Call-Off Schedule 1 (Transparency Reports)

1.1 The Supplier recognises that the Buyer is subject to PPN 01/17 (Updates to transparency principles v1.1 (https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles). The Supplier shall comply with the provisions of this Schedule in order to assist the Buyer with its compliance with its obligations under that PPN.

1.2 Without prejudice to the Supplier's reporting requirements set out in the Framework Contract, within three (3) Months of the Start Date the Supplier shall submit to the Buyer for Approval (such Approval not to be unreasonably withheld or delayed) draft Transparency Reports consistent with the content requirements and format set out in the Annex of this Schedule.

1.3 If the Buyer rejects any proposed Transparency Report submitted by the Supplier, the Supplier shall submit a revised version of the relevant report for further Approval within five (5) days of receipt of any notice of rejection, taking account of any recommendations for revision and improvement to the report provided by the Buyer. If the Parties fail to agree on a draft Transparency Report the Buyer shall determine what should be included. Any other disagreement in connection with Transparency Reports shall be treated as a Dispute.

1.4 The Supplier shall provide accurate and up-to-date versions of each Transparency Report to the Buyer at the frequency referred to in the Annex of this Schedule.

Annex A: List of Transparency Reports

Title	Content	Format	Frequency
[Performance]	[ ]	[ ]	[ ]
[Call-Off Contract Charges]	[ ]	[ ]	[ ]
[Key Subcontractors]	[ ]	[ ]	[ ]
[Technical]	[ ]	[ ]	[ ]
[Performance management]	[ ]	[ ]	[ ]

Call-Off Schedule 2 (Staff Transfer)

Not used.

Call-Off Schedule 3 (Continuous Improvement)

1. Buyer's Rights

1.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), the Buyer may give CCS the right to enforce the Buyer's rights under this Schedule.

2. Supplier's Obligations

2.1 The Supplier must, throughout the Contract Period, identify new or potential improvements to the provision of the Deliverables with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables and their supply to the Buyer.

2.2 The Supplier must adopt a policy of continuous improvement in relation to the Deliverables, which must include regular reviews with the Buyer of the Deliverables and the way it provides them, with a view to reducing the Buyer's costs (including the Charges) and/or improving the quality and efficiency of the Deliverables. The Supplier and the Buyer must provide each other with any information relevant to meeting this objective.

2.3 In addition to Paragraph 2.1, the Supplier shall produce at the start of each Contract Year a plan for improving the provision of Deliverables and/or reducing the Charges (without adversely affecting the performance of this Contract) during that Contract Year (**"Continuous Improvement Plan"**) for the Buyer's Approval. The Continuous Improvement Plan must include, as a minimum, proposals:

2.3.1 identifying the emergence of relevant new and evolving technologies;

2.3.2 changes in business processes of the Supplier or the Buyer and ways of working that would provide cost savings and/or enhanced benefits to the Buyer (such as methods of interaction, supply chain efficiencies, reduction in energy consumption and methods of sale);

2.3.3 new or potential improvements to the provision of the Deliverables including the quality, responsiveness, procedures, benchmarking methods, likely performance mechanisms and customer support services in relation to the Deliverables; and

2.3.4 measuring and reducing the sustainability impacts of the Supplier's operations and supply-chains relating to the Deliverables, and identifying opportunities to assist the Buyer in meeting their sustainability objectives.

2.4 The initial Continuous Improvement Plan for the first (1st) Contract Year shall be submitted by the Supplier to the Buyer for Approval within one hundred (100) Working Days of the first Order or six (6) Months following the Start Date, whichever is earlier.

2.5 The Buyer shall notify the Supplier of its Approval or rejection of the proposed Continuous Improvement Plan or any updates to it within twenty (20) Working Days of receipt. If it is rejected then the Supplier shall, within ten (10) Working Days of receipt of notice of rejection, submit a revised Continuous Improvement Plan reflecting the changes required. Once Approved, it becomes the Continuous Improvement Plan for the purposes of this Contract.

2.6 The Supplier must provide sufficient information with each suggested improvement to enable a decision on whether to implement it. The Supplier shall provide any further information as requested.

2.7 If the Buyer wishes to incorporate any improvement into this Contract, it must request a Variation in accordance with the Variation Procedure and the Supplier must implement such Variation at no additional cost to the Buyer or CCS.

