> party on behalf of the Supplier) specifically for the purposes of this Contract, including any modifications or enhancements to COTS Software. For the avoidance of doubt Specially Written Software does not constitute New IPR;

"Supplier System" the information and communications technology system used by the Supplier in supplying the Deliverables, including the COTS Software, the Supplier Equipment, configuration and management utilities, calibration and testing tools and related cabling (but excluding the Buyer System);

2. When this Schedule should be used

2.1. This Schedule is designed to provide additional provisions necessary to facilitate the provision of ICT Services which are part of the Deliverables.

3. Buyer due diligence requirements

- The Supplier shall satisfy itself of all relevant details, including but not limited to, details relating to the following;
 - 3.1.1. suitability of the existing and (to the extent that it is defined or reasonably foreseeable at the Start Date) future Operating Environment;
 - operating processes and procedures and the working methods of the Buyer;
 - 3.1.3. ownership, functionality, capacity, condition and suitability for use in the provision of the Deliverables of the Buyer Assets; and
 - 3.1.4. existing contracts (including any licences, support, maintenance and other contracts relating to the Operating Environment) referred to in the Due Diligence Information which may be novated to, assigned to or managed by the Supplier under this Contract and/or which the Supplier will require the benefit of for the provision of the Deliverables.
- 3.2. The Supplier confirms that it has advised the Buyer in writing of:
 - 3.2.1. each aspect, if any, of the Operating Environment that is not suitable for the provision of the ICT Services;
 - 3.2.2. the actions needed to remedy each such unsuitable aspect; and
 - 3.2.3. a timetable for and the costs of those actions.

4. Licensed software warranty

- 4.1. The Supplier represents and warrants that:
 - 4.1.1. it has and shall continue to have all necessary rights in and to the Licensed Software made available by the Supplier (and/or any Sub-Contractor) to the Buyer which are necessary for the performance of the Supplier's obligations under this Contract including the receipt of the Deliverables by the Buyer;
 - 4.1.2. all components of the Specially Written Software shall:
 - 4.1.2.1. be free from material design and programming errors;
 - 4.1.2.2. perform in all material respects in accordance with the relevant specifications contained in Call Off Schedule 14 (Service Levels) and Documentation; and
 - 4.1.2.3. not infringe any IPR.

5. Provision of ICT Services

- 5.1. The Supplier shall:
 - 5.1.1. ensure that the release of any new COTS Software in which the Supplier owns the IPR, or upgrade to any Software in which the Supplier owns the IPR complies with the interface requirements of the Buyer and (except in relation to new Software or upgrades which are released to address Malicious Software) shall notify the Buyer three (3) Months before the release of any new COTS Software or Upgrade;
 - 5.1.2. ensure that all Software including upgrades, updates and New Releases used by or on behalf of the Supplier are currently supported versions of that Software and perform in all material respects in accordance with the relevant specification;
 - 5.1.3. ensure that the Supplier System will be free of all encumbrances;
 - 5.1.4. ensure that the Deliverables are fully compatible with any Buyer Software, Buyer System, or otherwise used by the Supplier in connection with this Contract;
 - 5.1.5. minimise any disruption to the Services and the ICT Environment and/or the Buyer's operations when providing the Deliverables;

6. Standards and Quality Requirements

- 6.1. The Supplier shall develop, in the timescales specified in the Order Form, quality plans that ensure that all aspects of the Deliverables are the subject of quality management systems and are consistent with BS EN ISO 9001 or any equivalent standard which is generally recognised as having replaced it ("Quality Plans").
- 6.2. The Supplier shall seek Approval from the Buyer (not be unreasonably withheld or delayed) of the Quality Plans before implementing them.

> Approval shall not act as an endorsement of the Quality Plans and shall not relieve the Supplier of its responsibility for ensuring that the Deliverables are provided to the standard required by this Contract.

- 6.3. Following the approval of the Quality Plans, the Supplier shall provide all Deliverables in accordance with the Quality Plans.
- 6.4. The Supplier shall ensure that the Supplier Personnel shall at all times during the Call Off Contract Period:
 - be appropriately experienced, qualified and trained to supply the Deliverables in accordance with this Contract;
 - 6.4.2. apply all due skill, care, diligence in faithfully performing those duties and exercising such powers as necessary in connection with the provision of the Deliverables; and
 - 6.4.3. obey all lawful instructions and reasonable directions of the Buyer (including, if so required by the Buyer, the ICT Policy) and provide the Deliverables to the reasonable satisfaction of the Buyer.

7. ICT Audit

- 7.1. The Supplier shall allow any auditor access to the Supplier premises to:
 - inspect the ICT Environment and the wider service delivery environment (or any part of them);
 - 7.1.2. review any records created during the design and development of the Supplier System and pre-operational environment such as information relating to Testing;
 - review the Supplier's quality management systems including all relevant Quality Plans.

8. Maintenance of the ICT Environment

- 8.1. If specified by the Buyer in the Order Form, the Supplier shall create and maintain a rolling schedule of planned maintenance to the ICT Environment ("Maintenance Schedule") and make it available to the Buyer for Approval in accordance with the timetable and instructions specified by the Buyer.
- 8.2. Once the Maintenance Schedule has been Approved, the Supplier shall only undertake such planned maintenance (which shall be known as "Permitted Maintenance") in accordance with the Maintenance Schedule.
- 8.3. The Supplier shall give as much notice as is reasonably practicable to the Buyer prior to carrying out any Emergency Maintenance.
- 8.4. The Supplier shall carry out any necessary maintenance (whether Permitted Maintenance or Emergency Maintenance) where it reasonably suspects that the ICT Environment and/or the Services or any part thereof has or may have developed a fault. Any such maintenance shall be carried out in such a manner and at such times so as to avoid (or where this is not possible so as to minimise) disruption to the ICT Environment and the provision of the Deliverables.

9. Intellectual Property Rights in ICT

9.1. Assignments granted by the Supplier: Specially Written Software

- 9.1.1. The Supplier assigns (by present assignment of future rights to take effect immediately on it coming into existence) to the Buyer with full guarantee (or shall procure assignment to the Buyer), title to and all rights and interest in the Specially Written Software together with and including:
 - 9.1.1.1. the Documentation, Source Code and the Object Code of the Specially Written Software; and
 - 9.1.1.2. all build instructions, test instructions, test scripts, test data, operating instructions and other documents and tools necessary for maintaining and supporting the Specially Written Software and the New IPR (together the "Software Supporting Materials").
- 9.1.2. The Supplier shall:
 - 9.1.2.1. inform the Buyer of all Specially Written Software or New IPRs that are a modification, customisation, configuration or enhancement to any COTS Software;
 - 9.1.2.2. deliver to the Buyer the Specially Written Software and any computer program elements of the New IPRs in both Source Code and Object Code forms together with relevant Documentation and all related Software Supporting Materials within seven days of completion or, if a relevant Milestone has been identified in an Implementation Plan, Achievement of that Milestone and shall provide updates of them promptly following each new release of the Specially Written Software, in each case on media that is reasonably acceptable to the Buyer and the Buyer shall become the owner of such media upon receipt; and
 - 9.1.2.3. without prejudice to paragraph 9.1.2.2, provide full details to the Buyer of any of the Supplier's Existing IPRs or Third Party IPRs which are embedded or which are an integral part of the Specially Written Software or New IPR and the Supplier hereby grants to the Buyer and shall procure that any relevant third party licensor shall grant to the Buyer a perpetual, irrevocable, non-exclusive, assignable, royaltyfree licence to use, sub-license and/or commercially exploit such Supplier's Existing IPRs and Third Party IPRs to the extent that it is necessary to enable the Buyer to obtain the full benefits of ownership of the Specially Written Software and New IPRs.
- 9.1.3. The Supplier shall promptly execute all such assignments as are required to ensure that any rights in the Specially Written Software and New IPRs are properly transferred to the Buyer.

9.2. Licences for non-COTS IPR from the Supplier and third parties to the Buyer

9.2.1. Unless the Buyer gives its Approval the Supplier must not use any:

- a) of its own Existing IPR that is not COTS Software;
- b) third party software that is not COTS Software
- 9.2.2. Where the Buyer Approves the use of the Supplier's Existing IPR that is not COTS Software the Supplier shall grants to the Buyer a perpetual, royalty-free and non-exclusive licence to use adapt, and sub-license the same for any purpose relating to the Deliverables (or substantially equivalent deliverables) or for any purpose relating to the exercise of the Buyer's (or, if the Buyer is a Central Government Body, any other Central Government Body's) business or function including the right to load, execute, store, transmit, display and copy (for the purposes of archiving, backing-up, loading, execution, storage, transmission or display) for the Call Off Contract Period and after expiry of the Contract to the extent necessary to ensure continuity of service and an effective transition of Services to a Replacement Supplier.
- 9.2.3. Where the Buyer Approves the use of third party Software that is not COTS Software the Supplier shall procure that the owners or the authorised licensors of any such Software grant a direct licence to the Buyer on terms at least equivalent to those set out in Paragraph 9.2.2. If the Supplier cannot obtain such a licence for the Buyer it shall:
 - 9.2.3.1. notify the Buyer in writing giving details of what licence terms can be obtained and whether there are alternative software providers which the Supplier could seek to use; and
 - 9.2.3.2. only use such third party IPR as referred to at paragraph 9.2.3.1 if the Buyer Approves the terms of the licence from the relevant third party.
- 9.2.4. Where the Supplier is unable to provide a license to the Supplier's Existing IPR in accordance with Paragraph 9.2.2 above, it must meet the requirement by making use of COTS Software or Specially Written Software.
- 9.2.5. The Supplier may terminate a licence granted under paragraph 9.2.1 by giving at least thirty (30) days' notice in writing if there is an Authority Cause which constitutes a material Default which, if capable of remedy, is not remedied within twenty (20) Working Days after the Supplier gives the Buyer written notice specifying the breach and requiring its remedy.

9.3. Licenses for COTS Software by the Supplier and third parties to the Buyer

- 9.3.1. The Supplier shall either grant, or procure that the owners or the authorised licensors of any COTS Software grant, a direct licence to the Buyer on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 9.3.2. Where the Supplier owns the COTS Software it shall make available the COTS software to a Replacement Supplier at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 9.3.3. Where a third party is the owner of COTS Software licensed in accordance with this Paragraph 9.3 the Supplier shall support the Replacement Supplier to make arrangements with the owner or authorised licencee to renew the license at a price and on terms no less favourable than those standard commercial terms on which such software is usually made commercially available.
- 9.3.4. The Supplier shall notify the Buyer within seven (7) days of becoming aware of any COTS Software which in the next thirty-six (36) months:
 - 9.3.4.1. will no longer be maintained or supported by the developer; or
 - 9.3.4.2. will no longer be made commercially available

9.4. Buyer's right to assign/novate licences

- 9.4.1. The Buyer may assign, novate or otherwise transfer its rights and obligations under the licences granted pursuant to paragraph 9.2 (to:
 - 9.4.1.1. a Central Government Body; or
 - 9.4.1.2. to any body (including any private sector body) which performs or carries on any of the functions and/or activities that previously had been performed and/or carried on by the Buyer.
- 9.4.2. If the Buyer ceases to be a Central Government Body, the successor body to the Buyer shall still be entitled to the benefit of the licences granted in paragraph 9.2.

