



Single Source  
Regulations Office

# Security and information Risk Advisor (SIRA) services

## Appendix 4: Terms and Conditions

David Galpin  
Director of Legal and Policy  
3<sup>rd</sup> floor, Finlaison House  
15-17 Furnival Street  
London  
EC4A 1AB  
**☎: 0203 771 4786**  
**M: 07710 763 386**  
**✉: [David.Galpin@ssro.gov.uk](mailto:David.Galpin@ssro.gov.uk)**

This **AGREEMENT** is made on the \_\_\_\_\_ day of \_\_\_\_\_ 2019

**BETWEEN:**

- (1) **SINGLE SOURCE REGULATIONS OFFICE** of 3<sup>rd</sup> Floor Finlaison House, 15-17 Furnival Street, London EC4A 1AB (the “**SSRO**”) of the one part; and
- (2) [**CONTRACTOR DETAILS**] with registered company number [\_\_\_\_\_] and whose registered address is [\_\_\_\_\_] (the “**Contractor**”) of the other part

individually a “**Party**” and together the “**Parties**”.

**WHEREAS:**

- A. The SSRO requires the provision of Security and information Risk Advisor (SIRA) services.
- B. The SSRO has carried out a procurement exercise to appoint a suitable contractor to deliver those services and the Contractor has been selected.
- C. The Contractor agrees to deliver the services as required and in accordance with the terms and conditions set out herein.

**NOW IT IS HEREBY AGREED as follows:**

**1. Definitions**

- 1.1. In the Contract the following capitalised words shall have the relevant meanings ascribed to them as detailed below (unless the context suggests otherwise):
  - (a) “**Clarifications**” means the SSRO’s response to questions raised by the Contractor during the tender period and which form part of the Specification;
  - (b) “**Client Officer**” means an officer of the SSRO representing the SSRO and as notified to the Contractor from time to time;
  - (c) “**Commencement Date**” means [\_\_\_\_\_] ;
  - (d) “**Complaint**” means a complaint made by a Data Subject;
  - (e) “**Compliance Forms**” means the Form of Tender and Statement of Conduct completed by the Contractor during the tender process and contained in the Contractor’s Proposal;
  - (f) “**Contract**” means the agreement for the Contractor to provide the Services to the SSRO in accordance with these terms and conditions;
  - (g) “**Contract Period**” means the period referred to at clause 2.1
  - (h) “**Contract Price**” is determined in accordance with the rates in the Pricing Schedule, subject to any variation agreed in writing by the SSRO under clause 5;

- (i) **“Contractor’s Confidential Information”** means the Information belonging to the Contractor in respect of which one of the following is satisfied:
  - It comprises Protected Data; or
  - Disclosure of the Information would, or would be likely to, prejudice the commercial interests of any person (including one of the Parties) and the public interest in maintaining non-disclosure would outweigh the public interest in disclosure; or
  - Disclosure of the Information would constitute a breach of confidence actionable by either Party or a third party;
- (j) **“Contractor’s Manager”** means the Employee of the Contractor with principal responsibility for providing the Services;
- (k) **“Contractor’s Proposal”** means the Contractor’s methodology for carrying out the Services as attached at Schedule 5;
- (l) **“Data Controller”** has the meaning given to it by the Data Protection Act 2018;
- (m) **“Data Processor”** has the meaning given to it by the Data Protection Act 2018;
- (n) **“Data Subject”** means an individual who is the subject of Protected Data;
- (o) **“Data Subject Request”** means a request by a Data Subject pursuant to Data Protection Laws;
- (p) **“Data Protection Laws”** means the EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
- (q) **“Deliverable”** means any product, tangible or intangible, resulting from the performance of the Services;
- (r) **“Employee”** shall include any person who is an employee or director of the Contractor or a partner in the Contractor, or who occupies the position of a director of the Contractor, by whatever title given;
- (s) **“EU Data Protection Laws”** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State (including the Data Protection Act 2018) and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
- (t) **“GDPR”** means EU General Data Protection Regulation 2016/679;
- (u) **“Information”** means information or data recorded in any form disclosed to one Party by or on behalf of the other Party under or in connection with the Contract, including information provided in the tender or negotiations which preceded the award of the Contract;
- (v) **“Intellectual Property Rights”** means any patent, patent application, know how, trade mark or name, service mark, design right, registered design, copyright, moral right, rights in commercial or technical information or any other intellectual property rights, whether registered or unregistered and including applications for the grant of any such rights and all rights or forms of protection having equivalent or similar effect anywhere in the world;

- (w) **“International Organisation”** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
- (x) **“Key Personnel”** means members of the Contractor’s staff who are specifically identified in the Contractor’s Response as the main providers of the Services, including those staff designated as Lead Practitioner and Senior Practitioner;
- (y) **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to, Protected Data transmitted, stored, or otherwise processed;
- (z) **“Pricing Schedule”** means the document containing the Contractor’s quoted rates for delivering the Services and included in the Contractor’s Proposal;
- (aa) **“Protected Data”** means any personal data within the meaning of the Data Protection Act 2018 processed by the Data Processor on behalf of the Data Controller in performing the Services;
- (bb) **“Processing Instructions”** means the SSRO’s instructions for the processing of Protected Data by the Contractor;
- (cc) **“Secret Matter”** means any matter connected with the Contract, or its performance which is designated in writing by the SSRO as 'TOP SECRET' or 'SECRET', and shall include any information concerning the content of such matter and anything which contains or may reveal that matter;
- (dd) **“Security Conditions”** means all the requirements of Schedule 1 to the Contract;
- (ee) **“Security Measures”** means all the requirements of Schedule 2 to the Contract;
- (ff) **“Security Policy Framework”** means the HMG Security Policy Framework relating to the Government Security Classification policy as published by the Cabinet Office;
- (gg) **“Sensitive Information”** has the meaning given in the Security Conditions;
- (hh) **“Services”** means such services described in the Specification which the SSRO requires the Contractor to provide;
- (ii) **“Specification”** means the document appended at Schedule 4 provided by the SSRO to the Contractor together with the Clarifications (where applicable), which together set out the SSRO’s requirements for the Services;
- (jj) **“Stage”** means a defined section of the Services as stated in the Specification;
- (kk) **“Supervisory Authority”** means an independent public authority responsible for monitoring the application of the Data Protection Laws in the United Kingdom;
- (ll) **“Working Day”** means any day other than a Saturday, Sunday or public holiday in England and Wales.

1.2. In these terms and conditions:

- (a) a reference to a person includes a natural person and anybody or organisation with a separate legal personality;
- (b) a reference to a party includes its personal representatives, successors or permitted assigns; and
- (c) a reference to a statute or statutory provision is a reference to such statute or provision as amended or re-enacted and includes a subordinate instrument or provision of such instrument as amended or re-enacted.

## **2. Commencement and duration**

- 2.1 The Contract shall commence on the Commencement Date and expire on 24 months thereafter, extended in accordance with clause 2.2 below or terminated earlier in accordance with the provisions of this Contract or by operation of statute or common law.
- 2.2 At the SSRO's sole discretion, it may extend the contract duration on up to two occasions, each for a period of 12 months, by giving the Contractor at least one month's written notice on each occasion.

## **3. SSRO's obligations**

- 3.1 The SSRO shall pay to the Contractor the Contract Price in accordance with clause 6.
- 3.2 The SSRO shall provide the Contractor with such information and instructions as the Contractor reasonably requires for the purposes of providing the Services.
- 3.3 The SSRO does not guarantee any level or volume of business or a minimum number of hours' Services to be delivered under the Contract and the SSRO shall be under no obligation to offer the same to the Contractor.

