Manslaughter and Corporate Homicide Act 2007. 4. principal exclusions 4.1 war and related perils. 4.2 nuclear/radioactive risks. 4.3 liability for death, illness, disease or bodily injury sustained by employees of the insured arising out of the course of their employment. 4.4 liability arising out of the use of mechanically propelled vehicles whilst required to be compulsorily insured by legislation in respect of such vehicles. 4.5 liability in respect of predetermined penalties or liquidated damages imposed under any contract entered into by the insured. 4.6 events more properly covered under a professional indemnity insurance policy. 4.7 liability arising from the ownership, possession or use of any aircraft or marine vessels. 4.8 liability arising from seepage and pollution unless caused by a sudden, unintended and unexpected occurrence.	
Section 2 – Professional Indemnity Insurance 1. insured *Consultant* 2. interest To indemnify the insured for all sums which the insured shall become legally liable to pay (including claimants costs and expenses) as a result of any claim or claims first made against the insured during the period of	Limit of indemnity The limit of indemnity shall be not less than ten million pounds (£10,000,000) in respect of any one claim without limit to the number of claims in any annual policy period, but ten million pounds (£10,000,000) any one claim and in the aggregate per annum for liability arising out of pollution or contamination (to the extent insured by the relevant policy) and one million pounds (£1,000,000) any one claim and in the

insurance specified in this Annex 4 by reason of any act, error and/or omission arising from or in connection with the Services and/or arising out of or in connection with this Contract. 3. cover features and extensions 3.1 loss of documents and computer records extension. 3.2 legal liability assumed under contract, duty of care agreements and collateral warranties. 3.3 retroactive cover from the date of this Contract in respect of any policy provided on a claims made policy wording. 4. principal exclusions 4.1 war and related perils. 4.2 nuclear/radioactive risks. 4.3 insolvency of the insured. 4.4 bodily injury, sickness, disease or death sustained by any employee of the insured arising out of the course of their employment.	aggregate per annum in respect of liability arising out of asbestos (to the extent insured by the relevant policy). Period of insurance From the date of this Contract until the *end of liability date*, renewable on an annual basis unless agreed otherwise by the parties.
Section 3 – Insurances required by law in the United Kingdom .1 The *Consultant* is required to meet its United Kingdom and all other statutory or insurances required by law in full. Insurances are required to comply with all statutory requirements including, but not limited to, United Kingdom employers' liability insurance and motor third party liability insurance. 2 Employers liability insurance 2.1 The limit of indemnity for the employers' liability insurance shall be any one occurrence inclusive of costs, the number of occurrences being unlimited in any annual	Limit of Indemnity The limit of indemnity shall be not less than the amount required by applicable law Period of insurance From the date of this Contract until Completion of the whole of the *service* or earlier termination of this Contract, renewable on an annual basis unless agreed otherwise by the parties.

period of insurance. 2.2 The employers' liability insurance shall contain an indemnity to principals clause. 3 Motor vehicle insurance 3.1 The limit of indemnity for motor vehicle third party liability insurance is any one occurrence the number of occurrences being unlimited in any annual period of insurance. 3.2 The motor vehicle insurance contains an indemnity to principals clause.	

Design Service Contract (DSC)

East Region
Scope

Annex 6

Information Systems

CONTENTS AMENDMENT SHEET

Amend. No.	Revision No.	Amendments	Initials	Date
0	0	Tender Issue	SEL	18/3/19

LIST OF CONTENTS

1 INFORMATION SYSTEMS

1.1 General Requirements

1.1.1 This Annex sets out the requirements in respect of Information Systems, including Systems that:

(1) are developed, procured, provided and made available to the *Client* by the *Consultant* for the purposes of performing the information requirements under this contract,

(2) are developed, procured and provided by the *Consultant* relating to its own corporate business and operations of performing the information requirements under this contract,

(3) are provided or made available by the *Client* for use by the *Consultant* for the purposes of performing the information requirements under this contract and

(4) are likely to be provided or made available by the *Client* for use by the *Consultant* for the purposes of performing the information requirements under this contract.