9.5. Licence granted by the Buyer

9.5.1. The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Contract Period to use the Buyer Software and the Specially Written Software solely to the extent necessary for providing the Deliverables in accordance with this Contract, including the right to grant sub-licences to Sub-Contractors provided that any relevant Sub-Contractor has entered into a confidentiality undertaking with the Supplier on the same terms as set out in Clause 15 (Confidentiality).

9.6. Open Source Publication

- 9.6.1. Unless the Buyer otherwise agrees in advance in writing (and subject to paragraph 9.6.3) all Specially Written Software and computer program elements of New IPR shall be created in a format, or able to be converted (in which case the Supplier shall also provide the converted format to the Buyer) into a format, which is:
 - 9.6.1.1. suitable for publication by the Buyer as Open Source; and
 - 9.6.1.2. based on Open Standards (where applicable),
- and the Buyer may, at its sole discretion, publish the same as Open Source.
- 9.6.2. The Supplier hereby warrants that the Specially Written Software and the New IPR:
 - 9.6.2.1. are suitable for release as Open Source and that the Supplier has used reasonable endeavours when developing the same to ensure that publication by the Buyer will not enable a third party to use them in any way which could reasonably be foreseen to compromise the operation, running or security of the Specially Written Software, New IPRs or the Buyer System;
 - 9.6.2.2. have been developed using reasonable endeavours to ensure that their publication by the Buyer shall not cause any harm or damage to any party using them;
 - 9.6.2.3. do not contain any material which would bring the Buyer into disrepute;
 - can be published as Open Source without breaching the rights of any third party;
 - 9.6.2.5. will be supplied in a format suitable for publication as Open Source ("the Open Source Publication Material") no later than the date notified by the Buyer to the Supplier; and
 - 9.6.2.6. do not contain any Malicious Software.
- 9.6.3. Where the Buyer has Approved a request by the Supplier for any part of the Specially Written Software or New IPRs to be excluded from the requirement to be in an Open Source format due to the intention to embed or integrate Supplier Existing IPRs and/or Third Party IPRs (and where the Parties agree that such IPRs are not intended to be published as Open Source), the Supplier shall:
 - 9.6.3.1. as soon as reasonably practicable, provide written details of the nature of the IPRs and items or Deliverables based on IPRs which are to be excluded from Open Source publication; and
 - 9.6.3.2. include in the written details and information about the impact that inclusion of such IPRs or Deliverables based on

> such IPRs, will have on any other Specially Written Software and/or New IPRs and the Buyer's ability to publish such other items or Deliverables as Open Source.

9.7. Malicious Software

- 9.7.1. The Supplier shall, throughout the Contract Period, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for, contain the spread of, and minimise the impact of Malicious Software.
- 9.7.2. If Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Government Data, assist each other to mitigate any losses and to restore the provision of the Deliverables to its desired operating efficiency.
- 9.7.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraph 9.7.2 shall be borne by the Parties as follows:
 - 9.7.3.1. by the Supplier, where the Malicious Software originates from the Supplier Software, the third party Software supplied by the Supplier or the Government Data (whilst the Government Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and
 - 9.7.3.2. by the Buyer, if the Malicious Software originates from the Buyer Software or the Buyer Data (whilst the Buyer Data was under the control of the Buyer).

10. [Supplier-Furnished Terms NOT APPLICABLE

10.1. Software Licence Terms

- 10.1.1.1 Terms for licensing of non-COTS third party software in accordance with Paragraph 9.2.3 are detailed in [insert reference to relevant Schedule].
- 10.1.1.2.Terms for licensing of COTS software in accordance with Paragraph 9.3 are detailed in [insert reference to relevant Schedule].

10.2. Software as a Service Terms

10.2.1.1.Additional terms for provision of a Software as a Service solution are detailed in [insert reference to relevant Schedule].

10.3. Software Support & Maintenance Terms

> 10.3.1.1.Additional terms for provision of Software Support & Maintenance Services are detailed in [insert reference to relevant Schedule]]

Call-Off Schedule 7 (Key Supplier Staff) Call-Off Ref: Crown Copyright 2018

Call-Off Schedule 7 (Key Supplier Staff)

- 1.1 The Annex 1 to this Schedule lists the key roles ("Key Roles") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.
- 1.2 The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.
- 1.3 The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.
- 1.4 The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:
 - 1.4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);
 - 1.4.2 the person concerned resigns, retires or dies or is on maternity or longterm sick leave; or
 - 1.4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.
- 1.5 The Supplier shall:
 - 1.5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);
 - ensure that any Key Role is not vacant for any longer than ten (10) Working Days;
 - 1.5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least three (3) Months' notice;
 - 1.5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and
 - 1.5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent

Call-Off Schedule 7 (Key Supplier Staff) Call-Off Ref: Crown Copyright 2018

to carry out the tasks assigned to the Key Staff whom he or she has replaced.

1.6 The Buyer may require the Supplier to remove or procure that any Subcontractor shall remove any Key Staff that the Buyer considers in any respect unsatisfactory. The Buyer shall not be liable for the cost of replacing any Key Staff.

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

1. Definitions

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

"BCDR Plan"	 1 has the meaning given to it in Paragraph 2.2 of this Schedule;
"Business Continuity Plan"	2 has the meaning given to it in Paragraph 2.3.2 of this Schedule;
"Disaster Recovery Deliverables"	3 the Deliverables embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Disaster Recovery Plan"	4 has the meaning given to it in Paragraph 2.3.3 of this Schedule;
"Disaster Recovery System"	5 the system embodied in the processes and procedures for restoring the provision of Deliverables following the occurrence of a Disaster;
"Related Supplier"	6 any person who provides Deliverables to the Buyer which are related to the Deliverables from time to time;
"Review Report"	7 has the meaning given to it in Paragraph 6.3 of this Schedule; and
"Supplier's Proposals"	8 has the meaning given to it in Paragraph 6.3 of this Schedule;

2. BCDR Plan

- 2.1 The Buyer and the Supplier recognise that, where specified in Schedule 4 (Framework Management), CCS shall have the right to enforce the Buyer's rights under this Schedule.
- 2.2 At least ninety (90) Working Days prior to the Start Date the Supplier shall prepare and deliver to the Buyer for the Buyer's written approval a plan (a "BCDR Plan"), which shall detail the processes and arrangements that the Supplier shall follow to:
 - 2.2.1 ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Deliverables; and

- 2.2.2 the recovery of the Deliverables in the event of a Disaster
- 2.3 The BCDR Plan shall be divided into three sections:
 - Section 1 which shall set out general principles applicable to the BCDR Plan;
 - 2.3.2 Section 2 which shall relate to business continuity (the "Business Continuity Plan"); and
 - 2.3.3 Section 3 which shall relate to disaster recovery (the "Disaster Recovery Plan").
- 2.4 Following receipt of the draft BCDR Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the BCDR Plan. If the Parties are unable to agree the contents of the BCDR Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

3. General Principles of the BCDR Plan (Section 1)

- 3.1 Section 1 of the BCDR Plan shall:
 - 3.1.1 set out how the business continuity and disaster recovery elements of the BCDR Plan link to each other;
 - 3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the provision of the Deliverables and any goods and/or services provided to the Buyer by a Related Supplier;
 - 3.1.3 contain an obligation upon the Supplier to liaise with the Buyer and any Related Suppliers with respect to business continuity and disaster recovery;
 - 3.1.4 detail how the BCDR Plan interoperates with any overarching disaster recovery or business continuity plan of the Buyer and any of its other Related Supplier in each case as notified to the Supplier by the Buyer from time to time;
 - 3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;
 - 3.1.6 contain a risk analysis, including:
 - failure or disruption scenarios and assessments of likely frequency of occurrence;
 - (b) identification of any single points of failure within the provision of Deliverables and processes for managing those risks;
 - identification of risks arising from the interaction of the provision of Deliverables with the goods and/or services provided by a Related Supplier; and
 - (d) a business impact analysis of different anticipated failures or disruptions;

3.1.7 provide for documentation of processes, including business processes, and procedures;

- 3.1.8 set out key contact details for the Supplier (and any Subcontractors) and for the Buyer;
- 3.1.9 identify the procedures for reverting to "normal service";
- 3.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;
- 3.1.11 identify the responsibilities (if any) that the Buyer has agreed it will assume in the event of the invocation of the BCDR Plan; and
- 3.1.12 provide for the provision of technical assistance to key contacts at the Buyer as required by the Buyer to inform decisions in support of the Buyer's business continuity plans.
- 3.2 The BCDR Plan shall be designed so as to ensure that:
 - 3.2.1 the Deliverables are provided in accordance with this Contract at all times during and after the invocation of the BCDR Plan;
 - 3.2.2 the adverse impact of any Disaster is minimised as far as reasonably possible;
 - 3.2.3 it complies with the relevant provisions of ISO/IEC 27002; ISO22301/ISO22313 and all other industry standards from time to time in force; and
 - 3.2.4 it details a process for the management of disaster recovery testing.
- 3.3 The BCDR Plan shall be upgradeable and sufficiently flexible to support any changes to the Deliverables and the business operations supported by the provision of Deliverables.
- 3.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators (PI's) or Service levels, or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Contract.

4. Business Continuity (Section 2)

- 4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Deliverables remain supported and to ensure continuity of the business operations supported by the Services including:
 - 4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Deliverables; and
 - 4.1.2 the steps to be taken by the Supplier upon resumption of the provision of Deliverables in order to address the effect of the failure or disruption.

- 4.2 The Business Continuity Plan shall:
 - 4.2.1 address the various possible levels of failures of or disruptions to the provision of Deliverables;
 - 4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Deliverables;
 - 4.2.3 specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Business Continuity Plan; and
 - 4.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

5. Disaster Recovery (Section 3)

- 5.1 The Disaster Recovery Plan (which shall be invoked only upon the occurrence of a Disaster) shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Buyer supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.
- 5.2 The Supplier's BCDR Plan shall include an approach to business continuity and disaster recovery that addresses the following:
 - 5.2.1 loss of access to the Buyer Premises;
 - 5.2.2 loss of utilities to the Buyer Premises;
 - 5.2.3 loss of the Supplier's helpdesk or CAFM system;
 - 5.2.4 loss of a Subcontractor;
 - 5.2.5 emergency notification and escalation process;
 - 5.2.6 contact lists;
 - 5.2.7 staff training and awareness;
 - 5.2.8 BCDR Plan testing;
 - 5.2.9 post implementation review process;
 - 5.2.10 any applicable Performance Indicators (PI's) with respect to the provision of the disaster recovery services and details of any agreed relaxation to the Performance Indicators (PI's) or Service Levels in respect of the provision of other Deliverables during any period of invocation of the Disaster Recovery Plan;
 - 5.2.11 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

- 5.2.12 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and
- 5.2.13 testing and management arrangements.