## **4. Contractor's General Obligations**

- 4.1 The Contractor shall provide the Services at the SSRO's reasonable request and meet any performance dates and other requirements for the Services in the Specification or otherwise notified by the SSRO to the Contractor in the manner set out in the Contractor's Proposal.
- 4.2 In providing the Services, the Contractor shall:
  - (a) co-operate with the SSRO in all matters relating to the Services and comply with the SSRO's instructions;
  - (b) perform the Services with the reasonable care, skill and diligence in accordance with best practice in the Contractor's industry, profession or trade;
  - (c) allocate the Key Personnel to discharge the Contractor's obligations under the Contract and, in the event the Key Personnel are no longer available, shall obtain the SSRO's consent to any replacement personnel (who shall be suitably skilled and experienced employees);
  - (d) ensure that the Services conform with the Specification and the SSRO's instructions and that the Deliverables are fit for any purpose expressly or impliedly made known to the Contractor by the SSRO;

- (e) provide all equipment, tools and other items required to provide the Services;
- (f) use the best quality goods, materials, standards and techniques, and ensure that the Deliverables, and all goods and materials supplied and used in the Services or transferred to the SSRO will be free from defects in workmanship, installation and design;
- (g) not use any branding (including its own) other than the SSRO's on the Deliverables, except with the consent of the SSRO;
- (h) maintain complete and accurate records of the time spent and materials used by the Contractor in providing the Services and allow the SSRO to inspect such records at reasonable times on request;
- (i) obtain and at all times maintain all necessary licences and consents, and comply with all applicable laws and regulations;
- (j) comply with all applicable laws, enactments, orders, regulations and other similar instruments as amended from time to time; and
- (k) observe all health and safety rules and regulations and any other security requirements that apply at the SSRO's premises.

**4.3 The Contractor warrants and represents that:**

- (a) it has full capacity and authority and all necessary consents to enter into and perform the Contract and that the Contract is executed by a duly authorised representative of the Contractor; and
- (b) it owns, has obtained or shall obtain valid licences for all Intellectual Property Rights that are necessary for the performance of the Contract.

**4.4 The Contractor agrees that any breach of clauses 4.2 and 4.3 shall be remedied as a matter of urgency at no additional cost to the SSRO.**

**4.5 The Contractor shall attend review meetings and submit performance reports on the dates, times and in the form specified in the Specification, or as otherwise reasonably required by the SSRO.**

**4.6 The Contractor shall make adjustments to the Services in response to any reasonable request from the SSRO.**

**4.7 The Contractor shall notify the SSRO as soon as it becomes aware of an event occurring, or which it believes is likely to occur, which will cause material delay to or materially impede the performance of the Services or any part thereof and the Contractor shall take all necessary steps consistent with good practice to minimise the delay to the SSRO.**

**4.8 In the event that the Contractor fails due to its default to fulfil an obligation by the date specified in the Contract (or such incidental documents created during the Contract Period, including but not exclusively Court Orders) for such fulfilment, the Contractor shall, at the request of the SSRO and without prejudice to the SSRO's other rights and remedies, arrange all such additional resources as are necessary to fulfil the said obligation as early as practicable thereafter and at no additional charge to the SSRO.**

**4.9 In the event that any obligation of the Contractor specified in the Contract is delayed as a result of a default by the SSRO, then:**

- (a) the date associated with the relevant obligation as specified in the Contract (and the dates similarly associated with any subsequent obligations specified in the Contract) shall be amended by a period of time equal to the period of delay resulting from such SSRO's default (or such other period as the parties may agree in writing); and
  - (b) both parties shall use all reasonable endeavours to mitigate the impact of such delay and to recover any resultant delay to the performance of the Services.
- 4.10 The Contractor shall not instruct, or cause to be instructed, any third party or otherwise incur liabilities in the name of the SSRO without the prior written consent of the Client Officer.
- 4.11 The Contractor accepts that the SSRO shall have the right after consultation with the Contractor to require the removal of any person from involvement in the performance of the Services, including Key Personnel, if in the SSRO's reasonable opinion the performance or conduct of such person is or has been unsatisfactory or if it shall not be in the public interest for the person to work on the Contract.
- 4.12 The Contractor shall provide the Services and comply with the terms of the Contract in such a way so as not to cause any undue injury or damage to the image or reputation of the SSRO.
- 4.13 The Contractor will provide all reasonable assistance and support to the SSRO and the in-coming contractor in a timely fashion on the expiry or earlier termination of the Contract in order to facilitate the transition of the Contract to the in-coming contractor. This shall include the provision of records and data and any Deliverables over which the SSRO has proprietary interest or Intellectual Property Rights.

## **5. Additional Services**

- 5.1 Where the SSRO requires the Contractor to carry out services which are in addition to those identified in the Specification (identified as "Additional Services" in the Specification), the SSRO may request a variation to the Services in writing.
- 5.2 Upon receipt of the request referred to in clause 5.1, the Contractor shall provide to the SSRO a written response detailing at least:
  - (a) a statement as to how additional services will be provided;
  - (b) any variation in price (including a decrease in price where the total Services to be provided are reduced); and
  - (c) a statement of the impact on the remainder of the Services caused by such a variation.
- 5.3 In any event the Contractor shall not act on any proposed variation under clause 5.1 until the SSRO has agreed the response referred to in clause 5.25.2 in writing and the Contract shall remain unvaried until such time.
- 5.4 Any additional work carried out without obtaining the prior written consent of the SSRO shall not be chargeable to the SSRO.

## **6. Charges and Payment**

- 6.1 The Day Rates identified in the Pricing Schedule shall be the full and exclusive remuneration of the Contractor for delivery of the Services over the Contract Period, including any extension periods. The Rates shall not include value added tax (VAT), but shall be deemed

to include all fees, charges, disbursements, costs, expenses and other associated expenditure incurred in providing the Services, including all materials and utility costs.

- 6.2 The SSRO will reimburse the Contractor for disbursements which it has agreed in writing to pay, but the Contractor shall not incur any disbursements without the prior written agreement of the SSRO.
- 6.3 The Contractor must submit an invoice for payment, which must also be valid for VAT purposes. The SSRO will pay the Contractor such VAT as is chargeable on the delivery and supply of the Services.
- 6.4 Invoices shall be submitted no more frequently than on a monthly basis and shall have attached to the invoice a detailed bill of costs in respect of each matter worked on in that month to include, at least, the following information:
  - (i) Matter name;
  - (ii) SSRO Officer's name;
  - (iii) Purchase order number provided by the SSRO;
  - (iv) Type of activity;
  - (v) Relevant day rate(s) and apportionment;
  - (vi) Detailed breakdown of time spent per activity, per day and per fee earner;
  - (vii) Running total of fees accrued to date on each matter included in that bill; and
  - (viii)** a breakdown of any disbursements which the SSRO has agreed to pay.
- 6.5 The Contractor must not submit invoices more than 31 days after the period to which the invoice relates.
- 6.6 The Contractor shall not charge the SSRO for time spent opening a matter, preparing invoices, managing or training staff, or on administrative or secretarial work.
- 6.7 The SSRO shall pay undisputed sums to the Contractor within 30 days of receipt of a valid invoice.

## **7. Disbursements**

- 7.1 The Contractor shall not incur any disbursements for which the SSRO will be liable to pay without the prior written agreement of the SSRO. The SSRO will reimburse the Contractor for disbursements which it has agreed in writing to pay, but otherwise the rates specified in the Pricing Schedule shall be deemed to include all fees, charges, disbursements, costs, expenses, travel and subsistence and other associated expenditure incurred in providing the Services, including all materials and utility costs.

## **8. Third Party disclaimer and records**

- 8.1 Neither the Deliverables nor any of the Services provided pursuant to the Contract are intended, either expressly or by implication, to confer any benefit on any third party and the Contractor's liability to any third party is expressly disclaimed. Any third party that has access to and seeks to rely upon the Deliverables does so at their own risk and without recourse to



the Contractor, save where it is expressly agreed in advance that they may rely on the Deliverables or Services.

8.2 The Contractor shall keep and maintain until six months after the agreement has been completed, or as long a period as may be agreed between the parties, full and accurate records of the agreement including:

- a) the Services provided under it;
- b) all expenditure reimbursed by the SSRO; and
- c) all payments made by the SSRO.