1.1.2 To the extent that the *Consultant* is required to create or maintain any information under this contract in electronic format, the *Consultant* ensures that, at all times:

(1) such a format is agreed with the *Client*;

(2) such information is maintained to allow fast and efficient electronic transfer of information to the *Client* or agreed third parties (including Consultants) without additional expenditure by the *Client* or the need for complex or expensive procedures or processes, and in any event in such format as complies with the *Client's* requirements for such transfer,

(3) such information is backed-up and copies are held in off-site storage in accordance with procedures agreed with the *Client* and

(4) it implements and complies with (and ensures that its Sub Consultants implement and comply with) all procedures for information back-up and off-site storage referred to in this paragraph.

1.1.3 The *Consultant* maintains all its Information Systems so as to enable their:

(1) segregation from any other computer or electronic storage devices, Systems, materials or information of the *Consultant* and

(2) transfer to the *Client* or an Incoming Consultant,

efficiently and without additional expense or delay immediately on termination or expiry of this contract.

1.2 *Consultant* Information Systems

1.2.1 The *Consultant*, at the *starting date*:

(1) has in place and provides or makes available to the *Client* appropriate Information Systems (and relevant hardware required to use such Information Systems) of the type set out in Table 1, to comply with the *Client* information requirements and the contract management information requirements,

(2) has in place Information Systems (electronic or otherwise) of the type set out in the non-exhaustive list in Table 2, to comply with the *Consultant* information requirements concerning its own corporate business and operations and

(3) has proof of compliance with the HMG Security Policy Framework (SPF) in respect of those Information Systems.

1.3 *Client* Information Systems

1.3.1 Unless otherwise agreed with the *Client*, the *Consultant* uses and interfaces with the *Client's* Current Systems (Table 3) and New Systems (Table 4) when available.

1.4 Access Requirements to Information Systems provided by the *Client*

1.4.1 Gateway access requirements

(1) The Business Information Gateway or its successor (the Gateway) is the interface through which:

- the *Consultant* is required to access the Highways Agency Business IT Network and the *Client* Information Systems held within Highways Agency Business IT Network and
- the *Client* may access one or more of the *Consultant* Information Systems and documents.

1.4.2 Unless otherwise agreed with the *Client*, the *Consultant* connects to the Gateway, using a Virtual Private Network specified by the *Client*.

1.4.3 The *Consultant*:

(1) Applies to the *Client* for authorisation to connect to the Gateway and connects to the Gateway in a manner to be specified by the *Client*,

(2) procures and pays for the installation and ongoing costs of connection of any of its premises or Information Systems to the Gateway through a telecommunications network, taking into account the data volume and the number of the *Consultant's* staff that it expects to use the link;,

(3) arranges suitable support and business continuity for connection to the Gateway,

(4) facilitates the installation and maintenance of the Gateway by the *Client's* Consultants,

(5) employs appropriate requirements and procedures, and trains its staff to operate the Current Systems,

(6) attends training in connection with the implementation, and where appropriate, the *Consultant* facilitates the implementation of New Systems and any other systems required by the *Client* and

(7) does not alter any documents provided by the *Client* through the Gateway (which are the exclusive property of the *Client*) without the prior acceptance of the *Client*.

1.4.4 The *Consultant* acknowledges that:

(1) the network technology underlying the Gateway is subject to change from time to time,

(2) access through and continued membership of the Gateway depends on the *Consultant* complying with (and the *Consultant* will comply with),

- Applicable user access requirements,
- Her Majesty's Government Security Policy Framework and
- other technical and security requirements set out in Annex 8 (Confidentiality and Security).

1.4.5 The connection point to the Gateway situated at the *Consultant's* premises is located in a room that is secured from theft, damage, unauthorised or malicious use to reduce risk to the connection point to the appropriate Impact Level as set out in Her Majesty's Government Security Policy Framework. The location remains fixed for the duration of the contract unless the *Consultant* requests and the *Client* approves a new location.

