

Contents

Schedules

1	Specification	1
2	Prices and invoicing.....	2
3	Change control	8
4	Commercially sensitive information.....	11
5	Reports and Record Retention.....	13
6	Information assurance & security	19
7	Prisons.....	36
8	Statutory obligations and corporate social responsibility	38
9	Data processing.....	43
10	Tender	49
11	Performance Management/PIP and Action Plan Process.....	50
12	Key Personnel and Key Sub-Contractors.....	53
13	Regional Annex	55
14	Sample Forms	56
15	ESF Publicity Requirements.....	58
16	Training and Apprenticeships	59
17	Access to Authority Case Management System	61
18	Industry Standard Partnering Agreement.....	67
19	Market Stewardship Principles	85
20	Financial Distress	88

Appendices

A	Baseline security requirements	30
B	Data Processing Consent Form	45

Schedule 1

Specification



ESF Specification -
CFO Activity Hubs IT

Schedule 2

Prices and invoicing

Part 1

1 Fees

- 1.1 The Price shall be made up of the following fee elements:
- 1.1.1 Fixed Delivery Fee as further described at paragraph 1.5;
 - 1.1.2 Compliance Fee as further described at paragraph 1.6;
 - 1.1.3 Enrolment Fee as further described at paragraph 1.7; and
 - 1.1.4 Activity Fee as further described at paragraph 1.8; and
 - 1.1.5 Any Profile Payments payable in accordance with paragraphs 1.7 and 1.8.
- 1.2 The Price across the term shall be capped at the ESF Funding Cap and the Authority shall not be obliged to make any payment in excess of the ESF Funding Cap during or after Term
- 1.3 Each fee element of the Price shall be calculated and paid in accordance with this Schedule 2 as supplemented by Part 5 (Payment Mechanism) of the Specification. In the event of any conflict or inconsistency between the provisions in this Schedule 2 and any provisions in the Specification, the provisions in this Schedule 2 shall prevail and take priority.
- 1.4 Any rights in this Schedule 2 for the Authority to suspend the payment of particular fee element of the Price in particular circumstances shall be without prejudice to any other rights or remedies of the Authority under the Contract, including (without limitation) any rights under Schedule 11 (Performance Management/PIP and Action Plan Process).
- 1.5 **Fixed Delivery Fee**
- 1.5.1 Subject to the Supplier's compliance with the Expected Standards, the Authority shall pay a Fixed Delivery Fee in accordance with this paragraph 1.5.
 - 1.5.2 The Fixed Delivery Fee for the whole Term shall be a total sum of £4968,750.00, which shall be payable Monthly in arrears in equal Monthly instalments during the Term.
 - 1.5.3 The Supplier may not invoice for, and the Authority shall not be obliged to pay, any Fixed Delivery Fees (excluding any DAF Funding) during any Expected Standards Failure Period. The Supplier may invoice for any Fixed Delivery Fees accrued but not invoiced during an Expected Standards Failure Period, following the expiry of such Expected Standards Failure Period.
 - 1.5.4 DAF Funding
 - (a) The Supplier may in its Profile allocate a sum no greater than 10% of the Monthly Fixed Delivery Fees (the **DAF Funding**) to a discretionary access fund.
 - (b) The Supplier must comply with the requirements set out in Part 5 of the Specification and in the DAF Guidance (which is made available by the Authority from time to time) and any ESF Requirements in the treatment and use of the DAF Funding.
 - (c) Any DAF Funding must be kept separately from any other funds of the Supplier, and the Supplier shall on request from the Authority provide any information as the Authority may reasonably require in respect of the DAF Funding.

- (d) The Supplier shall use the DAF for spot purchasing of items of ESF Eligible Expenditure (as the same is defined in the ESF Requirements) to support Participants into work and to help individuals overcome specific barriers to work (such as travel and small items of expenditure) subject to and in accordance with the DAF Guidance. All DAF purchases must be Approved by the Authority prior to any invoice being submitted in respect of them.
- (e) The Supplier may not use any DAF Funding for any purposes other than those described in part 5.10 of the Specification.
- (f) Each payment made using the DAF must be linked to a Participant Enrolled on the Authority Case Management System and be used only to reimburse ESF Eligible Expenditure and the Supplier shall provide such evidence and reports in relation to any such payment as may be reasonably required by the Authority from time to time.

1.6 **Compliance Fee**

- 1.6.1 Subject to the Supplier's performance against the Compliance Measures and paragraph 1.6.3 below, the Authority shall pay a Monthly Compliance Fee in accordance with this paragraph 1.6.
- 1.6.2 The Compliance Fee for the whole Term shall be total sum of £993,750.00, which, subject to paragraph 1.6.3, shall be payable Monthly in arrears in equal Monthly instalments during the Term.
- 1.6.3 In the event that in respect of any Month either:
 - (a) any four (4) Compliance Measures are allocated a Red Status in accordance with the relevant process described in Part 5 of the Specification; or
 - (b) the Supplier fails to perform to an acceptable level against any single Critical Compliance Measure;
- 1.6.4 then the Supplier's overall level of performance shall be treated by reference to the relevant process described in Part 5 of the Specification as being "Non-Compliant" meaning that the Compliance Fee for that Month shall be suspended and the Supplier may not invoice for, and the Authority shall not be obliged to pay, that Compliance Fee or the Compliance Fee for any subsequent Month until such time as the Supplier's overall level of performance is treated as being "Compliant". In these circumstances, once the Authority has determined by reference to the relevant process in Part 5 of the Specification that the Supplier's overall level of performance is "Compliant", the relevant suspension of the Compliance Fees shall no longer apply and the Supplier shall be entitled to invoice, and the Authority shall pay in accordance with the terms of this Contract, all of the relevant previously suspended Compliance Fees.
- 1.6.5 For the avoidance of doubt, for the purposes of this paragraph 1.6 and the associated provisions of Part 5 of the Specification, the following matters shall be determined by the Authority, acting reasonably and (where appropriate) after discussion with the Supplier via the relevant Performance Meeting process described in clause 28:-
 - (a) the nature of the Variable Compliance Measures (VCMs) that will be applicable from time to time;
 - (b) the designation of any particular Compliance Measure as being a Critical Compliance Measure; and
 - (c) the assessment of the Supplier's performance against each of the Compliance Measures, including the allocation of a "Red", "Amber" or "Green" status for these purposes.

1.7 Enrolment Fee

- 1.7.1 The Enrolment Fee shall be a fixed unit cost of £200 per Acceptance of Enrolment per Participant in accordance with the Specification. Acceptance of Enrolment in accordance with the relevant requirements set out in the Specification must be evidenced by the Supplier by submitting an Enrolment Form to the Authority Case Management System.
- 1.7.2 Subject to paragraphs 1.7.3 to 1.7.4, the Supplier may invoice for Enrolment Fees at the end of each Month in which the Acceptance of Enrolment occurs.
- 1.7.3 The total Enrolment Fees per Activity Hub available during the Term shall be no higher than £263,600 (the **EF Cap**), and the Authority shall not be obliged to pay for any Enrolment Fees per Activity Hub in excess of the EF Cap.
- 1.7.4 The parties agree and acknowledge that:-
- (a) the number of Accepted Enrolments in each Month during the Term is not intended to exceed the Monthly Enrolment Target set out in the Profile;
 - (b) as at the end of each Month during the Term, the cumulative number of Accepted Enrolments is not intended to exceed a number which equals the sum of the Monthly Enrolment Target for that Month plus the Monthly Enrolment Target for all previous Months during the Term, if any (such cumulative number being the "**Cumulative Enrolment Target**"); and
 - (c) given the EF Cap, the total number of Enrolments is not intended to exceed 1,318 per Activity Hub over the Term (the Total Enrolment Target).
- 1.7.5 Having regard to paragraph 1.7.4 and in respect of any Activity Hub, the Supplier shall not be entitled to invoice for and the Authority shall not be obliged to pay, any Enrolment Fees in respect of Accepted Enrolments in any Month exceeding the Cumulative Enrolment Target. In these circumstances, for each Accepted Enrolment which exceeds the relevant Cumulative Enrolment Target, the Enrolment Fee shall be carried forward to the next following Month. In that next following Month, the Supplier may then invoice for the relevant Enrolment Fees carried forward from the previous Month, together with Enrolment Fees for Enrolments which are Accepted in that next following Month, provided that this does not result in the total number of Accepted Enrolments invoiced by the Supplier in that Month and all preceding Months during the Term (if any) exceeding the Cumulative Enrolment Target. If the relevant total number does exceed the relevant Cumulative Enrolment Target then the Enrolment Fees applicable to the excess number of Accepted Enrolments shall be carried forward and the same process as described in this paragraph 1.7.5 shall apply for each successive Month.
- 1.7.6 From the third full calendar Month following the Services Commencement Date, where, in any Month, the Supplier delivers Accepted Enrolments in respect of any Activity Hub which mean that the total number of Enrolments Accepted during that Month and all previous Months during the Term is between 100% and 115% of the Cumulative Enrolment Target, an additional Monthly Profile Payment of £2,255 per Activity Hub shall be payable, Monthly in arrears. The total Profile Payments available during the Term shall be no higher than £67,650 per Activity Hub and the Authority shall not be obliged to pay any Profile Payments in excess of this sum.
- 1.7.7 In the event that in any Month, having regard to paragraph 1.7.6 and in respect of each Activity Hub the Supplier fails to deliver Accepted Enrolments which mean that the total number of Enrolments Accepted during the Term is not between 100% and 115% of the Cumulative Enrolment Target, the Profile Payment for that Month shall be suspended and the Supplier shall not be entitled to invoice for and the Authority shall not be obliged to pay the relevant Monthly Profile Payment or

any Profile Payment for any subsequent Month until, as at the end of any Month, the total number of Enrolments Accepted in that Month and all previous Months during the Term is between 100% and 115% of the Cumulative Enrolment Target. In these circumstances, once a position is reached as at the end of any subsequent Month in which the total number of Enrolments Accepted in that Month and all previous Months during the Term is between 100% and 115% of the Cumulative Enrolment Target, the relevant suspension of Profile Payments shall cease to apply and the Supplier shall be entitled to invoice for, and the Authority shall pay, all relevant previously suspended Profile Payments.

1.8 Activity Fee

1.8.1 The Activity Fee shall be a fixed unit cost as follows for each of the following Activity Types payable on Acceptance of each relevant Activity in accordance with the Specification:

- (a) SL2 (Human/Citizenship): £200
- (b) SL3 (Community and Social): £100
- (c) SL4 (Interventions and Services): £400

Acceptance of each Activity must be evidenced by the Supplier by submitting an HCAT for each Activity to the Authority Case Management System demonstrating that the relevant Minimum Activity Baseline has been completed and any Activity shall only be treated for the purposes of this schedule 2 as having completed where completion of the relevant Minimum Baseline Activity has been demonstrated to the reasonable satisfaction of the Authority.

1.8.2 Subject to paragraphs 1.8.3 and 1.8.4, the Supplier may invoice for Activity Fees at the end of each Month in which the Completion occurs.

1.8.3 The total Activity Fees available during the Term for each of the following Activity Types shall be no higher than:

- (a) SL2 (Human/Citizenship): £256,000 (per Activity Hub)
- (b) SL3 (Community and Social): £256,000 (per Activity Hub)
- (c) SL4 (Interventions and Services): £256,000 (per Activity Hub)

(the **AF Caps**), and the Authority shall not be obliged to pay for any Activity Fees in excess of the AF Caps.

1.8.4 The parties agree and acknowledge that:

- (a) the number of Accepted Activities in each Month during the Term is not intended to exceed the Monthly Activity Target set out in the Profile;
- (b) as at the end of each Month during the Term, the cumulative number of Accepted Activities is not intended to exceed a number which equals the sum of the Monthly Activity Target for that Month plus the Monthly Activity Target for all previous Months during the Term, if any (such cumulative number being the "**Cumulative Activity Target**"); and
- (c) given the AF Caps, the total number of Activities is not intended to exceed the following for each of the following Activity Types:
 - (i) SL2 (Human/Citizenship): 1,280 (per Activity Hub)
 - (ii) SL3 (Community and Social): 2,560 (per Activity Hub)
 - (iii) SL4 (Interventions and Services): 640 (per Activity Hub)

over the Term (the **Total Activity Targets**).

- 1.8.5 Having regard to paragraph 1.8.4 and in respect of any Activity Hub, the Supplier shall not be entitled to invoice for and the Authority shall not be obliged to pay, any Activity Fees in respect of Accepted Activities in any Month exceeding the Cumulative Activity Target. In these circumstances, for each Accepted Activity which exceeds the relevant Cumulative Activity Target, the Activity Fee shall be carried forward to the next following Month. In that next following Month, the Supplier may then invoice for the relevant Activity Fees carried forward from the previous Month, together with Activity Fees for Activities which are Accepted in that next following Month, provided that this does not result in the total number of Accepted Activities invoiced by the Supplier in that Month and all preceding Months during the Term (if any) exceeding the Cumulative Activity Target. If the relevant total number does exceed the relevant Cumulative Activity Target then the Activity Fees applicable to the excess number of Accepted Activities shall be carried forward and the same process as described in this paragraph 1.8.5 shall apply for each successive Month.
- 1.8.6 From the fifth full calendar Month following the Services Commencement Date, where, in any Month, the Supplier delivers Accepted Activities in respect of any Activity Hub which mean that the total number of Activities Accepted during that Month and all previous Months during the Term is between 100% and 115% of the Cumulative Activity Target, an additional Monthly Profile Payment of £3,010 (per Activity Hub and in respect of each Activity Type) shall be payable, Monthly in arrears. The total Profile Payments available during the Term shall be no higher than £75,250 (per Activity Hub) in respect of each Activity Type and the Authority shall not be obliged to pay any Profile Payments in excess of this sum.
- 1.8.7 In the event that in any Month, having regard to paragraph 1.8.6 and in respect of each Activity Hub the Supplier fails to deliver Accepted Activities which mean that the total number of Activities Accepted during the Term is not between 100% and 115% of the Cumulative Activity Target, the Profile Payment for that Month shall be suspended and the Supplier shall not be entitled to invoice for and the Authority shall not be obliged to pay the relevant Monthly Profile Payment or any Profile Payment for any subsequent Month until, as at the end of any Month, the total number of Activities Accepted in that Month and all previous Months during the Term is between 100% and 115% of the Cumulative Activity Target. In these circumstances, once a position is reached as at the end of any subsequent Month in which the total number of Activities Accepted in that Month and all previous Months during the Term is between 100% and 115% of the Cumulative Activity Target, the relevant suspension of Profile Payments shall cease to apply and the Supplier shall be entitled to invoice for, and the Authority shall pay, all relevant previously suspended Profile Payments.

Part 2

1 Invoice requirements

- 1.1 The Supplier shall comply with all payment requirements set out in section 5 (Payment Mechanism) of the Specification.
- 1.2 All invoices submitted to the Authority must clearly state the word **invoice** and contain the following information:
 - 1.2.1 a breakdown of Activities and Enrolments to which the invoice relates;
 - 1.2.2 a unique identification number (invoice number);
 - 1.2.3 the Supplier's name, address and contact information;
 - 1.2.4 the address of the Premises and the date on which work was undertaken;
 - 1.2.5 the name and address of the department/agency in the Authority with which the Supplier is working;
 - 1.2.6 a clear description of the services, works or goods being invoiced for;
 - 1.2.7 the date the goods or service were provided;
 - 1.2.8 the date of the invoice;
 - 1.2.9 the amount being charged;
 - 1.2.10 VAT amount if applicable;
 - 1.2.11 the total amount owed;
 - 1.2.12 the Purchase Order number; and
 - 1.2.13 the amount of the invoice in sterling or any other currency which is Approved.
- 1.3 All invoices submitted by email must meet the following criteria:
 - 1.3.1 email size must not exceed 4mb
 - 1.3.2 one invoice per file attachment (PDF). Multiple invoices can be attached as separate files; and
 - 1.3.3 any supporting information, backing data etc. must be contained within the invoice PDF file.
- 1.4 Unless Approved, invoices must:
 - 1.4.1 not contain any lines for items which are not in the Purchase Order; and
 - 1.4.2 replicate, as far as possible, the structure of and the information contained in the Purchase Order in respect of the number of lines, line descriptions, price and quantity.
- 1.5 If required by the Authority, the Supplier shall:
 - 1.5.1 register and comply with any reasonable eMarketplace solution adopted for invoicing and procurement catalogues by the Authority; and
 - 1.5.2 submit a structured electronic invoice in an Electronic Data Interchange or XML format

Schedule 3

Change control

Change Notice

(For completion by the Party requesting the Change)



CHANGE NOTICE FORM	
Supporting Documentation should accompany this form where possible	
1. Contract Detail	HMPPS Co-financing Organisation (CFO) provision for the European Social Fund (ESF) 2014-2020 CFO Activity Hubs 2020-2023 in the [region]
2. The Authority / Prime Provider proposes the following variation (Change) to the Contract as follows:	
NOTE: The Change Notice (CN) reference number below will be made up of the first 2 letters of the region e.g. North West = NW or London = LO, a dash, then "CN", a dash, then the number of the CN, e.g. 01, followed by the year, e.g. 2015 = 15. The last letter of the reference will be A if initiated by the Authority, C if initiated by the Contractor. For example for an Authority CN: NW-CN-01-15-A	5. Title of CN:
3. CN No:	
4. Date CN No. (originally) issued/raised:	6 Version No.
7. CN Originator (named lead) and initiating Party/Parties and initiating Party/Parties	
8. Details of proposed Change(s)	<i>Background to changes</i> <i>Detailed proposal</i> <i>Impact of proposed Change(s) including to Profiles (where applicable)</i> <i>Financial implications</i>

	<i>Proposed / Actual timetable for implementation</i> <i>Potential implications if Change Notice is not approved</i>
9. Contract documentation section or sections proposed to be varied or changed	<i>Detail the sections of the Contract that will be affected by this Notice.</i> <i>Detail any proposed updated Profiles (supplied as an attachment(s) with this Notice).</i>
10. If new supply chain partners are to be introduced please describe why and how they were selected	
11. Any other considerations	
12. Expiry of Validity of CN, if applicable	

	Date	Signature
Approved by: Head of Co-Financing Mark Nickson		

Variation Form

(For completion by the Authority once the Change has been agreed in principle by both Parties.
Changes do not become effective until this form has been signed by both Parties.)



Ministry
of Justice

Variation to Contract Form



1. Contract Title:	HMPPS Co-financing Organisation (CFO) provision for the European Social Fund (ESF) CFO Activity Hubs in [region]
2. Contract Reference:	[insert reference]
3. Variation Number:	[insert number]
4. Date Effective From:	[insert date]
5. Supplier Name	[insert supplier]

6. Between:

The Secretary of State for The Ministry of Justice, represented by the Commercial and Contract Management Directorate (hereinafter called "the Authority") & [insert supplier]

7. It is agreed that the Contract is amended, in accordance with Regulation 72 of the Public Contracts Regulations 2015, as follows:

--

8. Where significant changes have been made to the Contract, information previously published on Contracts Finder will be updated.

9. The Parties hereto accept the proposals set out above in this Variation, as well as the contents of any attachments referenced herein, as a Change / variation to the Contract (cited in sections 1 and 2 of this form above) and as witness thereof have duly executed this Variation.

10. Save as herein expressly amended all other terms and conditions of the Contract shall remain unaltered and shall continue in full force and effect.

11. Save where the context otherwise requires, terms defined in the Contract, its Schedules and Appendices shall have the same meaning where used in this Variation.

12. The Contract, including any previous Variation Forms, shall remain effective and unaltered except as amended by this Variation Form

13. This form may be executed in any number of counterparts, all of which when taken together shall constitute one and the same instrument for authorising this Variation.

Signed for and on behalf of the Secretary of State for Justice		Signed for and on behalf of [insert name of Supplier]	
Signature		Signature	
Name		Name	
Title		Title	
Date		Date	

Schedule 4

Commercially sensitive information

- 1 Without prejudice to the Authority's general obligation of confidentiality, the Parties acknowledge that the Authority may have to disclose Information in or relating to the Contract following a Request for Information pursuant to clause 25 (Freedom of Information).
- 2 In this Schedule 4 the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be contrary to the public interest.
- 3 Where possible the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule 4 applies.
- 4 Without prejudice to the Authority's obligation to disclose Information in accordance with the FOIA and the EIR, the Authority will, acting reasonably but in its sole discretion, seek to apply the commercial interests exemption set out in s.43 of the FOIA to the Information listed below.