The contractor shall on request afford the SSRO or the SSRO's representatives such access to those records as may reasonably be required in connection with the agreement.

## **9. Performance Review**

9.1 At regular intervals throughout the Contract Period, the SSRO and the Contractor shall meet to discuss and review the performance of the Contract.

## **10. Meetings**

10.1 The Contractor will attend such meetings as may reasonably be required by the SSRO in performing work under the Contract.

10.2 All the Contractor's costs and expenses associated with attendance at meetings in performing work under the Contract shall be deemed to be included in the Charges.

## **11. Stages and Performance**

11.1 Upon completion of the Services, or at the end of any Stage (where applicable) the Contractor shall notify the SSRO that the Services or as the case may be the relevant Stage is complete.

11.2 Upon notification in accordance with clause 11.1, the SSRO will review the performance of the relevant Services.

11.3 Notwithstanding any other legal right of the SSRO (either as stated in the Contract or under the law as specified in clause 28 of the Contract), where a review of the Services identifies that any part of the Services has not been provided in accordance with the Contract, then the SSRO may require either:

- (a) the Contractor to re-perform such Services until the relevant part of the Services have been completed in accordance with the Contract entirely at the Contractor's risk and expense; or
- (b) a reduction in any sum owing to the Contractor in such amount as is proportionate to the level which the performed Services failed to meet the requirements of the Contract.

11.4 Where re-performance is required of part or all of the Services, the SSRO shall:

- (a) set a reasonable timescale for the re-performance; and

- (b) review the re-performed Services and clauses 5.2 to **Error! Reference source not found.** shall apply to such review.

## **12. Intellectual Property Rights**

- 12.1 The SSRO will own the intellectual property rights in the final version of the Deliverables, subject to payment of the Contractor's fees, however the intellectual property rights in any materials created by or licensed to the Contractor outside of the performance of the Services will be owned by the Contractor (or by its licensors) and the SSRO will have a non-exclusive, not-transferable licence to use such materials for the purposes for which the Deliverables were provided. The Contractor shall seek the consent of the SSRO to use any intellectual property in the Deliverables that is owned by the SSRO, which consent shall not be unreasonably withheld.

## **13. Use of SSRO Facilities**

- 13.1 Where the Contractor is required to enter onto premises owned or operated by the SSRO or a third party, for the purposes of delivering the Services, the Contractor shall abide by all reasonable instructions of the person or persons in charge of such premises, including in relation to health and safety.
- 13.2 Such instructions referred to in clause 13.1 may include (but not exclusively):
  - (a) wearing identification badges;
  - (b) exclusion from restricted areas; and
  - (c) compliance with emergency evacuation procedures.
- 13.3 Notwithstanding the provisions of this clause, the Contractor is responsible for the health and safety of its own staff whilst the staff are present at such premises.

## **14. Termination**

- 14.1 The SSRO may terminate the Contract forthwith by notice in writing given to the Contractor in the event that:
  - (a) the Contractor commits a material breach of the Contract;
  - (b) the Contractor breaches the Contract on more than one occasion over a 3 month period and the SSRO considers that such failure is or may compromise the delivery of the Services;
  - (c) the Contractor suspends or threatens to suspend, or ceases or threatens to cease, all or a substantial part of the Contractor's business;
  - (d) the Contractor (or a partner of the Contractor) suspends or threatens to suspend payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or is deemed by legislation to be unable to pay its debts or as having no reasonable prospect of doing so;
  - (e) the Contractor is bankrupt or the subject of a bankruptcy petition;

- (f) the Contractor enters into negotiations for, or makes, a voluntary agreement with its creditors to compromise, reschedule or arrange repayment of outstanding sums;
- (g) a petition is filed, a notice is given, a resolution is passed, or an order is made, for or in connection with the winding up of the Contractor;
- (h) an administrator and or administrative receiver is appointed to manage the affairs of the Contractor, or an application is made to a court for the same;
- (i) a person becomes entitled to appoint a receiver over the assets of the Contractor or a receiver is appointed over the assets of the Contractor;
- (j) a creditor or other entitled person attaches or takes possession of the whole or any part of the Contractor's assets, or a distress, execution, sequestration or other such process is levied, enforced or sued against the Contractor's assets and such process is not discharged within 14 days;
- (k) any event occurs, or proceeding is taken with respect to the Contractor in any jurisdiction that has an effect equivalent or similar to clause 14.1(c) to 14.1(j);
- (l) the Contractor's business is taken over in whole or in part either by sale of a controlling interest in the share capital of the Contractor or by a sale of the assets relevant to the part of the Contractor's business that is performing the Contract;
- (m) the Contractor dies or, by reason of illness or incapacity, is incapable of managing the Contractor's affairs for a period of time; and
- (n) any part of the Contractor's Proposal, including the Compliance Forms, is found to be or have been incorrect, false or misleading.

14.2 The SSRO may terminate the Contract for any reason whatsoever by giving three month's written notice to the Contractor.

14.3 For the avoidance of doubt, the allowance by the Contractor of the actions detailed in clause 14.1 and the subsequent sub-clauses constitute a material breach of the Contract.

## **15. Liability and insurance**

15.1 Neither Party shall be liable to the other Party for any:

- (a) indirect, special or consequential loss; or
- (b) loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

15.2 The Contractor's aggregate liability to the SSRO of whatever nature, whether in contract, tort or otherwise, for any loss whatsoever and howsoever caused by or arising from this Engagement, shall not exceed the sum of one hundred thousand pounds.

15.3 For all services where any loss is suffered by the SSRO for which the Contractor would otherwise be jointly and severally liable with any third parties, the extent to which such loss shall be recoverable by the SSRO from the Contractor, as opposed to the third party, shall be limited so as to be in proportion to the Contractor's contribution to the overall fault for such damage or loss, as agreed between the parties, or in the absence of agreement, as finally determined by an English Court (ignoring for these purposes the ability of the third party to pay or any limitation of liability that the SSRO might have agreed with such third party).

- 15.4 Nothing in this Contract shall exclude or restrict the liability of any person for that person's fraud or dishonesty or purport to exclude or restrict a liability which cannot be excluded or restricted by law.
- 15.5 Throughout the Contract Period and for six years afterwards the Contractor shall take out and maintain with a reputable insurance company on generally available commercially acceptable terms public and employer's liability insurance to a minimum value of five million pounds for each and every claim or series of claims arising out of one event, and professional indemnity insurance to a minimum value of one hundred thousand pounds for each and every claim or series of claims arising out of one event.
- 15.6 From time to time when reasonably requested by the SSRO the Contractor shall send to the SSRO proof of payment of the premiums in respect of the insurance and a copy of the policy schedule and any other reasonable information for the SSRO to satisfy itself that the insurances referred to in clause 15.5 are in effect.

## **16. Transfer and Sub-Contracting**

- 16.1 The SSRO may assign, novate, or sub-contract the whole or any part of the Contract to anybody which performs functions previously performed by the SSRO upon giving written notice to the Contractor.
- 16.2 The Contractor shall not assign or sub-contract the whole or any part of the Contract or the Services without the prior written consent of the SSRO, which consent shall not be unreasonably withheld or delayed but may be given subject to such conditions, if any, as the SSRO in its sole discretion may consider reasonable or necessary to protect the interests of the SSRO.
- 16.3 The Contractor shall submit any request for the SSRO's consent to sub-contract in writing to the Client Officer and shall provide:
- (a) the name of the proposed sub-contractor;
  - (b) a statement of the work to be carried out;
  - (c) a statement of whether any Secret Matter or Sensitive Information will be disclosed to the sub-contractor;
  - (d) a statement of whether the sub-contractor is located in another country; and
  - (e) any other details known to the Contractor which the SSRO shall reasonably require.
- 16.4 Where the Contractor assigns or sub-contracts the whole or any part of the Contract without the consent referred to in clause 16.2 (without limitation whether or not due to company take-over by asset or share sale) the SSRO may terminate the Contract forthwith.
- 16.5 If consent is granted by the SSRO for the Contractor to sub-contract, whether following consent under clause 16.2 or otherwise, any services, goods, or other supplies or works will remain the responsibility of the Contractor.
- 16.6 Notwithstanding any sub-contract permitted under this clause, the Contractor shall remain responsible for providing the Services as if there had been no sub-contract and shall be responsible for the acts, defaults or neglect of any sub-contractor, their employees or agents in all respect as if they were the acts, defaults or neglect of the Contractor.

