Highways England Company Limited

Concrete Roads Framework - Reconstruction

Scope

Information Systems & Security

Annex 09

CONTENTS AMENDMENT SHEET

Amend. No.	Revision No.	Amendments	Initials	Date
0	0	Tender Issue	SOS	04/08/2020

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 *Contractor* for the purposes of performing the information requirements under the contract,
- are developed, procured and provided by the *Contractor* relating to its own corporate business and operations of performing the information requirements under the contract,
- are provided or made available by the *Client* for use by the *Contractor* for the purposes of performing the information requirements under the contract and
- are likely to be provided or made available by the *Client* for use by the *Contractor* for the purposes of performing the information requirements under the contract.

1.1.2 To the extent that the *Contractor* is required to create or maintain any information under the contract in electronic format, the *Contractor* 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 Others without additional expenditure by the *Client* or Others, 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 *Contractor*s implement and comply with) all procedures for information back-up and off-site storage referred to in this paragraph.

1.1.3 The *Contractor* maintains all its Information Systems so as to enable its

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

- transfer to the *Client* or an Incoming Contractor,

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

1.2 *Contractor* Information Systems

1.2.1 The *Contractor* 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 *Contractor* 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 & Training

1.3.1 Unless otherwise agreed with the *Client*, the *Contractor* uses and interfaces with the *Client's* current systems (Table 2, in 1.10 below) and new systems (Table 3) when available.

1.3.2 The *Client* provides relevant training for all relevant systems provided by the *Client* that are listed in this Annex.

1.3.3 The *Contractor* proposes a list of appropriate Staff to be trained for each requirement for acceptance by the *Project Manager*. The *Contractor* liaises with the *Project Manager* to programme the training to optimise efficiencies.

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 *Contractor* is required to access the *Client* business IT network and the *Client* Information Systems and
- the *Client* may access one or more of the *Contractor's* Information Systems and documents.

1.4.2 Unless otherwise agreed with the *Client*, the *Contractor* connects to the Gateway, using a virtual private network specified by the *Client*.

1.4.3 The *Contractor*

- 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 *Contractor's* staff that it expects to use the Gateway,
- arranges suitable support and business continuity for connection to the Gateway,
- facilitates the installation and maintenance of the Gateway by the *Client's* or Other'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 *Contractor* 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 *Contractor* 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 *Contractor* complying with (and the *Contractor* will complies with)
- applicable user access requirements,
- Her Majesty's Government Security Policy Framework and
- other confidentiality, technical and security requirements set out in the contract.

1.4.5 The connection point to the Gateway situated at the *Contractor'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 *Contractor* requests and the *Client* approves a new location.

1.4.6 Other access requirements

- *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 *Contractor* systems. They are not subject to the same security and related access requirements that apply to *Client* Information Systems accessed through the Gateway.
- The *Contractor* may request authorisation and other details regarding Internet access to such *Client* Information Systems from the *Client*.
- The *Contractor* ensures that any device which is used to process *Client* data meets all of the security requirements set out in the statement Security Centre (NCSC) "End User Devices Platform Security Guidance" (see link in **Annex 02**).

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

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

- 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 *Contractor* must be made available via the Gateway or by other remote access methods agreed by the *Client*.

1.6 *Contractor* Security and User Access

1.6.1 The *Contractor* ensures that all persons who use *Client* Information Systems for or on behalf of the *Contractor* comply with the *Client's* security requirements.

1.6.2 The *Contractor* is responsible for determining any formal application and security clearance requirements to enable the *Client* to access any Information Systems provided by the *Contractor*. The *Contractor* informs the *Client* of those requirements, including timescales, no later than four weeks after the *starting date*.

1.6.3 The *Contractor* immediately notifies the *Client's* IT Security Team (see link in **Annex 02**) 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 *Contractor* 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 *Contractor* 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 *Contractor* 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 *Contractor*, 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 *Contractor*, and in all these cases the *Client* is not liable for any financial penalty or other expense incurred as a result of the *Contractor* failing to meet its commitments.