Supplier's commercially sensitive information	Date	Duration of confidentiality
All references to specific people and partners and members of our Supply Chain/subcontractors and any Management Fees: We consider information pertaining to our Supply Chain arrangements to be Commercially Sensitive Information (CSI), particularly specific references to Management Fees applied to specific partnership arrangements. This is due to the harm that access to elements of our service delivery models could cause. We believe this information is exempt from disclosure pursuant to section 43 of the FOIA.	22/10/20	Contract Lifetime
Performance statistics set out in our proposal showing existing performance under analogous contracts: Our Proposal contains current statistics as to performance which are not public information and are not published by other procurers. This information is	22/10/20	Contract lifetime and indefinitely thereafter

Commercially Sensitive Information (CSI), and disclosure of it could prejudice our legitimate commercial interests on existing contracts and as part of this procurement as other providers seek to replicate this performance. Further, the statistical information is subject to confidentiality restrictions in accordance with the terms of our contracts with other procurers. This information should consequently be exempt from disclosure under either ss. 43 and 41 of the FOIA.		

Schedule 5

Reports and Record Retention

1 Reports

General instructions

- 1.1 The Supplier shall produce Reports as directed by the Authority and in compliance with this Schedule 5. The Supplier shall submit an original hard copy and an electronic copy of each Report to the Authority's Representative.
- 1.2 The Supplier shall provide a Monthly report (in such format as the Authority may request from time to time) including an overview of events during the reporting period and the following as a minimum:
 - 1.2.1 Details of any proposed Key Personnel changes, staffing compliment and vacancies;
 - 1.2.2 Details of any Fixed/Voluntary Compliance Measures;
 - 1.2.3 Targets and outputs achieved will be in accordance with Schedule 10 (Tender) including Project Budget & Pricing Profile and Participant Throughput and Activity Profile;
 - 1.2.4 Area of concerns or any weakness in the performance of the contract together with any corresponding actions;
 - 1.2.5 Incidents, Data Breaches, Health & Safety Concerns;
 - 1.2.6 Quality visit feedback, recommendations and actions;
 - 1.2.7 Such other information as the Authority may reasonably request from time to time.
- 1.3 Reporting requirements will be reviewed upon contract award and finalised during the Implementation Period.

2 Management and control of documentation

2.1 Supplier's records

- 2.1.1 The Supplier shall keep secure and maintain, until twelve (12) years after the final payment of all sums due under the Contract, or such longer period as may be agreed between the parties, full and accurate records of the Contract, all expenditure reimbursed by the Authority and all payments made by the Authority sufficient to permit a detailed audit trail, unless a shorter period of document retention is permissible in accordance with paragraph 2.5.
- 2.1.2 The Supplier shall at all times:
 - (a) maintain a full record of the particulars of the costs of performing the Contract, including those relating to subcontracted Services. Such records shall further include details of any commitments made by the Supplier for future expenditure and details of any funds held by the Supplier; and
 - (b) when requested by the Authority the aforementioned costs in such form and detail as the Authority may reasonably require.
- 2.1.3 For the duration of the Contract the Supplier shall furnish to the Authority:
 - (a) as soon as they become available (and in any event within six (6) calendar Months of the end of each of its financial periods) copies of its audited financial

statements for that period which shall contain an income statement and a balance sheet and a cash flow statement and be audited and certified without qualification by a firm of independent accountants;

- (b) as soon as they become available (and in any event within three (3) calendar Months of the end of each of its financial half-years and within three (3) calendar Months of each review date) copies of its un-audited financial statements for that half-year or year (as the case may be) which shall contain an income statement, a balance sheet and a cash flow statement;
- (c) shall prepare their financial statements on a basis consistently applied in accordance with generally accepted accounting principles in England and Wales and those financial statements shall give a true and fair view of results of its operations for the period in question and the state of its affairs as at the date to which the financial statements are made up and shall disclose or reserve against all liabilities (actual or contingent) of the Supplier; and
- (d) shall submit to the Authority, within three (3) calendar Months of the end of each contract year, a financial statement for that period, including only the income and expenditure relating to this Contract.

2.1.4 The Supplier shall keep books of account in accordance with best accountancy practise with respect to the Contract showing in detail:

- (a) expenditure on wages and salaries;
- (b) administrative overheads;
- (c) expenditure on consumable items;
- (d) payments made to Sub-Contractors/contractors;
- (e) capital and revenue expenditure;
- (f) other expenditure incurred by the Supplier in the day to day performance of the Contract;
- (g) record of all goods or services obtained at no charge from the Authority or any other government agency; and
- (h) the Supplier shall have items available above for inspection by the Authority upon reasonable notice, and shall present a report of the same to the Authority as and when requested.

2.1.5 The Supplier shall procure that the following are maintained:

- (a) an accurate record of the Authority's Property at the Authority's Premises (where applicable);
- (b) an accurate record of the Supplier's Property at the Authority's Premises (where applicable);
- (c) a full record of all incidents relating to health, safety and security which occur during the Term; and
- (d) the Supplier shall have the items required by paragraph 2.1.5 available for inspection by the Authority as and when requested. The Supplier shall maintain such other records and make the same available to the Authority as the Authority may reasonably require.

2.2 The Documentation

- 2.2.1 During the term of this Contract, certain documentation shall be produced by or for the Supplier. For the purpose of these Administrative Instructions, documentation shall be defined as any item or document which relates to the performance of the Contract ("the **Documentation**") and shall, without limitation, include such other documents which relate to the performance of the Contract, including, whether as hard copy or electronic data.

2.3 **Security and confidentiality of documentation**

- 2.3.1 From the Commencement Date the Supplier shall be responsible for the security and confidentiality of all Documentation. The Supplier shall control and monitor the issue, use and return of the Documentation issued by the Supplier to his Sub-contractors, contractors and third parties and the security and safe storage of such Documentation.
- 2.3.2 The Supplier shall procure that the Documentation is managed and controlled by its Sub-contractors and contractors (as appropriate) in the manner set out in this Schedule.
- 2.3.3 The Supplier shall use best endeavours to ensure that, after the Commencement Date, Documentation shall only be issued for review outside the Authority where it is absolutely necessary.
- 2.3.4 The Supplier shall at all times comply with the National Offender Management Service Security Manual, The Home Office IT Security Manual, the British Standard of Information Security Management BS 7799-2:1999 (as amended or replaced from time to time), such other instructions relating to Document Security (including the Authority's Construction Unit "Technical Instructions") and any other relevant NOMS guidance and policies as may be issued by the Authority (including any revisions or amendments thereto).
- 2.3.5 Documentation issued to the Supplier remains at all times the premises of the Authority and on termination or expiry of the Contract shall either be returned to the Authority in accordance with the Contract, or be certified by the Supplier as having been destroyed in a secure manner or shall be retained by the Supplier pursuant to this Schedule.
- 2.3.6 The Authority operates a procedure to control and monitor the issue, use and return of Documentation issued to others. The Supplier will notify the Authority in writing of their nominated Document Security Officer, who will be the focal point for inquiries on all matters related to this subject and shall provide all reasonable support and assistance to the Authority in any control or monitoring it requires of the Documentation.
- 2.3.7 These security requirements have been incorporated in order to prevent information detrimental to the security of the Authority coming into the possession of unauthorised persons and at the same time establish an audit trail of Documentation movement.
- 2.3.8 The Supplier shall be responsible at all times for the security of all Documentation in the keeping of the Supplier whether issued by the Authority or copied or produced by the Supplier or its agents.
- 2.3.9 The Supplier shall notify all Supplier's Staff handling Documentation of the requirements imposed by the Authority and of the procedures for maintaining security. The Supplier shall notify all others (including (without limitation) Sub-Contractors) having an interest in the Contract of the particular requirements imposed regarding Documentation security.
- 2.3.10 The Supplier shall include in all contracts with Sub-Contractors similar but no less strict conditions of Documentation security and shall be responsible for their compliance.

- 2.3.11 The Supplier shall be responsible for ensuring that Documentation issued to others is returned.
- 2.3.12 The Supplier shall arrange for the secure destruction and recording of any Documentation that is no longer required, have been superseded or are additional to the Supplier's requirements.
- 2.3.13 The Supplier shall provide secure computer systems.
- 2.3.14 Lockable cabinets and cupboards will be used for storing Documentation and these shall be kept locked at all times when not in use and secured at all times when offices are unoccupied.
- 2.3.15 The Supplier shall report immediately to the Authority's Representative by the most expedient method the loss of any Documentation stating details of the loss and what the Supplier is doing to secure its recovery. A record of the loss, action taken by the Supplier and outcome will be made in the Supplier's Monthly report.

2.4 Arrangements upon termination or expiry of this contract

- 2.4.1 The Supplier shall safeguard and secure Documentation throughout the Contract or until the Contract is terminated. Upon expiry or termination of the Contract, the Supplier shall agree with the Authority in writing what Documentation shall be returned or destroyed or retained by the Supplier. Any Documentation that the Supplier is required to retain shall be securely stored in accordance with this Schedule.

2.5 Retention of records

- 2.5.1 The following table details the minimum period for which the Supplier shall retain Documentation. The retention periods are on a rolling basis. All Documentation held by the Supplier upon expiry or earlier termination of the Contract must be retained for a period of twelve (12) years after the end of the Contract regardless of the period specified below:-

Document Type	Retention Period
Financial records	12 years beyond contract end date
Incident records	12 years beyond contract end date
Complaint records	12 years beyond contract end date
Record of visitors	12 years beyond contract end date
Personnel records	12 years beyond contract end date
Staffing details	12 years beyond contract end date
Administrative records	12 years beyond contract end date

- 2.5.2 The Supplier shall notify the Authority if there are any legislative requirements, which would necessitate the retention of certain Documentation for longer periods than those specified above and the parties shall agree a reasonable extension of such periods.

- 2.5.3 The retention periods apply to the primary source documents and any electronic or other types of records produced.
- 2.5.4 All Documentation including those which provide full and accurate records of the Services, all expenditure reimbursed by the Authority and all payments made by the Authority, must be retained securely for a period of twelve (12) years after the final payment of all sums due under the Contract, regardless of the period specified above.
- 2.5.5 To those records as they may reasonably require in order to review the Supplier's compliance with the Contract or for the extraction of information. Clause 32 of the Contract refers.

2.6 **Alternative methods of documentation storage**

- 2.6.1 The provision of the Services will generate a large volume of Documentation. The Supplier may propose alternative means of storage such as microfiche or electronic format for Approval. Any such proposals must comply with Relevant Legislation such as: Public Records Acts 1958 and 1967, the Taxes Management Act 1970, the Value Added Tax Act 1994, the Companies Act 1985, EU Regulations and the Statute of Limitations.
- 2.6.2 The National Audit Office requires sight of certain original documents when conducting its audits. These include documents such as contracts, agreements, guarantees and titles to property, which may also be required as evidence to the courts. The Supplier shall ensure that if alternative methods of document storage are proposed there must be stated methods of minimising the potential risks that may arise.

Examples of potential risks are:
 - (a) The creation of unauthorised records;
 - (b) The creation of duplicated records;
 - (c) Corrupt, incomplete or illegible copies;
 - (d) Misleading copies e.g. alterations to the original not shown, subject to unauthorised alteration (accidental or deliberate), not the current version, not indexed to related documents;
 - (e) Unavailable for use due to system failure;
 - (f) Lost within the system; and
 - (g) Lost outside the system or destroyed.
- 2.6.3 Any such proposed system shall offer no opportunity for records/documents to be amended without an audit trail. The Supplier shall detail to the Authority for Approval how it shall minimise these risks.
- 2.6.4 Effective document management systems normally provide the following facilities:
 - (a) Data capture – the means of transferring the originals to the alternative means of storage and after data capture a quality assurance process to ensure that the document has been captured accurately and can be reproduced;
 - (b) Indexing - identifies and classifies documents for retrieval and a quality assurance process to ensure that a document has been properly indexed;
 - (c) Storage media - which provide sufficient capacity and security;

- (d) Manipulation - enables the stored documents to be combined or manipulated to create new documents;
- (e) Networks - enable the stored documents to be shared and exchanged;
- (f) Workflow – systems and/or software which enables only particular personnel to view, authorise, edit, annotate, print etc. the stored records;
- (g) Retrieval, display and print.

2.6.5 The Supplier shall advise the Authority what facilities would be included under this Contract to be Approved.

3 Document Retention Policy

- 3.1 The Supplier shall produce and maintain a Document Retention Policy detailing how they will comply with this Schedule 5, and shall provide a copy of such policy to the Authority upon request.

Schedule 6

Information assurance & security

1 General

- 1.1 This Schedule 6 sets out the obligations of the Parties in relation to information assurance and security, including those which the Supplier must comply with in delivering the Services under the Contract.
- 1.2 The Parties acknowledge that the purpose of the ISMS and Security Plan is to ensure a robust organisational approach to information assurance and security under which the specific requirements of the Contract will be met.
- 1.3 The Parties shall each appoint and/or identify a board level individual or equivalent who has overall responsibility for information assurance and security, including personnel security and information risk. The individual appointed by the Supplier, who is the Chief Security Officer, Chief Information Officer, Chief Technical Officer or equivalent and is responsible for compliance with the ISMS, is identified as Key Personnel and the provisions of clause 12 apply in relation to that person.
- 1.4 The Supplier shall act in accordance with Good Industry Practice in the day to day operation of any system which is used for the storage of Information Assets and/or the storage, processing or management of Authority Data and/or that could directly or indirectly affect Information Assets and/or Authority Data.
- 1.5 The Supplier shall ensure that an information security policy is in place in respect of the operation of its organisation and systems, which shall reflect relevant control objectives for the Supplier System, including those specified in the ISO27002 control set or equivalent, unless otherwise agreed by the Authority. The Supplier shall, upon request, provide a copy of this policy to the Authority as soon as reasonably practicable. The Supplier shall maintain and keep such policy updated and provide clear evidence of this as part of its Security Plan.
- 1.6 The Supplier acknowledges that a compromise of Information Assets and/or Authority Data represents an unacceptable risk to the Authority requiring immediate communication and co-operation between the Parties. The Supplier shall provide clear evidence of regular communication with the Authority in relation to information risk as part of its Security Plan.

2 Information security management system

- 2.1 The Supplier shall, within 30 Working Days of the Commencement Date, submit to the Authority a proposed ISMS which:
 - 2.1.1 has been tested; and
 - 2.1.2 complies with the requirements of paragraphs 2.2 and 2.3.
- 2.2 The Supplier shall at all times ensure that the level of security, include cyber security, provided by the ISMS is sufficient to protect the confidentiality, integrity and availability of Information Assets and Authority Data used in the provision of the Services and to provide robust risk management.
- 2.3 The Supplier shall implement, operate and maintain an ISMS which shall:
 - 2.3.1 protect all aspects of and processes of Information Assets and Authority Data, including where these are held on the ICT Environment (to the extent that this is under the control of the Supplier);
 - 2.3.2 be aligned to and compliant with the relevant standards in ISO/IEC 27001: 2013 or equivalent and the Certification Requirements in accordance with paragraph 5 unless otherwise Approved;

- 2.3.3 provide a level of security which ensures that the ISMS and the Supplier System:
 - (a) meet the requirements in the Contract;
 - (b) are in accordance with applicable Law;
 - (c) demonstrate Good Industry Practice, including the Government's 10 Steps to Cyber Security, currently available at: <https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>;
 - (d) comply with the Security Policy Framework and any other relevant Government security standards;
 - (e) comply with the Baseline Security Requirements;
 - (f) comply with the Authority's policies, including, where applicable, the Authority's Information Assurance Policy in PSI 24/2014;
- 2.3.4 address any issues of incompatibility with the Supplier's organisational security policies;
- 2.3.5 address any specific security threats of immediate relevance to Information Assets and/or Authority Data;
- 2.3.6 document:
 - (a) the security incident management processes, including reporting, recording and management of information risk incidents, including those relating to the ICT Environment (to the extent that this is within the control of the Supplier) and the loss of protected Personal Data, and the procedures for reducing and raising awareness of information risk;
 - (b) incident response plans, including the role of nominated security incident response companies; and
 - (c) the vulnerability management policy, including processes for identification of system vulnerabilities and assessment of the potential effect on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing and application of security patches and the reporting and audit mechanism detailing the efficacy of the patching policy;
- 2.3.7 include procedures for the secure destruction of Information Assets and Authority Data and any hardware or devices on which such information or data is stored; and
- 2.3.8 be certified by (or by a person with the direct delegated authority of) the Supplier's representative appointed and/or identified in accordance with paragraph 1.3.
- 2.4 If the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies notified to the Supplier from time to time, the Supplier shall immediately notify the Authority of such inconsistency and the Authority shall, as soon as practicable, notify the Supplier of the provision that takes precedence.
- 2.5 The Supplier shall, upon request from the Authority or any accreditor appointed by the Authority, provide sufficient design documentation detailing the security architecture of its ISMS to support the Authority's and/or accreditor's assurance that it is appropriate, secure and complies with the Authority's requirements.
- 2.6 The Authority shall review the proposed ISMS submitted pursuant to paragraph 2.1 and shall, within 10 Business Days of its receipt notify the Supplier as to whether it has been approved.

- 2.7 If the ISMS is Approved, it shall be adopted by the Supplier immediately and thereafter operated and maintained throughout the Term in accordance with this Schedule 6.
- 2.8 If the ISMS is not Approved, the Supplier shall amend it within 10 Business Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Authority shall, within a further 10 Working Days notify the Supplier whether the amended ISMS has been approved. The Parties shall use reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 30 Working Days from the date of its first submission to the Authority. If the Authority does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with clause 46 (Dispute Resolution).
- 2.9 Approval of the ISMS or any change to it shall not relieve the Supplier of its obligations under this Schedule 6.
- 2.10 The Supplier shall provide to the Authority, upon request, any or all ISMS documents.

3 Security plan

- 3.1 The Supplier shall, within 30 Working Days of the Service Start Date, submit to the Authority for approval a Security Plan which complies with paragraph 3.2.
- 3.2 The Supplier shall effectively implement the Security Plan which shall:
- 3.2.1 comply with the Baseline Security Requirements;
 - 3.2.2 identify the organisational roles for those responsible for ensuring the Supplier's compliance with this Schedule 6;
 - 3.2.3 detail the process for managing any security risks from those with access to Information Assets and/or Authority Data, including where these are held in the ICT Environment;
 - 3.2.4 set out the security measures and procedures to be implemented by the Supplier, which are sufficient to ensure compliance with the provisions of this Schedule 6;
 - 3.2.5 set out plans for transition from the information security arrangements in place at the Commencement Date to those incorporated in the ISMS;
 - 3.2.6 set out the scope of the Authority System that is under the control of the Supplier;
 - 3.2.7 be structured in accordance with ISO/IEC 27001: 2013 or equivalent unless otherwise Approved;
 - 3.2.8 be written in plain language which is readily comprehensible to all Staff and to Authority personnel engaged in the Services and reference only those documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule 6; and
 - 3.2.9 comply with the Security Policy Framework and any other relevant Government security standards.
- 3.3 The Authority shall review the Security Plan submitted pursuant to paragraph 3.1 and notify the Supplier, within 10 Business Days of receipt, whether it has been approved.
- 3.4 If the Security Plan is Approved, it shall be adopted by the Supplier immediately and thereafter operated and maintained throughout the Term in accordance with this Schedule 6.
- 3.5 If the Security Plan is not Approved, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit it to the Authority for approval. The Authority shall notify the Supplier within a further 10 Business Days whether it has been approved.

- 3.6 The Parties shall use reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 30 Working Days from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter shall be resolved in accordance with clause 46 (Dispute Resolution).
- 3.7 Approval by the Authority of the Security Plan pursuant to paragraph 3.3 or of any change to the Security Plan shall not relieve the Supplier of its obligations under this Schedule 6.