- 16.7 If so required by the SSRO any sub-contracting may be subject to the provision of collateral warranties or the SSRO may itself require third party rights as referred to in the Contracts (Rights of Third Parties) Act 1999 in any sub-contracting arrangement.
- 16.8 The Contractor undertakes to procure and agrees that it shall be a term of any sub-contract to which clause 16.6 refers that:
- (a) the employment of the sub-contractor under the sub-contract shall terminate immediately upon the termination of (for whatsoever reason) the Contract; and
  - (b) the sub-contractor's services are being provided for the benefit of the SSRO and accordingly, unless the sub-contractor shall have provided a warranty to the SSRO in a form approved by the Client Officer, the SSRO shall be entitled to enforce the terms of the sub-contract against the sub-contractor pursuant to section 1 of the Contracts (Rights of Third Parties) Act 1999.

## **17. Force Majeure**

- 17.1 Neither party shall be liable to the other party for any failure to perform its obligations under the Contract where such failure to perform is due to circumstances beyond the reasonable control of the party who has failed to perform.
- 17.2 Where the Contractor seeks to rely on clause 17.1 the SSRO shall not be liable to pay for the Services for the period during which the Contractor is seeking to rely on clause 17.1.

## **18. Health and Safety**

- 18.1 The Contractor shall ensure that its personnel and any sub-contractor and any other person acting on behalf of the Contractor complies with all legislation in relation to the safety and health of its employees, of sub-contractors, of any other persons in or near the place where the Services are to be performed.
- 18.2 Notwithstanding the generality of clause 18.1 the Contractor shall comply with:
- (a) all legislation relating to health and safety at work;
  - (b) all specific requirements relating to health and safety contained in the Contract; and
  - (c) any reasonable instructions the SSRO may give to the Contractor in relation to health and safety.

## **19. Freedom of Information**

- 19.1 The Contractor agrees to use all reasonable endeavours, at the Contractor's expense, to assist the SSRO to comply with its legal obligations to disclose information, including under the Freedom of Information Act 2000 and the Data Protection Act 2018.
- 19.2 The Contractor acknowledges that the SSRO may be obliged by law to disclose Information, either:
- (a) without consulting the Contractor; or
  - (b) contrary to the views of the Contractor.

19.3 The Contractor acknowledges that Confidential Information is indicative only and that the SSRO may be obliged to disclose Confidential Information pursuant to the Environmental Information Regulations or the 2000 Act.

## **20. Confidentiality**

20.1 Subject to paragraphs 20.5 to 20.6 the Contractor shall:

- (a) treat in confidence all Information it receives from the SSRO;
- (b) not disclose any of that Information to any third party without the prior written consent of the SSRO, which consent shall not unreasonably be withheld;
- (c) shall not use any of that Information otherwise than for the purpose of this Contract; and
- (d) shall not copy any of that Information except to the extent necessary for the purpose of exercising its rights of use and disclosure under this Contract.

20.2 The Contractor shall take all reasonable precautions necessary to ensure that all Information disclosed to the Contractor by or on behalf of the SSRO under or in connection with this Contract:

- (a) is disclosed to its employees and Sub-Contractors, only to the extent necessary for the performance of this Contract; and
- (b) is treated in confidence by them and not disclosed except with prior written consent or used otherwise than for the purpose of performing work or having work performed for the SSRO under this Contract or any Sub-Contract under it.

20.3 Subject to paragraphs 20.5 to 20.7, the SSRO shall:

- (a) treat all Contractor's Confidential Information as confidential and safeguard it accordingly;
- (b) not disclose any Contractor's Confidential Information without the prior written consent of the Contractor; and
- (c) not use any Contractor's Confidential Information otherwise than for the purpose of or in connection with the Contract.

20.4 Each Party shall ensure that its employees are aware of the arrangements for discharging the obligations at paragraphs 20.1 to 20.3, as applicable, in relation to their receipt and use of Information and take such steps as may be reasonably practical to enforce such arrangements.

20.5 Paragraphs 20.1 to 20.4 inclusive shall not apply to any Information to the extent that either Party:

- (a) exercises rights of use or disclosure granted otherwise than in consequence of, or under, this Contract;
- (b) has the right to use or disclose the Information in accordance with other provisions of this Contract; or
- (c) can show:

- (i) that the Information was or has become published or publicly available for use otherwise than in breach of any provision of this Contract or any other agreement between the Parties;
- (ii) that the Information was already known to it (without restrictions on disclosure or use) prior to it receiving it under or in connection with this Contract;
- (iii) that the Information was received without restriction on further disclosure from a third party who lawfully acquired it and who is itself under no obligation restricting its disclosure; or
- (iv) from its records that the same information was derived independently of that received under or in connection with this Contract.

provided no other Information is revealed.

- 20.6 Neither Party shall be in breach of paragraphs 20.1 to 20.4 where it can show that any disclosure of Information was made solely and to the extent necessary to comply with a statutory, regulatory, professional body, judicial or parliamentary obligation or was made to professional advisers and insurers insofar as such disclosure is required to protect the professional position of the Party. Where such a disclosure is made, the Party making the disclosure shall ensure that the recipient of the Information is made aware of and asked to respect the confidentiality of the Information. Such disclosure shall in no way diminish the obligations of the Parties under paragraphs 20.1 to 20.4.
- 20.7 The SSRO shall not be in breach of this Contract where it can show that any disclosure of Information is made solely and to the extent necessary to comply with the Freedom of Information Act 2000 (the 'FOIA') or the Environmental Information Regulations 2004 (the 'EIR'). The SSRO may in its discretion consult the Contractor where the SSRO is considering the disclosure of Information under the FOIA or the EIR. The Contractor acknowledges and accepts that any representations on disclosure made during consultation may not be determinative and that the decision whether to disclose Information in order to comply with the FOIA or the EIR is a matter in which the SSRO shall exercise its own discretion, subject always to the provisions of the FOIA or the EIR.

## **21. Publicity**

- 21.1 The Contractor shall not, and shall procure that any member of the Contractor's employees, agents and or sub-contractors shall not, communicate with, or provide information to any representatives of the press, television, radio or other media on any matter concerning or arising out of the Contract without the prior written approval of the SSRO.
- 21.2 Prior to giving its consent referred to in clause 21.1 the SSRO may require the inclusion of material into the release to represent the SSRO's views.
- 21.3 In any event the Contractor shall not publish any release to the media which is detrimental to the SSRO's reputation.
- 21.4 Either Party may make a public statement or announcement concerning the completion of the Contract if required by law.
- 21.5 Subject to clause 20, the SSRO reserves the right to publish or disseminate information about the Contract as it may deem appropriate from time to time in order to raise the profile and awareness surrounding the Contract.

## **22. Data Protection**

22.1 The Contractor shall comply with SCHEDULE 3 – Data Protection, which sets out the requirements for data protection.

## **23. Security requirements**

23.1A At the Commencement Date and throughout the Contract Period all personnel who are engaged in delivering the Services (including, the Key Personnel) shall have and maintain UK HMG security clearance at SC level or above. The SSRO may at any time request evidence of the same and the Contractor shall provide it within 2 working days.

