Highways England Company Limited

Scope

Information Systems & Security Systems

Annex 09

LIST OF CONTENTS

1 INFORMATION SYSTEMS

1.1 General Requirement

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

- are developed, procured, provided and made available to the *Client* by the *Consultant* for the purposes of performing the information requirements under this contract,
- are developed, procured and provided by the *Consultant* relating to its own corporate business and operations of performing the information requirements under this contract,
- 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
- 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

- such a format is agreed with the *Client,*
- 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,
- such information is backed-up and copies are held in off-site storage in accordance with procedures agreed with the *Client* and
- it implements and complies with (and ensures that its Sub *Consultant*s 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

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

- 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*

- 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 Section 1.9, to comply with the *Client* information requirements and the contract management information requirements,
- has in place Information Systems (electronic or otherwise) of the type set out in the non-exhaustive list in Table 1, to comply with the *Consultant* information requirements concerning its own corporate business and operations and
- has proof of compliance with the HMG Security Policy Framework (SPF) (see link in **Annex 02**) 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 2**) and new systems (**Table 3**) when available.

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

1.4.1 <u>Gateway access requirements</u>

- The Business Information Gateway or its successor (the Gateway) is the interface through which
- the *Consultant* is required to access the Highways England 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's* 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*

- 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*,

- 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,
- arranges suitable support and business continuity for connection to the Gateway,
- facilitates the installation and maintenance of the Gateway by the *Client's* Consultants,
- employs appropriate requirements and procedures, and trains its staff to operate the Current Systems,
- 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
- 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

- the network technology underlying the Gateway is subject to change from time to time,
- 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 confidentiality, technical and security requirements set out in this contract.

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 by using appropriate physical security controls 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 <u>Other access requirements</u>

- *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.

- The *Consultant* may request authorisation and other details regarding Internet access to such *Client* Information Systems from the *Client*.
- For guidance, the right column in **Table 2** and **3** indicates whether access to the *Client* Information Systems is required via the Gateway.
- The *Consultant* ensures that any device which is used to Process Client Data meets all of the security requirements set out in the National Cyber Security Centre (NCSC) End User Devices Platform Security Guidance, a copy of which can be found at: https://www.ncsc.gov.uk/guidance/end-user-device-security.

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

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

- either through the Gateway; or
- 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 *Client's* security requirements.

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, no 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* suspends any accounts supplied to persons who use *Client's* 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* deletes 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* immediately suspends 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"), or they are used from a device which is not issued by the *Consultant*, or they are used from a physical location not agreed with the *Client*. 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 Liaison and cooperation between *Client* and *Consultant*

1.8.1 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*.

1.9 Systems provided by the *Consultant* to meet *Client* and Contract Management Information Requirements

1.9.1 <u>Electronic Document and Records Management</u>

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 *Clients* record policy, a copy of which can be obtained from the *Client.*

1.9.2 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.

1.10 Information Systems provided by the *Consultant*

Table 1: 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
IT and Information Security Systems	It is expected that the *Consultant* will implement IT and Information Security systems to protect the confidentiality, integrity, and availability of this information it handles, and have those systems independently audited. The *Consultant* should align these systems to meet the *Client's* requirement for the services provided.
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
Primavera	Primavera (Management software) - enterprise project portfolio management software. It includes project management, product management, collaboration and control capabilities, and integrates with other enterprise software such as Oracle and SAP's ERP systems
Xactium	A Risk Management Tool
	or any revised systems notified by the *Client*

1.11 Current Systems provided by the *Client* to meet the contract management information requirements

Table 2 Current Systems

Current Information System	Description
Highways England Supply Chain Portal	An internet collaboration site for the *Client* and its partners
Highways England Management Information System (HAMIS)	Portal Information System providing access to HAGIS. A single platform for information for all directorates, from simple code look up utilities to more sophisticated forecasting and reporting tools.
Highway Agency Geographical Information System (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 Geographical Information Systems (GIS) tools

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; *Client* and *Consultant* 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, *Client* 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.
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
WebDAS	WebDAS provides service providers with an easy to use front end to Departures Approvals System (DAS) for submitting departures and searching past submissions. Database of departures from the *Client's* requirements and aspects not covered by requirements, including Specification for Highway Works (SHW) specification departures.
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.
Asset Visualisation and Information System (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.

1.12 New Systems to be used by the *Consultant* when available

Table 3 New Systems

New Information System	Description
Performance Management Information System	The *Client* may introduce a Performance Management Information System (PMIS) or other system for recording and reporting against the requirements of this Annex. When/ if provided, the *Consultant* provides performance data directly into the PMIS.

Finance and Works Management System	The *Client* intends to introduce a Finance and Works Management System which will be used to raise and manage works orders. The *Consultant* uses the system and provides such information to the *Client* as required to evidence the *service* provided and costs incurred to Provide the Service.

2 INFORMATION SECURITY

2.1 Security Plan

2.1.1 The *Consultant* prepares a robust information security plan complying with the *Client's* information security requirements and submits it to the *Client* for acceptance. The *Consultant* includes the security plan in its quality management system. The security plan complies with the requirements of ISO/IEC27001 and ISO/IEC27002 and includes procedures which

- ensure compliance with the Data Protection Legislations,
- protect information against accidental, unauthorised or unlawful processing, destruction, loss, damage or disclosure of Personal Data,
- ensure that unauthorised persons do not have access to Personal Data or to any equipment used to process Personal Data,
- protect IT systems from viruses and similar threats,
- provide for disaster recovery, and in particular ensure that the Personal Data is safely backed-up and
- provide for the vetting of its employees and subcontractors' staff in accordance with the *Client's* staff vetting procedures

2.1.2 The *Consultant* provides training for its employees and subcontractors in accordance with the security plan.

2.1.3 The *Consultant* does not use any confidential or proprietary information provided to or acquired by it for any purpose other than to Provide the Service. The *Consultant* implements measures to prevent the disclosure of such information by its employees or subcontractors.