4 Revision of the ISMS and security plan

- 4.1 The ISMS and Security Plan shall be reviewed in full and tested by the Supplier at least annually throughout the Term (or more often where there is a significant change to the Supplier System or associated processes or where an actual or potential Breach of Security or weakness is identified) to consider and take account of:
- 4.1.1 any issues in implementing the Security Policy Framework and/or managing information risk;
 - 4.1.2 emerging changes in Good Industry Practice;
 - 4.1.3 any proposed or actual change to the ICT Environment and/or associated processes;
 - 4.1.4 any new perceived, potential or actual security risks or vulnerabilities;
 - 4.1.5 any ISO27001: 2013 audit report or equivalent produced in connection with the Certification Requirements which indicates concerns; and
 - 4.1.6 any reasonable change in security requirements requested by the Authority.
- 4.2 The Supplier shall give the Authority the results of such reviews as soon as reasonably practicable after their completion, which shall include without limitation:
- 4.2.1 suggested improvements to the effectiveness of the ISMS, including controls;
 - 4.2.2 updates to risk assessments; and
 - 4.2.3 proposed modifications to respond to events that may affect the ISMS, including the security incident management processes, incident response plans and general procedures and controls that affect information security.
- 4.3 Following the review in accordance with paragraphs 4.1 and 4.2 or at the Authority's request, the Supplier shall give the Authority at no additional cost a draft updated ISMS and/or Security Plan which includes any changes the Supplier proposes to make to the ISMS or Security Plan. The updated ISMS and/or Security Plan shall, unless otherwise agreed by the Authority, be subject to clause 31 (Change) and shall not be implemented until Approved.
- 4.4 If the Authority requires any updated ISMS and/or Security Plan to be implemented within shorter timescales than those set out in clause 31, the Parties shall thereafter follow clause 31 for the purposes of formalising and documenting the relevant change for the purposes of the Contract.

5 Certification requirements

- 5.1 The Supplier shall ensure that any systems, including the ICT Environment, on which Information Assets and Authority Data are stored and/or processed are certified as compliant with:
- 5.1.1 ISO/IEC 27001:2013 or equivalent by a UKAS approved certification body or are included within the scope of an existing certification of compliance with ISO/IEC 27001:2013 or equivalent unless otherwise Approved; and

- 5.1.2 the Government's Cyber Essentials Scheme at the BASIC level unless otherwise agreed with the Authority and shall provide the Authority with evidence:
 - 5.1.3 of certification before the Supplier accessed the ICT Environment and receives, stores, processes or manages any Authority Data; and
 - 5.1.4 that such certification remains valid and is kept up to date while the Supplier (as applicable) continues to access the ICT Environment and receives, stores, processes or manages any Authority Data during the Term.
- 5.2 The Supplier shall ensure that it:
- 5.2.1 carries out any secure destruction of Information Assets and/or Authority Data at Supplier sites which are included within the scope of an existing certificate of compliance with ISO/IEC 27001:2013 or equivalent unless otherwise Approved; and
 - 5.2.2 is certified as compliant with the CESG Assured Service (CAS) Service Requirement Sanitisation Standard or equivalent unless otherwise Approved
- and the Supplier shall provide the Authority with evidence of its compliance with the requirements set out in this paragraph 5.2 before the Supplier may carry out the secure destruction of any Information Assets and/or Authority Data.
- 5.3 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier ceases to be compliant with the certification requirements in paragraph 5.1 and, on request from the Authority, shall:
- 5.3.1 immediately cease access to and use of Information Assets and/or Authority Data; and
 - 5.3.2 promptly return, destroy and/or erase any Authority Data in accordance with the Baseline Security Requirements and failure to comply with this obligation is a material Default.

6 Security testing

- 6.1 The Supplier shall, at its own cost, carry out relevant Security Tests from the Commencement Date and throughout the Term, which shall include:
- 6.1.1 a Monthly vulnerability scan and assessment of the Supplier System and any other system under the control of the Supplier on which Information Assets and/or Authority Data are held;
 - 6.1.2 an annual IT Health Check by an independent CHECK qualified company of the Supplier System and any other system under the control of the Supplier on which Information Assets and/or Authority Data are held and any additional IT Health Checks required by the Authority and/or any accreditor;
 - 6.1.3 an assessment as soon as reasonably practicable following receipt by the Supplier of a critical vulnerability alert from a provider of any software or other component of the Supplier System and/or any other system under the control of the Supplier on which Information Assets and/or Authority Data are held; and
 - 6.1.4 such other tests as are required:
 - (a) by any Vulnerability Correction Plans;
 - (b) by ISO/IEC 27001:2013 certification requirements or equivalent Approved;
 - (c) after any significant architectural changes to the ICT Environment;

- (d) after a change to the ISMS (including security incident management processes and incident response plans) or the Security Plan; and
 - (e) following a Breach of Security.
- 6.2 In relation to each IT Health Check, the Supplier shall:
 - 6.2.1 agree with the Authority the aim and scope of the IT Health Check;
 - 6.2.2 promptly, following receipt of each IT Health Check report, give the Authority a copy of the IT Health Check report;
 - 6.2.3 in the event that the IT Health Check report identifies any vulnerabilities:
 - (a) prepare a Vulnerability Correction Plan for Approval which sets out in respect of each such vulnerability:
 - (i) how the vulnerability will be remedied;
 - (ii) the date by which the vulnerability will be remedied;
 - (iii) the tests which the Supplier shall perform or procure to be performed (which may, at the Authority's discretion, include a further IT Health Check) to confirm that the vulnerability has been remedied;
 - (b) comply with the Vulnerability Correction Plan; and
 - (c) conduct such further Security Tests as are required by the Vulnerability Correction Plan.
- 6.3 Security Tests shall be designed and implemented by the Supplier so as to minimise any adverse effect on the Services and the date, timing, content and conduct of Security Tests shall be agreed in advance with the Authority.
- 6.4 The Authority may send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Authority with the results of Security Tests (in a form to be Approved) as soon as practicable and in any event within 5 Working Days after completion of each Security Test.
- 6.5 Without prejudice to any other right of audit or access granted to the Authority pursuant to the Contract, the Authority and/or its authorised representatives, including any accreditor, may at any time to carry out Security Tests (including penetration tests) as it may deem necessary as part of any accreditation process and/or to verify the Supplier's compliance with the ISMS and the Security Plan:
 - 6.5.1 upon giving reasonable notice to the Supplier where reasonably practicable to do so; and
 - 6.5.2 without giving notice to the Supplier where, in the Authority's view, the provision of such notice may undermine the Security Tests to be carried out and, where applicable, the Authority shall be granted access to the Supplier's premises for the purpose of undertaking the relevant Security Tests.
- 6.6 If the Authority carries out Security Tests in accordance with paragraphs 6.5.1 or 6.5.2, the Authority shall (unless there is any reason to withhold such information) notify the Supplier of the results of the Security Tests as soon as possible and in any event within 5 Working Days after completion of each Security Test.
- 6.7 If any Security Test carried out pursuant to paragraphs 6.1 or 6.4 reveals any:
 - 6.7.1 vulnerabilities during any accreditation process, the Supplier shall track and resolve them effectively; and

- 6.7.2 actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Authority of any proposed changes to the ICT Environment (to the extent that this is under the control of the Supplier) and/or to the ISMS and/or to the Security Plan (and the implementation thereof) which the Supplier intends to make in order to correct such failure or weakness. Subject to Approval and paragraph 4.3 and 4.4, the Supplier shall implement such changes to the ICT Environment (to the extent that this is under the control of the Supplier) and/or the ISMS and/or the Security Plan and repeat the relevant Security Tests in accordance with an Approved timetable or, otherwise, as soon as reasonably practicable.
- 6.8 If the Authority unreasonably withholds its approval to the implementation of any changes to the ICT Environment and/or to the ISMS and/or to the Security Plan proposed by the Supplier in accordance with paragraph 6.7, the Supplier is not in breach of the Contract to the extent that it can be shown that such breach:
 - 6.8.1 has arisen as a direct result of the Authority unreasonably withholding Approval to the implementation of such proposed changes; and
 - 6.8.2 would have been avoided had the Authority Approved the implementation of such proposed changes.
- 6.9 If a change to the ISMS or Security Plan is to address any non-compliance with ISO/IEC 27001:2013 requirements or equivalent, the Baseline Security Requirements or any obligations in the Contract, the Supplier shall implement such change at its own cost and expense.
- 6.10 If any repeat Security Test carried out pursuant to paragraph 6.7 reveals an actual or potential breach of security or weakness exploiting the same root cause failure, such circumstance shall constitute a material Default.
- 6.11 On each anniversary of the Commencement Date, the Supplier shall provide to the Authority a letter from the individual appointed or identified in accordance with paragraph 1.3 confirming that having made due and careful enquiry:
 - 6.11.1 the Supplier has in the previous year carried out all Security Tests in accordance with this Schedule 6 and has complied with all procedures in relation to security matters required under the Contract; and
 - 6.11.2 the Supplier is confident that its security and risk mitigation procedures in relation to Information Assets and Authority Data remain effective.

7 Security audits and compliance

- 7.1 The Authority and its authorised representatives may carry out security audits as it reasonably considers necessary in order to ensure that the ISMS is compliant with the principles and practices of ISO 27001: 2013 or equivalent (unless otherwise Approved), the requirements of this Schedule 6 and the Baseline Security Requirements.
- 7.2 If ISO/IEC 27001: 2013 certification or equivalent is provided; the ISMS shall be independently audited in accordance with ISO/IEC 27001: 2013 or equivalent. The Authority and its authorised representatives shall, where applicable, be granted access to the Supplier Sites and Sub-contractor premises for this purpose.
- 7.3 If, on the basis of evidence resulting from such audits, it is the Authority's reasonable opinion that ISMS is not compliant with any applicable principles and practices of ISO/IEC 27001: 2013 or equivalent, the requirements of this Schedule 6 and/or the Baseline Security Requirements is not being achieved by the Supplier, the Authority shall notify the Supplier of this and provide a reasonable period of time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) for the Supplier to implement any necessary remedy. If the Supplier does not ensure that the ISMS is compliant within this

period of time, the Authority may obtain an independent audit of the ISMS to assess compliance (in whole or in part).

- 7.4 If, as a result of any such independent audit as described in paragraph 7.3 the Supplier is found to be non-compliant with any applicable principles and practices of ISO/IEC 27001:2013 or equivalent, the requirements of this Schedule 6 and/or the Baseline Security Requirements the Supplier shall, at its own cost, undertake those actions that are required in order to ensure that the ISMS is compliant and shall reimburse the Authority in full in respect of the costs obtaining such an audit.

8 Security risks and breaches

- 8.1 The Supplier shall use its reasonable endeavours to prevent any Breach of Security for any reason, including as a result of malicious, accidental or inadvertent behaviour.
- 8.2 If either Party becomes aware of a Breach of Security or an attempted Breach of Security it shall act in accordance with the agreed security incident management processes and incident response plans as set out in the ISMS.
- 8.3 Without prejudice to the security incident management processes and incident response plans set out in the ISMS and any requirements to report incidents in accordance with PSI 24/2014 if applicable, upon becoming aware of any Breach of Security or attempted Breach of Security, the Supplier shall:
- 8.3.1 immediately notify the Authority and take all reasonable steps (which shall include any action or changes reasonably required by the Authority) that are necessary to:
 - (a) minimise the extent of actual or potential harm caused by any Breach of Security;
 - (b) remedy any Breach of Security to the extent that is possible and protect the integrity of the ICT Environment (to the extent that this is within its control) and ISMS against any such Breach of Security or attempted Breach of Security;
 - (c) mitigate against a Breach of Security or attempted Breach of Security; and
 - (d) prevent a further Breach of Security or attempted Breach of Security in the future resulting from the same root cause failure;
 - 8.3.2 provide to the Authority and/or the Computer Emergency Response Team for UK Government ("GovCertUK") or equivalent any data that is requested relating to the Breach of Security or attempted Breach of Security within 2 Working Days of such request; and
 - 8.3.3 as soon as reasonably practicable and, in any event, within 2 Working Days following the Breach of Security or attempted Breach of Security, provide to the Authority 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 if required by the Authority

and the Supplier recognises that the Authority may report significant actual or potential losses of Personal Data to the Information Commissioner or equivalent and to the Cabinet Office.

- 8.4 If any action is taken by the Supplier in response to a Breach of Security or attempted Breach of Security which occurred as a result of non-compliance of the ISMS with any ISO/IEC 27001: 2013 requirements or equivalent (as applicable), the Baseline Security Requirements and/or the requirements of this Schedule 6, any such action and change to the ISMS and/or Security Plan as a result shall be implemented at the Supplier's cost.

9 IT Environment

- 9.1 The Supplier shall ensure that the Supplier System:

- 9.1.1 functions in accordance with Good Industry Practice for protecting external connections to the internet;
 - 9.1.2 functions in accordance with Good Industry Practice for protection from malicious code;
 - 9.1.3 provides controls to securely manage (store and propagate) all cryptographic keys to prevent malicious entities and services gaining access to them, in line with the Authority's Cryptographic Policy as made available to the Supplier from time to time;
 - 9.1.4 is patched (and all of its components are patched) in line with Good Industry Practice, any Authority patching policy currently in effect and notified to the Supplier and any Supplier patch policy that is agreed with the Authority; and
 - 9.1.5 uses the latest versions of anti-virus definitions, firmware and software available from industry accepted anti-virus software vendors.
- 9.2 Notwithstanding paragraph 9.1, if a Breach of Security is detected in the ICT Environment, the Parties shall co-operate to reduce the effect of the Breach of Security and, if the Breach of Security causes loss of operational efficiency or loss or corruption of Information Assets and/or Authority Data, assist each other to mitigate any losses and to recover and restore such Information Assets and Authority Data.
- 9.3 All costs arising out of the actions taken by the Parties in compliance with paragraphs 8.2, 8.3 and 9.2 shall be borne by:
- 9.3.1 the Supplier if the Breach of Security originates from the defeat of the Supplier's security controls or Information Assets and/or Authority Data is lost or corrupted whilst under the control of the Supplier or its Sub-contractor; or
 - 9.3.2 the Authority if the Breach of Security originates from the defeat of the Authority's security controls or Information Assets and/or Authority Data is lost or corrupted whilst under the control of the Authority

and each Party shall bear its own costs in all other cases.

10 Vulnerabilities and corrective action

- 10.1 The Parties acknowledge that from time to time vulnerabilities in the ICT Environment and ISMS will be discovered which, unless mitigated, will present an unacceptable risk to Information Assets and/or Authority Data.
- 10.2 The severity of any vulnerabilities shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' according to the agreed method in the ISMS and using any appropriate vulnerability scoring systems.
- 10.3 The Supplier shall procure the application of security patches to vulnerabilities categorised as 'Critical' within 7 days of public release, vulnerabilities categorised as 'Important' within 30 days of public release and vulnerabilities categorised as 'Other' within 60 days of public release, except where:
- 10.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of the Services being provided, including where it resides in a software component which is not being used, provided that, where those vulnerabilities become exploitable, they are remedied by the Supplier within the timescales in paragraph 10.3;
 - 10.3.2 the application of a security patch in respect of a vulnerability categorised as 'Critical' or 'Important' adversely affects the Supplier's ability to deliver the Services, in which case the Supplier shall be granted an extension to the

- timescales in paragraph 10.3 of 5 days, provided that the Supplier continues to follow any security patch test plan agreed with the Authority; or
- 10.3.3 the Authority agrees a different timescale after consultation with the Supplier in accordance with the processes defined in the ISMS.
- 10.4 The ISMS and the Security Plan shall include provision for the Supplier to upgrade software throughout the Term within 6 Months of the release of the latest version unless:
- 10.4.1 upgrading such software reduces the level of mitigation for known threats, vulnerabilities or exploitation techniques, provided always that such software is upgraded by the Supplier within 12 Months of release of the latest version; or
- 10.4.2 otherwise agreed with the Authority in writing.
- 10.5 The Supplier shall:
- 10.5.1 implement a mechanism for receiving, analysing and acting upon threat information provided by GovCertUK, or any other competent central Government Body;
- 10.5.2 ensure that the ICT Environment (to the extent that this is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;
- 10.5.3 ensure that it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment (to the extent that this is within the control of the Supplier) by actively monitoring the threat landscape during the Term;
- 10.5.4 pro-actively scan the ICT Environment (to the extent that this is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS;
- 10.5.5 from the Commencement Date and within 5 Working Days of the end of each subsequent Month during the Term provide a report to the Authority detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that this is within the control of the Supplier) and any elapsed time between the public release date of patches and either the time of application or, for outstanding vulnerabilities, the time of issue of such report;
- 10.5.6 propose interim mitigation measures in respect of any vulnerabilities in the ICT Environment (to the extent this is within the control of the Supplier) known to be exploitable where a security patch is not immediately available;
- 10.5.7 remove or disable any extraneous interfaces, services or capabilities that are no longer needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment to the extent this is within the control of the Supplier); and
- 10.5.8 inform the Authority when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the IT Environment (to the extent this is within the control of the Supplier) and provide initial indications of possible mitigations.
- 10.6 If the Supplier is unlikely to be able to mitigate any vulnerability within the timescales in paragraph 10.3, the Supplier shall notify the Authority immediately.
- 10.7 Any failure by the Supplier to comply with paragraph 10.3 shall constitute a material Default.

11 Sub-contracts

- 11.1 The Supplier shall ensure that all Sub-Contracts with Sub-Contractors who have access to Information Assets and/or Authority Data contain equivalent provisions in relation to information assurance and security that are no less onerous than those imposed on the Supplier under the Contract.

Appendix A

Baseline security requirements

1 Security Classifications and Controls

- 1.1 The Supplier shall, unless otherwise Approved in accordance with paragraph 5.2 of this Appendix A, only have access to and handle Information Assets and Authority Data that are classified under the Government Security Classifications Scheme as OFFICIAL.
- 1.2 There may be a specific requirement for the Supplier in some instances on a limited 'need to know basis' to have access to and handle Information Assets and Authority Data that are classified as 'OFFICIAL-SENSITIVE.'
- 1.3 The Supplier shall apply the minimum security controls required for OFFICIAL information and OFFICIAL-SENSITIVE information as described in Cabinet Office guidance, currently at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf.
- 1.4 The Supplier shall be able to demonstrate to the Authority and any accreditor that it has taken into account the "Technical Controls Summary" for OFFICIAL (in the above guidance) in designing and implementing the security controls in the Supplier System, which shall be subject to assurance and accreditation to Government standards.
- 1.5 Additional controls may be required by the Authority and any accreditor where there are aspects of data aggregation.

2 End User Devices

- 2.1 Authority Data shall, wherever possible, be held and accessed on paper or in the ICT Environment on secure premises and not on removable media (including laptops, removable discs, CD-ROMs, USB memory sticks, PDAs and media card formats) without Approval. If Approval is sought to hold and access data by other means, the Supplier shall consider the second-best option and third best option below and record the reasons why a particular approach should be adopted when seeking Approval:
 - 2.1.1 second best option means: secure remote access so that data can be viewed or amended over the internet without being permanently stored on the remote device, using products meeting the FIPS 140-2 standard or equivalent, unless Approved;
 - 2.1.2 third best option means: secure transfer of Authority Data to a remote device at a secure site on which it will be permanently stored, in which case the Authority Data and any links to it shall be protected at least to the FIPS 140-2 standard or equivalent, unless otherwise Approved, and noting that protectively marked Authority Data must not be stored on privately owned devices unless they are protected in this way.
- 2.2 The right to transfer Authority Data to a remote device should be carefully considered and strictly limited to ensure that it is only provided where absolutely necessary and shall be subject to monitoring by the Supplier and Authority.
- 2.3 Unless otherwise Approved, when Authority Data resides on a mobile, removable or physically uncontrolled device, it shall be:
 - 2.3.1 the minimum amount that is necessary to achieve the intended purpose and should be anonymised if possible;

- 2.3.2 stored in an encrypted form meeting the FIPS 140-2 standard or equivalent and using a product or system component which has been formally assured through a recognised certification process of CESG to at least Foundation Grade, for example, under the CESG Commercial Product Assurance scheme ("CPA") or equivalent, unless otherwise Approved;
- 2.3.3 protected by an authentication mechanism, such as a password; and
- 2.3.4 have up to date software patches, anti-virus software and other applicable security controls to meet the requirements of this Schedule 6.
- 2.4 Devices used to access or manage Authority Data shall be under the management authority of the Supplier and have a minimum set of security policy configurations enforced. Unless otherwise Approved, all Supplier devices shall satisfy the security requirements set out in the CESG End User Devices Platform Security Guidance ("CESG Guidance") (<https://www.gov.uk/government/collections/end-user-devices-security-guidance--2>) or equivalent.
- 2.5 Where the CESG Guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Authority and a joint decision shall be taken on whether the residual risks are acceptable. If the Supplier wishes to deviate from the CESG Guidance, this should be agreed in writing with the Authority on a case by case basis.