23.1 The Contractor shall take all reasonable steps to ensure that all its Employees engaged on any work in connection with the Contract have notice that the following shall apply to them and will continue so to apply after the completion or termination of the Contract:

- (a) Schedule 5 to the Defence Reform Act 2014; and
- (b) the Official Secrets Acts 1911-1989.

23.2 If directed by the SSRO, the Contractor shall ensure that any Employee shall sign a statement acknowledging that, both during the term of the Contract and after its completion or termination, he or she is bound by:

- (a) Schedule 5 to the Defence Reform Act 2014;
- (b) the Official Secrets Acts 1911-1989; and
- (c) where applicable, by any other legislation.

### **Sensitive Information**

23.3 The Contractor shall comply with the Security Conditions in relation to Sensitive Information.

### **Secret Matter**

23.4 The Contractor shall comply with the Security Measures in relation to Secret Matter.

### **Sub-contracts**

23.5 If the Contractor proposes to make a sub-contract which will involve the disclosure of Secret Matter or Sensitive Information to the sub-contractor, the Contractor shall:

- (a) incorporate into the sub-contract such secrecy and security obligations as the SSRO shall direct; and
- (b) inform the SSRO immediately the Contractor becomes aware of any breach by the sub-contractor of any secrecy or security obligation and, if requested to do so by the SSRO, terminate the sub-contract.

### **Termination**

23.6 The SSRO shall be entitled to terminate the Contract immediately if:

- (a) the Contractor is in breach of any obligation under this Clause;
- (b) the Contractor is in breach of any secrecy or security obligation imposed by any contract with the Crown; or



- (c) where the SSRO considers the circumstances of a breach jeopardise the secrecy or security of the Secret Matter.

## **24. Fraud**

- 24.1 The Contractor will use all reasonable endeavours and have reasonable business structures in place to safeguard against fraud and misapplication of funds in connection with this or any other agreement with the SSRO.
- 24.2 The Contractor will notify the SSRO immediately on discovering any instance of suspected fraud or financial irregularity in connection with the performance of the Contract.
- 24.3 If, in the reasonable opinion of the SSRO, the Contractor or any of its employees, officers, sub-contractors or agents has committed or is committing fraud or is otherwise bringing the SSRO into disrepute, the SSRO shall give notice of its intention to terminate the Contract in writing. The Contractor shall have 14 days to respond in writing. If the Contractor either fails to respond within the 14 days or cannot reasonably substantiate what appears to be fraudulent or irregular financial activity then the SSRO may terminate the Contract forthwith.

## **25. Prevention of Bribery and Corruption**

- 25.1 The SSRO shall be entitled in any of the circumstances set out in clauses 25.2 to 25.5 below to terminate the Contract forthwith and recover from the Contractor the amount of any loss resulting from such termination and damage to the SSRO's reputation.
- 25.2 The first set of circumstances are where the Contractor has:
  - (a) offered or given a financial or other advantage to any person as an inducement or reward to them to perform improperly a public function or business activity or knowing or believing the acceptance in itself would constitute improper performance; or
  - (b) requested or accepted an advantage or reward;
    - (i) intending personally or through another to perform improperly a public function or business activity, or
    - (ii) when the request or acceptance would constitute improper performance of a public function or business activity, or
    - (iii) showing or forbearing to show favour or disfavour to any person in relation to the Contract or any other Contract with the SSRO; or
  - (c) improperly performed such a function or activity in anticipation of receiving such an advantage.
- 25.3 The second set of circumstances are where the acts referred to in clauses 25.2(a) to 25.2(c) have been done by any person employed by the Contractor or acting on the Contractor's behalf (whether or not the acts were performed with or without the knowledge of the Contractor).
- 25.4 The third set of circumstances are where an associated person (including an employee, agent or subsidiary providing services for the organisation) bribes another person:
  - (a) to obtain or retain business for the organisation; or
  - (b) to obtain or retain an advantage in the conduct of business for the organisation.

- 25.5 The fourth set of circumstances are where in relation to the Contract or any other agreement with the SSRO the Contractor shall have or any person employed by it or acting on its behalf shall have committed any offence under the Bribery Act 2010.

## **26. Third Party Rights**

- 26.1 The SSRO will not bring any claim in respect of any loss against any Employees save in so far as that claim arises out of the fraud of that person. This will not limit or exclude the liability of the Contractor for the acts or omissions of the Employees. Save for this provision, nothing in the Contract shall entitle any person who is not a party to the Contract to enforce any rights or obligations under the Contract in respect of the Contracts (Rights of Third Parties) Act 1999.

## **27. Equality and Diversity**

- 27.1 The Contractor agrees to operate and actively demonstrate in all workforce matters the provisions of its Equalities Policy which has been approved by the SSRO prior to entering into the Contract.
- 27.2 The Contractor shall ensure that its Equalities Policy complies with all statutory obligations as regards discrimination on the grounds of any protected characteristic within the meaning of the Equality Act 2010 in relation to:
- (a) the running of the Contractor's business; and
  - (b) the performance of the Contract.
- 27.3 Without prejudice to the generality of the foregoing, the Contractor will comply with the Equality Act 2010, the Human Rights Act 1998 and all other anti-discrimination legislation from time to time in force including all relevant regulations and statutory codes of practice.
- 27.4 Any amended version of the Equalities Policy will be sent to the SSRO promptly following any amendment.
- 27.5 The Contractor shall comply with any request for information by the SSRO in order that the SSRO is able to discharge its obligations under the Equality Act 2010, the Human Rights Act 1998 and all other anti-discrimination legislation.

## **28. Law and Jurisdiction**

- 28.1 The Contract shall be subject to the laws of England and Wales and both parties submit to the exclusive jurisdiction of the English courts.

## **29. Waiver and cumulative remedies**

- 29.1 A waiver of any right under the Contract is only effective if it is in writing.
- 29.2 The failure or delay by the SSRO to exercise any rights or remedies under the Contract shall not be deemed to be a waiver of any right of the SSRO under the Contract.
- 29.3 Where the SSRO has expressly waived its rights under the Contract in respect of any occurrence such waiver shall not be deemed to be effective in respect of any subsequent occurrence.

### 30. Conflict of Interest

- 30.1 In undertaking the Contract, the Contractor shall at all times act in the best interests of the SSRO and shall at no time subordinate or otherwise undermine the SSRO's interests to the advantage of its own interests or those of any third party.
- 30.2 The Contractor shall immediately notify the SSRO in writing upon becoming aware of any actual or potential conflict of interest between the interests of the SSRO and itself or any other third party, invoke its conflict of interests policies, and take all necessary steps to remove or avoid the cause of such conflict of interest to the reasonable satisfaction of the SSRO. Such notification shall not occur in the event that it would prejudice the SSRO in any claim or other right available to the SSRO.
- 30.3 Where the Contractor is unable to reasonably satisfy the SSRO in respect of a conflict of interest the SSRO may terminate the Contract.

### 31. Dispute Resolution

- 31.1 If any dispute arises between the Parties to the Contract in connection with or arising out of the Contract, it shall, in the first instance, be referred to the SSRO's Director of Corporate Resources (or in his absence another officer nominated by the SSRO's Chief Executive) and the Contractor's equivalent for their determination.
- 31.2 A party may not commence any Court proceedings in relation to any dispute arising out of or in connection with the Contract until the parties shall have attempted to settle the dispute in accordance with this provision and may do so 14 days after it has terminated the determination process in writing.
- 31.3 Unless the Contract shall already have been terminated or abandoned by the Contractor, the Contractor shall continue to perform its obligations in accordance with the Contract and shall give effect forthwith to all reasonable decisions, notices and instructions of the SSRO's Officer unless and until the same shall have been revised in any reference or proceeding commenced in accordance with clause 3**Error! Reference source not found.** or 31.2.
- 31.4 The SSRO shall continue to make all payments properly due and undisputed to the Contractor in accordance with the Contract.