6. Review and changing the BCDR Plan

- 6.1 The Supplier shall review the BCDR Plan:
 - 6.1.1 on a regular basis and as a minimum once every six (6) Months;
 - 6.1.2 within three (3) calendar Months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and
 - 6.1.3 where the Buyer requests in writing any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2 of this Schedule) whereupon the Supplier shall conduct such reviews in accordance with the Buyer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Buyer for the Buyer's approval. The costs of both Parties of any such additional reviews shall be met by the Buyer except that the Supplier shall not be entitled to charge the Buyer for any costs that it may incur above any estimate without the Buyer's prior written approval.
- 6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall assess its suitability having regard to any change to the Deliverables or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDR Plan or the last review of the BCDR Plan, and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the BCDR Plan. The review shall be completed by the Supplier within such period as the Buyer shall reasonably require.
- 6.3 The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDR Plan, provide to the Buyer a report (a "Review Report") setting out the Supplier's proposals (the "Supplier's Proposals") for addressing any changes in the risk profile and its proposals for amendments to the BCDR Plan.
- 6.4 Following receipt of the Review Report and the Supplier's Proposals, the Parties shall use reasonable endeavours to agree the Review Report and the Supplier's Proposals. If the Parties are unable to agree Review Report and the Supplier's Proposals within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 6.5 The Supplier shall as soon as is reasonably practicable after receiving the approval of the Supplier's Proposals effect any change in its practices or procedures necessary so as to give effect to the Supplier's Proposals. Any such change shall be at the Supplier's expense unless it can be reasonably

> shown that the changes are required because of a material change to the risk profile of the Deliverables.

7. Testing the BCDR Plan

- 7.1 The Supplier shall test the BCDR Plan:
 - 7.1.1 regularly and in any event not less than once in every Contract Year;
 - 7.1.2 in the event of any major reconfiguration of the Deliverables
 - 7.1.3 at any time where the Buyer considers it necessary (acting in its sole discretion).
- 7.2 If the Buyer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Buyer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Buyer unless the BCDR Plan fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.
- 7.3 The Supplier shall undertake and manage testing of the BCDR Plan in full consultation with and under the supervision of the Buyer and shall liaise with the Buyer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Buyer.
- 7.4 The Supplier shall ensure that any use by it or any Subcontractor of "live" data in such testing is first approved with the Buyer. Copies of live test data used in any such testing shall be (if so required by the Buyer) destroyed or returned to the Buyer on completion of the test.
- 7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test, provide to the Buyer a report setting out:
 - 7.5.1 the outcome of the test;
 - 7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and
 - 7.5.3 the Supplier's proposals for remedying any such failures.
- 7.6 Following each test, the Supplier shall take all measures requested by the Buyer to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at its own cost, by the date reasonably required by the Buyer.

8. Invoking the BCDR Plan

8.1 In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDR Plan (and shall inform the Buyer promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDR Plan only with the prior consent of the Buyer.

9. Circumstances beyond your control

9.1 The Supplier shall not be entitled to relief under Clause 20 (Circumstances beyond your control) if it would not have been impacted by the Force Majeure Event had it not failed to comply with its obligations under this Schedule.

Call-Off Schedule 9 (Security)

Due to the nature of the work being undertaken by both NHSD and the Supplier in relation to this contract, Part B (Long Form Security Requirements) will apply at all times.

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:
	 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 where the Buyer has required compliance therewith in accordance with paragraph 2.2;
"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 requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.
- 2.3 Where the Security Policy applies 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 where specified by the Buyer in accordance with paragraph 2.2 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, where necessary in accordance with paragraph 2.2 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) where necessary in accordance with paragraph 2.2, 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
 - 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 (where relevant in accordance with paragraph 2.2) 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: Long 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):

2 CONT	
"Breach of Security"	2 means the occurrence of:
	 any unauthorised access to or use of the Goods and/or 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,
	3 in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d;
"ISMS"	4 the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and
"Security Tests"	5 tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

2. Security Requirements

- 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 Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.3 The Parties shall each appoint a security representative to be responsible for Security. The initial security representatives of the Parties are:



- 2.4 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.
- 2.5 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.
- 2.6 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.
- 2.7 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.
- 2.8 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. Information Security Management System (ISMS)

- 3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.
- 3.2 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 the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.
- 3.3 The Buyer acknowledges that;
 - 3.3.1 If the Buyer has not stipulated during a Further Competition that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and
 - 3.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.

3.4 The ISMS shall:

- 3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, 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, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) 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;
- 3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;
- 3.4.3 at all times provide a level of security which:
 - a) is in accordance with the Law and this Contract;
 - b) complies with the Baseline Security Requirements;
 - c) as a minimum demonstrates Good Industry Practice;
 - where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;
 - e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) (https://www.gov.uk/government/publications/securitypolicy-framework/hmg-security-policy-framework)
 - f) takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk)
 - g) complies with HMG Information Assurance Maturity Model and Assurance Framework (<u>https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm</u>)
 - meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;
 - addresses issues of incompatibility with the Supplier's own organisational security policies; and
 - j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;
- 3.4.4 document the security incident management processes and incident response plans;
- 3.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Deliverables of any new threat, vulnerability

> or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

- 3.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).
- 3.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 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.
- 3.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.
- 3.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall 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 the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.
- 3.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

4. Security Management Plan

4.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

- 4.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);
- 4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;
- 4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;
- 4.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) 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;
- 4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) 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;
- 4.2.6 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 delivery of the Deliverables and 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 Schedule (including the requirements set out in Paragraph 3.4);
- 4.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);
- 4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

- 4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;
- 4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and
- 4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Deliverables and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.
- 4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of nonapproval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall 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 the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure 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.
- 4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

5. Amendment of the ISMS and Security Management Plan

- 5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:
 - 5.1.1 emerging changes in Good Industry Practice;
 - 5.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;
 - 5.1.3 any new perceived or changed security threats;
 - 5.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;
 - 5.1.5 any new perceived or changed security threats; and
 - 5.1.6 any reasonable change in requirement requested by the Buyer.
- 5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and

> Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

- 5.2.1 suggested improvements to the effectiveness of the ISMS;
- 5.2.2 updates to the risk assessments;
- 5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and
- 5.2.4 suggested improvements in measuring the effectiveness of controls.
- 5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.
- 5.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or 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.

6. Security Testing

- 6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.
- 6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.
- 6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet

> the KPIs, the Supplier shall be granted relief against any resultant underperformance for the period of the Buyer's test.

- 6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including unpatched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.
- 6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. Complying with the ISMS

- 7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.
- 7.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.
- 7.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. Security Breach

- 8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.
- 8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:
 - 8.2.1 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 or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;
 - c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;
 - d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and
 - e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and
 - f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.
- 8.3 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 ISMS with the Security Policy (where relevant) or the requirements of this

> Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

9. Vulnerabilities and fixing them

- 9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.
- 9.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:
 - 9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and
 - 9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.
- 9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:
 - 9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;
 - 9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or
 - 9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.
- 9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:
 - 9.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation
> techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

- 9.4.2 is agreed with the Buyer in writing.
- 9.5 The Supplier shall:
 - 9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;
 - 9.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
 - 9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;
 - 9.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.3.5;
 - 9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;
 - 9.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;
 - 9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and
 - 9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.
- 9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.
- 9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

Part B – Annex 1:

Baseline security requirements

1. Handling Classified information

1.1 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.

2. End user devices

- 2.1 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 National Cyber Security Centre ("NCSC") to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").
- 2.2 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 End User Devices Security Guidance (<u>https://www.ncsc.gov.uk/guidance/enduser-device-security</u>). 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 NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. Data Processing, Storage, Management and Destruction

- 3.1 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.
- 3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with Clause 14 (Data protection).

3.3 The Supplier shall:

- 3.3.1 provide the Buyer with all Government Data on demand in an agreed open format;
- 3.3.2 have documented processes to guarantee availability of Government Data in the event of the Supplier ceasing to trade;
- 3.3.3 securely destroy all media that has held Government Data at the end of life of that media in line with Good Industry Practice; and
- 3.3.4 securely erase any or all Government Data held by the Supplier when requested to do so by the Buyer.

4. Ensuring secure communications

- 4.1 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 NCSC, to at least Foundation Grade, for example, under CPA.
- 4.2 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.

5. Security by design

- 5.1 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.
- 5.2 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 NCSC certification (<u>https://www.ncsc.gov.uk/section/products-services/ncsc-certification</u>) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

6. Security of Supplier Staff

- 6.1 Supplier Staff shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.
- 6.2 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.
- 6.3 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.

- 6.4 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.
- 6.5 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.

7. Restricting and monitoring access

7.1 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.

8. Audit

- 8.1 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:
 - 8.1.1 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.
 - 8.1.2 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 log-on and log-off 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.
- 8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
- 8.3 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

TBC

Call-Off Schedule 10 (Exit Management)

1. Definitions

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

and) enan eappiernent eente ee	include i (e chininghi)
"Exclusive Assets"	Supplier Assets used exclusively by the Supplier or a Key Subcontractor in the provision of the Deliverables;
"Exit Information"	has the meaning given to it in Paragraph 3.1 of this Schedule;
"Exit Manager"	the person appointed by each Party to manage their respective obligations under this Schedule;
"Net Book Value"	the current net book value of the relevant Supplier Asset(s) calculated in accordance with the Framework Tender or Call-Off Tender (if stated) or (if not stated) the depreciation policy of the Supplier (which the Supplier shall ensure is in accordance with Good Industry Practice);
"Non-Exclusive Assets"	those Supplier Assets used by the Supplier or a Key Subcontractor in connection with the Deliverables but which are also used by the Supplier or Key Subcontractor for other purposes;
"Registers"	the register and configuration database referred to in Paragraph 2.2 of this Schedule;
"Replacement Goods"	any goods which are substantially similar to any of the Goods and which the Buyer receives in substitution for any of the Goods following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Replacement Services"	any services which are substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services following the End Date, whether those goods are provided by the Buyer internally and/or by any third party;
"Termination Assistance"	the activities to be performed by the Supplier pursuant to the Exit Plan, and

	pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	has the meaning given to it in Paragraph 5.1 of this Schedule;
"Termination Assistance Period"	the period specified in a Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to Paragraph 5.2 of this Schedule;
"Transferable Assets"	Exclusive Assets which are capable of legal transfer to the Buyer;
"Transferable Contracts"	Sub-Contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are necessary to enable the Buyer or any Replacement Supplier to provide the Deliverables or the Replacement Goods and/or Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	has the meaning given to it in Paragraph 8.2.1 of this Schedule;
"Transferring Contracts"	has the meaning given to it in Paragraph 8.2.3 of this Schedule.

other assistance required by the Buyer

2. Supplier must always be prepared for contract exit

- 2.1 The Supplier shall within 30 days from the Start Date provide to the Buyer a copy of its depreciation policy to be used for the purposes of calculating Net Book Value.
- 2.2 During the Contract Period, the Supplier shall promptly:
 - 2.2.1 create and maintain a detailed register of all Supplier Assets (including description, condition, location and details of ownership and status as either Exclusive Assets or Non-Exclusive Assets and Net Book Value) and Sub-contracts and other relevant agreements required in connection with the Deliverables; and
 - 2.2.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Deliverables

("Registers").