3 Data Storage, Processing, Management, Transfer and Destruction

- 3.1 The Parties recognise the need for Authority Data to be safeguarded and for compliance with the Data Protection Legislation. To that end, the Supplier shall inform the Authority the location within the United Kingdom where Authority Data is stored, processed and managed. The import and export of Authority Data from the Supplier System must be strictly controlled and recorded.
- 3.2 The Supplier shall inform the Authority of any changes to the location within the United Kingdom where Authority Data is stored, processed and managed and shall not transmit, store, process or manage Authority Data outside of the United Kingdom without Approval which shall not be unreasonably withheld or delayed provided that the transmission, storage, processing and management of Authority Data offshore is within:
 - 3.2.1 the European Economic Area ("EEA"); or
 - 3.2.2 another country or territory outside the EEA if that country or territory ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into which have been defined as adequate by the European commission.
- 3.3 The Supplier System shall support the requirement of the Authority to comply with Government policy and Cabinet Office guidance on Offshoring, currently set out at: <https://ogsirooffshoring.zendesk.com/hc/en-us/articles/203107991-HMG-sOffshoring-Policy>
by assessing, as required, any additional security risks associated with the storage, processing and/or transmission of any data and/or information offshore, including by an offshore Supplier (which may include the use of 'landed resources'), taking account of European Union requirements to confirm the 'adequacy' of protection of Personal Data in the countries where storage, processing and/or transmission occurs. No element of the Supplier System may be off-shored without Approval.
- 3.4 The Supplier shall ensure that the Supplier System provides internal processing controls between security domains to prevent the unauthorised high domain exporting of Authority Data to the low domain if there is a requirement to pass data between different security domains.

- 3.5 The Supplier shall ensure that any electronic transfer of Authority Data:
- 3.5.1 protects the confidentiality of the Authority during transfer through encryption suitable for the impact level of the data;
 - 3.5.2 maintains the integrity of the Authority Data during both transfer and loading into the receiving system through suitable technical controls for the impact level of the data; and
 - 3.5.3 prevents the repudiation of receipt through accounting and auditing.
- 3.6 The Supplier shall:
- 3.5.4 protect Authority Data, including Personal Data, whose release or loss could cause harm or distress to individuals and ensure that this is handled as if it were confidential while it is stored and/or processed;
 - 3.5.5 ensure that any official-sensitive information, including Personal Data is encrypted in transit and when at rest when stored away from the Supplier's controlled environment;
 - 3.5.6 on demand, provide the Authority with all Authority Data in an agreed open format;
 - 3.5.7 have documented processes to guarantee availability of Authority Data if it ceases to trade;
 - 3.5.8 securely destroy all media that has held Authority Data at the end of life of that media in accordance with any requirements in the Contract and, in the absence of any such requirements, in accordance with Good Industry Practice;
 - 3.5.9 securely erase any or all Authority Data held by the Supplier when requested to do so by the Authority;
 - 3.5.10 ensure that all material used for storage of Confidential Information is subject to controlled disposal and the Supplier shall:
 - (a) destroy paper records containing Personal Data by incineration, pulping or shredding so that reconstruction is unlikely; and
 - (b) dispose of electronic media that was used for the processing or storage of Personal Data through secure destruction, overwriting, erasure or degaussing for re-use.

4 Networking

- 4.1 Any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA or through the use of Public Sector Network ("PSN") compliant encrypted networking services or equivalent unless none are available in which case the Supplier shall agree the solution with the Authority.
- 4.2 The Supplier shall ensure that the configuration and use of all networking equipment in relation to the provision of the Services, including equipment that is located in secure physical locations, shall be at least compliant with Good Industry Practice.
- 4.3 The Supplier shall ensure that the ICT Environment (to the extent this is within the control of the Supplier) contains controls to maintain separation between the PSN and internet connections if used.

5 Security Architectures

- 5.1 When designing and configuring the ICT Environment (to the extent that this 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 those with a CESG Certified Professional certification (<http://www.cesg.gov.uk/awarenesstraining/IA-certification/Pages/index.aspx>) or equivalent for all bespoke or complex components.
- 5.2 The Supplier shall provide to the Authority and any accreditor sufficient design documentation detailing the security architecture of the ICT Environment and data transfer mechanism to support the Authority's and any accreditor's assurance that this is appropriate, secure and compliant with the Authority's requirements.
- 5.3 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 the ICT Environment used for the storage, processing and management of Authority Data. Users should only be granted the minimum necessary permissions to access Information Assets and Authority Data and must be automatically logged out of the Supplier System if an account or session is inactive for more than 15 minutes.

6 Digital Continuity

The Supplier shall ensure that each Information Asset is held in an appropriate format that is capable of being updated from time to time to enable the Information Asset to be retrieved, accessed, used and transferred to the Authority, including in accordance with any information handling procedures set out in PSI 24/2014 (Information Assurance) if applicable.

7 Personnel Vetting and Security

- 7.1 All Staff shall be subject to pre-employment checks that include, as a minimum, their employment history for at least the last 3 years, identity, unspent criminal convictions and right to work (including nationality and immigration status) and shall be vetted in accordance with:
 - 7.1.1 the BPSS or BS7858 or equivalent; and
 - 7.1.2 PSI 07/2014, if applicable, based on their level of access to Information Assets and/or Authority Data.
- 7.2 If the Authority agrees that it is necessary for any Staff to have logical or physical access to Information Assets and/or Authority Data classified at a higher level than OFFICIAL (such as that requiring 'SC' clearance), the Supplier shall obtain the specific Government clearances that are required for access to such Information Assets and/or Authority Data.
- 7.3 The Supplier shall prevent Staff who are unable to obtain the required security clearances from accessing Information Assets and/or Authority Data and/or the ICT Environment used to store, process and/or manage such Information Assets or Authority Data.
- 7.4 The Supplier shall procure that all Staff comply with the Security Policy Framework and principles, obligations and policy priorities stated therein, including requirements to manage and report all security risks in relation to the provision of the Services.
- 7.5 The Supplier shall ensure that Staff who can access Information Assets and/or Authority Data and/or the ICT Environment are aware of their responsibilities when handling such information and data and undergo regular training on secure information management principles. Unless otherwise Approved, this training must be undertaken annually.
- 7.6 If the Supplier grants Staff access to Information Assets and/or Authority Data, those individuals shall be granted only such levels of access and permissions that are necessary for them to carry out their duties. Once Staff no longer require such levels of access or

permissions or leave the organisation, their access rights shall be changed or revoked (as applicable) within one Working Day.

8 Identity, Authentication and Access Control

- 8.1 The Supplier shall operate a robust role-based access control regime, including network controls, to ensure all users and administrators of and those maintaining the ICT Environment are uniquely identified and authenticated when accessing or administering the ICT Environment to prevent unauthorised users from gaining access to Information Assets and/or Authority Data. Applying the 'principle of least privilege', users and administrators and those responsible for maintenance shall be allowed access only to those parts of the ICT Environment they require. The Supplier shall retain an audit record of accesses and users and disclose this to the Authority upon request.
- 8.2 The Supplier shall ensure that Staff who use the Authority System actively confirm annually their acceptance of the Authority's acceptable use policy.

9 Physical Media

- 9.1 The Supplier shall ensure that all:
- 9.1.1 OFFICIAL information is afforded physical protection from internal, external and environmental threats commensurate with the value to the Authority of that information;
 - 9.1.2 physical components of the Supplier System are kept in secure accommodation which conforms to the Security Policy Framework and CESG standards and guidance or equivalent;
 - 9.1.3 physical media holding OFFICIAL information is handled in accordance with the Security Policy Framework and CESG standards and guidance or equivalent; and
 - 9.1.4 Information Assets and Authority Data held on paper are:
 - (a) kept secure at all times, locked away when not in use on the premises on which they are held and secured and are segregated if the Supplier is co-locating with the Authority; and
 - (b) only transferred by an approved secure form of transfer with confirmation of receipt obtained.

10 Audit and Monitoring

- 10.1 The Supplier shall implement effective monitoring of its information assurance and security obligations in accordance with Government standards and where appropriate, in accordance with CESG Good Practice Guide 13 – Protective Monitoring or equivalent.
- 10.2 The Supplier shall collect audit records which relate to security events in the ICT Environment (where this is within the control of the Supplier), including those that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness, such Supplier audit records shall include:
- 10.2.1 logs to facilitate the identification of the specific asset which makes every outbound request external to the ICT Environment (to the extent it is within the control of the Supplier). To the extent, the design of the ICT Environment allows, such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers;
 - 10.2.2 regular reports and alerts giving details of access by users of the ICT Environment (to the extent that it is within the control of the Supplier) to enable

the identification of changing access trends any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data; and

- 10.2.3 security events generated in the ICT Environment (to the extent it is within the control of the Supplier) including account logon and logoff events, start and end of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.
- 10.3 The Parties shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
- 10.4 The Supplier shall retain audit records collected in compliance with paragraph 10.1 for at least 6 Months.

Schedule 7

Prisons

1 Access to prisons

- 1.1** If Staff are required to have a pass for admission to an Authority Premises, which is a prison, (a "Prison") the Authority shall, subject to satisfactory completion of approval procedures, arrange for passes to be issued. Any member of the Staff who cannot produce a proper pass when required to do so by any member of the Authority's personnel, or who contravenes any conditions on the basis of which a pass was issued, may be refused admission to a Prison or be required to leave a Prison if already there.
- 1.2** Staff shall promptly return any pass if at any time the Authority so requires or if the person to whom the pass was issued ceases to be involved in the performance of the Services. The Supplier shall promptly return all passes on expiry or termination of the Contract.
- 1.3** Staff attending a Prison may be subject to search at any time. Strip searches shall be carried out only on the specific authority of the Authority under the same rules and conditions applying to the Authority's personnel. The Supplier is referred to Rule 71 of Part IV of the Prison Rules 1999 as amended by the Prison (Amendment) Rules 2005 and Rule 75 of Part IV of the Young Offender Institution Rules 2000 as amended by the Young Offender Institution (Amendment) Rules 2005.
- 1.4** Searches shall be conducted only on the specific authority of the Authority under the same rules and conditions applying to the Authority's personnel and/or visitors. The Supplier is referred to Section 8 of the Prison Act 1952, Rule 64 of the Prison Rules 1999 and PSI 67/2011.

2 Security

- 2.1** Whilst at Prisons Staff shall comply with all security measures implemented by the Authority in respect of staff and other persons attending Prisons. The Authority shall provide copies of its written security procedures to Staff on request. The Supplier and all Staff are prohibited from taking any photographs at Prisons unless they have Approval and the Authority's representative is present so as to have full control over the subject matter of each photograph to be taken. No such photograph shall be published or otherwise circulated without Approval.
- 2.2** The Authority may search vehicles used by the Supplier or Staff at Prisons.
- 2.3** The Supplier and Staff shall co-operate with any investigation relating to security which is carried out by the Authority or by any person who is responsible for security matters on the Authority's behalf, and when required by the Authority shall:
- 2.3.1** take all reasonable measures to make available for interview by the Authority any members of Staff identified by the Authority, or by a person who is responsible for security matters, for the purposes of the investigation. Staff may be accompanied by and be advised or represented by another person whose attendance at the interview is acceptable to the Authority; and
- 2.3.2** subject to any legal restriction on their disclosure, provide all documents, records or other material of any kind and in whatever form which may be reasonably required by the Authority, or by a person who is responsible for security matters on the Authority's behalf, for the purposes of investigation as long as the provision of that material does not prevent the Supplier from performing the Services. The Authority may retain any such material for use in connection with the investigation and, as far as possible, may provide the Supplier with a copy of any material retained.

3 Offences and authorisation

3.1 In providing the Services the Supplier shall comply with PSI 10/2012 (Conveyance and Possession of Prohibited Items and Other Related Offences) and other applicable provisions relating to security as published by the Authority from time to time.

3.2 Nothing in the Contract is deemed to provide any "authorisation" to the Supplier in respect of any provision of the Prison Act 1952, Offender Management Act 2007, Crime and Security Act 2010, Serious Crime Act 2015 or other relevant legislation.

Schedule 8

Statutory obligations and corporate social responsibility

1 What the Authority expects from the Supplier

- 1.1 In September 2017, Her Majesty's Government published a Supplier Code of Conduct (the "Code") setting out the standards and behaviours expected of suppliers who work with government. The Code can be found online at:
- 1.2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-3_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf
- 1.3 The Authority expects the Supplier and its Sub-Contractors to comply with their legal obligations, in particular those set out in Part 1 of this Schedule 8, and to meet the standards set out in the Code as a minimum. The Authority also expects the Supplier and its Sub-Contractors to use reasonable endeavours to comply with the standards set out in Part 2 of this Schedule 8.

Part 1 Statutory Obligations

2 Equality and Accessibility

- 2.1 The Supplier shall:
- 2.1.1 perform its obligations under the Contract in accordance with:
- (a) all applicable equality Law (whether in relation to race, sex, gender reassignment, age, disability, sexual orientation, religion or belief, pregnancy maternity or otherwise);
 - (b) the Authority's equality, diversity and inclusion policy as given to the Supplier from time to time;
 - (c) any other requirements and instructions which the Authority reasonably imposes regarding any equality obligations imposed on the Authority at any time under applicable equality law; and
- 2.1.2 take all necessary steps and inform the Authority of the steps taken to prevent unlawful discrimination designated as such by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation).

3 Modern Slavery

- 3.1 The Supplier shall, and procure that each of its Sub-Contractors shall, comply with:
- 3.1.1 the MSA; and
- 3.1.2 the Authority's anti-slavery policy as provided to the Supplier from time to time ("**Anti-slavery Policy**").
- 3.2 The Supplier shall:
- 3.2.1 implement due diligence procedures for its Sub-Contractors and other participants in its supply chains, to ensure that there is no slavery or trafficking in its supply chains;
- 3.2.2 respond promptly to all slavery and trafficking due diligence questionnaires issued to it by the Authority from time to time and shall ensure that its responses to all such questionnaires are complete and accurate;

- 3.2.3 prepare and deliver to the Authority each year, an annual slavery and trafficking report setting out the steps it has taken to ensure that slavery and trafficking is not taking place in any of its supply chains or in any part of its business;
 - 3.2.4 maintain a complete set of records to trace the supply chain of all Services provided to the Authority regarding the Contract;
 - 3.2.5 report the discovery or suspicion of any slavery or trafficking by it or its Sub-Contractors to the Authority and to the Modern Slavery Helpline; and
 - 3.2.6 implement a system of training for its employees to ensure compliance with the MSA.
- 3.3 The Supplier represents, warrants and undertakes throughout the Term that:
- 3.3.1 it conducts its business in a manner consistent with all applicable laws, regulations and codes including the MSA and all analogous legislation in place in any part of the world;
 - 3.3.2 its responses to all slavery and trafficking due diligence questionnaires issued to it by the Authority from time to time are complete and accurate; and
 - 3.3.3 neither the Supplier nor any of its Sub-Contractors, nor any other persons associated with it:
 - (a) has been convicted of any offence involving slavery and trafficking; or
 - (b) has been or is the subject of any investigation, inquiry or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence regarding slavery and trafficking.
- 3.4 The Supplier shall notify the Authority as soon as it becomes aware of:
- 3.4.1 any breach, or potential breach, of the Anti-Slavery Policy; or
 - 3.4.2 any actual or suspected slavery or trafficking in a supply chain which relates to the Contract.
- 3.5 If the Supplier notifies the Authority pursuant to paragraph 3.4 of this Schedule 8, it shall respond promptly to the Authority's enquiries, co-operate with any investigation, and allow the Authority to audit any books, records and/or any other relevant documentation in accordance with the Contract.
- 3.6 If the Supplier is in Default under paragraphs 3.2 or 3.3 of this Schedule 8 the Authority may by notice:
- 3.6.1 require the Supplier to remove from performance of the Contract any Sub-Contractor, Staff or other persons associated with it whose acts or omissions have caused the Default; or
 - 3.6.2 immediately terminate the Contract.

4 Income Security

- 4.1 The Supplier shall:
- 4.1.1 ensure that all pay and benefits paid for a standard working week meet, at least, national legal standards in the country of employment;
 - 4.1.2 provide all Staff with written and readily understandable information about their employment conditions in respect of pay before they enter employment and about their pay for the pay period concerned each time that they are paid;

- 4.1.3 not make deductions from pay:
- (a) as a disciplinary measure;
 - (b) except where permitted by Law and the terms of the employment contract; and
 - (c) without express permission of the person concerned
- 4.1.4 record all disciplinary measures taken against Staff.

5 Working Hours

5.1 The Supplier shall ensure that:

- 5.1.1 the working hours of Staff comply with the Law, and any collective agreements;
- 5.1.2 the working hours of Staff, excluding overtime, is defined by contract, do not exceed 48 hours per week unless the individual has agreed in writing, and that any such agreement is in accordance with the Law;
- 5.1.3 overtime is used responsibly, considering:
- (a) the extent;
 - (b) frequency; and
 - (c) hours worked;
- 5.1.4 the total hours worked in any seven-day period shall not exceed 60 hours, except where covered by paragraph 5.1.1;
- 5.1.5 working hours do not exceed 60 hours in any seven-day period unless:
- (a) it is allowed by Law;
 - (b) it is allowed by a collective agreement freely negotiated with a worker's organisation representing a significant portion of the workforce;
 - (c) appropriate safeguards are taken to protect the workers' health and safety; and
 - (d) the Supplier can demonstrate that exceptional circumstances apply such as during unexpected production peaks, accidents or emergencies;
- 5.1.6 all Staff are provided with at least:
- (a) 1 day off in every 7-day period; or
 - (b) where allowed by Law, 2 days off in every 14-day period.

6 Right to Work

6.1 The Supplier shall:

- 6.1.1 ensure that all Staff, are employed on the condition that they are permitted to work in the UK, and;
- 6.1.2 notify the authority immediately if an employee is not permitted to work in the UK.

7 Health and Safety

7.1 The Supplier shall perform its obligations under the Contract in accordance with:

- 7.1.1 all applicable Law regarding health and safety; and

7.1.2 the Authority's Health and Safety Policy while at the Authority's Premises.

7.2 Each Party shall notify the other as soon as practicable of any health and safety incidents or material health and safety hazards at the Authority's Premises of which it becomes aware and which relate to or arise in connection with the performance of the Contract. The Supplier shall instruct Staff to adopt any necessary safety measures in order to manage the risk.

8 Welsh Language Requirements

8.1 The Supplier shall comply with the Welsh Language Act 1993 and the Welsh Language Scheme as if it were the Authority to the extent that the same relate to the provision of the Services.

9 Fraud and Bribery

9.1 The Supplier represents and warrants that neither it, nor to the best of its knowledge any Staff, have at any time prior to the Commencement Date:

9.1.1 committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act; and/or

9.1.2 been listed by any Government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in Government procurement programmes or contracts on the grounds of a Prohibited Act.

9.2 The Supplier shall not during the Term:

9.2.1 commit a Prohibited Act; and/or

9.2.2 do or suffer anything to be done which would cause the Authority or any of its employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

9.3 The Supplier shall, during the Term:

9.3.1 establish, maintain and enforce, and require that its Sub-Contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act;

9.3.2 have in place reasonable prevention measures (as defined in section 45(3) and 46(4) of the Criminal Finance Act 2017) to ensure that Associated Persons of the Supplier do not commit tax evasion facilitation offences as defined under that Act;

9.3.3 keep appropriate records of its compliance with its obligations under paragraph 9.3.1 and 9.3.2 and make such records available to the Authority on request; and

9.3.4 take account of any guidance about preventing facilitation of tax evasion offences which may be published and updated in accordance with section 47 of the Criminal Finances Act 2017

9.4 The Supplier shall immediately notify the Authority in writing if it becomes aware of any breach of paragraphs 9.1 and/or 9.2, or has reason to believe that it has or any of the Staff have:

9.4.1 been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

9.4.2 been listed by any Government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in Government procurement programmes or contracts on the grounds of a Prohibited Act; and/or

- 9.4.3 received a request or demand for any undue financial or other advantage of any kind in connection with the performance of the Contract or otherwise suspects that any person directly or indirectly connected with the Contract has committed or attempted to commit a Prohibited Act.
- 9.5 If the Supplier notifies the Authority pursuant to paragraph 9.4, the Supplier shall respond promptly to the Authority's enquiries, co-operate with any investigation, and allow the Authority to Audit any books, records and/or any other relevant documentation.
- 9.6 If the Supplier is in Default under paragraphs 9.1 and/or 9.2, the Authority may by notice:
- 9.6.1 require the Supplier to remove from performance of the Contract any Staff whose acts or omissions have caused the Default; or
- 9.6.2 immediately terminate the Contract.
- 9.7 Any notice served by the Authority under paragraph 9.6 shall specify the nature of the Prohibited Act, the identity of the party who the Authority believes has committed the Prohibited Act and the action that the Authority has taken (including, where relevant, the date on which the Contract terminates).