### 32. Notices

- 32.1 No formal notice or other communication from one party to the other shall have any validity under the Contract unless made in writing by or on behalf of the party concerned. For the purposes of the Contract "in writing" excludes facsimile or email transmission or any other mode which is not hard copy letter format.
- 32.2 Any formal notice or other communication which is to be given by either party to the other shall be given by letter (sent by hand or pre-paid first class post). The notice or communication shall be deemed to have been given 2 Working Days after the day on which the letter was posted, or the same Working Day if personally delivered before midday and the next Working Day if delivered after midday.
- 32.3 In each case the notice must:
- (a) refer to the Contract; and
  - (b) be marked for the attention of the appropriate officer or department as notified to the other party in writing.

- 32.4 The notices shall be sent to the addresses of each party to the Contract specified at the beginning of this Contract or to such addresses as each party shall notify the other in writing within 5 (five) Working Days of any change in its address for service.
- 32.5 Any notice served on a non-Working Day shall be deemed to be served on the following Working Day.
- 32.6 Any purported serving of a formal notice or communication in any other manner will be deemed ineffective.

### **33. Variations to these Terms**

- 33.1 The terms and conditions of the Contract may only be varied by agreement between the parties in writing.
- 33.2 Where the Parties to the Contract enter into discussions with the intention to agree a variation to the terms of the Contract, the Contract shall remain un-amended and the Contractor's performance of the Contract shall continue as if the terms were un-amended until such time as any relevant variation has been agreed in writing between the parties.

### **34. General matters**

- 34.1 Except as expressly stated in the Contract, all warranties and conditions, whether express or implied by statute, Common Law or otherwise (including fitness for purpose) are hereby excluded to the extent permitted by law.
- 34.2 The Contract governs the overall relationship of the Contractor and the SSRO with respect to the provision of the Services.
- 34.3 If a court or any other competent authority finds that any provision (or part of any provision) of the Contract is invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed deleted, and the validity and enforceability of the other provisions of the Contract shall not be affected.
- 34.4 If any invalid, unenforceable or illegal provision of the Contract would be valid, enforceable and legal if some part of it were deleted, the provision shall apply with the minimum modification necessary to make it legal, valid and enforceable.

### **35. Priority of documents**

- 35.1 In the event of ambiguity or inconsistency between the documents incorporated into the Contract, the following order of precedence shall apply:
- i. The terms and conditions in the body of the Contract.
  - ii. Schedule 1: Security Conditions.
  - iii. Schedule 2: Security Measures.
  - iv. Schedule 3: Data Protection.
  - v. Schedule 4: Specification (including Clarifications).
  - vii. Schedule 5: Contractor's Proposal (including Pricing Schedule).

**Security and information Risk Advisor (SIRA): Terms and Conditions**

This Agreement has been executed by the Parties on the date first before written

Executed by  
SINGLE SOURCE REGULATIONS OFFICE  
Under the hands of a  
Duly authorised officer

---

Executed by  
[CONTRACTOR NAME]  
Acting by:

[ATTESTATION TAILORED TO THE LEGAL ENTITY]

## SCHEDULE 1 – Security Conditions

### 1. Interpretation

1.1 In these Security Conditions, the following capitalised terms have the meanings ascribed to them below:

- “Foundation Grade product” has the meaning ascribed by the CESG Commercial Product Assurance scheme, which is available at:  
<https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa>
- “Sensitive Information” means:
  - (i) Information to which Schedule 5 of the Defence Reform Act 2014 applies; and
  - (ii) OFFICIAL-SENSITIVE information within the meaning of the Government Security Classifications.
- “SSRO” means the Single Source Regulations Office.

### 2. Security grading

- 2.1 The SSRO shall in writing to the Contractor identify the information furnished to the Contractor, or developed by the Contractor, under the Contract, which is Sensitive Information.
- 2.2 The Contractor shall mark all OFFICIAL-SENSITIVE documents which it originates or copies, during the Contract Period, clearly with the OFFICIAL-SENSITIVE classification.
- 2.3 The Contractor shall include a suffix in electronic file names to indicate the OFFICIAL-SENSITIVE classification and any relevant DESCRIPTOR. The following indicates the appropriate suffix for the OFFICIAL-SENSITIVE classification and core descriptors –

Classification and descriptor	Suffix
OFFICIAL SENSITIVE	-OS
OFFICIAL SENSITIVE COMMERCIAL	-OSC
OFFICIAL SENSITIVE LOCSEN	-OSL
OFFICIAL SENSITIVE PERSONAL	-OSP

### 3. Defence Reform Act 2014 and Official Secrets Acts

3.1 The Contractor's attention is drawn to the following –

- (a) The provisions of Part 2 of the Defence Reform Act 2014, Schedule 5 to that Act, and the Single Source Contract Regulations 2014, particularly Regulation 56.
- (b) The provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 5 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular.

- 3.2 The Contractor shall take all reasonable steps to make sure that all individuals employed on any work in connection with the Contract (including sub-contractors) have notice that these statutory provisions, or any others provided by the SSRO, apply to them and shall continue so to apply after the completion or earlier termination of the Contract.

#### **4. Protection of Sensitive Information**

- 4.1 The Contractor shall protect Sensitive Information provided to it or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the SSRO. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.
- 4.2 Sensitive Information shall be protected in a manner to avoid unauthorised access. The Contractor shall take all reasonable steps to prevent the loss or compromise of the information or from deliberate or opportunist attack.
- 4.3 All Sensitive Information not held electronically, including documents, media and other material shall be physically secured to prevent unauthorised access. When not in use Sensitive Information shall be stored under lock and key. As a minimum, when not in use, Sensitive Information shall be stored in a lockable room, cabinets, drawers or safe and the keys/combinations are themselves to be subject to a level of physical security and control.
- 4.4 Disclosure of OFFICIAL-SENSITIVE information shall be strictly in accordance with the "need to know" principle as set out in the Government Security Classifications. Except with the written consent of the SSRO, the Contractor shall not disclose any of the classified aspects of the Contract specified in writing by the SSRO, other than to a person directly employed by the Contractor.
- 4.5 Access to Sensitive Information shall be confined to those individuals who have a "need-to-know" and whose access is essential for the purpose of his or her duties.
- 4.6 The Contractor shall ensure that all individuals having access to OFFICIAL-SENSITIVE information have undergone basic recruitment checks. Contractors shall apply the requirements of HMG Baseline Personnel Security Standard (BPSS) for all individuals having access to OFFICIAL-SENSITIVE information. Further details and the full requirements of the BPSS can be found at the GOV.UK website at:  
<https://www.gov.uk/government/publications/security-policyframework>.

#### **5. Hard Copy Distribution of Information**

- 5.1 Documents containing Sensitive Information shall be distributed, both within and outside the Contractor's premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post or Commercial Couriers in two envelopes, one inside the other. The words OFFICIAL-SENSITIVE shall not appear on the outer envelope and shall not be visible on examination of the outer envelope. The outer envelope shall bear a stamp or details that clearly indicate the full address of the office from which it was sent.
- 5.2 Advice on the distribution of OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of OFFICIAL-SENSITIVE hardware shall be sought from the SSRO.

## **6. Electronic Communication, Telephony and Facsimile Services**

- 6.1 Sensitive Information shall normally be transmitted over the internet encrypted using a Foundation Grade product or equivalent.
- 6.2 Exceptionally, in urgent cases, Sensitive Information may be emailed unencrypted over the internet only where there is a strong business need to do so and only with the prior approval of the SSRO.
- 6.3 Sensitive Information shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the SSRO shall require. Such limitations, including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.
- 6.4 Sensitive Information may be discussed on fixed and mobile types of telephone within the UK, but not with (or within earshot of) unauthorised persons.
- 6.5 Sensitive Information may be faxed to UK recipients, provided that the recipient has been notified and is waiting to receive the fax.

## **7. Use of Information Systems**

- 7.1 The detailed functions that must be provided by an IT system to satisfy the minimum requirements described below cannot be described here; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.
- 7.2 As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.
- 7.3 The following describes the minimum security requirements for processing and accessing Sensitive Information on IT systems.