2.8 Once the first Continuous Improvement Plan has been Approved in accordance with Paragraph 2.5:

2.8.1 the Supplier shall use all reasonable endeavours to implement any agreed deliverables in accordance with the Continuous Improvement Plan; and

2.8.2 the Parties agree to meet as soon as reasonably possible following the start of each quarter (or as otherwise agreed between the Parties) to review the Supplier's progress against the Continuous Improvement Plan.

2.9 The Supplier shall update the Continuous Improvement Plan as and when required but at least once every Contract Year (after the first (1st) Contract Year) in accordance with the procedure and timescales set out in Paragraph 2.3.

2.10 All costs relating to the compilation or updating of the Continuous Improvement Plan and the costs arising from any improvement made pursuant to it and the costs of implementing any improvement, shall have no effect on and are included in the Charges.

2.11 Should the Supplier's costs in providing the Deliverables to the Buyer be reduced as a result of any changes implemented, all of the cost savings shall be passed on to the Buyer by way of a consequential and immediate reduction in the Charges for the Deliverables.

2.12 At any time during the Contract Period of the Call-Off Contract, the Supplier may make a proposal for gainshare. If the Buyer deems gainshare to be applicable then the Supplier shall update the Continuous Improvement Plan so as to include details of the way in which the proposal shall be implemented in accordance with an agreed gainshare ratio.

Call-Off Schedule 4 (Call Off Tender)

Not used.

Call-Off Schedule 5 (Pricing Details)

Not Used.

Call-Off Schedule 6 (ICT Services)

Not Used

Call-Off Schedule 7 (Key Supplier Staff)

Not used.

Call-Off Schedule 8 (Business Continuity and Disaster Recovery)

Not used.

Call-Off Schedule 9 (Security)

Part A: Short Form Security Requirements

1. Definitions

1.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Breach of Security"	the occurrence of: a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract, in either case as more particularly set out in the Security Policy;
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time;

2. Complying with security requirements and updates to them

2.1 The Buyer and the Supplier recognise that, where specified in Framework Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.

2.2 The Supplier shall comply with the Security Policy and the requirements in this Schedule including the Security Management Plan and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.3 The Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any

increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

2.5 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Variation Procedure the Supplier shall continue to provide the Deliverables in accordance with its existing obligations.

3. Security Standards

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Deliverables and/or the Government Data; and

3.2.4 complies with the Security Policy and the ICT Policy.

3.3 The references to standards, guidance and policies contained or set out in Paragraph 3.2 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer's Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer's Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. Security Management Plan

4.1 Introduction

4.1.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Schedule. The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

4.2 **Content of the Security Management Plan**

4.2.1 The Security Management Plan shall:

(a) comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

(b) identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

(c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with

access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

(d) be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

(e) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Contract;

(f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and the Security Policy; and

(g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

4.3 **Development of the Security Management Plan**

4.3.1 Within twenty (20) Working Days after the Start Date and in accordance with Paragraph 4.4, the Supplier shall prepare and deliver to the Buyer for Approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan.

4.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours

to ensure that the approval process takes as little time as possible, and in any event, no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.3.3 The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph 4.3.2. However a refusal by the Buyer to Approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.3.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3.2 or of any change to the Security Management Plan in accordance with Paragraph 4.4 shall not relieve the Supplier of its obligations under this Schedule.

4.4 **Amendment of the Security Management Plan**

4.4.1 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Deliverables and/or associated processes;

(c) any change to the Security Policy;

(d) any new perceived or changed security threats; and

(e) any reasonable change in requirements requested by the Buyer.

4.4.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

(a) suggested improvements to the effectiveness of the Security Management Plan;

(b) updates to the risk assessments; and

(c) suggested improvements in measuring the effectiveness of controls.

4.4.3 Subject to Paragraph 4.4.4, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.4.1, a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

4.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without

prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. Security breach

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

5.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

(a) minimise the extent of actual or potential harm caused by any Breach of Security;

(b) remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

(c) prevent an equivalent breach in the future exploiting the same cause failure; and

(d) as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security policy or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.

Part B – Annex 1:

Baseline security requirements

6. Handling Classified information

6.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

7. End user devices

7.1 When Government Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the UK Government Communications Electronics Security Group ("CESG") to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA").

7.2 Devices used to access or manage Government Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the CESG End User Devices Platform Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the CESG guidance, then this should be agreed in writing on a case by case basis with the Buyer.

8. Data Processing, Storage, Management and Destruction

8.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Government Data will be subject to at all times.