Part 2 Corporate Social Responsibility

1 Zero Hours Contracts

- 1.1 Any reference to zero hours contracts, for the purposes of this Contract, means as they relate to employees or workers and not those who are genuinely self-employed and undertaking work on a zero hours arrangement.
- 1.2 When offering zero hours contracts, the Supplier shall consider and be clear in its communications with its employees and workers about:
- 1.2.1 whether an individual is an employee or worker and what statutory and other rights they have;
- 1.2.2 the process by which work will be offered and assurance that they are not obliged to accept work on every occasion; and
- 1.2.3 how the individual's contract will terminate, for example, at the end of each work task or with notice given by either party.

2 Sustainability

- 2.1 The Supplier shall:
- 2.1.1 comply with the applicable Government Buying Standards;
- 2.1.2 provide, from time to time, in a format reasonably required by the Authority, reports on the environmental effects of providing the Goods and Services;
- 2.1.3 maintain ISO 14001 or BS 8555 or an equivalent standard intended to manage its environmental responsibilities; and
- 2.1.4 perform its obligations under the Contract in a way that:
- (a) supports the Authority's achievement of the Greening Government Commitments;
 - (b) conserves energy, water, wood, paper and other resources;
 - (c) reduces waste and avoids the use of ozone depleting substances; and
 - (d) minimises the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment

Schedule 9

Data processing

- 1 The contact details of the Authority's Data Protection Officer are: **[REDACTED]** uk or Data Protection Officer, 102 Petty France, London, SW1H 9AJ.
- 2 The contact details of the Supplier's Data Protection Officer are: **[REDACTED]**
- 3 The Supplier shall comply with any further written instructions with respect to processing by the Authority.
- 4 Any such further instructions shall be incorporated into this Schedule 9.

Description	Details
Subject matter of the processing	The processing of data allows for information owned by HMPPS Co-Financing Office, such as data held on the Case Assessment and Tracking System (CATS+) to be utilised by the Data Recipient to fulfil the requirements of delivering the HMPPS CFO funded ESF programme, and for no other purpose.
Duration of the processing	The duration of the processing commenced upon signature by the Parties and shall continue in effect until the data share has been completed in accordance with the requirements of the Contract unless otherwise subject to earlier termination in accordance with the Contract.
Nature and purposes of the processing	The sharing of data allows the Data Recipient to utilise CATS+, which allows for: • Storage and collation of information that ensures contractual compliance to record all actions and activities relating to delivery of the HMPPS CFO contract and to assist case management. • Easier sourcing of participants who may be eligible to enrol on the programme. • Ensure the compliance management of ESF requirements and provide relevant information to auditing authorities. • Uploading and storage of scanned information (including evidence of activities and achievements, progress and payments) relating to participants • Collation and production of data to support calculations of payments and performance of delivery, and evaluations of effectiveness.

Type of Personal Data being Processed	Personal data held in CATS+, is gathered from existing HMPPS systems (PNOMIS and nDelius) as well as through CATS+ user input, and will include: • Names (offender, the offender managers and the CATS+ user) • Offender Date of birth • Offender NI Number • Contact details (address details and phone numbers of offenders, offender managers and the CATS+ user) • Offender employment and education details • Offence and associated risk information
Categories of Data Subject	Offenders in both custody and community
Plan for return and destruction of the data once the processing is complete Unless requirement under union or member state law to preserve that type of data	In accordance with ESF and HMPPS CFO requirements data retention is outlined in Schedule 5, where it states that data should be retained for 12 years following the closure of the project. With consideration also being given to Schedule 5 which states, the Supplier shall retain all original copies of documents, which have been scanned and uploaded onto CATS+ until the Authority has approved and made a payment for the associated enrolment or achievement, as referenced in the Supplier Guidance.

Data Processing Consent Form

CFO PROJECT ENROLMENT GUIDANCE

Introduction

Part A of this document is intended for use by the Support Worker, providing guidance and support to complete the enrolment form correctly.

Part B of this document contains the CFO project outline, enrolment and privacy policies. The highlighted areas **must be explained to and understood by** the potential participant before they agree to participate in the ESF funded CFO project, and sign the CFO Enrolment Form. Part B of this guidance can also be given to the potential participant if they request a copy of it.

This CFO Project Enrolment Guidance should only be used in conjunction with the corresponding (matching) version number of the CFO Enrolment Form.

PART A

The following guidance relates to each section of the Enrolment Form. All sections on the form must be completed correctly for the individual to proceed with the Enrolment process.

Section 1 - Personal Details

All sections are mandatory, apart from the National Insurance number.

Section 2 - Eligibility

All potential participants must be unemployed to be eligible. The minimum eligibility age is 16 in the North West, West Midlands and London, 18 in all other contract areas. Additional information may be required to determine the legal right to live and work in the UK (see Section 3 of the Enrolment Form.)

*The Support Worker **must** confirm the following details relating to eligibility:*

- The individual has permission to legally live and work in the UK
- **Custody only** (Veterans Hub)– the earliest possible release date is within the next 3 years.

Note: Additional permission from the participant will be required should you wish to share details with other agencies e.g. to obtain identification or open a bank account.

Section 3 - Nationality

For all Non EU nationals, evidence of right to work must be approved by CFO when submitting the Enrolment Form.

Additional information for the Support Worker –

In addition to the existing restrictions on the right to live and work in the UK for individuals from outside the European Economic Area (EEA), Support Worker should be aware of the following position for Croatian nationals:

From 1st July 2013, Croatian nationals have been able to move and reside freely in any European Union (EU) Member State. However, Croatian nationals wanting to work in the UK need to obtain work authorisation (permission to work) before starting any employment, unless they are exempt from this requirement. Work authorisation is normally in the form of an accession worker authorisation certificate (or "purple registration certificate"). A Croatian national with an offer of employment in the UK must obtain this document from the Home Office before commencing work. This document will contain an endorsement restricting the holder to a particular job or type of employment. Those qualifying for a purple registration certificate will generally be skilled workers who meet the criteria for the issue of a certificate of sponsorship.

Section 4 – Support Worker Confirmation

The potential participant must have the project details and eligibility criteria explained to them and the Support Worker must sign and date the form.

Section 5 - Potential Participant Confirmation

The Support Worker must ensure the **Project Outline**, **Enrolment** and **Privacy Policy** (from Part B) are explained to and understood by the potential participant, who must sign to confirm this, as well as agree to participate in the project.

*The Support Worker **must** also explain the following details relating to project participation:*

- The enrolment process requires completion of an assessment to determine suitability for CFO, agreeing to participate does not automatically lead to enrolment.
- If agreement to participate is not received, the individual cannot participate in the CFO project
- The potential participant should also be informed that their information will be shared with ESF for audit and evaluation purposes
- If there are additional provider criteria in place to be accepted on to the project this should be described at this stage

Part B begins on the following page...

PART B

PROJECT OUTLINE:

The Co-Financing Organisation (CFO) is a European Social Fund (ESF) financed project which aims to support offenders into mainstream work, training and education opportunities.

The CFO is subject to the Data Protection Act (2018), the General Data Protection Regulation (GDPR) and the Rehabilitation of Offenders Act (ROA) 1974 (as revised by the Legal Aid, Sentencing and Punishment of Offenders Act 2012 (LASPO)).

ENROLMENT POLICY:

To provide you with the best service possible, by signing the enrolment form and agreeing with the Project Outline, Enrolment and Privacy Policy, you are agreeing to join the ESF funded CFO project. This means that HMPPS, and its CFO provider staff from the following organisations:

[Supplier names]

and their sub-contractors and other appropriate delivery staff may securely share and have access to your information (where appropriate) and will process your information on behalf of the CFO and ESF.

Your agreement to participate in the CFO project, permits us to access and share your relevant information with representatives of:

- HM Prison and Probation Service (HMPPS)
- National Probation Service (NPS)
- Community Rehabilitation Companies (CRCs)
- CFO prime providers, sub-contractors and delivery partners
- Previous, potential or actual employers, education and training providers
- Referring organisations and their agencies (if applicable)
- Charities and / or Voluntary Agencies
- Health Care providers and professionals
- Appropriate Work Programme providers (if applicable).
- The European Social Fund

In accordance with our obligations to reduce re-offending and rehabilitate offenders, which is in accordance with the Offender Management Act 2007.

Only information considered relevant to enable support to be provided to you will be shared. This may include information which allows the CFO to successfully deliver the project and secure future funding for similar projects, or that would contribute to improvements within Criminal Justice delivery.

Enrolment Policy continues on following page...

ENROLMENT POLICY (*continued*):

Relevant information may include your name, address, date of birth, National Insurance number, other relevant personal information, as well as offending history (where necessary) and specific project progress information.

If you no longer wish to participate, then please inform your Support Worker who will cease working with you and close your case. Your data will no longer be used for the project purposes outlined above and you cannot re-join the project at a later date.

Information held by the CFO will also be used to evaluate the project and to report to the CFO, DWP and European Social Fund for project monitoring purposes. You may be contacted by (or on behalf of) these agencies for research and evaluation purposes. You can choose to opt out when contacted (by informing the person who contacts you) and this will have no bearing on the service provided by CFO and its providers.

Information held by the CFO will not be shared with any other agencies without your permission unless there are over-riding concerns of: security, child or public protection. Information held will be destroyed within 12 years of the end of the project delivery, or sooner if no longer needed by CFO or its auditors and you have the right to access, and rectify the data we hold on you.

PRIVACY POLICY:

Your details will be stored securely and retained in compliance with the Data Protection Act (2018) and the General Data Protection Regulation (GDPR) 2018. The DWP is the data controller in respect of information processed which relates to your participation in the project funded by the European Social Fund, whilst the CFO is the data processor. Further information on the DWP Personal Information Charter can be found here: <http://www.gov.uk/dwp/personal-information-charter> - please inform your Support Worker if you require further information.

Schedule 10

Tender

[REDACTED]

Schedule 11

Performance Management/PIP and Action Plan Process

Definitions

Action Plan	means a plan issued to the Supplier by the Authority relating to the Supplier's underperformance of the Contract as described in paragraph 2 of this Schedule 11
Performance Improvement Plan	means a plan Approved by the Authority relating to the Supplier's underperformance of the Contract as described in paragraph 1 of this Schedule 11

1 Introduction and Scope

- 1.1** This Schedule 11 sets out the process by which the Authority and the Supplier will work together to address underperformance by the Supplier of the Contract. This process includes, but is not limited to, improvements that the Supplier will be required to make or action that it will be required to take that (either case) arise from its underperformance of the Contract.
- 1.2** Under performance of the Contract includes any underperformance of or failure to perform any of its obligations under the Contract, including but without limitation its obligations arising under or by reference to any Supplier Failure.
- 1.3** The operation of this Schedule 11 shall:
- 1.3.1** be without prejudice to the Authority's other rights and remedies (including without limitation under clause 37 (Termination on Default)), and the requirement for the Supplier to comply with its obligations and to deliver the Services, in each case as set out in the Contract; and
- 1.3.2** not constitute any waiver of such rights, remedies and requirements.

2 Performance Improvement Plan

- 2.1** If, in the reasonable opinion of the Authority, the Supplier is not delivering any aspect of the Services or the Contract as required under the Contract, the Authority may require the Supplier to, within 10 Working Days from notification from the Authority of such failing, at any time during the Term, prepare and provide to the Authority a Performance Improvement Plan for Approval.
- 2.2** The Performance Improvement Plan shall be in a format determined by the Authority as being appropriate to the nature of the concerns and will document:
- 2.2.1** the nature of the Supplier Failure and all of the concerns raised by the Authority by reference to the Contract;
- 2.2.2** what steps the Supplier will take to remedy any Supplier Failure or any other concerns;
- 2.2.3** how the Supplier will demonstrate to the Authority that such Supplier Failure or other concerns have been remedied;
- 2.2.4** the deadline by which such steps shall be completed and the Services returned to compliance with the terms of this Contract.
- 2.3** The Authority shall have final Approval of the terms of the Performance Improvement Plan before it is implemented by the Supplier and shall determine its duration.

- 2.4 Following Approval of the Performance Improvement Plan, it will then be implemented by the Supplier in accordance with its terms and will be reviewed by the parties no less than once every Month.
- 2.5 The Authority will monitor how the Supplier is progressing towards addressing the concerns of the Authority and whether the Performance Improvement Plan is proving useful.
- 2.6 If, at the end of the period allocated to the Performance Improvement Plan, either:
- 2.6.1 the actions and outcomes set out in the Performance Improvement Plan have not been achieved by the Supplier; and/or
 - 2.6.2 the delivery of the Services by the Supplier is still not satisfactory to the Authority (or if circumstances of Supplier Failure persist);
- the Authority may:
- 2.6.3 extend the duration of the Performance Improvement Plan (at its sole discretion);
 - 2.6.4 issue an Action Plan to the Supplier;
 - 2.6.5 perform or arrange for the performance by a Replacement Supplier of, all or part of the Contract, at the Supplier's cost; or
 - 2.6.6 terminate the Contract with immediate effect in accordance with clause 39.1.7 of the Contract.

3 Action Plan

- 3.1 If, in the opinion of the Authority, the Supplier is not delivering any aspects of the Services, the Contract or any Performance Improvement Plan, then the Authority may issue an Action Plan to the Supplier.
- 3.2 The Action Plan will be in a format determined by the Authority as being appropriate to the nature of the Authority's concerns and will document the concerns of the Authority with reference to the Contract. The duration of the Action Plan shall be determined by the Authority.
- 3.3 The Authority will prepare and provide the Action Plan to the Supplier setting out the terms which the Supplier must implement and the timeframe within which the Supplier will be expected to implement the terms of the Action Plan and improve its performance under the Contract.
- 3.4 To the extent that the Supplier does not agree to the terms of the Action Plan, and such dispute is not resolved within 10 Working Days, then the parties shall follow the dispute resolution procedure set out in clause 46 of the Contract.
- 3.5 The Action Plan shall be reviewed by the Authority not less than once per Month and the result of such review shall be shared with the Supplier.
- 3.6 If, at the end of the duration of the Action Plan, either:
- 3.6.1 the actions and outcomes set out in the Action Plan have not been achieved by the Supplier; and/or
 - 3.6.2 the delivery of the Services by the Supplier is still not satisfactory to the Authority or the circumstances of Supplier Failure persist;
 - 3.6.3 the Authority may:
 - 3.6.4 extend the duration of the Action Plan (at its sole discretion);

3.6.5 perform or arrange for the performance by a Replacement Supplier of, all or part of the Contract, at the Supplier's cost; or

3.6.6 terminate the Contract with immediate effect in accordance with clause 39.1.7 of the Contract.

4 Costs

4.1 Other than where expressly stated, each party will be responsible for its own costs incurred in relation to this Schedule 11, including in relation to the preparation and implementation of any Performance Improvement Plan or Action Plan.

4.2 Unless the Authority Approves otherwise in writing, the Supplier shall not be entitled to submit any claim for payment under the Contract or otherwise use any European Social Fund funding in respect of its costs incurred in relation to this Schedule 11.

Schedule 12

Key Personnel and Key Sub-Contractors

Key Personnel

KEY ROLE	Name of Key Personnel	Responsibilities / Authorities	Phase of the Services during which they will be a member of Key Personnel	Minimum period in key role
Operations Manager	[REDACTED]	• CFO/Together-Yorkshire • Performance • Quality • Accountability • HMPPS • Comms • Reporting	Full contract period	Full contract period
Hub Manager	[REDACTED]	• Day-to-day management of Hub and staff • Performance • Quality	Full contract period	Full contract period
Team Leader	[REDACTED]	• Performance • Quality	Full contract period	Full contract period (phased recruitment)
Support Worker	[REDACTED]	• End-to-end participant journey • Case-conferencing with Probation/local professionals	Full contract period	Full contract period (phased recruitment)
Tutor	[REDACTED]	• CFO activity • Intervention delivery	Full contract period	Full contract period (phased recruitment)
Hub Guide	[REDACTED]	• Welcoming participants to the Hub • Guiding and signposting participants	Full contract period	Full contract period (phased recruitment)

Chief Financial Officer	[REDACTED]	• Responsibility for information assurance and security, including personnel security • Information Risk Officer • Responsibility for compliance with the ISMS	Full contract period	Full contract period
Head of IT	[REDACTED]	• Deputy responsible for information assurance and security, including personnel security • Deputy Information Risk Officer • Deputy responsible for compliance with the ISMS	Full contract period	Full contract period

Key Sub-Contractors

Name of Key Sub-Contractor	Responsibilities / Element of the Services to be provided	Phase of the Services that they will be a Key-Sub-Contractor
Community Links	End-to-end provider (Leeds)	Full contract period
York Learning	End-to-end provider (York)	Full contract period

Schedule 13

Regional Annex



CFO Activity Hubs
Regional Annex Yorl

Schedule 14

Sample Forms

Part A - Example Enrolment Form

 HM Prison & Probation Service		 European Union European Social Fund				
HMPPS CFO ACTIVITY HUB ENROLMENT FORM						
Section 1 - Personal Details Case Ref First Name Last Name Date of Birth / / NI Number Location						
Section 2 - Eligibility Potential Participant is at least age 18 and currently unemployed? <input style="float: right;" type="checkbox"/> Potential Participant is legally able to live & work in the UK? <input style="float: right;" type="checkbox"/> <i>Both boxes above must be ticked for the potential participant to proceed with the Enrolment process.</i>						
Section 3 - Nationality Tick One <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Potential Participant is a national of the European Economic Area (EU + Iceland + Liechtenstein + Norway) or Switzerland</td> <td style="width: 50px; text-align: center; vertical-align: middle;">☐</td> </tr> <tr> <td style="padding: 5px;">OR Potential Participant is a national of a country outside the European Economic Area and has permission to work in the UK (Copy of permission must be attached) and no decision to deport has been made.</td> <td style="text-align: center; vertical-align: middle;">☐</td> </tr> </table>			Potential Participant is a national of the European Economic Area (EU + Iceland + Liechtenstein + Norway) or Switzerland	☐	OR Potential Participant is a national of a country outside the European Economic Area and has permission to work in the UK (Copy of permission must be attached) and no decision to deport has been made.	☐
Potential Participant is a national of the European Economic Area (EU + Iceland + Liechtenstein + Norway) or Switzerland	☐					
OR Potential Participant is a national of a country outside the European Economic Area and has permission to work in the UK (Copy of permission must be attached) and no decision to deport has been made.	☐					
Section 4 - Support Worker Confirmation I have explained the contents of this form referencing the CFO Activity Hub Project Enrolment Guidance to the potential participant. Staff Member Print Name Signed Date / /						
Section 5 - Potential Participant Confirmation I confirm I have had explained to me and I understand the <i>CFO Activities Hub Project Outline</i> , the <i>CFO Activities Hub Enrolment</i> and the <i>Privacy Policies</i> (Copies available from the Support Worker on request) <input style="float: right;" type="checkbox"/> I agree to participate in the ESF funded CFO Project. <input style="float: right;" type="checkbox"/> Note: Potential Participant must have ticked BOTH boxes to proceed with the CFO Activities Hub Enrolment process Potential Participant Signature Date / /						



Service Level 2 Human & Citizenship

CFO Hub is a European Social Fund Project that helps individuals move closer to mainstream provision and ultimately the labour market.

Please complete in BLOCK CAPITALS using black ink only

Participant's case number:			
Participant's full name:			
Participant's NINO:			
Activity code and Name:			
Delivery Route	☐ On-site delivery funded through the contract ☐ External (i.e. off-site delivery) funded through the contract ☐ Appropriate supported referral to an existing service not funded through the contract		
Rationale for activity specific to participant and expected timeframe of delivery:			
Number sessions completed to date (minimum of 1):		Date activity started:	
Representative's name, signature and position:	Name: Signature: Position: Date:		
Participant declaration and date:	Signature: Date:		
Company Stamp: (If the company stamp is not available, please refer to guidance for further information on supporting evidence.)			

Thank you for your assistance.