### **Access**

- 7.4 Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “least privilege” will be applied to System Administrators. Administrators should not conduct “standard” User functions using their privileged accounts.

### **Identification and Authentication (ID&A).**

- 7.5 All systems shall have the following functionality: (1) Up-to-date lists of authorised users. (2) Positive identification of all users at the start of each processing session.

### **Passwords.**

- 7.6 Passwords are part of most ID&A, Security Measures. Passwords shall be “strong” using an appropriate method to achieve this, for example including numeric and “special” characters (if permitted by the system) as well as alphabetic characters.

### **Internal Access Control.**

- 7.7 All systems shall have internal Access Controls to prevent unauthorised users from accessing or modifying the data.



**Data Transmission.**

7.8 Unless the SSRO authorises otherwise, Sensitive Information shall be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the Internet, using a Foundation Grade product or equivalent for encryption.

**Security Accounting and Audit.**

7.9 Security relevant events fall into two categories, namely legitimate events and violations.

7.10 The following events shall always be recorded:

- (a) All log on attempts whether successful or failed.
- (b) Log off (including time out where applicable).
- (c) The creation, deletion or alteration of access rights and privileges.
- (d) The creation, deletion or alteration of passwords.

7.11 For each of the events listed above, the following information is to be recorded:

- (a) Type of event;
- (b) User ID;
- (c) Date & Time; and
- (d) Device ID.

7.12 The accounting records shall have a facility to provide the System Manager with a hard copy of all or selected activity. There shall also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know. If the operating system is unable to provide this then the equipment shall be protected by physical means when not in use i.e. locked away or the hard drive removed and locked away.

**Integrity & Availability.**

7.13 The following supporting measures shall be implemented:

- (a) Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations);
- (b) Defined Business Contingency Plan;
- (c) Data backup with local storage;
- (d) Anti-Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software);
- (e) Operating systems, applications and firmware should be supported; and
- (f) Patching of Operating Systems and Applications used shall be in line with the manufacturers recommended schedule. If patches cannot be applied an understanding of the resulting risk will be documented.

## **Logon Banners**

- 7.14 Wherever possible, a “Logon Banner” shall be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text depending on national legal requirements could be: “Unauthorised access to this computer system may constitute a criminal offence”.

## **Unattended Terminals.**

- 7.15 Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, or systems must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

## **Internet Connections.**

- 7.16 Computer systems shall not be connected direct to the Internet or “untrusted” systems unless protected by a firewall (a software based personal firewall is the minimum) which is acceptable to the SSRO’s Senior Information Risk Officer.

## **Disposal**

- 7.17 Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files, which does not remove the data.

## **8. Laptops**

- 8.1 Laptops holding any supplied or contractor generated Sensitive Information are to be encrypted using a Foundation Grade product or equivalent.
- 8.2 Unencrypted laptops not on a secure site are to be recalled and only used or stored in an appropriately secure location until further notice or until approved full encryption is installed. Where the encryption policy cannot be met, a Risk Balance Case that fully explains why the policy cannot be complied with and the mitigation plan, which should explain any limitations on the use of the system, is to be submitted to the SSRO for consideration.
- 8.3 Unencrypted laptops and drives containing personal data or Sensitive Information are not to be taken outside of secure sites. For the avoidance of doubt the term “drives” includes all removable, recordable media (e.g. memory sticks, compact flash, recordable optical media (e.g. CDs and DVDs), floppy discs and external hard drives.
- 8.4 Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.
- 8.5 Portable Communication and Information Systems (CIS) devices are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

## **9. Loss and Incident Reporting**

- 9.1 The contractor shall immediately report any loss or other compromise of Sensitive Information to the SSRO.

- 9.2 Any security incident involving Sensitive Information shall be immediately reported to the SSRO.

## **10. Sub-Contracts**

- 10.1 When sub-contracting to a sub-contractor located in the UK the Contractor shall ensure that these Security Conditions shall be incorporated within the sub-contract document.

## **11. Destruction**

- 11.1 As soon as no longer required, Sensitive Information shall be destroyed in such a way as to make reconstitution unlikely, for example, by burning, shredding or tearing into small pieces.
- 11.2 Advice shall be sought from the SSRO when information cannot be destroyed or, unless already authorised by the SSRO, when its retention is considered by the Contractor to be necessary or desirable. Unwanted Sensitive Information which cannot be destroyed in such a way shall be returned to the SSRO.

## **12. Guidance**

- 12.1 Advice regarding the interpretation of the above requirements should be sought from the SSRO.

## **13. Audit**

- 13.1 Where considered necessary by the SSRO, the Contractor shall provide evidence of compliance with these Security Conditions.

## **SCHEDULE 2 – Security Measures**

### **1. Definition**

1.1 In this Schedule, the terms used have the same meanings as defined in the Contract.

### **2. Disclosure of Secret Matter**

2.1 Unless the Contractor has the written authorisation of the SSRO to do otherwise, neither the Contractor nor any of its Employees shall, either before or after the completion or termination of the Contract, do or permit to be done anything which they know or ought reasonably to know may result in Secret Matter being disclosed to or acquired by a person in any of the following categories:

- (a) who is not a British citizen;
- (b) who does not hold the appropriate authority for access to the protected matter;
- (c) in respect of whom the SSRO has notified the Contractor in writing that the Secret Matter shall not be disclosed to or acquired by that person;
- (d) who is not an Employee of the Contractor; or
- (e) who is an Employee of the Contractor and has no need to know the information for the proper performance of the Contract.

### **3. Reasonable steps to safeguard etc**

3.1 Unless he has the written permission of the SSRO to do otherwise, the Contractor and his Employees shall, both before and after the completion or termination of the Contract, take all reasonable steps to ensure that:

- (a) no photograph of, or pertaining to, any Secret Matter shall be taken and no copy of or extract from any Secret Matter shall be made except to the extent necessary for the proper performance of the Contract; and
- (b) any Secret Matter is at all times strictly safeguarded in accordance with the Security Policy Framework and upon request, is delivered up to the SSRO who shall be entitled to retain it.

3.2 A decision of the SSRO on the question of whether the Contractor has taken or is taking reasonable steps as required by this clause shall be final and conclusive.

### **4. Records and inspection**

4.1 The Contractor shall:

- (a) provide to the SSRO:
  - (i) upon request, such records giving particulars of those Employees who have had at any time, access to any Secret Matter;
  - (ii) upon request, such information as the SSRO may from time to time require so as to be satisfied that the Contractor and his Employees are complying with his obligations under this Clause, including the measures taken or proposed by the

Contractor so as to comply with his obligations and to prevent any breach of them;  
and

- (iii) full particulars of any failure by the Contractor and his Employees to comply with any obligations relating to Secret Matter arising under this Clause immediately upon such failure becoming apparent.

## **5. Unauthorised persons**

- 5.1 If at any time either before or after the completion or termination of the Contract, the Contractor or any of its Employees discovers or suspects that an unauthorised person is seeking or has sought to obtain information directly or indirectly concerning any Secret Matter, the Contractor shall forthwith inform the SSRO of the matter with full particulars thereof.

## **SCHEDULE 3 – Data Protection**

### **1. Data Processor and Data Controller**

- 1.1 The Parties agree that, for the Protected Data, the SSRO shall be the Data Controller and the Contractor shall be the Data Processor.
- 1.2 The Contractor shall comply with all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of the Contract.
- 1.3 The Contractor shall not by any act or omission cause the SSRO (or any other person) to be in breach of any Data Protection Laws.
- 1.4 The SSRO shall comply with all Data Protection Laws in respect of the performance of its obligations under this Contract.