1.4.6 Other access requirements

(1) *Client* Information Systems not covered by clause 1.4.1 may be accessed through the Internet via third party hosts and using relevant software applications installed on *Consultant* systems. They are not subject to the same security and related access requirements that apply to *Client* Information Systems accessed through the Gateway.

(2) The *Consultant* may request authorisation and other details regarding Internet access to such *Client* Information Systems from the *Client*.

(3) For guidance, the right column in Table 3 and 4 indicates whether access to the *Client* Information Systems is required via the Gateway.

1.5 Access Requirements to Information Systems provided by the *Consultant*

1.5.1 The *Consultant* provides the *Client* remote access to the *Consultant* Information Systems and related documents:

(1) either through the Gateway; or

(2) through another interface agreed by the *Client*.

1.5.2 Any access required by the *Client* to systems provided by the *Consultant* must be made available via the Gateway or by other remote access methods agreed by the *Client*.

1.6 *Consultant* Security and User Access

1.6.1 The *Consultant* ensures that all persons who use *Client* Information Systems for or on behalf of the *Consultant* comply with the security requirements set out in Annex 8 (Confidentiality and Security),

1.6.2 The *Consultant* is responsible for determining any formal application and security clearance requirements to enable the *Client* to access any Information Systems provided by the *Consultant*. The *Consultant* informs the *Client* of those requirements, including timescales, not later than four weeks after the *starting date*.

1.6.3 The *Consultant* notifies the *Client's* IT Security Team and the help desk when staff with access to the *Client's* IT network, leave their employment.

1.6.4 The *Client* will suspend any accounts supplied to persons who use *Client* Information Systems for or on behalf of the *Consultant* if they are not used for a continuous period of six months.

1.6.5 The *Client* will delete any accounts supplied to persons who use *Client* Information Systems for or on behalf of the *Consultant* if they are not used for a

continuous period of thirteen months.

1.6.6 The *Client* will immediately suspend any accounts supplied to persons who use *Client* Information Systems for or on behalf of the *Consultant* if they are used by anyone other than the person for whom they were created (the "authorised user"). Accounts suspended will not be re-opened until a formal explanation for the account's misuse is provided by the *Consultant*, and in all these cases the *Client* will not be liable for any financial penalty or other expense incurred as a result of the *Consultant* failing to meet its commitments.

1.7 Software and Licences

1.7.1 The *Consultant* grants, or procures the grant of, licences required to allow the *Client* to use the Information Systems developed, procured or otherwise provided by the *Consultant* to the *Client*.

1.7.2 The *Consultant* has in place or procures its own licences required to use common software applications that it may require to be able to interface with, or to access Client Information Systems.

1.7.3 The *Consultant* applies to the *Client* for licences to allow the *Consultant* to use certain Information Systems provided or made available by the *Client*.

1.8 Not Used

1.9 Liaison and cooperation between *Client* and *Consultant*

1.9.1 The *Client* is adopting an Information Technology Infrastructure Library best practice approach for Information Communication and Technology (ICT) services. The *Consultant* will be expected to demonstrate a formal approach to its ICT service management through the development of an ICT strategy and make its ICT strategy available to the *Client*.

Table 1: Systems provided by the *Consultant* to meet *Client* and Contract Management Information Requirements		
Information System	**Description**	**Reference / Comment**
Electronic Document and Records Management	The *Consultant* operates an Information System for the management of electronic documents and records (including e-mails) which are created and maintained on behalf of the *Client*. Documents and records are defined in The Highways England Records Policy, a copy of which can be obtained from the *Client*. The *Consultant* seeks agreement through the *Client*, regarding the development and implementation of an Information System for electronically managing both the electronic and physical records which the *Consultant* creates and maintains on behalf of the *Client*. This Information System is required for the capture, retention and disposal of all electronic format documents and other records	