Schedule 15

ESF Publicity Requirements

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836956/ESIF-GN-1-005_ESIF_Branding_and_Publicity_Requirements_v8_updated.pdf

Schedule 16

Training and Apprenticeships

1 Definitions and Interpretation

1.1 The following terms bear the following meanings for the purposes of this Schedule 16 (Training and Apprenticeships):

Apprentice	means a worker who is party to an apprenticeship agreement as defined in section 32 of the Apprenticeships, Skills, Children and Learning Act 2009
Trainee	means a worker who is employed by the Supplier under a contract of employment which provides for a scheme to allow the worker to obtain a National Vocational Qualification through paid study away from the workplace by working under the direction of experienced workers.

2 Training Requirements

2.1 The Supplier shall take all reasonable steps to employ Apprentices and/or Trainees, and report to the Authority the numbers of Apprentices and/or Trainees employed and wider skills training provided, during the delivery of this Contract.

2.2 Subject to its obligations in clause 13.1, the Supplier shall take all reasonable steps to ensure 5% of the employees, or that a similar specified proportion of hours worked in delivering the Contract, (which may include support staff and Sub-Contractors) are to be delivered by an employee on an Apprentice and/or Trainee programme.

2.3 The Supplier is required to make available to its Staff working on the Contract, information about the Government's Apprenticeship programme available at www.apprenticeships.org.uk, and wider skills opportunities provided by local authorities.

2.4 The Supplier shall provide any appropriate further skills training opportunities for Staff delivering the Contract.

2.5 The Supplier shall provide a written report detailing the following measures in the contract management reporting and be prepared to discuss Apprentices and/or Trainees at Performance Meetings:

2.5.1 The number of people during the reporting period employed on the Contract, including support staff and Sub-Contractors;

2.5.2 The number of Apprentices and/or Trainees and number of new Apprentices and/or Trainees directly initiated through the procurement process;

2.5.3 The percentage of all Staff which are Apprentices and/or Trainees;

2.5.4 Explanation from the Supplier as to why the Supplier has not achieved the specified percentage target of Apprentices and/or Trainees;

2.5.5 Actions being taken to increase the number of Apprentices and/or Trainees;

2.5.6 Other training and skills development being undertaken by employees in relation to the Contract, including:

(a) work experience placements for 14 to 16 year olds

- (b) work experience and work trial placements for other ages.
- (c) student sandwich and gap year placements
- (d) graduate placements
- (e) vocational training
- (f) skills training
- (g) on-site training provision and facilities.

Schedule 17

Access to Authority Case Management System

1 Definitions and Interpretation

1.1 For the purposes of this Schedule 17 the following terms shall bear the following meanings

Data User	means any Staff member or Sub-Supplier of the Supplier who is granted access to Authority Data or the Authority Case Management System
CATS+	means the Authority Case Management System as at the Commencement Date (and shall be deemed to be a reference to any updated Case Management System in place from time to time)
Train the Trainer	means the training practice where the Authority trains Supplier Staff to an accepted standard and such Staff can then provide the same training to other Supplier Staff as needed

2 General

2.1 To be permitted to have any type of access to Authority data, or to use the Authority Case Management System, it is a condition that, the Supplier shall procure that all Data Users have completed and signed a Data Usage Agreement (if so required by the Authority) and Security Operational Procedure in the form as the Authority may reasonably require (the **SyOps Forms**) prior to such access being granted and as may be updated from time to time by the Authority.

2.2 The Supplier shall retain all fully completed and individually signed SyOps Forms and shall provide copies of such SyOps Forms upon request by the Authority from time to time.

2.3 The Authority shall provide training in the format of Train the Trainer and this shall be disseminated by the Supplier to all relevant Staff and Sub-Contractors.

2.4 The Supplier shall procure that any Data User having access to the Authority Case Management System shall complete any training in respect of such use provided by the Authority.

2.5 The Supplier must ensure that SyOps Forms are reviewed by Data Users on an annual basis, with email acceptance that they have done so.

2.6 The Supplier must provide the Authority with a list of Supplier Staff that have been authorised to request new CATS+ user accounts before any CATS+ users can be created on the Authority Case Management System. This list is attached at Annex 1. Supplier Staff will be considered to have "Authority to Approve" provided that they:

2.6.1 are cleared to SC (Security Check) level;

2.6.2 are listed within Annex 1 to this Schedule;

2.6.3 and have completed, signed and returned to the Authority a copy of the Authority to Approve User Form, as available from the Authority and updated from time to time.

2.7 Supplier Staff with Authority to Approve must submit new CATS+ user account requests to the HMPPS CFO Service Desk. Once delivery locations are defined, an "NUA (New User

Application) Hub form" will be given to the Supplier to allow new user details to be submitted. The Authority will not accept new CATS+ user account requests sent by any other means or by Supplier Staff without Authority to Approve.

- 2.8 Supplier Staff with Authority to Approve must sign the statements within the NUA Hub form (as available from the Authority and updated from time to time) before a CATS+ account is created for a Data User.
- 2.9 The Supplier must ensure that there are appropriate mechanisms in place within their organisation to notify the Authority within 5 Working Days, via the HMPPS CFO Service Desk, of any Supplier Staff with CATS+ user account or who have Authority to Approve who cease to work for the Services provided by the Supplier under this Contract so that CATS+ user accounts can be disabled.
- 2.10 The Supplier must provide such assurance and evidence to the Authority as the Authority may reasonably require that security vetting checks as required by the Authority from time to time have been undertaken on all Staff where it is required, and ensure that evidence of this for existing Staff is available on request to allow the Authority to perform sample checks to assure compliance.
- 2.11 In the event of a suspected security breach, the Authority reserves the right to suspend any CATS+ user accounts in relation to that breach.

3 CATS+ supportive evidence and standard download documents

- 3.1 The Supplier shall ensure that all Data Users sign the relevant statement provided by the Authority that certifies any scanned documents uploaded to CATS+ are a true and accurate copy of the original. The Supplier must actively ensure that Supplier and Sub-Contractor Staff are compliant with this requirement.
- 3.2 The Supplier shall retain all original copies of documents which have been scanned and uploaded onto CATS+ until the Authority has Approved and allocated for payment for the associated Enrolment or Activity.
- 3.3 The Authority has absolute discretion to refuse payment for any Enrolment or Activity where the Supplier does not hold original copies of uploaded documents up to the point of payment being made to the Supplier for the same.
- 3.4 The Supplier shall make any such documentation available to the Authority or its auditors at any time as described in the Supplier Guidance or as required by clause 32 (Audit).
- 3.5 Once payment has been made by the Authority to the Supplier, the scanned version, uploaded onto CATS+ becomes the primary supporting documentation to support the associated Enrolment or Activity.
- 3.6 The original hard copy documentation shall be handled in accordance with Schedule 5 (Records and Reports).
- 3.7 Documents should not be uploaded to CATS+ that are not a relevant part of the required ESF audit trail.
- 3.8 Documents that are not a relevant part of the required ESF audit trail may be deleted by the Authority without notice
- 3.9 A list of standard templates, documents accompanied by their supportive guidance are available within the 'Help' section within CATS+ to assist with the providing the Suppliers' CATS+ outcome evidence. These documents are stored under the following sections:
 - 3.9.1 Access to CATS+
 - 3.9.2 Case Management
 - 3.9.3 CATS+ Guidance

- 3.9.4 Enrolment
- 3.9.5 Evidence Guidance
- 3.9.6 Security
- 3.9.7 Training
- 3.10 These documents will be updated on CATS+ when required and the Supplier will be informed accordingly.
- 3.11 Documents uploaded as outcome evidence should support achievements claimed on CFO Activity Hubs as part of the payment mechanism. The outcome should not be claimed as an achievement on any other contract which would attract a payment.
- 3.12 Documents that can be uploaded to CATS+ are capped at 1mb. There are no specific quality requirements, however documents should be deemed fully legible by the CFO and in a file format accepted by CATS+.
- 4 CATS+ access for offenders and ex-offenders**
- 4.1 The Supplier acknowledges that the Authority does not permit access to CATS+ to offenders, regardless of whether or not they are employed by the Supplier or any Sub-Supplier in the delivery of Services under this Contract or any other Contract with the Authority, including those relating to the HMPPS CFO ESF programme.
- 4.2 The Authority will permit access to CATS+ for ex-offenders who are employed by the Supplier in the delivery of Services under this Contract subject to the Supplier completing a risk and impact assessment which must be submitted to, and approved by, the Authority. This must take place prior to any new CATS+ user requests being raised by the Supplier and must take into account whether their personal information is held on the system and how the integrity of the CFO programmes and individuals data will be maintained.
- 5 CATS+ training**
- 5.1 The Supplier acknowledges that the successful completion of CATS+ training is mandatory for all users of the system before they will be permitted access to it by the Authority.
- 5.2 Training sessions will be provided by the Authority initially at regional locations, using a set timetable of dates or at the Authority's premises. Training will be by individual contract level and consist of Train the Trainer sessions to enable Suppliers to train their own staff.
- 5.3 In the event that training sessions become over-subscribed, extra training sessions will be made available by the Authority where possible and these sessions will be based at the Authority's premises and will be across contracts as a mop up exercise.
- 5.4 The Supplier must ensure that Supplier Staff who are nominated as CATS+ Trainers are available for the whole training session. The Supplier acknowledges that any Supplier Staff who are unable to complete the full session will not be allowed access to CATS+ or be allowed to conduct provider staff CATS+ training. The Authority will make details of start and end times for the training session available at the publication of training dates, along with any pre learning requirements.
- 5.5 In the event that any Supplier Staff are unable to complete the full training session, or that any Supplier Staff fail to attend a booked training session, then the Authority may request the Supplier to reimburse the Authority their reasonable costs associated with the training.
- 5.6 The Supplier acknowledges that Supplier Staff need to demonstrate a satisfactory level of competence in using CATS+, for their Train the Trainer role. If the Authority is not satisfied with the standard of CATS+ knowledge, the individual(s) will be denied access to the system and not be able to conduct CATS+ Training for Supplier staff without attending further training until a satisfactory level of competence is demonstrated.

- 5.7 Each Supplier is required to have a sufficient number of trainers throughout the life of the contract, fully trained by HMPPS CFO, to deliver CATS+ training to all their case workers (including sub providers) who require access to the CATS+ system. The minimum number of trainers should be 2 per Hub (or satellite delivery site), up to a maximum of 6 across each contract.
- 5.8 Each Supplier should ensure that they have no less than 2 trainers per Hub operational at any one point in time. When the numbers become critical HMPPS CFO will deliver new training to the appropriate prime and Sub-Contractor staff.
- 5.9 Training must be booked at least 28 days in advance. Maximum number for training (both CATS+ & Quality Assurance (QA)) is 6 staff.
- 5.10 Once trained as a "CATS+ Trainer", with relevant level of security checks completed, delivery of training can commence with the Supplier and Sub-Supplier Staff. The Supplier must inform the Authority service desk in advance (giving at least 5 Working Days' notice) of all CATS+ training sessions they plan to deliver to allow CATS+ Training Environment to be set up on system.
- 5.11 The Supplier must inform the Authority's service desk (or such other Authority personnel as the Authority Representative may nominate from time to time) of any CATS+ training sessions (at least 5 Working Days) as the first 2 training sessions delivered by CATS+ trainers will need to be monitored by Authority Representatives to ensure consistency of training. Periodic observations will also be conducted by Authority Representatives during the length of the project.
- 5.12 Any concerns or failures in the quality of the training delivery should be recorded by the Authority Representative and will be discussed at the subsequent Performance Meeting.
- 5.13 The Authority may issue a schedule of CATS+ Trainer training dates when the need arises or in the last quarter of the year via a Supplier Bulletin.
- 5.14 The Supplier shall ensure that they maintain an auditable log of their CATS+ Trained Trainers which should include their names and the date of training.
- 5.15 The Supplier shall ensure that they maintain an auditable log of their CATS+ users which should include their names and the dates they have been trained on CATS+.

6 European Social Fund and other funding

- 6.1 The Supplier shall within four (4) weeks of expiry or termination of this Contract provide evaluation information to the Authority which:
- 6.1.1 summarises the project, focusing on how it has helped to achieve the project objectives set out in the Specification; and
 - 6.1.2 is concise, being no more than one A4 page in length; and
 - 6.1.3 indicates whether the objectives have been fully achieved or only partly achieved and sets out any other relevant issues in this context.
- 6.2 The Supplier acknowledges the obligation the Authority has to evaluate all ESF projects by ESF measure and to submit, within strict timescales, a final claim to the Managing Authority including an assessment of performance in each of the measures. Accordingly, the Supplier agrees that time shall be of the essence in relation to its obligation under paragraph 6.1 above.
- 6.3 The Supplier understands and shall comply with the regular ESF management information reporting obligations set out in the ESF Regulations as available from the Managing Authority and updated from time to time. The Supplier acknowledges that the Authority depends on timely provision of this information in order to claim and receive ESF funds from the Managing Authority.

6.4 The Supplier shall indemnify and keep indemnified the Authority in respect of any and all costs, claims and losses howsoever incurred resulting from any breach by the Supplier of this paragraph 6. The Supplier's liability under this indemnity is not limited under Clause 33 of the Contract.

Annex 1

Service Provider Name (Supplier/Subcontractor)	Name	Job role/Title	Business Address	Telephone number	Email address
The Growth Company	[REDACTED]	Head of Specialist Services	Lee House, 90 Great Bridgewater Street, Manchester, M1 5JW	07834310286	[REDACTED]
The Growth Company	[REDACTED] Cheryl Collins	Head of Quality and Compliance	Lee House, 90 Great Bridgewater Street, Manchester, M1 5JW	[REDACTED]	[REDACTED]
The Growth Company	[REDACTED]	Compliance Assurance Manager	Lee House, 90 Great Bridgewater Street, Manchester, M1 5JW	[REDACTED]	[REDACTED]

Schedule 18

Industry Standard Partnering Agreement

INDUSTRY STANDARD PARTNERING AGREEMENT

[]

[CONTRACTOR]

and

[SUBCONTRACTOR]

[Notes:

1. This Industry Standard Partnering Agreement, or specific parts of it, may not be appropriate for all types of services contracts and may not include all contractual terms required. Suppliers should also refer to the requirements for sub-contracting in their agreement with the Authority.

2. Suppliers and Sub-Contractors should seek their own legal advice before entering into an Industry Standard Partnering Agreement.]

Contents

Clauses

1	Services And Service Commencement.....	69
2	Contract Management.....	70
3	Representations, warranties and undertakings.....	71
4	Liability.....	72
5	Insurance.....	73
6	Price and payment.....	73
7	Contract period and termination.....	74
8	Transparency and information.....	75
9	Assignment.....	76
10	Subcontracting.....	76
11	Miscellaneous.....	77

Schedules

1	Definitions and interpretation.....	80
---	-------------------------------------	----

This Agreement is made on []

Between:

- (1) [•] (registered in England under number [•]), whose registered office is at [•] (**Contractor**); and
- (2) [•] (registered in England under number [•]), whose registered office is at [•] (**Subcontractor**), each a **party** and together the **parties**.

Background:

- (A) On [•], the Secretary of State for Justice appointed the Contractor as a provider of services on the terms set out in a contract dated [•]) (**Services Agreement**).
- (B) The Contractor wishes to subcontract the provision of certain services in the Services Agreement to the Subcontractor on the terms set out in this Agreement.
- (C) The parties have entered into this Agreement in accordance with the Market Stewardship Principles having had regard to the Explanatory Guide.
- (D) The Subcontractor will complete the ISPA Questionnaire in relation to this Agreement and a copy of that completed Questionnaire is contained in Schedule 2 (Industry Standard Partnering Agreement Questionnaire) to this Agreement.

IT IS AGREED as follows:

1 Services And Service Commencement

1.1 Principal Obligations

- (a) The Subcontractor shall provide the Services to the Contractor with effect from the Service Commencement Date.
- (b) The Subcontractor shall at all times ensure that the Services comply with, and meet all the requirements of, and perform all its other obligations arising under or in connection with, this Agreement, in accordance with each of this Agreement, Good Industry Practice, and all Applicable Law. **[Explanatory Note: any other mandatory provisions required are to be listed here, the Contractor should refer to the requirements for sub-contracting in their agreement with the Authority.]**
- (c) The Contractor shall supply or make available to the Subcontractor:
 - (i) all information, data or access to systems that is reasonably requested by the Subcontractor which the Contractor agrees to provide, in respect of the Services; and
 - (ii) all information that the Subcontractor reasonably requires to assess the risk allocation to the Subcontractor in respect of the Services.
- (d) The Contractor agrees that the Subcontractor shall be entitled to request information from the Authority, as reasonably required by the Subcontractor, if the Contractor is unwilling or unable to provide the necessary information in accordance with Clause 1.1(c) above.
- (e) The Contractor shall provide to the Subcontractor for the Contract Period the support set out in the Marketing Stewardship Principles to assist the Subcontractor in providing the Services. **[Explanatory Note: This will refer to the Market Stewardship Principles set out in the Services Agreement.]**

1.2 Service Levels

- (a) Without limiting Clause 1.1, with effect from the Service Commencement Date, the Subcontractor shall meet or exceed the Service Levels in its provision of the relevant Services.
- (b) If, at any time after the Service Commencement Date, the Subcontractor fails to provide any of the Services in accordance with the Service Levels, without limiting the Contractor's other rights and remedies, the Subcontractor shall:
 - (i) advise the Contractor as soon as reasonably practicable [and in any event within [•] Business Days] of the failure and of the steps that the Subcontractor shall take to address the failure; and
 - (ii) at no additional cost to the Contractor:
 - (A) if applicable, perform or re-perform those elements of the Services in relation to which there was a failure to perform as are necessary to be performed or re-performed (as the case may be) to ensure that the relevant Services are compliant with the relevant Service Levels;
 - (B) to the extent practicable, rectify all direct operational consequences resulting from that failure to perform the Services in accordance with the relevant Service Levels; and
 - (C) as soon as practicable, arrange all additional resources as are reasonably necessary to perform its obligations set out in this Agreement and to ensure that the failure does not recur.

2 Contract Management

2.1 Contract Reviews

- (a) Within 40 Business Days after the end of a Contract Year, the Contractor and the Subcontractor shall meet to review the Subcontractor's performance of this Agreement during that Contract Year (the **Contract Review**). The parties agree that the Contract Review will focus on the strategic nature of the Services to the Contractor and the Authority and the importance to the Contractor and the Authority of assessing the performance of its strategic suppliers on a regular basis so that:
 - (i) performance issues can be monitored and addressed as they arise; and
 - (ii) the outcomes and feedback from the Contract Review can be incorporated as applicable or as reasonably requested by the Subcontractor into the Contractor's annual review under the Services Agreement.
- (b) The Subcontractor shall, for the purposes of Clause 2.1(a), send to the Contractor not less than 40 Business Days prior to the start of each Contract Year a copy of each of:
 - (i) a service report for the previous Contract Year completed to the end of the ninth month of that previous Contract Year; and
 - (ii) any other written reports that the Contractor or the Authority may reasonably request.

2.2 Remedial Plan Process

- (a) If at any time the Authority has serious concerns about:

- (i) the Contractor's continuing ability to meet its obligations under the Services Agreement; or
- (ii) public protection and safeguards,

and those concerns relate to the Services (**Serious Concerns**), the Contractor shall be entitled to initiate the process set out in Clause 2.2(b) (**Remedial Plan Process**).

(b) The Remedial Plan Process shall be as follows:

- (i) The Contractor shall notify the Subcontractor that the Authority has Serious Concerns and that the Contractor requires the Subcontractor to provide a plan to specify how the Serious Concerns will be addressed (**Remedial Plan**). The notice shall specify the Serious Concerns in outline but must contain sufficient detail so that it is reasonably clear to the Subcontractor the matters it has to remedy.
- (ii) The Subcontractor shall provide a draft Remedial Plan to the Contractor within 15 Business Days (or any other period agreed by the parties in writing) after the date of the notice referred to in Clause 2.2(b)(i) even if the Subcontractor disagrees with the Serious Concerns or disputes that it is responsible for the matters which are the subject of the Serious Concerns.
- (iii) The Subcontractor shall provide all reasonable assistance and information to the Contractor in connection with the Remedial Plan to enable the Contractor to meet its obligations in favour of the Authority under the Services Agreement.

3 Representations, warranties and undertakings

3.1 Warranty

Each party represents and warrants to the other party that:

- (a) it has the power to execute and deliver this Agreement and to perform its obligations under it and has taken all action necessary to authorise execution and delivery and the performance of its obligations;
- (b) this Agreement constitutes legal, valid and binding obligations of that party in accordance with its terms; and
- (c) authorisations, licences or consents from, and notices or filings with, each regulator or other governmental or other authority that are necessary to enable it to execute, deliver and perform its obligations under this Agreement have been obtained or made (as the case may be) and are in full force and effect and all conditions of each authorisation, licence, consent, notice or filing have been complied with.