2.1.4 The *Client's* security policy is set out in the documents "Statement of Highways England's IT Security Policy" and Chief Information Officer Memos 01/09, 05/08 and 04/08 (see link in **Annex 02)**.

2.1.5 At the end of the *service period* or termination, the *Consultant* gives to the *Client* all Personal Data held by them in a format specified by the *Client* (or any subcontractor at any stage of remoteness from the *Client*

and Sub-Processor) and destroys, and procures any subcontractor (at any stage of remoteness from the *Client*) and Sub-Processor destroys, any electronic and paper copies of such data in a secure manner.

2.1.6 Where the *Consultant* obtains or collects Personal Data on behalf of the *Client*, the *Consultant*

- provides to Data Subjects a data protection notice in a form accepted by the *Client* informing the Data Subject of the identity of the *Client*, the identity of any data protection nominated lead it may have appointed, the purpose or purposes for which their Personal Data will be processed and any other information which is necessary having regard to the specific circumstances in which the Personal Data is, or is to be, processed to enable processing in respect of the Data Subject to be fair and
- where applicable, obtains all necessary consents for the processing of Personal Data.

2.1.7 A failure to comply with this section is treated as a substantial failure by the *Consultant* to comply with its obligations.

2.2 Data Collection System

2.2.1 The *Consultant* captures all costs within a data collection system identified by the *Client* in Work Breakdown Structure (WBS) form as a minimum for use on the contract in respect of applications for payment.

2.2.2 If the *Client's* minimum requirements for the *Consultant's* data collection system are not met, the *Consultant* is required to effect such modifications or enhancements to its own data collection system, or those of its supply chain, as are required, to meet the *Client's* requirements.

2.2.3 Any investment costs associated with implementing such enhancements are borne totally by the *Consultant* or its subcontractor (at any stage of remoteness from the *Client)* and not charged back to the *Client*.

2.3 Data Handling Requirements

2.3.1 The *Consultant* complies with the *Client*'s data handling policy (see link in **Annex 02)** when working on the *Client*'s systems or handling the *Client*'s data.

When processing personal data on behalf of the *Client*, the *Consultant* submits a security plan to the *Client* for acceptance that complies with the requirements of ISO/IEC27001 and ISO/IEC27002.

2.3.2 A system on which the *Consultant* holds any *Client*'s data, including back-up data, is a secure system that complies with the security policy.

2.4 Breech of Security

2.4.1 "Breach of Security" is the occurrence of:

- any unauthorised access to or use of the Information Systems, the *Client* Premises, the Sites, the Service Provider System, the *Client* System (to the extent that it is under the control of the *Consultant*) and/or any IT, information or data (including the Confidential Information and the *Client* Data) used by the *Client* and/or the *Consultant* in connection with this contract; and/or
- the loss (physical or otherwise), corruption and/or unauthorised disclosure of any information or data (including the Confidential Information and the *Client* Data), including any copies of such information or data, used by the *Client* and/or the *Consultant* in connection with this contract.

2.4.2 The *Consultant* develops and maintain a Security Incident management and reporting policy in accordance with the Customer's 'Information Security Incident Management Requirements' (see link in **Annex 02)** and ISO27001. The *Consultant* makes a full log of Security Incidents available to the *Client* on request, and in any case on a quarterly basis. All Security Incidents defined as a Major Incident will be reported to the *Client* as soon as practicable (in any case within twenty four (24) hours of the *Consultant* becoming aware of the Incident).

2.4.3 The Security Incident Management Process (see link in **Annex 02**), as a minimum, requires the *Consultant* upon becoming aware of a Breach of Security or an attempted Breach of Security to:

- immediately take all reasonable steps (which includes any action or changes reasonably required by the *Client* which will be completed within such timescales as the *Client* may reasonably require) necessary to:
  - minimise the extent of actual or potential harm caused by such Breach of Security
  - remedy such Breach of Security to the extent possible and protect the integrity of the Information System against any such potential or attempted Breach of Security
  - apply a tested mitigation against any such Breach of Security or potential or attempted Breach of Security and, provided that reasonable testing has been undertaken by the *Consultant*, if the mitigation adversely affects the *Consultant*'s ability to deliver the Services so as to meet any Performance Indicator, the *Consultant* is granted relief against the failure to meet such affected Performance

Indicator for such period as the *Client*, acting reasonably, may specify by written notice to the Service Provider; and

- prevent a further Breach of Security or attempted Breach of Security in the future exploiting the same root cause failure

- as soon as reasonably practicable and, in any event, within 2 working days, following the Breach of Security or attempted Breach of Security, provide to the *Client* full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the *Client*.

2.4.4 In the event that any action is taken in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the information security management system (ISMS) outlined in ISO 27001 and/or the risk management with the Baseline Personnel Security standard outlined in the HMG SPF and/or this contract, then such action and any required change to the Information System and/or risk management will be completed by the *Consultant* at no cost to the *Client*.