8.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

8.3 The Supplier shall:

8.3.1 provide the Buyer with all Government Data on demand in an agreed open format;

8.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;

8.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and

8.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

9. Ensuring secure communications

9.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of pan-government accredited encrypted networking services via the Public Sector Network ("PSN") framework (which makes use of Foundation Grade certified products).

9.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

10. Security by design

10.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Government Data.

10.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (https://www.ncsc.gov.uk/content/files/protected_files/article_files/Guidance_to_CESG_Cerification_for_Cyber_Security_IA_Professionals_-_issue_2.2_-_Oct_16%20-%20version.pdf) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

11. Security of Supplier Staff

11.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

11.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Government Data.

11.3 The Supplier shall prevent Supplier Staff who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Government Data except where agreed with the Buyer in writing.

11.4 All Supplier Staff that have the ability to access Government Data or systems holding Government Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

11.5 Where the Supplier or Subcontractors grants increased ICT privileges or access rights to Supplier Staff, those Supplier Staff shall be granted only those permissions necessary for them to carry out their duties. When staff no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

12. Restricting and monitoring access

12.1 The Supplier shall operate an access control regime to ensure all users and administrators of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the ICT Environment that they require. The Supplier shall retain an audit record of accesses.

13. Audit

13.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

13.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier). To the extent the design of the Deliverables allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

13.1.2 Security events generated in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and shall include: privileged account logon and logoff events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

13.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.

13.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 Months.

Part B – Annex 2 – Security Management Plan

Security Policy Guidance for Highways England Staff Version 6.0 • 2017

Part 1- Introduction

The policy covers everyone who works for Highways England, whether permanent or temporary staff. It refers to all those who have access to the business assets and infrastructure.

We all have a responsibility for protecting ourselves and each other; our information and our assets and infrastructure.

The policy sets out the basic requirements of security performance within Highways England and the procedures that are in place to enable you to meet those requirements. Contact details for the security team and security liaison officers throughout the estate are included. They can be contacted for help and advice.

Links to Policies that include requirements and guidance for handling protectively marked documents, detailed definitions of the protective marking system and instructions for their storage and transmission are also included.

Rules and procedures covering access to and use of the computer systems can be found on the Portal within the ICT security advice section of the Finance & Business Services pages. The information is there to enable you to meet security requirements, however, if you have any queries, please address them in the first instance to your line manager or Highways England contract manager.

The Seven Golden Rules

1. Always wear your security pass in Highways England buildings and remove it before leaving the building. Challenge anyone whose pass is not visible in our buildings. Report lost or stolen passes immediately to your building Security Liaison Officer
2. Inform your Security Liaison Officer if you see anything that concerns you.
3. Keep valuable official and personal property locked away.
4. Lock up your storage units when leaving the room.
5. Clear your desk when going home or if away for long periods during the day, lock away all working papers and removable media.
6. Never tell anyone your computer password.
7. Make sure you lock your computer using “Ctrl + Alt + Del” followed by “Return”, whenever you leave your PC or laptop unattended.

Part 2 – Personnel Security approval and clearance:

BPSS Security approval:

Baseline Personnel Security Standard (BPSS) approval:

 The Baseline Personnel Security Standard (BPSS) check is carried for

all permanent staff, consultants and contractors. It consists of:

- ID verification
- 3 years’ employment references (including verifying any gaps in employment)
- Nationality and right to work checks

Basic Disclosure Scotland certificate (Criminal Records Check)

Successful completion of this check is a precursor to allowing unescorted access to our buildings and access to our IT systems

NUNS Application (New User Name System):

An application for IT access will be submitted by the Highways England Hiring Manager for contractors who will have access to Highways England offices, and the business or Area Team working with the Highways England business partners whose staff need Extranet access to some systems on our business IT network. These applications will be checked and wherever possible approved by the Highways England security team for contractors, and the IT security team for Extranet users.

Security Vetting:

Under the Government's Security Vetting Policy, staff occupying certain sensitive posts require a Security Clearance (SC) or Counter Terrorism Check (CTC). This is the decision of the hiring manager and not the Security Team, who must be contacted by the Line Manager to start the process.

CTC and SC checks are carried out by the DFT. Their decision is final, and they will not enter into any discussion regarding it.

Part 3 - Physical Security

For the safety and security of staff across the estate, and in compliance with the HMG Security Policy Framework, certain physical security measures are put into place.

These measures include:

Security Guards

Entry to all Highways England offices is through a staffed security control point. Members of staff and visitors will be issued with a security pass that will allow them access to the offices. Security guards are required to check all passes upon staff entry into each building unless there are automated, controlled access points in place. Visitors will be held in the reception area until their host arrives to escort them.