3.2 Exercise of rights

In exercising its rights under this Agreement, the Contractor shall act reasonably and proportionally.

3.3 Risk Assessment

The parties acknowledge and agree that:

- (a) they have entered into this Agreement having fully considered and assessed the allocation of risk to the Subcontractor and the ability of the Subcontractor to control that risk;

- (b) the Subcontractor has not been allocated a disproportionate amount of risk relative to the nature of the Services and the Charges.

3.4 Subcontractor Undertakings

The Subcontractor undertakes to the Contractor that, for the Contract Period, it will:

- (a) not reorganise or change the nature or scope of its activities in a way that may, in the reasonable opinion of the Authority, have a detrimental effect on the provision of the Services in accordance with this Agreement;
- (b) not, without the prior written consent of the Contractor, (and whether by a single transaction or by a series of transactions whether related or not) sell, transfer, lend or otherwise dispose of (other than by way of security) the whole or any material part of its business, employees or Assets which would materially affect the ability of the Subcontractor to perform its obligations under this Agreement;
- (c) not undertake the performance of its obligations under this Agreement for the provision of the Services otherwise than through itself or a subcontractor;
- (d) not, without the prior written consent of the Contractor, apply for the appointment of an administrator over its Assets;
- (e) provide the Services, charge for the Services, carry out its business and conduct its affairs according to the highest standards of corporate governance applicable from time to time to companies registered in the United Kingdom and in a responsible manner and shall observe principles of good social responsibility.

3.5 Reputational Damage

- (a) The Subcontractor shall provide the Services and perform all its other obligations arising under or in connection with this Agreement having regard to the standing and reputation of the Authority[and the Contractor] and, in particular, shall not do anything (by act or omission) that would, or would be reasonably likely to:
 - (i) damage the reputation of the Authority [or the Contractor];
 - (ii) bring the Authority [or the Contractor] into disrepute;
 - (iii) attract adverse publicity to the Authority [or the Contractor]; or
 - (iv) harm the confidence of the public in the Authority [or the Contractor].
- (b) The Subcontractor shall, when providing the Services, pay due regard to the need for persons in a public service environment to observe the highest standards of efficiency, economy, courtesy, consideration and hygiene.

4 Liability

4.1 Limitations of liability

- (a) Nothing in this Agreement excludes or limits any party's liability:
 - (i) for fraud, theft or any similar dishonesty offence or conduct which would amount to such an offence;
 - (ii) for wilful misconduct or wilful abandonment;
 - (iii) for death or personal injury caused by its negligence or that of its employees or agents and, in the case of the Subcontractor, any subcontractor or its employees or agents;

- (iv) arising as a result of a breach of Clause 18;
 - (v) arising as a result of a breach of any intellectual property indemnity provided by the Subcontractor; or
 - (vi) to the extent that any Applicable Law precludes or prohibits any exclusion or limitation of liability.
- (b) For the avoidance of doubt, any amounts payable by either party to the other party in respect of any of the above shall not count towards the financial cap[s] on liability set out in Clause 4.1(b).
- (c) Subject to Clause 4.1(a), the aggregate liability of each party to the other party under or in connection with this Agreement, whether arising in tort (including negligence), for breach of contract or otherwise shall be the greater of:
- (i) £[●]; or
 - (ii) the total amounts paid or payable by the Contractor to the Subcontractor under this Agreement.

4.2 Indirect and consequential loss

Subject to Clause 4.1(a) neither party shall be liable to the other party for any indirect or consequential or special loss or damage, whether arising in tort (including negligence), breach of contract or otherwise, whether or not that loss was foreseeable provided that the Contractor shall not be prevented from recovering as direct recoverable losses any losses arising from a claim by the Authority to the Contractor in respect of:

- (a) additional operational or administrative costs and expenses;
- (b) any wasted expenditure or charges;
- (c) any additional costs of procuring a replacement supplier and/or replacement deliverables;
- (d) any compensation or interest paid by the Authority to a third party;
- (e) any fine or penalty incurred by the Authority under law or any costs incurred in defending proceedings resulting in such fine or penalty

in each case as a consequence of the Sub-Contractor default

5 Insurance

The Subcontractor shall during the Contract Period take out and maintain or procure the maintenance of insurances as would be maintained by a reasonably prudent supplier of services similar to the Services in accordance with Good Industry Practice or as may be required by Applicable Law.

6 Price and payment

[The parties shall comply with their respective obligations under Schedule 6 (Charges).]

The Contractor shall pay all undisputed invoices raised by the Subcontractor in respect of the Charges within 30 days of the date of the invoice.

7 Contract period and termination

7.1 Contract Period

- (a) This Agreement shall commence on the date of this Agreement and shall continue until the Termination Date.
- (b) This Agreement shall terminate automatically on the date that the Services Agreement effectively terminates unless the Authority requires this Agreement to be novated to a New Contractor. The Contractor shall ensure that the Exit Period shall expire on the same date as the expiry of the Exit Period under the Services Agreement.
- (c) If this Agreement terminates pursuant to Clause 7.1(b) in circumstances where the Subcontractor is not in default of this Agreement, the Contractor shall pay to the Subcontractor an amount equal to the Breakage Costs.

7.2 Voluntary Termination

- (a) The parties agree that this Agreement cannot be terminated pursuant to this Clause 7.2 without the Authority's prior written consent.
- (b) Subject to Clause 7.2(a), either party may terminate this Agreement at any time by giving not less than six months written notice to the other party stating that it is terminating this Agreement under this Clause 7.2 provided that the six month period may not expire prior to the end of the Initial Term.
- (c) Notwithstanding Clause 7.2(b), the Contractor shall be entitled to require the Subcontractor to cease to provide the Services and to terminate this Agreement by giving written notice to the Subcontractor if directed to do so by the Authority under the terms of the Services Agreement.
- (d) For the purposes of Clauses 7.2(b) and (c), the Exit Period shall commence on the date specified in the notice and this Agreement shall effectively terminate on the Termination Date.
- (e) If this Agreement terminates pursuant to Clause 7.2(b) or, in circumstances where the Subcontractor is not in default of this Agreement pursuant to Clause 7.1(c), the Contractor shall pay to the Subcontractor an amount equal to the Breakage Costs.
- (f) During the Exit Period following termination pursuant to this Clause 7.2(b), during the Exit Period the Contractor shall notify the Subcontractor and provide the Subcontractor with written details of its intention to subcontract any services provided by the Contractor to the Authority under the Services Agreement and the Contractor shall, if the Subcontractor wishes, consider the Subcontractor's proposal for the provision of those services on behalf of the Contractor.

7.3 Termination on Insolvency

- (a) [Each party may, without limiting its other rights or remedies, terminate this Agreement by written notice to the other party (the **Defaulting Party**) if any step, process, application, filing in court, order, proceeding, notice or appointment is taken or made by or in respect of the Defaulting Party for a moratorium, composition, compromise or arrangement with creditors (by way of voluntary arrangement, scheme of arrangement or otherwise), administration, liquidation (other than for the purposes of amalgamation or reconstruction), dissolution, receivership (administrative or otherwise), distress or execution, or the Defaulting Party becomes insolvent or is deemed unable to pay its debts as they fall due, or anything analogous to the foregoing occurs in any applicable jurisdiction[, provided that the

- (b) Authority has provided its prior written consent to that termination].] [Explanatory Note: The additional language in parenthesis in the final sentence of this Clause 7.3(b) must be included where the Subcontractor is a Material Subcontractor under the Services Agreement].
- (c) The Exit Period shall commence on the date falling five Business Days after the date of the notice to terminate and this Agreement shall effectively terminate on the Termination Date.

7.4 Termination on Material Breach

- (a) Each party (the **Terminating Party**) may, without limiting its other rights or remedies, terminate this Agreement by written notice to the other party (the **Defaulting Party**), if:
 - (i) the Defaulting Party is in material breach of this Agreement (and for this purpose a material breach may be a single event or a series of events taken together) and either:
 - (A) that breach is not capable of remedy;
 - (B) that breach is capable of remedy and the Defaulting Party has failed to remedy that breach within 20 Business Days after receiving written notice from the Terminating Party requiring it to do so; or
 - (C) the Terminating Party has given notice under this Clause 7.4 within the preceding 60 Business Days for the same or a substantially similar breach,

and for this purpose a breach will be treated as (A) capable of remedy only if the Terminating Party can be put in the position that it would have been in but for the breach; and (B) remedied only if the Terminating Party is put in the position that it would have been in but for the breach[; and
 - (ii) the Authority has provided its prior written consent to that termination].]
- (b) The notice of termination for the purposes of this Clause 7.4 must specify:
 - (i) the type and nature of breach that has occurred, giving reasonable details; and
 - (ii) that the Exit Period will commence on the day falling 20 Business Days after the date the Non-Defaulting Party sends the notice of termination and this Agreement shall effectively terminate on the Termination Date unless, in the case of a breach which is capable of remedy, the Defaulting Party rectifies the breach within that period of [20] Business Days (**Rectification Period**).
- (c) If the Defaulting Party rectifies the breach within the Rectification Period, the notice of termination will be deemed to be revoked and this Agreement will continue in force.
- (d) If the Defaulting Party fails to rectify the breach within the Rectification Period, the Exit Period will commence on the date falling five Business Days after the expiry of the Rectification Period and this Agreement shall effectively terminate on the Termination Date.

8 Transparency and information

- (a) The Subcontractor shall:

- (i) provide to the Contractor copies of its annual report and accounts within 20 Business Days after their publication;
 - (ii) use all reasonable endeavours to assist the Contractor in its preparation of any report required by the Authority, from time to time; and
 - (iii) provide all information reasonably required by the Contractor in connection with changes in accordance with the provisions of any change protocol.
- (b) The Subcontractor agrees that performance related and financial information provided to the Contractor under this Agreement will be made available to the Authority and any Authority Related Party at its request for the purposes of contract management, assessing the suitability for bidders when considering the award of contracts and overseeing the management, and the performance, of relationships with strategic suppliers at a cross Government level.

8.2 Public Relations and Publicity

- (a) Subject to Clause 18.3(b), the Subcontractor shall be permitted to communicate with representatives of the press, television, radio or other communications media in order to promote and publicise its business and service capabilities as they relate to the Services.
- (b) The Subcontractor shall consult with the Contractor prior to engaging in any activity set out in Clause 18.3(a) that would involve the disclosure of any matter under this Agreement and shall not in any circumstances disclose any Confidential Information.
- (c) No facilities or permission to photograph or film in or on any property used for the provision of the Services by the Subcontractor shall be given by the Contractor to the Subcontractor without the prior written approval of the Authority.

8.3 Conflicts of Interest

The Subcontractor shall take appropriate steps to ensure that neither the Subcontractor nor any Subcontractor Personnel is placed in a position where there is or may be an actual conflict or potential conflict, between the interests of the Subcontractor and the duties owed to the Contractor under the provisions of this Agreement.

9 Assignment

- (a) Neither party shall assign, transfer or otherwise dispose of any of its rights or transfer (including by way of novation) or otherwise dispose of any of its obligations under this Agreement, without the prior written consent of the other party and any such purported assignment, transfer or disposal shall be void.
- (b) If the Services Agreement expires or terminates for whatever reason, the Subcontractor shall, at the request of the Authority, novate its obligations under this Agreement to a New Contractor.

10 Subcontracting

10.1 Contractor's consent

- (a) The Subcontractor shall not subcontract the provision of any part of the Services under this Agreement.

[Explanatory Note: ESF Rules and Regulations prohibit more than one level of subcontracting.]

11 Miscellaneous

11.1 Announcements

Neither party shall:

- (a) make or authorise any public or private announcement or communication concerning this Agreement; or
- (b) refer to or use any business name or trade mark of the other party in any promotional communications,

without the prior written consent of that other party, except where required by Applicable Law.

11.2 Notices

- (a) Any notice or other communication to be given under this Agreement to a party must be in writing [(which includes fax, but not any other form of electronic communication (as defined in the Electronic Communications Act 2000))] and must be delivered or sent by post [or facsimile] to the party to whom it is to be given at its address set out below:

- (i) [to the Contractor at:

[•]

Marked for the attention of: [•]]

- (ii) to the Subcontractor at:

[•]

Marked for the attention of: [•]

or at any other address [or facsimile number] as it shall have notified to the other party in accordance with this Clause 11. Any notice or other communication sent by post shall be sent by prepaid first class recorded delivery post (if within the United Kingdom) or by prepaid airmail (if elsewhere). The parties shall agree in writing within 20 Business Days after the date of this Agreement a protocol for the delivery of notices for the operational management of this Agreement (including by way of email) and the parties shall comply at all times with that protocol as updated from time to time.

- (b) Any notice or other communication shall be deemed to have been given:

- (i) if delivered, on the date of delivery;
 - (ii) if sent by post, on the second Business Day after it was put into the post; or
 - (iii) if sent by facsimile, on the date of transmission, if transmitted before 3.00 p.m. (local time at the country of destination) on any Business Day, and in any other case on the Business Day following the date of transmission.

- (c) In proving the giving of a notice or other communication it shall be sufficient to prove that delivery was made or that the envelope containing the communication was properly addressed and posted by prepaid first class recorded delivery post or by prepaid airmail or that the facsimile message was properly addressed and transmitted, as the case may be.

- (d) This Clause 11.2 shall not apply in relation to the service of any claim form, notice, order, judgement or other document relating to or in connection with any proceedings, suit or action arising out of or in connection with this Agreement.

11.3 Entire Agreement

- (a) This Agreement (and the documents referred to in it) contains the whole agreement between the parties relating to the transactions contemplated by this Agreement and supersedes all previous agreements between the parties relating to these transactions. Except as required by statute, no terms shall be implied (whether by custom, usage or otherwise) into this Agreement.
- (b) Each party acknowledges that, in agreeing to enter into this Agreement, it has not relied on any express or implied representation, warranty, collateral contract or other assurance (except those set out in this Agreement and the documents referred to in it) made by or on behalf of the other party at any time before the signature of this Agreement.
- (c) Each party waives all rights and remedies which, but for Clause 24.3(b), might otherwise be available to it in respect of any such express or implied representation, warranty, collateral contract or other assurance.
- (d) Nothing in Clause 24.3(a) limits or excludes any liability for fraud.

11.4 Third Party Rights

- (a) The Subcontractor acknowledges and agrees that the Contractor has entered into this Agreement for its own benefit and for the benefit of the Authority.
- (b) The Authority may enforce against the Subcontractor under the Contracts (Rights of Third Parties) Act 1999 any Clause in this Agreement even though the relevant Clause may be silent as to which person is intended to have the benefit of the relevant obligation, refer only to the Contractor or not specifically identify the Authority or an Authority Related Party but subject always to the liability provisions in this Agreement, which shall apply, making the necessary changes, to claims made by the Authority.
- (c) Subject to Clause 24.4(b), a person who is not a party to this Agreement may not enforce any of its terms under the Contracts (Rights of Third Parties) Act 1999.
- (d) This Agreement may not, without the prior written consent of the Authority (that consent not to be unreasonably withheld or delayed), be varied or terminated in any way that might affect the rights of the Authority and any Authority Related Party under this Clause 11.4.
- (e) This Clause 11.4 does not apply to the Crown and does not affect any right or remedy of a third party which exists or is available apart from the Contracts (Rights of Third Parties) Act 1999.

11.5 Waiver

The rights of each party under this Agreement:

- (a) may be exercised as often as necessary;
- (b) except as otherwise provided by this Agreement, are cumulative and not exclusive of rights or remedies provided by law; and
- (c) may be waived only in writing and specifically.

Delay in the exercise or non-exercise of any right is not a waiver of that right. A waiver of any right or remedy arising from a breach of this Agreement shall not constitute a waiver of any right or remedy arising from any other or subsequent breach of this Agreement.

11.6 No partnership or agency

At all times during the Contract Period, the Subcontractor shall be an independent contractor and nothing in this Agreement shall be construed as creating a partnership, a contract of employment or a relationship of principal and agent between the Authority and the Subcontractor or the Contractor and the Subcontractor and accordingly neither the Contractor nor the Subcontractor shall be authorised to act in the name of, or on behalf of, or otherwise bind the other party or the Authority save as expressly permitted by the terms of this Agreement.

11.7 Severability

The provisions contained in each Clause and paragraph of this Agreement shall be enforceable independently of each of the others and their validity shall not be affected if any of the others is invalid. If any provision is void but would be valid if some part of the provision were deleted, the provision in question shall apply with such modification as may be necessary to make it valid.

11.8 Further assurance

Each party undertakes, at the request and cost and expense of the other party, to sign all documents and to do all other acts which may be necessary to give full effect to this Agreement.

11.9 Counterparts

This Agreement may be executed in any number of counterparts, all of which taken together shall constitute one and the same agreement, and any party (including any duly authorised representative of a party) may enter into this Agreement by executing a counterpart.

11.10 Governing Law and Jurisdiction

- (a) This Agreement and any non-contractual obligations arising out of or in connection with it shall be governed by English law.
- (b) Subject to the Dispute Resolution Procedure, the courts of England shall have exclusive jurisdiction to settle any dispute, claim or controversy arising out of or in connection with this Agreement (including a dispute, claim or controversy relating to any non-contractual obligations arising out of or in connection with this Agreement) and the parties accordingly submit to the exclusive jurisdiction of the English courts.

THIS AGREEMENT has been signed on behalf of the parties by their duly authorised representatives on the date which appears on page 1.

Schedule 1

Definitions and interpretation

1 Interpretation

- 1.1 In this Agreement any reference, express or implied, to an enactment (which includes any legislation in any jurisdiction) includes:
- (a) that enactment as amended, extended or applied by or under any other enactment
 - (b) (before, on or after the execution of this Agreement);
 - (c) any enactment which that enactment re-enacts (with or without modification); and
 - (d) any subordinate legislation made (before, on or after the execution of this Agreement) under that enactment, including (where applicable) that enactment as amended, extended, or applied as described in paragraph 1.1(a), or under any enactment which it re-enacts as described in paragraph 1.1(b).
 - (e) In this Agreement:
 - (i) any reference to a **person** includes a body corporate, unincorporated association of persons (including a partnership), government, state, agency, organisation, and any other entity whether or not having a separate legal personality and an individual, his estate and personal representatives;
 - (ii) any reference to a party to this Agreement includes a reference to the successors or assigns (immediate or otherwise) of that party;
 - (iii) any reference importing a gender includes the other genders;
 - (iv) any reference to a time of day is to London time;
 - (v) subject to Clause 11.2, any reference to writing includes typing, printing, lithography and photography but excludes any form of electronic communication (as defined in the Electronic Communications Act 2000) to the other party by email (and Clause 11.2 shall not apply to those communications);
 - (vi) each reference to a document is to that document as amended, varied, assigned or novated from time to time otherwise than in breach of this Agreement or that document;
 - (vii) each reference to a Clause, Schedule or Appendix is to a clause of, or a schedule or appendix to, this Agreement;
 - (viii) each reference to a paragraph is to a paragraph of a Schedule or Appendix;
 - (ix) the Schedules form part of this Agreement;
 - (x) the headings do not affect the interpretation of this Agreement;
 - (xi) any reference to a company includes any company, corporation or other body corporate wherever incorporated; and
 - (xii) any reference to an indemnity being given on an after-Tax basis means that the amount payable pursuant to such indemnity (the **Payment**) shall be increased (or decreased, as the case may be) so as to ensure that, after taking into account:

- (A) the amount in respect of Tax required by law to be deducted or withheld from such amount (or increased or decreased amount, as the case may be);
- (B) the Tax that is chargeable (or would be chargeable but for the use, setting off or application of any relief) on such amount (or increased or decreased amount, as the case may be) in the hands of the recipient of the Payment; and
- (C) any Tax credit, repayment or other Tax benefit which is actually received and used by the recipient of the Payment solely as a result of the matter giving rise to the indemnity or as a result of receiving the Payment,

(which amount of Tax and Tax credit, repayment or other Tax benefit is, in the case of (B) and (C) above, to be determined by the recipient (acting reasonably and in good faith) and certified as such to the party making the Payment), the recipient of the Payment is in the same position as it would have been in had there been no such withholding, deduction, Tax, Tax credit, repayment or other Tax benefit, provided that nothing in this paragraph 1.1(e)(xii)(C) shall require the recipient to make any changes to the way in which it deals with any Tax Authority in relation to any Tax credit, repayment or other Tax benefit. References in this paragraph 1.1(e)(xii)(C) to the recipient of a payment include references to any person who is treated as receiving that payment for any Tax purpose.
- (f) In this Agreement each reference to indemnifying any person against any event, matter or circumstance shall be construed as a reference to indemnifying that person in full and holding that person harmless on an after Tax basis from and against all Losses suffered or incurred by that person, in each case arising out of any and all claims (whether or not successful, compromised or settled), actions, demands, proceedings or judgments which may be instituted, made, threatened, alleged, asserted or established in any jurisdiction against or otherwise involving that person, including Losses suffered or incurred in establishing a right to be indemnified under this Agreement, and indemnified and indemnify and similar expressions shall be interpreted accordingly.
- (g) A reference in this Agreement to any English legal term for any action, remedy, method or form of judicial proceeding, legal document, court or any other legal concept or matter will be deemed to include a reference to the corresponding or most similar legal term in any jurisdiction other than England, to the extent that jurisdiction is relevant to the transactions contemplated by this Agreement or the terms of this Agreement.
- (h) If there is any conflict or inconsistency between any of:
 - (i) a term in the main body of this Agreement;
 - (ii) a term in any of the Schedules;
 - (iii) a term in any of the Appendices to the Schedules; and
 - (iv) any term included in any other document incorporated by reference into this Agreement,

the term falling into the category first appearing in the list above shall, unless expressly stated otherwise, take precedence.
- (i) The *ejusdem generis* rule does not apply to this Agreement. Specific words indicating a type, class or category of thing do not restrict the meaning of general words following specific words, such as general words introduced by the word "other" or a similar expression. General words followed by specific words shall not be restricted in meaning to the type, class or category of thing indicated by the

specific words. The words including and include shall mean "including without limitation" and "include without limitation", respectively.