Table 2: Examples of Information Systems as provided by the *Consultant* to fulfil the requirements of the *Consultant*'s own business and effective delivery of the contract	
System	**Comment**
Quality Management System	It is expected that the *Consultant* will implement a quality management Information System which will ensure consistency and improvement of working practices. The *Consultant* should align its quality management Information System to meet the quality requirement used by the *Client*.
Collaboration System	It is expected that the *Consultant* will exploit collaboration technologies
Change Control System	This Information System will manage changes to processes and Systems
Customer Relationship Management System (CRM)	This Information System will manage the CRM strategy to ensure long lasting relationships with the *Consultant*'s customers The CRM Information System will seek to improve customer service by performing functions such as identifying what customers value the most and providing an effective mechanism to handle problems and complaints
Human Resource Management System (HRMS)	It is expected that the *Consultant* will use a HRMS to manage issues such as recruitment, skill sets, employee history and payroll
Financial Management System (FMS)	The *Consultant* will use a FMS to produce timely in-year and year-end management and accounting information
Project Management System	System to assist in the planning and organisation of activities in order to meet the *Consultant*'s objectives

Table 3: Current Systems provided by the *Client* to meet the contract management information requirements

Current Information System	Description	Reference / Comment	Access Via Gateway (Y/N)
WebTRIS - Traffic Information System and WEB	WebTRIS Highways England's Traffic Information System. It provides historic speed and flow data for the past 10 years in 15 minute time slices at count slices across the Highways England network. Data is currently taken from MIDAS, TMU, TAME count sites and also from legacy TRADS (Traffic Flow Database System) sites for older data. This contains hourly count data from inductive loops at approximately 1000 locations across the *Client's* network	Is available to all via the following link http://webtris.highwaysengland.co.uk/	N
Accident Incident Reporting System (AIRSweb)	The AIRSweb incident reporting Information System, allowing the completion of a single incident report online, which can be submitted to several organisations		N
Highways Agency Pavement Management System (HAPMS)	HAPMS is a set of IT systems that hold the following data sets: • Approved network master data set • pavement inventory master data set • pavement construction master data set • pavement condition master data set • inventory master data set • traffic data • accident data HAPMS also provides the following business capabilities: • Analysis and reporting of data both in map-based and textual formats • integrated tools for the whole life cost optimisation, of proposed pavement maintenance schemes	Access for information purposes only	Y

Table 3: Current Systems provided by the *Client* to meet the contract management information requirements

Current Information System	Description	Reference / Comment	Access Via Gateway (Y/N)
Structures Management Information System (SMIS)	SMIS provides operational support to structures management throughout the lifecycle of the structure	BD 62	Y
Highways Agency Geotechnical Data Management System (HAGDMS)	Internet hosted and GIS based geotechnical inventory.	HD22	N
Highways Agency Drainage Data Management System (HADDMS)	Shares the facilities developed for HAGDMS and exists on the same platform. This provides integrated geotechnical/drainage information.	Access for information purposes only	N
WebDAS	Database of departures from the *Client's* requirements and aspects not covered by requirements, including SHW specification departures.	CHE Memorandum 157/05 DMRB Vol1	Y

Table 3: Current Systems provided by the *Client* to meet the contract management information requirements

Current Information System	Description	Reference / Comment	Access Via Gateway (Y/N)
Technology Performance Management Services (TPMS)	TPMS is a set of IT systems to support the maintenance and management tasks for control and communications equipment. Currently provides the following functionality: • Technology Fault Management. • Technology Planned Maintenance recording. • Technology Asset Status recording (including for instance results of electrical testing). • Recording of asbestos risk in Technology equipment. • Recording the connection of Technology equipment via unmetered power supplies for payment for energy used by Technology. • Calculation of performance statistics on Technology equipment. Provision of data on Consultant performance to allow effective Performance Management.	More information at www.hatpms.com Access for information purposes only	N
HA Supply Chain Portal	An internet collaboration site for the *Client* and its partners		N
Highways Agency Management Information System (HAMIS)	Portal Information System providing access to HAGIS		Y
HAGIS	Stores information using the latest digital mapping, which allows users to view geographical data for a specific area of the UK by zooming in and out and using the built in GIS tools		Y