2.3 The Supplier shall:

- 2.3.1 ensure that all Exclusive Assets listed in the Registers are clearly physically identified as such; and
- 2.3.2 procure that all licences for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation (at no cost or restriction to the Buyer) at the request of the Buyer to the Buyer (and/or its nominee) and/or any Replacement Supplier upon the Supplier ceasing to provide the Deliverables (or part of them) and if the Supplier is unable to do so then the Supplier shall promptly notify the Buyer and the Buyer may require the Supplier to procure an alternative Subcontractor or provider of Deliverables.
- 2.4 Each Party shall appoint an Exit Manager within three (3) Months of the Start Date. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the expiry or termination of this Contract.

3. Assisting re-competition for Deliverables

- 3.1 The Supplier shall, on reasonable notice, provide to the Buyer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), such information (including any access) as the Buyer shall reasonably require in order to facilitate the preparation by the Buyer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence (the "Exit Information").
- 3.2 The Supplier acknowledges that the Buyer may disclose the Supplier's Confidential Information (excluding the Supplier's or its Subcontractors' prices or costs) to an actual or prospective Replacement Supplier to the extent that such disclosure is necessary in connection with such engagement.
- 3.3 The Supplier shall provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and notify the Buyer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Deliverables (and shall consult the Buyer in relation to any such changes).
- 3.4 The Exit Information shall be accurate and complete in all material respects and shall be sufficient to enable a third party to prepare an informed offer for those Deliverables; and not be disadvantaged in any procurement process compared to the Supplier.

4. Exit Plan

4.1 The Supplier shall, within three (3) Months after the Start Date, deliver to the Buyer an Exit Plan which complies with the requirements set out in Paragraph 4.3 of this Schedule and is otherwise reasonably satisfactory to the Buyer.

- 4.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of the latest date for its submission pursuant to Paragraph 4.1, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 4.3 The Exit Plan shall set out, as a minimum:
 - 4.3.1 a detailed description of both the transfer and cessation processes, including a timetable;
 - 4.3.2 how the Deliverables will transfer to the Replacement Supplier and/or the Buyer;
 - 4.3.3 details of any contracts which will be available for transfer to the Buyer and/or the Replacement Supplier upon the Expiry Date together with any reasonable costs required to effect such transfer;
 - 4.3.4 proposals for the training of key members of the Replacement Supplier's staff in connection with the continuation of the provision of the Deliverables following the Expiry Date;
 - 4.3.5 proposals for providing the Buyer or a Replacement Supplier copies of all documentation relating to the use and operation of the Deliverables and required for their continued use;
 - 4.3.6 proposals for the assignment or novation of all services utilised by the Supplier in connection with the supply of the Deliverables;
 - 4.3.7 proposals for the identification and return of all Buyer Property in the possession of and/or control of the Supplier or any third party;
 - 4.3.8 proposals for the disposal of any redundant Deliverables and materials;
 - 4.3.9 how the Supplier will ensure that there is no disruption to or degradation of the Deliverables during the Termination Assistance Period; and
 - 4.3.10 any other information or assistance reasonably required by the Buyer or a Replacement Supplier.
- 4.4 The Supplier shall:
 - 4.4.1 maintain and update the Exit Plan (and risk management plan) no less frequently than:
 - (a) every six (6) months throughout the Contract Period; and
 - no later than twenty (20) Working Days after a request from the Buyer for an up-to-date copy of the Exit Plan;
 - (c) as soon as reasonably possible following a Termination Assistance Notice, and in any event no later than ten (10) Working Days after the date of the Termination Assistance Notice;

- (d) as soon as reasonably possible following, and in any event no later than twenty (20) Working Days following, any material change to the Deliverables (including all changes under the Variation Procedure); and
- 4.4.2 jointly review and verify the Exit Plan if required by the Buyer and promptly correct any identified failures.
- 4.5 Only if (by notification to the Supplier in writing) the Buyer agrees with a draft Exit Plan provided by the Supplier under Paragraph 4.2 or 4.4 (as the context requires), shall that draft become the Exit Plan for this Contract.
- 4.6 A version of an Exit Plan agreed between the parties shall not be superseded by any draft submitted by the Supplier.

5. Termination Assistance

- 5.1 The Buyer shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Supplier (a "Termination Assistance Notice") at least four (4) Months prior to the Expiry Date or as soon as reasonably practicable (but in any event, not later than one (1) Month) following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:
 - 5.1.1 the nature of the Termination Assistance required; and
 - 5.1.2 the start date and period during which it is anticipated that Termination Assistance will be required, which shall continue no longer than twelve (12) Months after the date that the Supplier ceases to provide the Deliverables.
- 5.2 The Buyer shall have an option to extend the Termination Assistance Period beyond the Termination Assistance Notice period provided that such extension shall not extend for more than six (6) Months beyond the end of the Termination Assistance Period and provided that it shall notify the Supplier of such this extension no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Buyer shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Supplier.
- 5.3 In the event that Termination Assistance is required by the Buyer but at the relevant time the parties are still agreeing an update to the Exit Plan pursuant to Paragraph 4, the Supplier will provide the Termination Assistance in good faith and in accordance with the principles in this Schedule and the last Buyer approved version of the Exit Plan (insofar as it still applies).

6. Termination Assistance Period

- 6.1 Throughout the Termination Assistance Period the Supplier shall:
 - 6.1.1 continue to provide the Deliverables (as applicable) and otherwise perform its obligations under this Contract and, if required by the Buyer, provide the Termination Assistance;
 - 6.1.2 provide to the Buyer and/or its Replacement Supplier any reasonable assistance and/or access requested by the Buyer and/or its Replacement Supplier including assistance and/or access to facilitate the orderly transfer of responsibility for and conduct of the Deliverables to the Buyer and/or its Replacement Supplier;
 - 6.1.3 use all reasonable endeavours to reallocate resources to provide such assistance without additional costs to the Buyer;
 - 6.1.4 subject to Paragraph 6.3, provide the Deliverables and the Termination Assistance at no detriment to the Performance Indicators (PI's) or Service Levels, the provision of the Management Information or any other reports nor to any other of the Supplier's obligations under this Contract;
 - 6.1.5 at the Buyer's request and on reasonable notice, deliver up-to-date Registers to the Buyer;
 - 6.1.6 seek the Buyer's prior written consent to access any Buyer Premises from which the de-installation or removal of Supplier Assets is required.
- 6.2 If it is not possible for the Supplier to reallocate resources to provide such assistance as is referred to in Paragraph 6.1.2 without additional costs to the Buyer, any additional costs incurred by the Supplier in providing such reasonable assistance shall be subject to the Variation Procedure.
- 6.3 If the Supplier demonstrates to the Buyer's reasonable satisfaction that the provision of the Termination Assistance will have a material, unavoidable adverse effect on the Supplier's ability to meet one or more particular Service Levels, the Parties shall vary the relevant Service Levels and/or the applicable Service Credits accordingly.

7. Obligations when the contract is terminated

- 7.1 The Supplier shall comply with all of its obligations contained in the Exit Plan.
- 7.2 Upon termination or expiry or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Supplier's performance of the Deliverables and the Termination Assistance), the Supplier shall:
 - 7.2.1 vacate any Buyer Premises;
 - 7.2.2 remove the Supplier Equipment together with any other materials used by the Supplier to supply the Deliverables and shall leave the Sites in a clean, safe and tidy condition. The Supplier is solely

> responsible for making good any damage to the Sites or any objects contained thereon, other than fair wear and tear, which is caused by the Supplier;

- 7.2.3 provide access during normal working hours to the Buyer and/or the Replacement Supplier for up to twelve (12) Months after expiry or termination to:
 - such information relating to the Deliverables as remains in the possession or control of the Supplier; and
 - (b) such members of the Supplier Staff as have been involved in the design, development and provision of the Deliverables and who are still employed by the Supplier, provided that the Buyer and/or the Replacement Supplier shall pay the reasonable costs of the Supplier actually incurred in responding to such requests for access.
- 7.3 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Buyer to the Supplier in relation to the Deliverables shall be terminated with effect from the end of the Termination Assistance Period.

8. Assets, Sub-contracts and Software

- 8.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Supplier shall not, without the Buyer's prior written consent:
 - 8.1.1 terminate, enter into or vary any Sub-contract or licence for any software in connection with the Deliverables; or
 - 8.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Supplier Assets or acquire any new Supplier Assets.
- 8.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Supplier, the Buyer shall notify the Supplier setting out:
 - 8.2.1 which, if any, of the Transferable Assets the Buyer requires to be transferred to the Buyer and/or the Replacement Supplier ("Transferring Assets");
 - 8.2.2 which, if any, of:
 - the Exclusive Assets that are not Transferable Assets; and
 - (b) the Non-Exclusive Assets,

the Buyer and/or the Replacement Supplier requires the continued use of; and

8.2.3 which, if any, of Transferable Contracts the Buyer requires to be assigned or novated to the Buyer and/or the Replacement Supplier (the "Transferring Contracts"),

> in order for the Buyer and/or its Replacement Supplier to provide the Deliverables from the expiry of the Termination Assistance Period. The Supplier shall provide all reasonable assistance required by the Buyer and/or its Replacement Supplier to enable it to determine which Transferable Assets and Transferable Contracts are required to provide the Deliverables or the Replacement Goods and/or Replacement Services.

