shall enable the Supplier to complete and maintain a register throughout the Framework Period. For each risk the Supplier shall provide the following information:

(i) an assessment of the severity of the risk;

(ii) a description of the remediation action; and

(iii) a target date for remediation.

1.7 **Security Audit**

1.7.1 The Authority reserves the right to audit any evidence produced in support of claimed compliance with any Service and Security requirement.

1.8 **Service and Security Management**

1.8.1 The Supplier shall provide a suitably qualified nominated individual (the "**Supplier Security Assurance Manager**"), who is independent from the delivery team for the Services. The Supplier Security Assurance Manager shall have overall responsibility for assuring the security of the Services delivered under this Framework Agreement.

1.8.2 The Supplier shall also provide a suitably qualified deputy to act in the absence of the Supplier Security Assurance Manager.

1.9 **System Access Management**

1.9.1 The Supplier shall provide on-going account management for their systems which shall include:

(a) Implementation procedures in line with the individual Contracting Authority's security policy which provide access security control based on the individual's demonstrated need to view, add, change or delete data.

(b) User account profiles which include limiting normal users' execution permissions and enforcing the principle of 'least privilege'.

(c) Procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts.

(d) A control process to review and confirm access rights periodically.

(e) IT security administration to ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.

(f) Control over the IT process of ensuring systems security that satisfies the business requirement to safeguard information against unauthorised use, disclosure or modification, damage or loss and that is enabled by logical access controls which ensure that access to systems, data and programmes is restricted to authorised users and takes into consideration:

(i) Confidentiality and privacy requirements

(ii) Authorisation, authentication and access control

(iii) User identification and authorisation profiles

(iv) Need-to-have' and 'need-to-know' controls

(v) Cryptographic key management

(vi) Incident handling, reporting and follow-up

(vii) Virus prevention and detection

(viii) Firewalls

(ix) Centralised security administration

(x) User training

(xi) Tools for monitoring compliance, intrusion testing and reporting

1.10 **Requirements for a security breach notification**

1.10.1 The Contracting Authority shall specify its requirements in the event of a security breach at the Call Off Agreement stage.

1.11 **Encryption**

1.11.1 The Contracting Authority shall specify its encryption requirements at the Call Off Agreement stage.

1.12 **Software Support**

1.12.1 If the support for any software used by the Supplier in delivering the Services is due to expire, the Supplier shall ensure that it will move to a supported version of such software or to its replacement at least 6 months prior to the expiry of such support, unless otherwise specified by the Contracting Authority.

1.12.2 The Supplier shall continue to support current software versions whilst updating to future software versions, through to the end of the Framework Period or the expiry of the Call Off Agreements established, whichever is later.

1.13 **Information Exchange Policies**

1.13.1 Agreements on security conditions of the information exchange policies shall take into account the following:

(a) Management responsibilities for controlling and notifying transmission, despatch and receipt;

(b) Procedures for notifying sender, transmission, despatch and receipt;

(c) Minimum technical standards for transmission;

(d) Responsibilities and liabilities in the event of loss of data;

(e) Use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;

(f) Information and software ownership and responsibilities for data protection, software copyright compliance and similar considerations;

(g) Technical standards for recording and reading information and software;

(h) Any special controls that may be required to protect sensitive items.