Table 3: Current Systems provided by the *Client* to meet the contract management information requirements

Current Information System	Description	Reference / Comment	Access Via Gateway (Y/N)
Highways Agency Environmental Information System (HA) EnvIS	EnvIS consists of specific environmental data supplied by *Consultants*, the HA and other bodies which is collated and displayed in a read only format in the Highways Agency Geographical Information System (HAGIS). This data is used to assist in managing the environment, within and surrounding the trunk road network, and in the review and reporting of the environmental performance of both *Consultants* and the *Client*.	DMRB Vol 10 Section 0	Y
Collaborative Management Toolkit (CMT)	Methodology and tool used to measure and report on *Consultant* 's performance. Relates to the ALDM contract types. The CMT allows for the production of the Motivating Success Toolkit scores.	The CMT has its own Performance Management Manual, setting out the background of the CMT, timelines for reporting and roles and responsibilities.	N
Lean Tracker System	A system used to capture and track lean benefits.	Annex 18	N
SAS tools for Drainage, Geos and Structures	Tools for the whole life cost optimisation of maintenance at a Scheme level. The *Provider* shall at its own cost use the SAS tools for Drainage Geotechnical and Structures assets as directed by the *Client* in support of specific proposals for individual Schemes.		N
Scheme Appraisal Report (SAR)	Allows appraisal details of Local Network Management Schemes to be submitted to the *Client*.	Value Management Requirements	N
AVIS	AVIS is a driven survey consisting of video cameras viewing multiple directions, with a simultaneous LiDAR survey. The LiDAR survey provides 3D point cloud data, accurate to 30mm - essentially a 3D model of the network. It provides an inventory of assets along with GIS files.		N

Table 3: Current Systems provided by the *Client* to meet the contract management information requirements

Current Information System	Description	Reference / Comment	Access Via Gateway (Y/N)
Highways Agency Logging Environment (HALOGEN)	HALOGEN is the central source for Highways Agency Traffic Management Systems (HATMS) logged data. It records setting, state change and fault information for signals, signs and emergency roadside telephones on England's motorway network.	More information at http://www.highways.gov.uk/specialist-information/halogen-online/	N
Planned Engineering Works (PEW) System	System for the notification of planned engineering works that impact on the operational availability or functionality of HA Traffic Management Systems (HATMS) or require access to RCC Equipment/Control Rooms.	www.ha-pew.org.uk/PEW/	N
National Faults Database (NFDB)	Database for manual entry of faults and issues relating to Highways Agency Traffic Management Systems (HATMS) and other operational systems.	www.nfdb.co.uk/	N
Cultural Heritage Database	Part of HAGIS. Database of Cultural Heritage items.	Part of HAGDMS	Y
Noise Assessment and Insulation System (NAIS)	GIS based tool for predicting noise impacts on the environment surrounding the trunk road network		N
Highways Agency Management Information System (HAMIS)	Portal Information System providing access to HAGIS		Y
HAGIS	Stores information using the latest digital mapping, which allows users to view geographical data for a specific area of the UK by zooming in and out and using the built in GIS tools		Y