- 8.3 With effect from the expiry of the Termination Assistance Period, the Supplier shall sell the Transferring Assets to the Buyer and/or the Replacement Supplier for their Net Book Value less any amount already paid for them through the Charges.
- 8.4 Risk in the Transferring Assets shall pass to the Buyer or the Replacement Supplier (as appropriate) at the end of the Termination Assistance Period and title shall pass on payment for them.
- 8.5 Where the Buyer and/or the Replacement Supplier requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Supplier shall as soon as reasonably practicable:
 - 8.5.1 procure a non-exclusive, perpetual, royalty-free licence for the Buyer and/or the Replacement Supplier to use such assets (with a right of sub-licence or assignment on the same terms); or failing which
 - 8.5.2 procure a suitable alternative to such assets, the Buyer or the Replacement Supplier to bear the reasonable proven costs of procuring the same.
- 8.6 The Supplier shall as soon as reasonably practicable assign or procure the novation of the Transferring Contracts to the Buyer and/or the Replacement Supplier. The Supplier shall execute such documents and provide such other assistance as the Buyer reasonably requires to effect this novation or assignment.
- 8.7 The Buyer shall:
 - 8.7.1 accept assignments from the Supplier or join with the Supplier in procuring a novation of each Transferring Contract; and
 - 8.7.2 once a Transferring Contract is novated or assigned to the Buyer and/or the Replacement Supplier, discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Supplier does the same.
- 8.8 The Supplier shall hold any Transferring Contracts on trust for the Buyer until the transfer of the relevant Transferring Contract to the Buyer and/or the Replacement Supplier has taken place.
- 8.9 The Supplier shall indemnify the Buyer (and/or the Replacement Supplier, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Buyer (and/or Replacement Supplier) pursuant to Paragraph 8.6 in relation to any matters arising prior to the date of assignment or novation of such Transferring Contract. Clause 19 (Other

> people's rights in this contract) shall not apply to this Paragraph 8.9 which is intended to be enforceable by Third Parties Beneficiaries by virtue of the CRTPA.

9. No charges

9.1 Unless otherwise stated, the Buyer shall not be obliged to pay for costs incurred by the Supplier in relation to its compliance with this Schedule.

10. Dividing the bills

- 10.1 All outgoings, expenses, rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Buyer and/or the Replacement and the Supplier as follows:
 - 10.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;
 - 10.1.2 the Buyer or Replacement Supplier (as applicable) shall be responsible for or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and
 - 10.1.3 the Supplier shall be responsible for or entitled to (as the case may be) the rest of the invoice.

Call-Off Schedule 13 (Implementation Plan and Testing)

Part A - Implementation

1. Definitions

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

"Delay"	 a) a delay in the Achievement of a Milestone by its Milestone Date; or
	b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;
"Deliverable Item"	an item or feature in the supply of the Deliverables delivered or to be delivered by the Supplier at or before a Milestone Date listed in the Implementation Plan;
Implementation Period"	has the meaning given to it in Paragraph 7.1;

2. Agreeing and following the Implementation Plan

- 2.1 A draft of the Implementation and Mobilisation Plan is set out in the Annex to this Schedule. The Supplier shall provide Delivery Handbook including a further draft Implementation Plan 20 working days after the Call-Off Contract Start Date as detailed in Appendix 1.
- 2.2 The draft Implementation Plan:
 - 2.2.1 must contain information at the level of detail necessary to manage the implementation stage effectively and as the Buyer may otherwise require; and
 - 2.2.2 it shall take account of all dependencies known to, or which should reasonably be known to, the Supplier.
- 2.3 Following receipt of the draft Implementation Plan from the Supplier, the Parties shall use reasonable endeavours to agree the contents of the Implementation Plan. If the Parties are unable to agree the contents of the Implementation Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
- 2.4 The Supplier shall provide each of the Deliverable Items identified in the Implementation Plan by the date assigned to that Deliverable Item in the

> Implementation Plan so as to ensure that each Milestone identified in the Implementation Plan is Achieved on or before its Milestone Date.

2.5 The Supplier shall monitor its performance against the Implementation Plan and Milestones (if any) and report to the Buyer on such performance.

3. Reviewing and changing the Implementation Plan

- 3.1 Subject to Paragraph 4.3, the Supplier shall keep the Implementation Plan under review in accordance with the Buyer's instructions and ensure that it is updated on a regular basis.
- 3.2 The Buyer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan.
- 3.3 Changes to any Milestones shall only be made in agreement with the Buyer.

4. Security requirements before the Start Date

- 4.1 The Supplier shall note that it is incumbent upon them to understand the lead-in period for security clearances and ensure that all Supplier Staff have the necessary security clearance in place before the Call-Off Start Date. The Supplier shall ensure that this is reflected in their Implementation Plans.
- 4.2 The Supplier shall ensure that all Supplier Staff and Subcontractors do not access the Buyer's IT systems, or any IT systems linked to the Buyer, unless they have satisfied the Buyer's security requirements.
- 4.3 The Supplier shall be responsible for providing all necessary information to the Buyer to facilitate security clearances for Supplier Staff and Subcontractors in accordance with the Buyer's requirements.
- 4.4 The Supplier shall provide the names of all Supplier Staff and Subcontractors and inform the Buyer of any alterations and additions as they take place throughout the Call-Off Contract.
- 4.5 The Supplier shall ensure that all Supplier Staff and Subcontractors requiring access to the Buyer Premises have the appropriate security clearance. It is the Supplier's responsibility to establish whether or not the level of clearance will be sufficient for access. Unless prior approval has been received from the Buyer, the Supplier shall be responsible for meeting the costs associated with the provision of security cleared escort services.
- 4.6 If a property requires Supplier Staff or Subcontractors to be accompanied by the Buyer's Authorised Representative, the Buyer must be given reasonable notice of such a requirement, except in the case of emergency access.

5. What to do if there is a Delay

- 5.1 If the Supplier becomes aware that there is, or there is reasonably likely to be, a Delay under this Contract it shall:
 - 5.1.1 notify the Buyer as soon as practically possible and no later than within two (2) Working Days from becoming aware of the Delay or anticipated Delay;
 - 5.1.2 include in its notification an explanation of the actual or anticipated impact of the Delay;
 - 5.1.3 comply with the Buyer's instructions in order to address the impact of the Delay or anticipated Delay; and
 - 5.1.4 use all reasonable endeavours to eliminate or mitigate the consequences of any Delay or anticipated Delay.
 - 5.1.5 Delays during implementation will be tracked as part of Performance Management.

6. Implementation Plan

- 6.1 The Implementation Period will be agreed in Delivery Handbook Walkthrough.
- 6.2 The supplier shall have no responsibility for any services until the Call-Off Start Date or as otherwise formally agreed with the Buyer. The Supplier's full-service obligations shall formally be assumed on the Call-Off Start Date as set out in Order Form.
- 6.3 In accordance with the Implementation Plan, the Supplier shall:
 - 6.3.1 work cooperatively and in partnership with the Buyer, and other Framework Supplier(s), where applicable, to understand the scope of Services to ensure a mutually beneficial handover of the Services;
 - 6.3.2 work with the Buyer to assess the scope of the Services and prepare a plan which demonstrates how they will mobilise the Services;
 - 6.3.3 liaise with the Buyer to enable the full completion of the Implementation Period activities; and
 - 6.3.4 produce a Implementation Plan, to be agreed by the Buyer, for carrying out the requirements within the Implementation Period including, key milestones and dependencies.
 - 6.4 The Implementation Plan will include detail stating:
 - 6.4.1 how the Supplier will work with the Buyer Authorised Representative to capture and load up information such as asset data; and
 - 6.4.2 a communications plan, to be produced and implemented by the Supplier, but to be agreed with the Buyer, including the

> frequency, responsibility for and nature of communication with the Buyer.

- 6.5 In addition, the Supplier shall:
 - 6.5.1 appoint a Supplier Authorised Representative who shall be responsible for the management of the Implementation Period, to ensure that the Implementation Period is planned and resourced adequately, and who will act as a point of contact for the Buyer;
 - 6.5.2 mobilise all the Services specified in the Specification within the Call-Off Contract;
 - 6.5.3 produce an Implementation Plan report to encompass the programmes of work that will fulfil all the Buyer's obligations:
 - the format of reports and programmes shall be in accordance with the Buyer's requirements and particular attention shall be paid to establishing the operating requirements; and
 - (b) the Parties shall use reasonable endeavours to agree the contents of the report but if the Parties are unable to agree the contents within twenty (20) Working Days of its submission by the Supplier to the Buyer, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.
 - 6.5.4 manage and report progress against the Implementation Plan;
 - 6.5.5 construct and maintain a Implementation risk and issue register in conjunction with the Buyer detailing how risks and issues will be effectively communicated to the Buyer in order to mitigate them;
 - 6.5.6 attend progress meetings (frequency of such meetings shall be as set out in the Order Form) in accordance with the Buyer's requirements during the Implementation Period. Implementation meetings shall be chaired by the Buyer and all meeting minutes shall be kept and published by the Supplier; and
 - 6.5.7 ensure that all risks associated with the Implementation Period are minimised to ensure smooth commencement of the service.

Annex 1: Implementation Plan

The Implementation Plan is set out below and the Milestones to be Achieved are identified below:



Framework Ref: RM6170 Print Management Services Project Version: v1.0 Model Version: v3.2

Call-Off Schedule 14 (Service Levels)

1. Definitions

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

"Critical Service Level Failure"	Means failure to meet the Critical Service Level performance measures set out in the Annex to Part A
"Service Credits"	Service Credits are a financial remedy for a service performance failure.
	Any service credits specified in the Annex to Part A of this Schedule are 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"	[not used]
"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.

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

- 2.1 The Supplier shall at all times provide the Deliverables to meet or exceed the Service Level Performance Measure for each Service Level.
- 2.2 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.
- 2.3 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.

- 2.4 A Service Credit shall be the Buyer's exclusive financial remedy for a Service Level Failure except where:
 - 2.4.1 [sub-clause deleted]
 - 2.4.2 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
 - 2.4.3 the Buyer is otherwise entitled to or does terminate this Contract pursuant to Clause 10.4 (CCS and Buyer Termination Rights).

For the avoidance of doubt, Service Credits shall not be the exclusive financial remedy for any Service Level Failure which also amounts to a breach of warranty under the Contract and/or a breach of Laws.

- 2.5 Not more than once in each Contract Year, the Buyer may, on giving the Supplier at least three (3) Months' notice, change the weighting or the 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:
 - 2.5.1 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;
 - 2.5.2 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

3. [SUB-CLAUSE DELETED] CRITICAL Service Level Failure

On the occurrence of a Critical Service Level Failure:

- 3.1 The Supplier will rectify critical service errors without additional cost to the Buyer
- 3.2 any Service Credits that would otherwise have accrued during the relevant Service Period shall not accrue; and
- 3.3 the Buyer shall 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.

Part A: Service Levels and Service Credits

1. Service Levels

If the level of performance of the Supplier:

- 1.1 is likely to or fails to meet any Service Level Performance Measure; or
- 1.2 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 require remedial action by the Supplier to "make good" the failure at no additional cost to the Buyer.
- 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).

2. Service Credits

- 2.1 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.
- 2.2 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 the Annex to Part A of this Schedule.

3. SERVICE CREDITS

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



4. Production Of Sample on Receipt of Cohort

The Supplier can turnaround a sample, within the timeframes specified below, from the receipt of a sample data set, templates, and letters.