### **2. Instructions and details of processing**

- 2.1 Insofar as the Contractor processes Protected Data on behalf of the SSRO, the Contractor:
  - (a) unless required to do otherwise by applicable law, shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Processing Instructions; and
  - (b) if applicable law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the SSRO of any such requirement before processing the Protected Data (unless applicable Law prohibits such information on important grounds of public interest).
- 2.2 The Contractor shall as soon as reasonably practicable inform the SSRO in writing if, in the Contractor's opinion, a Processing Instruction infringes the Data Protection Laws or any other applicable laws relating to data protection and explain the reasons for its opinion.
- 2.3 The processing to be carried out by the Contractor under the Contract shall comprise such processing as agreed by the parties in writing from time to time.

### **3. Technical and organisational measures**

- 3.1 The Contractor shall implement and maintain, at its cost and expense, appropriate technical and organisational measures in relation to the processing of Protected Data by the Contractor:
  - (a) such that the processing will meet the requirements of Data Protection Laws and ensure the protection of the rights of Data Subjects;
  - (b) so as to ensure a level of security in respect of Protected Data processed by it that is appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed; and
  - (c) without prejudice to clause 3.1 of this Schedule insofar as is possible, to assist the SSRO in the fulfilment of the SSRO's obligations to respond to Data Subject Requests relating to Protected Data.

- 3.2 Without prejudice to clause 3.1 of this Schedule, the Contractor shall, in respect of the Protected Data processed by it under this Contract comply with the requirements regarding security of processing set out in Data Protection Laws (as applicable to Data Processors) and in this Contract.
- 3.3 The Contractor shall not engage another Data Processor (or any replacement) for carrying out any processing activities in respect of the Protected Data without the SSRO's prior written consent.
- 3.4 The Contractor shall, by contract, require any Data Processor that it engages to comply with the obligations imposed by this Contract on the Contractor, when carrying out any processing activities in respect of the Protected Data.
- 3.5 The Contractor shall ensure that any Employee and all other persons authorised by it, or by any person acting on its behalf (including by any Data Processor pursuant to clause 3.1 of this Schedule), to process Protected Data are subject to a binding written contractual obligation with the Contractor or with the Data Processor that has engaged them to keep the Protected Data confidential (except where disclosure is required in accordance with applicable law, in which case the Contractor shall, where practicable and not prohibited by applicable law, notify the SSRO of any such requirement before such disclosure).
- 3.6 Without prejudice to any other provision of this Schedule, the Contractor shall ensure that any Employee processing Protected Data are reliable and have received adequate training on compliance with this Schedule and the Data Protection Laws applicable to the processing.
- 3.7 The Contractor shall ensure that access to Protected Data is limited to the authorised persons who need access to it to supply the Services.

#### **4. Assistance with the SSRO's compliance and Data Subject rights**

- 4.1 The Contractor shall (at no cost to the SSRO):
  - (a) promptly record and then refer all Data Subject Requests it receives to the SSRO within three Working Days of receipt of the request;
  - (b) provide such information and cooperation and take such action as the SSRO reasonably requests in relation to each Data Subject Request, within the timescales reasonably required by the SSRO; and
  - (c) not respond to any Data Subject Request or Complaint without the SSRO's prior written approval.
- 4.2 Without prejudice to clause 2.1 of this Schedule, the Contractor shall, at its cost and expense, provide such information, cooperation and other assistance to the SSRO as the SSRO reasonably requires (taking into account the nature of processing and the information available to the Contractor) to ensure compliance with the SSRO's obligations under Data Protection Laws, including with respect to:
  - (a) security of processing;
  - (b) data protection impact assessments (as such term is defined in Data Protection Laws);
  - (c) prior consultation with a Supervisory Authority regarding high risk processing; and

- (d) any remedial action and/or notifications to be taken in response to any Personal Data Breach and/or Complaint, including (subject in each case to the SSRO's prior written authorisation) regarding any notification of the Personal Data Breach to Supervisory Authorities and/or communication to any affected Data Subjects.

## **5. International data transfers**

- 5.1 The Contractor shall not transfer any Protected Data to any country outside the European Economic Area or to any International Organisation (an "International Recipient") without the SSRO's prior written consent.

## **6. Records, information and audit**

- 6.1 The Contractor shall maintain complete, accurate and up-to-date written records of all categories of processing activities carried out on behalf of the SSRO, containing such information as the SSRO may reasonably require, including:
  - (a) the name and contact details of the Data Processor(s) and of each Data Controller on behalf of which the Data Processor is acting, and of the Contractor's representative and data protection officer (if any);
  - (b) the categories of processing carried out on behalf of each Data Controller;
  - (c) where applicable, details of transfers of Protected Data to an International Recipient; and
  - (d) a general description of the technical and organisational security measures referred to in clause 3.1 of this Schedule.
- 6.2 The Contractor shall make available to the SSRO on request in a timely manner (and in any event within three Working Days):
  - (a) copies of the records under clause 6.1 of this Schedule; and
  - (b) such other information as the SSRO reasonably requires to demonstrate the Contractor's and the SSRO's compliance with their respective obligations under Data Protection Laws and this Contract.
- 6.3 If any audit or inspection reveals a material non-compliance by the Contractor with its obligations under Data Protection Laws or a breach by the Contractor of this Schedule, the Contractor shall pay the reasonable costs of the SSRO or its mandated auditors, of the audit or inspection.
- 6.4 The Contractor shall promptly resolve, at its own cost and expense, all data protection and security issues discovered by the SSRO and reported to the Contractor that reveal a breach or potential breach by the Contractor of its obligations under this Schedule.
- 6.5 The SSRO shall be entitled to share any notification, details, records or information provided by or on behalf of the Contractor under this Schedule with its professional advisors and the Supervisory Authority.



## 7. Breach notification

7.1 In respect of any Personal Data Breach, the Contractor shall:

- (a) notify the SSRO of the Personal Data Breach without undue delay (but in no event later than 48 hours after becoming aware of the Personal Data Breach); and
- (b) provide the SSRO without undue delay (wherever possible, no later than 48 hours after becoming aware of the Personal Data Breach) with such details as the SSRO reasonably requires regarding:
  - (i) the nature of the Personal Data Breach, including the categories and approximate numbers of Data Subjects and Protected Data records concerned;
  - (ii) any investigations into such Personal Data Breach;
  - (iii) the likely consequences of the Personal Data Breach; and
  - (iv) any measures taken, or that the Contractor recommends, to address the Personal Data Breach, including to mitigate its possible adverse effects,

provided that, (without prejudice to the above obligations) if the Contractor cannot provide all these details within the timeframes set out in this clause 7.1(b), it shall (before the end of such timeframes) provide the SSRO with reasons for the delay and when it expects to be able to provide the relevant details (which may be phased), and give the SSRO regular updates on these matters.

7.2 The Contractor shall promptly (and in any event within two Working Days) inform the SSRO if it receives a Complaint and provide the SSRO with full details of such Complaint.

## 8. Deletion or return of Protected Data and copies

8.1 The Contractor shall (and shall ensure that all persons acting on its behalf and any Employee shall) without delay (and in any event within three days), at the SSRO's written request, either securely delete (to the extent that it is technologically able to do so) or securely return all the Protected Data to the SSRO in such form as the SSRO reasonably requests after the earlier of:

- (a) the end of the provision of the relevant Services related to processing of such Protected Data; or
- (b) once processing by the Contractor of any Protected Data is no longer required for the purpose of the Contractor's performance of its relevant obligations under this Contract,

and securely delete existing copies (unless storage of any data is required by applicable law and, if so, the Contractor shall inform the SSRO of any such requirement).

## 9. Conflicts

9.1 Unless otherwise expressly stated in this Contract:

- (a) the Contractor's obligations and the SSRO's rights and remedies under this Schedule are cumulative with, and additional to, any other provisions of this Contract;
- (b) nothing in this Contract relieves the Contractor of any responsibilities or liabilities under any Data Protection Laws; and
- (c) this Schedule shall prevail over any other provision of this Contract in the event of any conflict.

## **SCHEDULE 4 – Specification and Clarifications**

## **SCHEDULE 5 – Contractor’s Proposal**