Table 4: New Systems to be used by the *Consultant* when available			
New Information System	**Description**	**Reference / Comment**	**Access Via Gateway (Y/N)**
Integrated Asset Management Information System (IAM IS)	During the Contract Period it is intended that the IAM IS will replace the following Highways England data management systems: • Network Occupancy and EToN (SRW) • Pavement and Approved Network Model (HAPMS) • Structures (SMIS) • Geotechnical (HAGDMS) • Drainage (HADMS)	IAM IS Service Access Requirements Document (SARD) IAM IS Code of Connection (CoCo) NOMS – NRSWA 1991 as amended by TMA NOMS – Technical Specification for EToN Structures – BD62	N
Financial System	The *Client's* new finance and accounting Information System which supports major business transaction processing requirements.	Will replace the *Client's* System for Managing (SfM)	Y
CEMAR – (Contract Event Management Analytics and Reporting)	CEMAR is a cloud based NEC contract management system. It is a collaborative tool that requires the two parties Highways England (*Client*) and Contractors to manage contract events through the system as required by good practice NEC contract management. System features include the following: • Contract event management through registers e.g. Early Warnings, Compensation Events, Project Manager Instructions and more. • Application for payments / Invoices • Technical Queries and Defect management • General Communications • Multiple in built reports and charts and graphs proving reports and dashboards across one or multiple contracts to allow effective management of contracts through outputs on communication behaviour, cost, quality, risk and time.		N

Table 4: New Systems to be used by the *Consultant* when available			
New Information System	**Description**	**Reference / Comment**	**Access Via Gateway (Y/N)**
Finance and Works Management System (PB Confirm)	The *Client* intends to introduce a Finance and Works Management System which will be used to raise and manage works orders. The Contractor uses the system and provides such information to the *Client* as required to evidence the *service* provided and costs incurred to Provide the Service.	Scope	Y

Asset Delivery (AD)

Scope

Annex 8

Confidentiality, Security and Conflict of Interest

CONTENTS AMENDMENT SHEET

Amend. No.	Revision No.	Amendments	Initials	Date
0	0	Tender Issue	SEL	18/3/19

LIST OF CONTENTS

1 CONFIDENTIALITY AND SECURITY

1.1 Mandatory Obligations

1.1.1 The *Client* is required to adopt the Personnel Security requirements and management arrangements set down in Security Policy No 3: Personnel Security of HMG Security Policy Framework July 2014 issued by the Cabinet Office as amended from time to time (the "**Security Policy Framework**").

1.1.2 The Security Policy Framework is available to be downloaded from the Cabinet Office website and is referred to as a Reference Document in 3 Table 1. The Contractor familiarises himself with the objectives and principles embodied within the Security Policy Framework, in addition to the mandatory obligations abstracted from the Security Policy Framework and set down in this Annex.

1.1.3 The Contractor ensures that the appropriate level of Personnel Security is obtained and maintained for all Staff in accordance with the Security Policy Framework.

1.1.4 The *Service Manager* notifies the Contractor of any revisions to the Personnel Security requirements arising as a consequence of subsequent amendments to the Security Policy Framework.

1.2 Security Checks – Minimum Requirement

1.2.1 The Baseline Personnel Security Standard (BPSS) forms the minimum security check requirement for all Staff whose duties include

- working unsupervised by the *Client* at their premises, including offices, Regional Operations Centres (ROC), the National Traffic Operations Centre (NTOC), depots and any outstations owned and/or operated by the *Client*,
- usage of the *Client's* Information Systems
- handling the *Client's* information where that information is marked "OFFICIAL" with or without the SENSITIVE rider (formerly "PROTECT" or "RESTRICTED" which may still apply to historical documents), or

The *Service Manager* may notify the Contractor of a modification to the categories of Staff requiring BPSS checks at any time.

1.2.2 The BPSS is available to be downloaded from the Cabinet Office website and is referred to as a Reference Document in Annex Gen 3 Table 1.

1.2.3 Procedural and other details for ensuring compliance with the BPSS are set down in Part One below.

1.3 Security Checks – Additional Vetting Requirement

1.3.1 Where Staff require unrestricted access to or are required to regularly handle information marked SECRET or TOP SECRET), the *Service Manager* will additionally instruct the Contractor to carry out the appropriate level of National Security Vetting (NSV) as a change to the Scope.