Internal door codes

In some buildings, internal access and access to the car park is gained through door lock codes. It is the responsibility of the local Facilities Manager to review and modify the codes in use on a six-monthly basis.

Identification passes

All permanent and temporary members of staff will be issued with a Highways England identification pass which will allow unescorted access to any of our buildings.

Operational Traffic staff will also receive an ID card which will act as a form of identification.

If you discover that you have lost your security pass you must report it immediately to either of the following, Amey Birmingham (if the pass is for The Cube, Ash House, WMRCC or NTOC) or OneStopPasses (for any other building) once completed.

Closed circuit television

The entrances and exits of all offices are covered by CCTV monitors. The images are recorded for crime prevention purposes.

Emergency procedures

Every office has special procedures to be activated in the event of an emergency. These will vary between sites and can be found at this link. You should ensure that you make yourself familiar with the local guidance. These will be covered in your induction.

Response levels

All Highways England buildings, as part of the Government estate, are covered by the Cabinet Office response level warnings. The daily response level is displayed on the home page of the Portal. Further information can also be viewed via a link through the Portal page. These levels are not to be displayed in our buildings.

Part 4 - Information Security

The measures outlined in this section are designed to protect business information. They are applicable to all information whether physical or electronic, whether held within a Highways England Estate site, by a member of staff in a home working environment or a consultant or contractor working in their own offices.

Information should only be shared with people on a need to know basis. It should not be shared any wider than is required for the efficient conduct of the business in hand and restricted to those who are authorised to have access.

Protective markings

The author or owner of an information asset is responsible for applying the appropriate protective marking to that asset according to an assessment of the impact upon confidentiality; integrity and availability of the asset should it be inappropriately disclosed. There are three HMG protective markings:

1. **OFFICIAL** - The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

2. **SECRET** - Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.

3. **TOP SECRET** - HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

OFFICIAL information does not have to be marked, and is not marked in Highways England unless it has particular sensitivity, when it is marked OFFICIAL SENSITIVE. You can find more information on this in the Highways England Data Handling Procedure.

If you are still in doubt as to whether information should be marked, you should discuss the appropriate marking with your line manager or contact the Records Management Advice Inbox.

The Clear Desk Policy

Highways England operates a clear desk policy to support its security, health & safety and business continuity responsibilities.

A copy of the clear desk policy document can be found in at this link.

Out-Of-Hours Security Inspections

As part of their security responsibilities, Facilities Management will carry out periodic out-of-hours clear desk audits to monitor and improve compliance.

Any breach of the policy observed during a clear desk audit will require the following:

 Request for a report stating reason for breach and action taken

 All breaches reported to local Designated Director

Storage of Documents

All information must be stored appropriately, whatever format it is held in. Requirements are set out in the Data Handling Policy.

Transmission of Documents

Information on document storage and transmission of documents can also be found in the Data Handling Policy.

Containers and Keys

At the end of the working day, the following **must** be adhered to:

• All lockers, cabinets and drawers should be closed and locked with no keys left available.
• All spare keys should be locked securely in a key press or removed from the premises.
• PC should be closed down and switched off.

Destruction and Disposal of Confidential Waste

Waste paper should be disposed of in the recycling bins situated around all offices, RCCs and Outstations. To remove the risk of being read by unauthorised persons, any restricted waste papers must be placed in confidential waste bins.
Any unwanted sensitive material held on CD-ROMs must be physically destroyed. For advice, please seek guidance from the IT Security Team.

Using computer equipment out of the office

All staff have a duty to ensure that both Highways England computer equipment loaned to them, and the information stored on it, are well protected when out of the office. Guidance and advice on this is found in the Mobile Working Security operating procedure (SyOps) which everyone issued with mobile Highways England IT equipment is required to read and sign.

Using computer equipment overseas

The threat to Highways England information overseas can be greater than in the UK. Staff should be aware of:

• Requirements to allow Customs officials to inspect IT equipment and all information stored on it;
• Risk of theft of IT equipment (and the information stored on it);
• Risk of eavesdropping and interception of electronic communication.

The level of threat varies from time to time and from country to country. Before travelling abroad with Highways England IT equipment, staff must obtain approval from the IT Security Team, who will be able to advise on the level of threat, and any special measures that may be needed when abroad.