1.7 Software and Licences

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

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

1.8 Liaison and cooperation between *Client* and *Contractor*

1.8.1 The *Client* is adopting an Information Technology Infrastructure Library best practice approach for Information Communication and Technology (ICT) services. The *Contractor* demonstrates 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 *Contractor* to meet *Client* and Contract Management Information Requirements

1.9.1 Electronic Document and Records Management

The *Contractor* 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 *Contractor* 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 *Contractor* 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 *Contractor*

Table 1: Information Systems as provided by the *Contractor* to fulfil the requirements of the *Contractor's* own business and effective delivery of the contract

System	Comment
IT and Information Security Systems	The *Contractor* implements IT and Information Security systems to protect the confidentiality, integrity, and availability of this information it handles, and have those systems independently audited. The *Contractor* aligns these systems to meet the *Client's* requirement for the services provided.
Quality Management System	It is expected that the *Contractor* will implement a quality management Information System which will ensure consistency and improvement of working practices. The *Contractor* should align its quality management Information System to meet the quality requirement used by the *Client.*
Collaboration System	The *Contractor* fully utilises collaboration technologies.
Change Control System	This Information System will manage changes to processes and systems.
Human Resource Management System (HRMS)	The *Contractor* uses a HRMS to manage issues such as recruitment, skill sets, employee history and payroll.

Financial Management System (FMS)	The *Contractor* uses 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 *Contractor*'s objectives.
Korec/Trimble K-mobile License	Surveying and mapping system, video enabled, Laser scanning, 3D modelling system, construction and site control, augmented reality and BIM model capable – enables viewing and access to information held by the *Client.*
Impulse geophysics	Video enable, 2D GPR – This is to enable viewing of visual and GPR survey data collected by the *Client.*
	or any revised systems notified by the *Project Manager*

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
Customer Relationship Management System (CRM)	The CRM is a Microsoft Dynamics 365 system that manages the CRM strategy to ensure long lasting relationships with the Contractor's customers. It acts as one central and consistent stakeholder / customer database where all interactions with stakeholders and associated tasks are managed on one platform. It is associated to the Confirm system.
HAMIS	The *Client's* Management Information System. 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.

HAGIS	The *Client's* Geographical Information System. 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 *Contractor* 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, and • 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.
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.
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 Motorway Incident Detection and Automatic Signalling (MIDAS), Traffic Monitoring Units (TMU), Traffic Appraisal, Modelling and Economics (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

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
Structures Management Information System (SMIS)	SMIS provides operational support to structures management throughout the lifecycle of the structure. This system is being phased out. Note: IAM IS has replaced SMIS. SMIS is currently available as “read only” – access will only be provided if or when required.
Highways Agency Geotechnical Data Management System (HAGDMS)	Internet hosted and GIS based geotechnical inventory. Holds details of the Highways England geotechnical asset, together with geological maps, borehole details, and specialist reports.
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.
Lean Tracker System	A system used to capture and track lean benefits.
Cultural Heritage Database	Part of HAGIS. Database of Cultural Heritage items.

Highways Agency Environmental Information System (HA) EnvIS	EnvIS consists of specific environmental data supplied by *Contractors*, 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 *Contractors* and the *Client*.
Scheme Analysis System (SAS) tools for Drainage, Geos and Structures	Tools for the whole life cost optimisation of maintenance at a Scheme level. The *Contractor* 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.
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 regional Control Centre (RCC) Equipment/Control Rooms.
Noise Assessment and Insulation System (NAIS)	GIS based tool for predicting noise impacts on the environment surrounding the trunk road network
Severe Weather Information System (SWIS)	Provides the *Client* with information on the state of the network and weather related incidents
Network Occupancy Management System (NOMS)	The *Client* provides a Network Occupancy Management System (NOMS) as part of the Integrated Asset Management Information System (IAMIS) that is fully compliant with the national specification for the Electronic Transfer of Notifications (EToN) and is used to • record, update and manage all occupancies on the Affected Property including their delay and impact, • record, update and manage all information as necessary for the fulfilment of obligations relating to: • Traffic Management Act 2004 • New Roads and Street Works Act 1991 • other legislation associated to the delivery of the TMA 2004 s16 Network Management Duty and associated secondary legislation NOMS provides direct information feeds to external stakeholders for public use and feeds to the *Clients* National Traffic Information Service (NTIS) for publication to customers.