1.3.2 Procedural and other details for ensuring compliance with NSV are set down in Part Two below.

PART ONE – BPSS COMPLIANCE

1.4 Procedures

1.4.1 The Contractor undertakes security checks to ensure the confidentiality, integrity and availability of the *Client's* asset.

1.4.2 The recruitment controls of the BPSS are required to have been carried out for all Staff to whom paragraph 1.2.1 applies prior to their employment on this contract. The recruitment control process is completed satisfactorily before an individual

- is issued with a security pass giving unsupervised access to the *Client's* premises,
- potentially has access to the *Client's* sensitive, possibly protectively-marked, information or
- is given access to the *Client's* IT network.

1.4.3 The Contractor takes all necessary measures to confirm that any previous security checking carried out on existing Staff meets the requirements of the BPSS, either in full or by exception using the risk management assessment process guidance contained in the Security Policy Framework. The Contractor must notify which Staff have met or not met these requirements. The *Client* may from time to time carry out independent audits of these findings and their methodology.

1.4.4 The Contractor should note that, for existing Staff with more than three years continuous employment and who have not had any access passes or permits revoked in that time, then the requirements for references in the BPSS check can be deemed to be discharged by a letter from a Director or Head of Personnel of the Contractor certifying the same. The remainder of the BPSS check must be carried out.

1.4.5 The Contractor rectifies any unacceptable gaps identified between the BPSS and existing security checking in accordance with the requirements of the BPSS.

1.4.6 Any new Staff to whom paragraph 1.2.1 applies are assessed strictly in accordance with the requirements of the BPSS.

1.4.7 The Contractor keeps full and auditable records of all security checks carried out on Staff and makes such records available to the *Client* or its appointed representatives for audit purposes at all reasonable times.

1.4.8 If

- the *Client* discovers any non-compliance with the requirements of the BPSS from the audit process,
- the Contractor fails to keep full records of security checks carried out on Staff or

- the Contractor fails to make such records available on reasonable request,

the *Service Manager* may

- invoke individual withdrawal of permits or passes to Staff,
- invoke systematic withdrawal of permits or passes to Staff or
- require that an independent audit of the Contractor's BPSS check procedure is undertaken at the expense of the Contractor.

The Contractor takes the appropriate action to immediately address any non-compliance with the BPSS notified to it by the *Service Manager*.

1.4.9 It should be noted that the BPSS does not constitute a formal security clearance. It is designed to provide a level of assurance as to the trustworthiness, integrity and reliability of the individual involved.

1.4.10 The Contractor submits a monthly report to the *Service Manager* on all its employees and former employees who no longer need Extranet access to *Client's* business IT network including nil returns.

1.5 Security check process for BPSS

1.5.1 The security check process of the BPSS follows the guidance provided in the BPSS.

1.5.2 The BPSS comprises verification of four main elements

- identity,
- nationality and immigration status (including an entitlement to undertake the work in question),
- employment history (past three years) and
- criminal record declaration (unspent convictions only).

Additionally, prospective Staff are required to give a reasonable account of any significant periods (six months or more in the past three years) of time spent abroad.

1.5.3 The specific requirements for verification of each of the four main elements are set down in Part II, The Verification Process of the BPSS. An outline description of the core requirements is included below but does not relieve the Contractor from his obligation to comply with all the requirements of the BPSS.

1.5.4 Information collected at each stage of the process is reviewed, assessed and recorded on the BPSS Verification Record (Annex B of the BPSS). References of the BPSS Verification Record forms are listed in this Annex as Annex A for information

1.6 Verification of Identity – Outline Requirements

1.6.1 Identity may be verified by physically checking a range of appropriate documentation (e.g. passport or other photo ID together with utility bills, bank statements etc) or by means of a commercially available ID verification service.

1.6.2 Only original documents should be used for identification purposes: copies are not appropriate.

1.6.3 There is no definitive list of identifying documents. The Contractor should note that not all documents listed in the BPSS are of equal value. The objective is a document that is issued by a trustworthy and reliable source, is difficult to forge, has been dated and is current, contains the owner's name, photograph and signature and itself requires some evidence of identity before being issued (e.g. passport or ID card).