NOTE: All times are stated in UK local time

4.1 COMPLEX (includes inserts, pictures etc.)

- If sent within business hours (9am 5pm), then the turnaround time is 48hrs, from the time of receipt.
- If sent outside business hours (after 5pm), then the turnaround time is 48hrs, from 9am the next business day.
- If sent outside business hours (before 9am), then the turnaround time is 48hrs, from 9am the same business day.

(Note – If sent on Friday, the 48hrs will expire on the following Tuesday at the receipt time as in the stated rules above. Or Wednesday is sent after 5pm)

4.2 SIMPLE (one A4 letter)

- If sent within business hours (9am 5pm), then the turnaround time is 24hrs, from the time of receipt.
- If sent outside business hours (after 5pm), then the turnaround time is 24hrs, from 9am GMT the next business day.
- If sent outside business hours (before 9am), then the turnaround time is 24hrs, from 9am the same business day.

(Note – If sent on Friday, the 24hrs will expire on the following Monday at the receipt time as in the stated rules above. Or Tuesday is sent after 5pm)

5. Production Of Mailouts on Receipt of Cohort

The third-party Supplier can send out cohort communications, within the timeframe specified below, starting from the timestamp that the approval confirmation of sample communication has been received from the team.

TIMEFRAME

- Small Trials 1 working day
- Medium Trials 2 working days
- Large Trials 3 working days

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

requirements and performance monitoring, including periods of measurement, reporting periods and GDPR measures are A Summary of Service Level Requirements is listed in the table below. A further comprehensive guide to service level included in the embedded excel document at the end of this table.

Payment	Quarterfy credit invoice	Quarterfy credit invoice	Quarterly credit invoice
Remedy or Service credit % measure			
Period/ Unit of Measure ment	Per Batch	Per Batch	Per Batch
Required Service Level Threshold	100% accuracy	100% accuracy	100% accuracy
Service Level Performance Measure	The Supplier will send the correct template (letter, inserts, envelope.) and all associated materials and digital comms which form part of the mail out, in the correct format, to the correct Cohort associated with the trial specified by the Customer.	The print Supplier will meet the sample creation timeline (see Schedule 14, 4 for details) using the correct template, which requires subsequent approval by the Buyer to validate the timelines have been met	The print Supplier will meet the sample creation timeline (see Schedule 14, 4 for details) which requires subsequent approval by the Buyer to validate the timelines have been met
Key Indicator	Correct Mailout templates sent to Cohort	Sample Creation Timeline - Simple	Sample Creation Timeline - Complex
Service Level Performa nce Criterion	Critical Service Failure	Service Level Failure	Service Level Faiture
Ref	4 KPI	KPI 2	3 3 KPI

Framework Ref: RM 6170 Print Management Services Project Version: v1.0 Model Version: v3.1

ω

80
-
3
2
#
yrigh
-¥'
S.
0
0
S
-
¥
2
2
0

Quarterly credit invoice	Quarterly credit invoice	Quarterly credit invoice	N/A	NIA	MIA
Per Batch	Per Batch	Per Batch	Per Batch	Per Batch	Per Batch
100% accuracy	100% accuracy	100% accuracy	100%	100%	100%
The print Supplier will meet the mailout timeline (see Schedule 14,5 for details)	The print Supplier will meet the mailout timeline (see Schedule 14,5 for details)	The print Supplier will meet the mailout timeline (see Schedule 14,5 for details)	The print Supplier will delete/destroy the cohort file in the agreed timeframe (within 20 days and no earlier than 10 days) It will send confirmation of deletion to the Buyer within the agreed timeframe	The print Supplier will destroy the (physical) Returned Cohort Communication letters in the agreed timeframe (within 20 days and no earlier than 10 days) It will send confirmation of deletion to the Buyer within the agreed timeframe	The Print Supplier will provide a quotation with agreed timeline
Cohort Mailout timeline - Small Trial	Cohort Mailout timeline - Medium Trial	Cohort Mailout timeline - Large Trial	Cohort File Destruction	Returned letter destruction	Quotation
Service Level Failure	Service Level Failure	Service Level Failure	Service Level Failure	Service Level Failure	Performa nce Manage ment
4 4	s KPI	6 KPI	КРI 7	8 ⁸⁰	RPI 9

Framework Ref: RM 6170 Print Management Services Project Version: v1.0 Model Version: v3.1

~

4 Z	N/N	A/A
z	Z	Z
Monthly	Per Batch	Batch
100%	100%	100%
Supplier will send monthly involces by the 5th of each month which should be for services delivered the preceding month. Involces should be without errors	The print Supplier will not process the cohort data without an associated approved sample being available	The print Supplier will send the *SENT* Communication notification to the Buyer in the specified timeframe
Invoicing	Processing Cohort data without an approved sample	Batch SENT confirmation
Performa nce Manage ment	Performa nce Manage ment	Performa nce Manage ment
10 I	KPI E	KPI 12

Embedded Document

KPI Final



ice Levels)		
edule 14 (Servi		ight 2018
Call-Off Sch	Call-Off Ref:	Crown Copyr

Part B: Performance Monitoring

PERFORMANCE MONITORING AND PERFORMANCE REVIEW

- 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. 6.1
- with the process and timescales agreed pursuant to paragraph 6.1 of Part B of this Schedule which shall contain, as a minimum, The Supplier shall provide the Buyer with performance monitoring reports ("Performance Monitoring Reports") in accordance the following information in respect of the relevant Service Period just ended: 6.2
- for each Service Level, the actual performance achieved over the Service Level for the relevant Service Period. 6.2.1
- a summary of all failures to achieve Service Levels that occurred during that Service Period. 6.2.2
- 6.2.3 details of any Critical Service Level Failures.
- for any repeat failures, actions taken to resolve the underlying cause and prevent recurrence. 6.2.4
- 6.2.5 Work packages rejected by the Supplier.
- 6.2.6 Escalations to senior management either within the Buyer or the Supplier.
- 6.2.7 Any work undertaken outside of normal operations and standard SLAs.
- 6.2.8 Supplier Sub-Contractor performance (If required).
- 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 6.2.9
- 6.2.10 such other details as the Buyer may reasonably require from time to time.

6.3	The P	The Parties shall attend meetings to discuss Performance Monitoring Reports ("Performance Review Meetings") on a Monthly
	basis. Moni	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:
	6.3.1	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.
	6.3.2	be attended by the Supplier's Representative and the Buyer's Representative; and
	6.3.3	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.
6.4	The n Repre	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.
6.5	The S the p	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.
 Satist	Satisfaction Surveys	surveys
	The E entitl the Si set ou	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 and, without prejudice to other remedies set out in this Contract, the Supplier shall take any reasonable steps required by the Customer to remedy any issues raised.

Call-Off Schedule 15 (Call-Off Contract Management) Call-Off Ref: Crown Copyright 2018

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

1. Definitions

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

"Operational	the board established in accordance with paragraph
Board"	4.1 of this Schedule;
"Project Manager"	the manager appointed in accordance with paragraph 2.1 of this Schedule;

2. Project Management

- 2.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.
- 2.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.
- 2.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

3. Role of the Supplier Contract Manager

- 3.1 The Supplier's Contract Manager's shall be:
 - 3.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;
 - 3.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;
 - 3.1.3 able to cancel any delegation and recommence the position himself; and
 - 3.1.4 replaced only after the Buyer has received notification of the proposed change.
- 3.2 The Buyer may provide revised instructions to the Supplier's Contract Manager's in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

Call-Off Schedule 15 (Call-Off Contract Management) Call-Off Ref: Crown Copyright 2018

3.3 Receipt of communication from the Supplier's Contract Manager's by the Buyer does not absolve the Supplier from its responsibilities, obligations or liabilities under the Contract.

4. Role of the Operational Board

- 4.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.
- 4.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.
- 4.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.
- 4.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member's attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.
- 4.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

5. Contract Risk Management

- 5.1 Both Parties shall pro-actively manage risks attributed to them under the terms of this Call-Off Contract.
- 5.2 The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:
 - 5.2.1 the identification and management of risks;
 - 5.2.2 the identification and management of issues; and
 - 5.2.3 monitoring and controlling project plans.
- 5.3 The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.
- 5.4 The Supplier will maintain a risk register of the risks relating to the Call Off Contract which the Buyer's and the Supplier have identified.

Call-Off Schedule 15 (Call-Off Contract Management) Call-Off Ref: Crown Copyright 2018

Annex: Contract Boards

The Parties agree to operate the following boards at the locations and at the frequencies set out below:

Operational Board

This meeting will be held in the main on-line on a monthly basis. However, once every 3/6 months the meeting may be held face-2-face at either an NHSD site or the supplier site to be determined by DigiTrials.

During periods of intense delivery DigiTrials reserve the right to hold meetings more frequently.

There may be a requirement to create sub-groups comprising of both DigiTrials and Supplier staff to work on individual issues as directed by the Operational Board.



NHS DigiTrials Communication Service – Schedule 20

Improving lives with data and technology

Copyright © 2021 NHS Digital

Call-Off Schedule 20 (Call-Off Specification) Call-Off Ref:

Document filename: Ca	all-Off Schedule 20	(Call-Off Specification)	
Project / Programme Di	igiTrials	Project	DigiTrials Comms Support
Document Reference			
		Status	Issued
Owner		Version	FINAL
Author		Version issue date	20/06/2022

Call-Off Schedule 20 (Call-Off Specification) Call-Off Ref:

Contents

Call-Off Schedule 20 (Call-Off Specification)		4
1.	Purpose	4
2.	NHSD Organisation Background	4
3.	Service Requirements	4
4.	Service Timescales	7
5.	GDPR/DPIA	7
6.	Demand	7
7.	Automation of Content Approvals Process	9
8.	Equality, Diversity, and Inclusion	9
Appendix A: Glossary		11
Call-Off Schedule 20 (Call-Off Specification)

1. Purpose

1.0 This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract to provide a mailout service on behalf of NHS Digital (NHSD) in support of clinical trials.

2. NHSD Organisation Background

- 2.0 NHSD is the national information and technology partner to the health and social care system using digital and technology to transform the NHS and social care.
- 2.1 Founded in 2013, headquartered in Leeds and with over 3500 staff, our systems serve 53M citizens and 1.3M NHS Staff. Our mission is to the harness the power of information and technology to make health and care better.
- 2.2 At NHSD we:
 - Run the core IT infrastructure and services of the health and care system
 - Design, build and procure new digital services and systems
 - Collect, process, link and disseminate data for the health and care system
 - Develop and disseminate IT and data standards
 - Are the cyber security partner to the health and care system
- 2.3 As such we are uniquely positioned to enhance communications between clinical trialists, patients and their general practitioners before, during and after a trial.
- 2.4 The aim of the NHS DigiTrials Communications Mailout Service is to enhance communications between clinical trialists, patients and other relevant stakeholders throughout the trial lifecycle. In addition, the service aims to enhance participant engagement the patient-centricity throughout the participants research journey.
- 2.5 The scope covers postal mail, SMS, and email on behalf of clinical trials, sending communications such as, but not limited to, invitations, trial results, patient information sheets, newsletters, and letters of thanks on behalf of clinical trials using a third-party communications provider.
- 2.6 The plan is to conduct the procurement of a mailing provider over Q1 2021 with a decision being made in May 2022 and the service being up and running by the end of Q2 2022.