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) • structures (SMIS) IAM IS provides functionality for the asset support contractor to manage customer enquiries, record defects, schedule inspections and record incident data. This information will be available to the *Client* to better understand the condition of the asset and manage the contract using enhanced reporting capabilities. Information within the *Client's* current data systems, HAGDMS, HADDMS, HAPMS and SMIS is incorporated in to IAM IS.
PBA Web Portal	Cost Intelligence tool for capturing payments to Tier 2 suppliers from Project Bank Accounts on live contracts.

1.12 New Systems to be used by the *Contractor* when made available

Table 3 New Systems	
New Information System	**Description**
Financial System	The *Client's* new finance and accounting Information System which supports major business transaction processing requirements.
Emergency Services Network (ESN)	ESN will provide 'next generation integrated critical voice and broadband data services' and will replace Airwave.
Green Claims	System to enable the electronic submission of Green Claims information.
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 *Contractor* provides performance data directly into the PMIS.

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 *works* provided and costs incurred to Provide the Works.
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 will provide functionality for the asset support contractor to manage customer enquiries, record defects, schedule inspections and record incident data. This information will be available to the *Client* to better understand the condition of the asset and manage the contract using enhanced reporting capabilities. Information within the *Client's* current data systems, HAGDMS, HADDMS, HAPMS and SMIS will be incorporated in to IAM IS.
PRISM	Cost management system.
Xactium	A Risk Management Tool.

2 INFORMATION SECURITY

2.1 Security Plan

2.1.1 The *Contractor* prepares a robust information security plan complying with the *Client's* information security requirements and submits it to the *Project Manager* for acceptance. The *Contractor* 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 *Contractor* provides training for its employees and Subcontractors in accordance with the security plan.

2.1.3 The *Contractor* does not use any confidential or proprietary information provided to or acquired by it for any purpose other than to Provide the Works. The *Contractor* 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 2)**.

2.1.5 On Completion, or if requested by the *Project Manager*, the *Contractor* gives to the *Project Manager* all Personal Data held by them in a format specified by the *Project Manager* (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 *Contractor* obtains or collects Personal Data on behalf of the *Client*, the *Contractor*

- provides to Data Subjects a data protection notice in a form accepted by the *Project Manager* 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 *Contractor* to comply with its obligations.

2.1.8 *Project Manager* to undertake information risk assessment in line with the *Client*'s guidance and set out any constraints on how the *Contractor* handles personal data; include any further contract specific requirements, such as the need for the security plan to comply with ISO/IEC27002 and ISO/IEC27001.

2.2 Data Collection System

2.2.1 The *Contractor* 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 *Contractor's* data collection system are not met, the *Contractor* 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.

2.3 Data Handling Requirements

2.3.1 The *Contractor* 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 *Contractor* submits a security plan to the *Project Manager* for acceptance that complies with the requirements of ISO/IEC27001 and ISO/IEC27002.

2.3.2 A system on which the *Contractor* 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 *Contractor*) and/or any IT, information or data (including the Confidential Information and the *Client* Data) used by the *Client* and/or the *Contractor* in connection with the 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 *Contractor* in connection with the contract.

2.4.2 The *Contractor* 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 *Contractor* makes a full log of Security Incidents available to the *Project Manager* on request, and in any case on a quarterly basis. All Security Incidents defined as a Major Incident will be reported to the *Project Manager* as soon as practicable (in any case within twenty four (24) hours of the *Contractor* becoming aware of the Incident).

2.4.3 The Security Incident management process (see **Annex 02**), as a minimum, requires the *Contractor* 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 *Project Manager* which will be completed within such timescales as the *Project Manager* 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 *Contractor*, if the mitigation adversely affects the *Contractor*'s ability to deliver the *works* so as to meet any Performance Indicator, the *Contractor* is granted relief against the failure to meet such affected Performance Indicator for such period as the *Project Manager*, acting reasonably, may specify by written notice to the *Contractor*, 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 *Project Manager* full details of the breach of security or attempted breach of security, including a root cause analysis where required by the *Project Manager*.

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 the contract, then such action and any required change to the Information System and/or risk management will be completed by the *Contractor* at no cost to the *Client*.