Highways England Security Contacts

Personnel and physical Security (including lost passes)	**Security Team inbox**
Information Security	**Records Management Advice inbox**
IT Security	**IT Security Advice inbox**

Call-Off Schedule 10 (Exit Management)

Not used.

Call-Off Schedule 11 (Installation Works)

Not Used.

Call-Off Schedule 12 (Clustering)

Not used.

Call-Off Schedule 13 (Implementation Plan & Testing)

Not used.

Call-Off Schedule 14 (Service Levels)

14. Definitions

14.1 In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

"Service Credits"	any service credits specified in the Annex to Part A of this Schedule being payable by the Supplier to the Buyer in respect of any failure by the Supplier to meet one or more Service Levels;
"Service Credit Cap"	has the meaning given to it in the Order Form;
"Service Level Failure"	means a failure to meet the Service Level Performance Measure in respect of a Service Level;
"Service Level Performance Measure"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule; and
"Service Level Threshold"	shall be as set out against the relevant Service Level in the Annex to Part A of this Schedule.

15. What happens if you don't meet the Service Levels

15.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.

15.2 The Supplier acknowledges that any Service Level Failure shall entitle the Buyer to the rights set out in Part A of this Schedule including the right to any Service Credits and that any Service Credit is a price adjustment and not an estimate of the Loss that may be suffered by the Buyer as a result of the Supplier's failure to meet any Service Level Performance Measure.

15.3 The Supplier shall send Performance Monitoring Reports to the Buyer detailing the level of service which was achieved in accordance with the provisions of Part B (Performance Monitoring) of this Schedule.

15.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:

15.4.1 the Supplier has over the previous (twelve) 12 Month period exceeded the Service Credit Cap; and/or

15.4.2 the Service Level Failure:

(a) exceeds the relevant Service Level Threshold;

(b) has arisen due to a Prohibited Act or wilful Default by the Supplier;

(c) results in the corruption or loss of any Government Data; and/or

(d) results in the Buyer being required to make a compensation payment to one or more third parties; and/or

15.4.3 the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

15.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting of Service Level Performance Measure in respect of one or more Service Levels and the Supplier shall not be entitled to object to, or increase the Charges as a result of such changes, provided that:

15.5.1 the total number of Service Levels for which the weighting is to be changed does not exceed the number applicable as at the Start Date;

15.5.2 the principal purpose of the change is to reflect changes in the Buyer's business requirements and/or priorities or to reflect changing industry standards; and

15.5.3 there is no change to the Service Credit Cap.

16. Critical Service Level Failure

On the occurrence of a Critical Service Level Failure:

16.1 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and

16.2 the Buyer shall (subject to the Service Credit Cap) be entitled to withhold and retain as compensation a sum equal to any Charges which would otherwise have been due to the Supplier in respect of that Service Period ("Compensation for Critical Service Level Failure"),

provided that the operation of this paragraph 3 shall be without prejudice to the right of the Buyer to terminate this Contract and/or to claim damages from the Supplier for material Default.

16.3 The Supplier shall immediately issue a credit note to the value of £300 per vehicle per week that the Delivery of the ordered Deliverables is overdue in the event that the Deliverables are not delivered by the dates specified in the Order Form and Award Letter, provided that the value of such credit note shall not exceed 15% of the Charges arising from the Order to which the relevant vehicle(s) relate. The Parties agree that the credit note amount is a genuine pre-estimate of the loss likely to be suffered by the Buyer and does not constitute a penalty.

Part A: Service Levels and Service Credits

17. Service Levels

If the level of performance of the Supplier:

17.1 is likely to or fails to meet any Service Level Performance Measure; or

17.2 is likely to cause or causes a Critical Service Failure to occur,

the Supplier shall immediately notify the Buyer in writing and the Buyer, in its absolute discretion and without limiting any other of its rights, may:

1.2.1 require the Supplier to immediately take all remedial action that is reasonable to mitigate the impact on the Buyer and to rectify or prevent a Service Level Failure or Critical Service Level Failure from taking place or recurring;

1.2.2 instruct the Supplier to comply with the Rectification Plan Process;

1.2.3 if a Service Level Failure has occurred, deduct the applicable Service Level Credits payable by the Supplier to the Buyer; and/or

1.2.4 if a Critical Service Level Failure has occurred, exercise its right to Compensation for Critical Service Level Failure (including the right to terminate for material Default).

18. Service Credits

18.1 The Buyer shall use the Performance Monitoring Reports supplied by the Supplier to verify the calculation and accuracy of the Service Credits, if any, applicable to each Service Period.