3. Service Requirements

- 3.0 Suppliers will be expected to provide the following Services under the Contract in accordance with the Service Level Performance Measures set out under Call-Off Schedule 14 (Service Levels):
 - Prepare sample communication and upload via Proof Approval Portal
 - Prepare validated cohort file data
 - Produce and send cohort communication once approvals have been obtained. Mailout can be:
 - (a) Postal, or

- (b) Digital communication covering email & SMS
- Destruction of validated cohort file within 20 working days of send date but no earlier than 10 working days
- Processing of returned cohort communications
- Send returned cohort communications data to NHSD
- Destruction of returned cohort communications within 20 working days of receipt, but no earlier than 10 working days
- 3.1 See Call-Off Schedule 14 for details on performance management and Service Level Performance Measures.
- 3.2 For further details on security requirements see Schedule 9.
- 3.3 For further details on contract management see Schedule 15.
- 3.4 A diagram detailing Communication Mailout Process is provided, below, for information purposes to assist in the understanding of our requirements.
- 3.5 All file and data transfers will ONLY be done via NHSD secure protocols, which are SEFT and MESH
- 3.6 There is a requirement for the mailout provider to be able to handle ad-hoc changes and amendments from NHSD and their customers.
- 3.7 The mailout provider must have secure storage provision for uploaded content e.g., samples files, templates, redacted content and produced communication samples
- 3.8 The mailout provider must have a process to notify/inform NHSD of whether the batching (or grouping) of communications will save time and/or costs. This functionality should be seamless, on-going, and proactive. This will allow NHSD and their customers to make the relevant decision suitable for every communication
- 3.9 The mailout provider shall have the ability to deliver the same content in alternative formats and in other languages.
- 3.10 The mailout provider shall have the ability to generate / manage unique patient reference codes (possibly using QR codes or similar) that enable letters to be scanned to come back into a digital journey.
- 3.11 The mailout provider shall have the ability show the progress of work done (real time tracking capability) to enable the team to monitor progress. This will include the acknowledgement notification of cohort size received.
- 3.12 The mailout provider shall have the ability provide daily reporting metrics of all cohort communications, for example notification of sent, return to sender email and SMS and opened information.
- 3.13 The mailout provider shall have the ability to enable the team to specify which email address is shown as the sender of an email communication.

4. Service Timescales

4.0 The core mailout service needs to be available Monday through Friday, 8am to 6pm UK Local Time. However, there may be occasions, sometimes on very short notice, when the service needs to be available outside of these hours including weekends in order to help support our service delivery needs.

5. GDPR/DPIA

- 5.0 Further to section 14 of the Core Terms v3.0.8.
- 5.1 The General Data Protection Regulation (GDPR) has been in effect since 25th May 2018 outlining rigorous rules on how personal data should be handled, and also allows individuals to have complete control of their personal data.
- 5.2 For this service it is important that NHSD contract with a supplier that is GDPR compliant. The service supplier must document compliance with ISO27001/-2 standards or similar. In addition, the mailout service supplier must complete the DSP Toolkit as part of the award process. The toolkit can be found at the following link:

Data Security and Protection Toolkit (dsptoolkit.nhs.uk)

5.3 It is a legal requirement under the Data Protection Regulations 2018 that every organisation that processes personal information needs to register with the Information Commissioners Office. The mailout service supplier can do so using the following link:

https://ico.org.uk/for-organisations/data-protection-fee/

- 5.4 As part of the submission response the prospective supplier will have to provide evidence that both the DSP Toolkit and ICO Registrations have been completed. In addition, the prospective supplier will need to provide details of their GDPR policies, procedures, and processes.
- 5.5 As part of the procurement process and at regular intervals throughout the duration of any contract NHSD reserve the right to conduct surveys to understand the mailing providers readiness and compliance level with GDPR.
- 5.6 NHSD also reserves the right to conduct on-site audits of the mailing provider if required.

6. Demand

6.0 NHSD have created a simplified demand model for the next three years. In order to simplify this, we have made a number of assumptions, including categorisation of trials into the size groupings detailed below. Call-Off Schedule 20 (Call-Off Specification) Call-Off Ref:



Trial Sizes





- 6.1 There are a number of factors that can influence the duration and uptake of a trial that are not factored into our model due to the level of complexity:
 - Trial format (virtual vs site-based)
 - Number of sites
 - Disease / condition being investigated
- 6.2 The following assumptions have been made when forecasting expected volumes over the next 4 years:
 - The demand model is based on NHS DigiTrials Commercial Model of receiving a new Recruitment trial every guarter and new Communication trial bi-

monthly. Additional profiling has been added to categorise small/medium/large trials across the 3-year period, with an optional 4th year

- Assumes that the Recruitment Service will be postal which has been the case to-date but digital invitations may start to be introduced. It is likely that the Communication will want to use a blend of postal and digital (using email and SMS) but volumes of each are yet unknown
- Recruitment volumes are based on uptake of those invited signing up to take part in each study
- Recruitment profiling assumes a ramp up and cool down period
- Assumes that clinical trials come to use NHS DigiTrials in phases (e.g. a study looking to recruit

7. Automation of Content Approvals Process

- 7.0 NHSD are in the process of developing a portal that will for the automation of significant parts of the content approvals process using SharePoint Online, PowerApps, Power Automate and SPFX technologies.
- 7.1 This portal will facilitate the upload, review and approval of sample communications as described in the Communication process.
- 7.2 It is a condition of contract letting that suppliers use this portal for all aspects of sample communications once it is operational.

8. Equality, Diversity, and Inclusion

- 8.0 Further to section 28 of the Core Terms v3.0.8.
- 8.1 NHS Digital is committed to promoting equality, diversity, and inclusion.
 - Equality is making sure everyone has the same opportunity to participate and fulfil their potential.
 - Diversity means employing and promoting people from a variety of backgrounds with different styles, needs, perspectives, values, and beliefs.
 - Inclusion is ensuring complete acceptance and a sense of belonging, engagement, and progression for everyone.
- 8.2 In order to fulfil our organisational commitment to creating a fairer society and an equal, inclusive, and diverse workplace we have set ourselves six objectives.
- 8.3 We have three Workforce objectives:
 - deliver appropriate learning and development to ensure that all staff develop a good level of equality and diversity awareness
 - work towards having no difference in the employment outcomes for staff or potential recruits because of protected characteristics

- develop best practice in workforce equality and diversity by creating internal and external networks and supporting positive action initiatives
- 8.4 We also have three service objectives.
 - Guided by industry best practice, when we communicate with the public and service users, we will seek to deliver clearer, more representative, and more accessible information and guidance.
 - We will establish a network of staff who will investigate the ways in which we can
 ensure that our products, policies, and behaviours reflect the communities we serve
 and do not disadvantage or otherwise negatively impact the public and users of our
 services.
 - As the trusted national provider of high-quality information and data about health and social care, we will improve our focus on protected characteristics in the information that we collect and share. By doing so, we will improve knowledge about the health of, and care experienced by, those with protected characteristics.
- 8.5 It is therefore important that we engage with suppliers that share those values.
- 8.6 In particular, for this type of service we may need to be sensitive to the needs of clients whose first language is not English, or those with disabilities (including but not limited to those with hearing or visual impairments).

Call-Off Schedule 20 (Call-Off Specification) Call-Off Ref:

Appendix A: Glossary

Acronym	Title	Brief Description
сти	Clinical Trails Unit	
DPA	Data Processing Agreement	
DPIA	Data Protection Impact Assessment	
DSA	Data Sharing Agreement	Contractual document between the Data Controller(s) and NHS Digital
DSFC	Data Sharing Framework Contract	
DSP	Data Services Platform	
GDPR	General Data Protection Regulation	
ICO	Information Commissioners Office	
NHSD	NHS Digital	





Crown Commercial Service

Core Terms

PSC Core Terms

1. Definitions used in the contract

1.1 Interpret this Contract using Joint Schedule 1 (Definitions).

2. How the contract works

- 2.1 The Supplier is eligible for the award of Call-Off Contracts during the Framework Contract Period.
- 2.2 CCS doesn't guarantee the Supplier any exclusivity, quantity or value of work under the Framework Contract.
- 2.3 CCS has paid one penny to the Supplier legally to form the Framework Contract. The Supplier acknowledges this payment.
- 2.4 If the Buyer decides to buy Deliverables under the Framework Contract it must use Framework Schedule 7 (Call-Off Award Procedure) and must state its requirements using Framework Schedule 6 (Order Form Template and Call-Off Schedules). If allowed by the Regulations, the Buyer can:
- make changes to Framework Schedule 6 (Order Form Template and Call-Off Schedules)
- create new Call-Off Schedules
- exclude optional template Call-Off Schedules
- use Special Terms in the Order Form to add or change terms
- 2.5 Each Call-Off Contract:
- is a separate Contract from the Framework Contract
- is between a Supplier and a Buyer
- includes Core Terms, Schedules and any other changes or items in the completed Order Form
- survives the termination of the Framework Contract
- 2.6 Where the Supplier is approached by an eligible buyer requesting Deliverables or substantially similar goods or services, the Supplier must tell them about this Framework Contract before accepting their order. The Supplier will promptly notify CCS if the eligible buyer won't use this Framework Contract.
- 2.7 The Supplier acknowledges it has all the information required to perform its obligations under each Contract before entering into a Contract. When information is provided by a Relevant Authority no warranty of its accuracy is given to the Supplier.

PSC Core Terms

- 2.8 The Supplier won't be excused from any obligation, or be entitled to additional Costs or Charges because it failed to either:
- verify the accuracy of the Due Diligence Information
- properly perform its own adequate checks
- 2.9 CCS and the Buyer won't be liable for errors, omissions or misrepresentation of any information.
- 2.10 The Supplier warrants and represents that all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

3. What needs to be delivered

3.1 All deliverables

3.1.1 The Supplier must provide Deliverables:

- that comply with the Specification, the Framework Tender Response and, in relation to a Call-Off Contract, the Call-Off Tender (if there is one)
- to a professional standard
- using reasonable skill and care
- using Good Industry Practice
- using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract
- on the dates agreed
- that comply with Law
- 3.1.2 The Supplier must provide Deliverables with a warranty of at least 90 days from Delivery against all obvious defects.