- (j) In the Schedules and Appendices, capitalised terms that are not defined in this Schedule 1 (Definitions and Interpretation) shall have the meaning given to them in the relevant Schedule or Appendix.
- (k) Paragraphs 1.1(a) to 1.1(g) (inclusive) of this Schedule 1 (Definitions and Interpretation) apply unless expressly stated otherwise in this Agreement.

2 Definitions

Affiliate means, in relation to any person, any Holding Company or subsidiary of that person or any subsidiary of that holding company and "holding company" and "subsidiary" shall have the meaning given to them in Section 1159 of the Companies Act 2006, save that, for the purposes of determining whether one entity is an Affiliate of another, any transfer of shares by way of security or to a nominee of the transferor shall be disregarded;

Agreement means this agreement and its Schedules and Appendices;

Applicable Law means all Legislation, Directions and any applicable judgement of a relevant court of law which changes a binding precedent;

Assets means all assets and rights to enable the Contractor or a successor subcontractor to provide the Services in accordance with this Agreement, including:

- (a) any books and records (including operating and maintenance manuals, health and safety manuals and other know-how);
- (b) any revenues and any other contractual rights; and
- (c) any intellectual property rights,

but excluding any assets and rights in respect of which the Contractor is full legal and beneficial owner;

Authority means the Secretary of State for Justice;

Authority Related Party means any or all of (i) the Authority, (ii) the Police and Crime Commissioners, (iii) a government department, agency or a non-departmental government body, in each case as the Authority may specify and (iv) an officer, agent, contractor, employee or subcontractor of the Authority acting in the course of his office or employment or appointment (as appropriate) but excluding, in each case, the Contractor, any Contractor Related Party and the Subcontractor;

Authority Website means that part of www.[] headed [] or headed with a similar title or heading; *[Explanatory Note: MOJ will provide the domain name for this website at a later date.]*

Breakage Costs means costs that have been reasonably incurred by the Subcontractor as a direct result of the termination of this Agreement, but only to the extent that:

- (a) the costs that have been incurred for the provision of Services including:
 - (i) any materials or goods ordered or subcontracts between the Subcontractor and the Third Party placed that cannot be cancelled without those costs being incurred;
 - (ii) any expenditure incurred in anticipation of the provision of the Services in the future;

- (iii) the cost of demobilisation including the cost of any relocation of equipment used in connection with the Services; and
- (iv) redundancy payments for employees of the Subcontractor; and
- (b) the costs are incurred under a subcontract entered into by the Subcontractor in accordance with this Agreement that is consistent with terms that have been entered into in the ordinary course of business and on reasonable commercial terms;

Business Day means a day (other than a Saturday or Sunday) on which banks are open for domestic business in the City of London;

Charges means the payment calculated in accordance with Schedule [] (Charges);

Commencement Date means [DATE]

Contract Period means the period from and including the Service Commencement Date to the Termination Date;

Contract Review has the meaning given to it in Clause 2.1(a);

Contract Year means a period of 12 months commencing on the date of this Agreement or on an anniversary of the date of this Agreement except for the first Contract Year which shall commence on the date of this Agreement and terminate on the December 31 following the date of this Agreement and the last Contract Year which shall commence on the January 1 prior to the Termination Date and end on the Termination Date;

Contractor Related Party means each of the Contractor, Contractor's Affiliates, agents and contractors and its or their subcontractors and its or their directors, officers and employees, but excluding the Subcontractor and its directors, officers and employees;

Crown means Her Majesty's Government which shall be deemed to include any government department, office or agency and any Secretary of State;

Direction means any applicable guidance or direction with which the Contractor is bound to comply;

Explanatory Guide means the explanatory guide to the terms in the Industry Standard Partnering Agreement published on the Authority Website from time to time;

Good Industry Practice means that degree of skill, care, prudence and foresight and operating practice which would reasonably and ordinarily be expected from time to time of a skilled and experienced operator (engaged in the same or similar type of undertaking as that of the Contractor) or any Subcontractor under the same or similar circumstances;

Holding Company has the meaning given to it in Section 1159 of the Companies Act 2006, save that for the purposes of determining whether one entity is a Holding Company of another any transfer of shares by way of security or to a nominee of the transferor shall be disregarded;

Industry Standard Partnering Agreement (ISPA) means the Authority's standard form contract for subcontracting arrangements;

ISPA Questionnaire means the questionnaire set out in Schedule 2 (Industry Standard Partnering Agreement Questionnaire);

Legislation means any Act of Parliament or subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, any exercise of the Royal Prerogative, and any enforceable EU right within the meaning of Section 2 of the European Communities Act 1972 (as amended), in each case in the United Kingdom;

Losses means all damages, losses, liabilities, costs, expenses (including legal and other professional charges and expenses), and charges whether arising under statute, contract or at common law or in connection with judgments, proceedings, internal costs or demands;

Market Stewardship Principles means the principles set out in Schedule 19 (Market Stewardship Principles) of the Services Agreement;

New Contractor means the person who has entered or who will enter into an agreement with the Authority for the provision of services the same as or substantially the same as the services under the Services Agreement in substitution for the services that the Contractor currently provides under the Services Agreement;

Remedial Plan has the meaning given to it in Clause 2.2(b)(i);

Remedial Plan Process has the meaning given to it in Clause 2.2(a);

Service Levels means the service levels set out in Schedule 5] (Service Levels);

Services means the services set out in Schedule [] (Services);

Services Agreement means the contract dated [•] 20[] between the Secretary of State for Justice and the Contractor pursuant to which the Secretary of State for Justice appointed the Contractor as a provider of rehabilitation services;

Subcontractor Personnel means all employees, agents and consultants of the Subcontractor and its Affiliates and any subcontractor engaged in the performance of the Subcontractor's obligations arising under or in connection with this Agreement (including the Services);

Termination Date means the date on which the exit period expires and this Agreement is effectively terminated in accordance with Clause 7;

Third Party means each person or entity that is not a party to this Agreement; and

VAT means any value added taxes.

ISPA Questionnaire



ISPA Sub Provider
Review Document v.

Schedule 19

Market Stewardship Principles

1 Introduction

- 1.1 These Market Stewardship Principles cover the key principles that must underpin the Supplier's provision of the Services and its engagement with all entities to which it Sub-Contracts the provision of the Services.
- 1.2 Each of the principles set out in this Schedule details how the Supplier should respond to its obligations against each of the principles governs how the Supplier must engage with its Sub-Contractors.

2 Principles

2.1 Adherence to appropriate management of risk in the supply chain

All contractual and other risk should be appropriately managed. This should extend to not passing risk down supply chains disproportionately, the management of volume fluctuations and other events and the management of intellectual property rights.

2.2 Meaningful volume of work allocation

The Supplier should be able to evidence its approach in allocating work to supply chain partners in a manner which meets its obligations under the Contract. Where a Sub-Contractor is specified in the Contract, the Supplier shall refer meaningful volumes of work to that Sub-Contractor. These volumes should be set out in the Sub-Contract.

The Supplier shall record details of all issues arising out of complaints from Sub-Contractors that they have not received expected volumes of work and shall refer these complaints to the Authority.

2.3 Systems for allocation of work to a Sub-Contractor

The Supplier should have systems for allocation of specific work to a Sub-Contractor where the delivery of that element of the Services is best served by calling on the particular expertise of a Sub-Contractor. The allocations should ensure that the Participants receive Services from a Sub-Contractor that has the correct level of expertise. Examples would include Sub-Contractors who have the skills and experience required to work with offenders with a range of different needs including without limitation; protected characteristics, female offenders, BAME, and offenders with learning difficulties or dyslexia etc.

2.4 Volume Fluctuations

The Supplier must demonstrate to the Authority's satisfaction how it manages any volume fluctuations in referrals and the reallocation of the Services to Sub-Contractors. The potential impact of both increases and particularly reductions in work allocation and associated drop in income, and actions to mitigate these risks, must be set out in the Industry Standard Partnering Agreement or the Sub-Contract (as applicable). Any changes should be communicated through the change process set out in this Contract.

2.5 Spot purchase arrangements

Spot purchase arrangements may be entirely appropriate but can be detrimental to Sub-Contractors as opposed to more standard contracts that guarantee an income. Sub-Contractors generally, but also in seeking funding or additional business may be disadvantaged in only being able to reference spot purchase contracts. The Supplier should therefore ensure that, wherever 'spot purchase' arrangements are utilised, options to transition to more stable contractual referral systems are reviewed at regular periods.

2.6 Payment terms

The Supplier should detail a full exploration of payment terms and the impact of these on the supply chain including the requirement for any clawback/ repayment if targets are not met. The implications of this should be worked through for each year of the Industry Standard Partnering Agreement or Sub-Contract (as applicable).

2.7 Minimum contract term

Consideration should be given to the needs of Sub-Contractors in relation to the Term. The contract length, if inadequate, may damage the ability of the Sub-Contractor in seeking new business or additional funding from elsewhere. Supporting statements around expected minimum term of Sub-Contracts may be helpful for Sub-Contractors to avoid this.

2.8 Intellectual Property Rights (IPR)

The Supplier should set out in the Industry Standard Partnering Agreement or Sub-Contract an approach for the handling of intellectual property rights to be established as part of the supply chain selection process.

2.9 Alignment of ethos in the supply chain

The Authority envisages that a sustainable relationship is fostered throughout the Term, which meets the expectations of both parties according to the position established at contract inception. In entering into a Sub-Contract, there should be an understanding of what is important to both the Supplier and the Sub-Contractor and this should go on to form part of the Sub-Contract which will be reviewed throughout the Term to ensure that expectations are being met. The Authority's market engagement has reinforced that this is an important expectation for many organisations and key to building trust, especially in the early stages of such business relationships.

2.10 Audit trail

The Supplier must maintain an audit trail of engagement with Sub-Contractors that demonstrates compliance with the principles established at the outset of the working relationship and shall include any additional support the Supplier offers.

2.11 Referrals of clients to non-contracted partners

The Supplier may wish to refer services to organisations who already deliver similar support services. The Supplier must not exploit the services delivered by these organisations, particularly those that do not enter into a formal contractual or grant funding arrangement with the Supplier. The Authority will require the Supplier to articulate how it is supporting and sustaining all organisations that the Supplier intends to refer a significant volume of work. In this context, 'significant' should be interpreted in proportion to the size of the organisation rather than the Supplier's caseload.

2.12 Meetings

The Supplier must record details of the conduct of all meetings with Sub-Contractors and any other members of its supply chain and review these records to ensure that they are timely and appropriate and reinforce good relationship management.

2.13 Visibility across the supply chain

The Authority expects that all parties have visibility of participation within the supply chain. This should include payment terms against contractual targets, the volume of business handled by Sub-Contractors, fair apportionment of referrals with regard to easier cases, and how the supply chain adjusts to changing volumes or demographics.

2.14 Supply chain sourcing, selection and refresh process

The Supplier must ensure that the sourcing, selection and refresh process for Sub-Contractors is transparent. This information must be made freely available to both the Authority and each potential Sub-Contractor on request.

2.15 Reward and recognition of good performance

The Authority considers it important that Sub-Contractors receive appropriate reward for good performance. Recognition of good performance should be shared across the chain and this should include the sharing of good practice.

Schedule 20

Financial Distress

1 Definitions

1.1 In this Schedule, the following definitions shall apply:

- | | |
|----------------------------------|---|
| "Credit Rating Level" | means a credit rating level as specified in Annex 1 of this Schedule |
| "Credit Rating Threshold" | means the minimum Credit Rating Level for the Supplier as set out in Annex 2 of this Schedule |
| "Rating Agency" | means the rating agency listed in Annex 1 of this Schedule |

2 Warranties and duty to notify

- 2.1 The Supplier warrants and represents to the Authority for the benefit of the Authority that as at the Commencement Date the long term credit ratings issued for the Supplier by the Rating Agency is as set out in Annex 2 of this Schedule.
- 2.2 The Supplier shall promptly notify the Authority in writing where (a) a Financial Distress Event occurs; or (b) any fact or circumstance which would cause a Financial Distress Event occurs; or (c) if there is any downgrade in the credit rating issued by the Rating Agency for the Supplier (and in any event within 5 Working Days of the occurrence of the event).

3 Financial distress events

3.1 The following shall be Financial Distress Events:

- (a) the credit rating of the Supplier dropping below the applicable Credit Rating Threshold or a Rating Agency that holds the Credit Rating for the Supplier ceases to hold a Credit Rating for that entity;
- (b) the Supplier or Key Sub-Contractor issuing a profits warning to a stock exchange or making any other public announcement, in each case about a material deterioration in its financial position or prospects;
- (c) there being a public investigation into improper financial accounting and reporting, suspected fraud or any other impropriety of the Supplier or Key Sub-Contractor;
- (d) the Supplier or Key Sub-Contractor committing a material breach of covenant to its lenders;
- (e) a Key Sub-Contractor notifying the Authority that the Supplier has not satisfied any material sums properly due under a specified invoice and not subject to a genuine dispute which is not remedied within 10 days of notification by the Authority;
- (f) any of the following:
 - (i) commencement of any litigation against the Supplier or Key Sub-Contractor with respect to financial indebtedness greater than £5m or obligations under a service contract with a total contract value greater than £5m;
 - (ii) non-payment by the Supplier or Key Sub-Contractor of any financial indebtedness;

- (iii) any financial indebtedness of the Supplier or Key Sub-Contractor becoming due as a result of an event of default;
- (iv) the cancellation or suspension of any financial indebtedness in respect of the Supplier or Key Sub-Contractor; or
- (v) the external auditor of the Supplier or Key Sub-Contractor expressing a qualified opinion on, or including an emphasis of matter in, its opinion on the statutory accounts of the Supplier or Key Sub-Contractor;

in each case which the Authority reasonably believes (or would be likely reasonably to believe) could directly impact on the continued performance and delivery of the Services in accordance with this Contract.

4 Consequences of financial distress events

4.1 Immediately upon notification by the Supplier of a Financial Distress Event (or if the Authority becomes aware of a Financial Distress Event without notification and brings the event to the attention of the Supplier), the Supplier shall have the obligations and the Authority shall have the rights and remedies as set out in paragraphs 4.2 to 4.4.

4.2 The Supplier shall (and shall procure that any Key Sub-Contract shall):

- (a) at the request of Authority, meet the Authority as soon as reasonably practicable (and in any event within 3 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing) to review the effect of the Financial Distress Event on the continued performance and delivery of the Services in accordance with this Agreement; and
- (b) where the Authority reasonably believes (taking into account the discussions and any representations made under paragraph 4.3(a) that the Financial Distress Event could impact on the continued performance of the Services in accordance with this Contract:
 - (i) submit to the Authority for its approval, a draft Financial Distress Remediation Plan as soon as reasonably practicable (and in any event, within 10 Working Days of the initial notification (or awareness) of the Financial Distress Event or such other period as the Authority may permit and notify to the Supplier in writing); and
 - (ii) to the extent that it is legally permitted to do so and subject to the terms of this Contract, provide such information relating to the Supplier and/or any Key Sub-Contractors as the Authority may reasonably require in order to understand the risk to the Services, which may include forecasts in relation to cash flow, orders and profits and details of financial measures being considered to mitigate the impact of the Financial Distress Event.

4.3 The Authority shall not withhold its approval of a draft Financial Distress Remediation Plan unreasonably. If the Authority does not Approve the draft Financial Distress Remediation Plan, it shall inform the Supplier of its reasons and the Supplier shall take those reasons into account in the preparation of a further draft Financial Distress Remediation Plan, which shall be resubmitted to the Authority within 5 Working Days of the rejection of the first draft. This process shall be repeated until the Financial Distress Remediation Plan is Approved by the Authority or referred to the Dispute Resolution Procedure under clause 46.

4.4 Following approval of the Financial Distress Remediation Plan by the Authority, the Supplier shall:

- (a) Review and update (with prior approval of the Authority) the Financial Distress Remediation Plan on a regular basis (which shall not be less than fortnightly) so

that it ensures the continued performance of the Services in accordance with this Agreement;

- (b) Regularly update the Authority on its progress against the Financial Distress Remediation Plan and any proposed changes to the Financial Distress Remediation Plan.
- (c) comply with the Financial Distress Remediation Plan (including any updated Financial Distress Remediation Plan) and ensure that it achieves the financial and performance requirements set out in the Financial Distress Remediation Plan in accordance with any deadlines set out in therein.

5 Termination rights

5.1 The Authority shall be entitled to terminate this Agreement under clause 36.1 if:

- (a) the Supplier fails to notify the Authority of a Financial Distress Event in accordance with paragraph;
- (b) the parties fail to agree a Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with paragraphs 4.2 to; and/or
- (c) the Supplier fails to comply with the terms of the Financial Distress Remediation Plan (or any updated Financial Distress Remediation Plan) in accordance with paragraph 4.4(c).

Annex 1: Rating Agencies and their Standard Rating System

- The Rating Agency is Dun and Bradstreet, Inc.
- The Credit Rating Level for the Supplier as at the Commencement Date is:

Financial Strength : [REDACTED]

Risk Indicator : [REDACTED]

The Credit Rating Level is set out under the heading D&B Rating in the attached D&B report.

[REDACTED]

Table 1 – Rating Agency Risk Indicators

Failure Score	Risk Indicator	Probability of Failure
86-100	1	Minimum Risk
51-85	2	Lower than average Risk
11-50	3	Higher than average Risk
1-10	4	High Risk
-	-	Insufficient Information

Table 2 - Rating Agency Financial Strength Indicators

Financial Strength Indicator	Tangible Net Worth (in £)	
Net Worth	From	To
5A	35,000,000	And above
4A	15,000,000	34,999,999
3A	7,000,000	14,999,999
2A	1,500,000	6,999,999
1A	700,000	1,499,999

A	350,000	699,999
B	200,000	349,000
C	100,000	199,999
D	70,000	99,999
E	35,000	69,999
F	20,000	34,999
G	8,000	19,999
H	0	7,999
Alternate Symbols Used		
N	Negative net worth	
O	Net worth undetermined (accounts unavailable or older than 2 years)	

Annex 2: Credit Rating and Credit Rating Thresholds

Entity	Credit Rating (Long term)	Credit Rating Threshold
Supplier	[REDACTED]	[REDACTED]

IN WITNESS of which the Contract is duly executed by the Parties on the date which appears at the head of page 1.

Signed for and on behalf of the Secretary of State for Justice

Signature: **[REDACTED]**

Name (block capitals): **[REDACTED]**

Position: **[REDACTED]**

Date: **[REDACTED]**

Signed for and on behalf of the Supplier

Signature: **[REDACTED]**

Name (block capitals): **[REDACTED]**

Position: **[REDACTED]**

Date: **[REDACTED]**