18.2 Service Credits are a reduction of the amounts payable in respect of the Deliverables and do not include VAT. The Supplier shall set-off the value of any Service Credits against the appropriate invoice in accordance with calculation formula in the Annex to Part A of this Schedule.

Annex A to Part A: Services Levels and Service Credits Table

Service Levels				Service Credit for each Service Period
Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Level Threshold	
Accurate and timely billing of Buyer	Accuracy /Timelines	at least 98% at all times	90%	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure
Access to Buyer support	Availability	at least 98% at all times	90%	0.5% Service Credit gained for each percentage under the specified Service Level Performance Measure

The Service Credits shall be calculated on the basis of the following formula:

Formula: x% (Service Level Performance Measure) - x% (actual Service Level performance)	=	x% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer
Worked example: 98% (e.g. Service Level Performance Measure requirement for accurate and timely billing Service Level) - 75% (e.g. actual performance achieved against this Service Level in a Service Period)	=	23% of the Charges payable to the Buyer as Service Credits to be deducted from the next Invoice payable by the Buyer

Part B: Performance Monitoring

19. Performance Monitoring and Performance Review

19.1 Within twenty (20) Working Days of the Start Date the Supplier shall provide the Buyer with details of how the process in respect of the monitoring and reporting of Service Levels will operate between the Parties and the Parties will endeavour to agree such process as soon as reasonably possible.

19.2 The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") in accordance with the process and timescales agreed pursuant to paragraph 1 of Part B of this Schedule which shall contain, as a minimum, the following information in respect of the relevant Service Period just ended:

19.2.1 for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period;

19.2.2 a summary of all failures to achieve Service Levels that occurred during that Service Period;

19.2.3 details of any Critical Service Level Failures;

19.2.4 for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

19.2.5 the Service Credits to be applied in respect of the relevant period indicating the failures and Service Levels to which the Service Credits relate; and

19.2.6 such other details as the Buyer may reasonably require from time to time.

19.3 The Parties shall attend meetings to discuss Performance Monitoring Reports ("Performance Review Meetings") on a Monthly basis. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports. The Performance Review Meetings shall:

19.3.1 take place within one (1) week of the Performance Monitoring Reports being issued by the Supplier at such location and time (within normal business hours) as the Buyer shall reasonably require;

19.3.2 be attended by the Supplier's Representative and the Buyer's Representative; and

19.3.3 be fully minuted by the Supplier and the minutes will be circulated by the Supplier to all attendees at the relevant meeting and also to the Buyer's Representative and any other recipients agreed at the relevant meeting.

19.4 The minutes of the preceding Month's Performance Review Meeting will be agreed and signed by both the Supplier's Representative and the Buyer's Representative at each meeting.

19.5 The Supplier shall provide to the Buyer such documentation as the Buyer may reasonably require in order to verify the level of the performance by the Supplier and the calculations of the amount of Service Credits for any specified Service Period.

20. Satisfaction Surveys

20.1 The Buyer may undertake satisfaction surveys in respect of the Supplier's provision of the Deliverables. The Buyer shall be entitled to notify the Supplier of any aspects of their performance of the provision of the Deliverables which the responses to the Satisfaction Surveys reasonably suggest are not in accordance with this Contract.

Call-Off Schedule 15 (Call-Off Contract Management)

Not used.

Call-Off Schedule 16 (Benchmarking)

Not used.

Call-Off Schedule 17 (MOD Terms)

Not Used.

Call-Off Schedule 18 (Background Checks)

Not Used.

Call-Off Schedule 19 (Scottish Law)

Not Used.

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make available to the Buyers under this Call-Off Contract

CUSTOMER CORE GOODS REQUIREMENTS

Goods required
[redacted] off- off 'BMW G05 X5 xDrive45e AC (PHEV)', to the following specification:

- Exterior Colour: Alpine White
- Transmission: Automatic
- Fuel Type: PHEV

Fitted Options:

As per your quote QT-PRI-13971 & QT-SEC-13971 and specification dated 05 October 2021

Fitted Conversion Options:

As per your quote QT-PRI-13971 & QT-SEC-13971 and specification dated 05 October 2021
Conversion address/supplier to be confirmed.

Warranty Period (Goods only)
warranty period of [redacted] mileage

Location/Sites of Delivery and Dates for Delivery of the Goods

TBC

Period for providing the Rectification Plan
In line with Manufacturer's Warranty