3.2 Goods clauses

- 3.2.1 All Goods delivered must be new, or as new if recycled, unused and of recent origin.
- 3.2.2 All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.
- 3.2.3 The Supplier transfers ownership of the Goods on Delivery or payment for those Goods, whichever is earlier.
- 3.2.4 Risk in the Goods transfers to the Buyer on Delivery of the Goods, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.
- 3.2.5 The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.

- 3.2.6 The Supplier must deliver the Goods on the date and to the specified location during the Buyer's working hours.
- 3.2.7 The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.
- 3.2.8 All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.
- 3.2.9 The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.
- 3.2.10 The Supplier must indemnify the Buyer against the costs of any Recall of the Goods and give notice of actual or anticipated action about the Recall of the Goods.
- 3.2.11 The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable steps to minimise these costs.
- 3.2.12 The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with Clause 3. If the Supplier doesn't do this it will pay the Buyer's costs including repair or resupply by a third party.

3.3 Services clauses

- 3.3.1 Late Delivery of the Services will be a Default of a Call-Off Contract.
- 3.3.2 The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the Delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions.
- 3.3.3 The Supplier must at its own risk and expense provide all Supplier Equipment required to Deliver the Services.
- 3.3.4 The Supplier must allocate sufficient resources and appropriate expertise to each Contract.
- 3.3.5 The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.
- 3.3.6 The Supplier must ensure all Services, and anything used to Deliver the Services, are of good quality and free from defects.

PSC Core Terms

3.3.7 The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

4 Pricing and payments

- 4.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the Charges in the Order Form.
- 4.2 CCS must invoice the Supplier for the Management Charge and the Supplier must pay it using the process in Framework Schedule 5 (Management Charges and Information).
- 4.3 All Charges and the Management Charge:
- exclude VAT, which is payable on provision of a valid VAT invoice
- include all costs connected with the Supply of Deliverables
- 4.4 The Buyer must pay the Supplier the Charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds using the payment method and details stated in the Order Form.
- 4.5 A Supplier invoice is only valid if it:
- includes all appropriate references including the Contract reference number and other details reasonably requested by the Buyer
- includes a detailed breakdown of Delivered Deliverables and Milestone(s) (if any)
- doesn't include any Management Charge (the Supplier must not charge the Buyer in any way for the Management Charge)
- 4.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier if notice and reasons are provided.
- 4.7 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this doesn't happen, CCS or the Buyer can publish the details of the late payment or non-payment.
- 4.8If CCS or the Buyer can get more favourable commercial terms for the supply at cost of any materials, goods or services used by the Supplier to provide the Deliverables and that cost is reimbursable by the Buyer, then CCS or the Buyer may either:
- require the Supplier to replace its existing commercial terms with the more favourable terms
 offered for the relevant items
- enter into a direct agreement with the Subcontractor or third party for the relevant item
- 4.9 If CCS or the Buyer uses Clause 4.8 then the Framework Prices (and where applicable, the Charges) must be reduced by an agreed amount by using the Variation Procedure.

PSC Core Terms

- 4.10 CCS and the Buyer's right to enter into a direct agreement for the supply of the relevant items is subject to both:
- the relevant item being made available to the Supplier if required to provide the Deliverables
- any reduction in the Framework Prices (and where applicable, the Charges) excludes any
 unavoidable costs that must be paid by the Supplier for the substituted item, including any
 licence fees or early termination charges
- 4.11 The Supplier has no right of set-off, counterclaim, discount or abatement unless they're ordered to do so by a court.

5. The buyer's obligations to the supplier

5.1 If Supplier Non-Performance arises from an Authority Cause:

- neither CCS or the Buyer can terminate a Contract under Clause 10.4.1
- the Supplier is entitled to reasonable and proven additional expenses and to relief from Delay Payments, liability and Deduction under this Contract
- the Supplier is entitled to additional time needed to make the Delivery
- the Supplier cannot suspend the ongoing supply of Deliverables

5.2 Clause 5.1 only applies if the Supplier:

- gives notice to the Party responsible for the Authority Cause within 10 Working Days of becoming aware
- demonstrates that the Supplier Non-Performance only happened because of the Authority Cause
- mitigated the impact of the Authority Cause

6. Record keeping and reporting

- 6.1 The Supplier must attend Progress Meetings with the Buyer and provide Progress Reports when specified in the Order Form.
- 6.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the End Date.
- 6.3 The Supplier must allow any Auditor access to their premises to verify all contract accounts and records of everything to do with the Contract and provide copies for an Audit.
- 6.4 The Supplier must provide information to the Auditor and reasonable co-operation at their request.

PSC Core Terms

- 6.5 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:
- tell the Relevant Authority and give reasons
- propose corrective action
- provide a deadline for completing the corrective action
- 6.6 The Supplier must provide CCS with a Self Audit Certificate supported by an audit report at the end of each Contract Year. The report must contain:
- the methodology of the review
- the sampling techniques applied
- details of any issues
- any remedial action taken
- 6.7 The Self Audit Certificate must be completed and signed by an auditor or senior member of the Supplier's management team that is qualified in either a relevant audit or financial discipline.

7. Supplier staff

- 7.1 The Supplier Staff involved in the performance of each Contract must:
- be appropriately trained and qualified
- be vetted using Good Industry Practice and the Security Policy
- comply with all conduct requirements when on the Buyer's Premises
- 7.2 Where a Buyer decides one of the Supplier's Staff isn't suitable to work on a contract, the Supplier must replace them with a suitably qualified alternative.
- 7.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach Clause 27.
- 7.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's Premises and say why access is required.
- 7.5 The Supplier indemnifies CCS and the Buyer against all claims brought by any person employed by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.

8. Rights and protection

8.1 The Supplier warrants and represents that:

- · it has full capacity and authority to enter into and to perform each Contract
- each Contract is executed by its authorised representative
- · it is a legally valid and existing organisation incorporated in the place it was formed

PSC Core Terms

- there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its Affiliates that might affect its ability to perform each Contract
- it maintains all necessary rights, authorisations, licences and consents to perform its obligations under each Contract
- it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform each Contract
- it is not impacted by an Insolvency Event
- it will comply with each Call-Off Contract
- 8.2 The warranties and representations in Clauses 2.10 and 8.1 are repeated each time the Supplier provides Deliverables under the Contract.
- 8.3 The Supplier indemnifies both CCS and every Buyer against each of the following:
- wilful misconduct of the Supplier, Subcontractor and Supplier Staff that impacts the Contract
- non-payment by the Supplier of any tax or National Insurance
- 8.4 All claims indemnified under this Contract must use Clause 26.
- 8.5 CCS or a Buyer can terminate the Contract for breach of any warranty or indemnity where they are entitled to do so.
- 8.6 If the Supplier becomes aware of a representation or warranty that becomes untrue or misleading, it must immediately notify CCS and every Buyer.
- 8.7 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

9. Intellectual Property Rights (IPRs)

- 9.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a nonexclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable it to both:
- receive and use the Deliverables
- make use of the deliverables provided by a Replacement Supplier
- 9.2 Any New IPR created under a Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and New IPRs for the purpose of fulfilling its obligations during the Contract Period.
- 9.3 Where a Party acquires ownership of IPRs incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.

- 9.4 Neither Party has the right to use the other Party's IPRs, including any use of the other Party's names, logos or trademarks, except as provided in Clause 9 or otherwise agreed in writing.
- 9.5 If there is an IPR Claim, the Supplier indemnifies CCS and each Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result.
- 9.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:
- obtain for CCS and the Buyer the rights in Clause 9.1 and 9.2 without infringing any third party IPR
- replace or modify the relevant item with substitutes that don't infringe IPR without adversely affecting the functionality or performance of the Deliverables

10. Ending the contract

- 10.1 The Contract takes effect on the Start Date and ends on the End Date or earlier if required by Law.
- 10.2 The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 3 Months' written notice before the Contract expires.

10.3 Ending the contract without a reason

- 10.3.1 CCS has the right to terminate the Framework Contract at any time without reason or liability by giving the Supplier at least 30 days' notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.
- 10.3.2 Each Buyer has the right to terminate their Call-Off Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice and if it's terminated Clause 10.5.2 to 10.5.7 applies.

10.4 When CCS or the buyer can end a contract

- 10.4.1 If any of the following events happen, the Relevant Authority has the right to immediately terminate its Contract by issuing a Termination Notice to the Supplier:
- there's a Supplier Insolvency Event
- · there's a Contract Default that is not corrected in line with an accepted Rectification Plan
- the Relevant Authority rejects a Rectification Plan or the Supplier does not provide it within 10 days of the request
- there's any material Default of the Contract
- there's any material Default of any Joint Controller Agreement relating to any Contract;
- there's a Default of Clauses 2.10, 9, 14, 15, 27, 32 or Framework Schedule 9 (Cyber Essentials) (where applicable) relating to any Contract

- there's a consistent repeated failure to meet the Performance Indicators in Framework Schedule 4 (Framework Management)
- there's a Change of Control of the Supplier which isn't pre-approved by the Relevant Authority in writing
- there's a Variation to a Contract which cannot be agreed using Clause 24 (Changing the contract) or resolved using Clause 34 (Resolving disputes)
- if the Relevant Authority discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded
- the Court of Justice of the European Union uses Article 258 of the Treaty on the Functioning
 of the European Union (TFEU) to declare that the Contract should not have been awarded to
 the Supplier because of a serious breach of the TFEU or the Regulations
- the Supplier or its Affiliates embarrass or bring CCS or the Buyer into disrepute or diminish the public trust in them
- 10.4.2 CCS may terminate the Framework Contract if a Buyer terminates a Call-Off Contract for any of the reasons listed in Clause 10.4.1.
- 10.4.3 If there is a Default, the Relevant Authority can, without limiting its other rights, request that the Supplier provide a Rectification Plan.
- 10.4.4 When the Relevant Authority receives a requested Rectification Plan it can either:
- reject the Rectification Plan or revised Rectification Plan, giving reasons
- accept the Rectification Plan or revised Rectification Plan (without limiting its rights) and the Supplier must immediately start work on the actions in the Rectification Plan at its own cost, unless agreed otherwise by the Parties
- 10.4.5 Where the Rectification Plan or revised Rectification Plan is rejected, the Relevant Authority:
- must give reasonable grounds for its decision
- may request that the Supplier provides a revised Rectification Plan within 5 Working Days
- 10.4.6 If any of the events in 73 (1) (a) to (c) of the Regulations happen, the Relevant Authority has the right to immediately terminate the Contract and Clause 10.5.2 to 10.5.7 applies.

10.5 What happens if the contract ends

- Where the Relevant Authority terminates a Contract under Clause 10.4.1 all of the following apply:
- 10.5.1 The Supplier is responsible for the Relevant Authority's reasonable costs of procuring Replacement Deliverables for the rest of the Contract Period.