1.6.4 National Insurance numbers (NINOs) can be obtained fraudulently and cannot be relied on as a sole means of establishing identity or right to work. Temporary numbers beginning with TN or ending in a letter from E to Z inclusive are not acceptable.

1.6.5 Where verification of identity is not straightforward but a decision is nevertheless taken to employ an individual, the Contractor notifies the *Service Manager* and records the matter on the Risk Register.

1.7 Nationality and Immigration Status (including an entitlement to undertake the work in question) – Outline Requirements

1.7.1 Nationality and Immigration Status may be verified by physically checking appropriate documentation or, in exceptional circumstances only, by means of an independent check of UK Visas and Immigration records.

1.7.2 The Contractor takes the necessary steps to ensure that an individual has the right to remain in the United Kingdom and undertake the work in question.

1.7.3 Checks need to be applied evenly and the Contractor needs to be aware of his obligations under the Race Relations Act 1976.

1.8 Employment history (past 3 years) – Outline Requirements

1.8.1 Employment history may be verified by checking with previous employers, by following up references or by means of a commercially available CV checking service or, in exceptional circumstances only, by means of an independent check of HMRC records.

1.8.2 To ensure that prospective employees are not concealing associations or gaps, the Contractor as a minimum verifies the individual's recent (past 3 years) employment or academic history.

2 CONFLICT OF INTEREST

2.1.1 The Contractor does not take an action which would cause a conflict of interest to arise in connection with this contract.

2.1.2 The Contractor notifies his employees and subcontractors (at any stage of remoteness from the *Client*), and procures that any subcontractor (at any stage of remoteness from the *Client*) notifies its employees, who are engaged in the performance of contractual duties that they must not take an action which would cause an actual or potential conflict of interest to arise in connection with the *service*.

2.1.3 The Contractor ensures that any employee of the Contractor or of any subcontractor (at any stage of remoteness from the *Client*) who is engaged in performance of contractual duties completes a declaration of interests and conflict of interests in the form set out in Appendix B. The Contractor issues to the *Service Manager* any completed declaration of interests and conflict of interests.

2.1.4 The Contractor:

- immediately notifies the *Service Manager* and
- procures that any subcontractor (at any stage of remoteness from the *Client*) immediately notifies the Contractor

if there is any uncertainty about whether a conflict of interest may exist or arise.

2.1.5 Following a notification from the Contractor, the *Service Manager* may

- require the Contractor to stop Providing the Services until any conflict of interest is resolved or
- require the Contractor to submit to the *Service Manager* for acceptance a proposal to remedy the actual or potential conflict of interest.

A reason for not accepting the submission is that it does not resolve the conflict of interest. The Contractor amends the proposal in response to any comments from the *Service Manager* and resubmits it to the *Service Manager* for acceptance. The Contractor complies with the proposal once it has been accepted.

2.1.6 A failure to comply with this section is treated as the Contractor having substantially hindered the *Client* or Others.

3 DISCLOSURE OF INFORMATION

3.1.1 The Contractor acknowledges that the *Client* is obliged to publish the provisions of the contract in accordance with Procurement Policy Note 01/17 entitled "The Transparency of Suppliers and Government to the Public" dated 16th February 2017 (or any later revision) (the "PPN"), except to the extent that any information in it is exempt from disclosure pursuant to the Freedom of Information Act 2000. The *Client* consults with the Contractor before deciding whether information is exempt, but the Contractor acknowledges that the *Client* has the final decision.

3.1.2 The Contractor:

- co-operates with and assists the *Client* to comply with its obligation under clause 3.1 above,
- agrees with the *Client* a schedule for the release to the public of information relating to the contract in accordance with the terms of the PPN,
- provides information to assist the *Client* in responding to queries from the public as required by the PPN and
- supplies the *Client* with financial data relating to the contract in the form and at the times specified in the PPN.