# DPS Schedule 6 (Order Form Template and Order Schedules)

# Order Form

| | |
|---|---|
| ORDER REFERENCE: | Project_26513 |
| ORDER CONTRACT TITLE: | Cyber Security Assurance Contractor |
| ORDER CONTRACT DESCRIPTION: | The provision of an augmented resource to deliver consultancy, advice, and penetration testing for the department's Dynamic Trust Hub (DTH) environment prior to deployment into production. |
| THE BUYER: | The Department for Work and Pensions |
| BUYER ADDRESS | Caxton House, Tothill Street, London, SW1H 9NA |
| THE SUPPLIER: | Cyber Security Specialists Ltd |
| SUPPLIER ADDRESS: | Unit 10, Altrincham Business Park, Altrincham, Manchester, WA14 5GL |
| REGISTRATION NUMBER: | 5896325 |
| DUNS NUMBER: | 220841348 |

DPS SUPPLIER REGISTRATION SERVICE ID: SQ-AG6BE44

**APPLICABLE DPS CONTRACT:**

This Order Form is for the provision of the Deliverables and dated 9th September 2024. It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

**DPS FILTER CATEGORIES:**


© Crown Copyright 2020

Non-assured NCSC Services, Risk Management, Risk Assessment, Security Architecture, Business Continuity and Disaster Recovery - BCDR, Certification (e.g. Cyber Essentials), Security Specialist, Security Strategy, Cyber Transformation, Penetration Testing/Pen test, IT Health Check, Cyber Essentials Plus, CREST/Tiger/Cyber/Other Qualified, Clearance: Security Check, Networks, Database, Internet, Cloud, Endpoint/applications, GDPR, Government, Critical National Infrastructure.

**ORDER INCORPORATED TERMS:**

The following documents are incorporated into this Order Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM3764iii
3. The following Schedules in equal order of precedence:
    - Joint Schedules for RM3764iii
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)
        - Joint Schedule 5 (Corporate Social Responsibility)
        - Joint Schedule 6 (Key Subcontractors)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)
    - Order Schedules for RM3764iii
        - Order Schedule 1 (Transparency Reports)
        - Order Schedule 4 (Order Tender)
        - Order Schedule 7 (Key Supplier Staff)
        - Order Schedule 8 (Business Continuity and Disaster Recovery)
        - Order Schedule 9 (Security)
        - Order Schedule 15 (Order Contract Management)
        - Order Schedule 20 (Order Specification)
        - Order Schedule 22 (Secret Matters)
4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Annexes A & B to Order Schedule 6

No other Supplier terms are part of the Order Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

**ORDER SPECIAL TERMS:**


© Crown Copyright 2020

**Project_26513 – Contract for Cyber Security Assurance Contractor**

The following Special Terms are incorporated into this Order Contract:

Special Term 1 – Order Form – Appendix 1 (Statements of Work): During the Order Contract Period, the Buyer and Supplier may agree and execute completed Statement of Works. Upon execution of a Statement of Work the provisions detailed therein shall be incorporated into the Order Contract at Appendix 1 to this Order Form.

Special Term 2 – Core Terms – Clause 10.3.2 (Ending the Contract without a reason) is amended as follows: "Each Buyer has the right to terminate their DPS Contract or any Statement of Work at any time without reason by giving the Supplier not less than: (a) 30 days for a Statement of Work; or (b) 30 days for the DPS Contract, written notice and if it's terminated Clauses 10.5.2 to 10.5.7 shall apply. The Buyer shall have no liability in respect of any costs incurred by the Supplier arising from such termination."

Special Term 3 – Core Terms – Clause 10.2 (Ending the Contract) is amended as follows: "The Relevant Authority can extend the Contract for the Extension Period by giving the Supplier no less than 30 Days' written notice before the contract expires."

Special Term 4 - IR35 Status - The provision of Annex A to this Order Form shall apply in respect of any Statement of Work concluded under this Order Contract.

Special Term 5 – Order Schedule 9 (Security) - In addition to section 18 'SECURITY AND CONFIDENTIALITY REQUIREMENTS' of Attachment 3 (Specification), Annex B to this Order Form containing the DWP minimum security schedule will be included and form a part of the final Order Contract within Order Schedule 9:

DWP%20Minimum%
20Security%20Schedu

**ORDER START DATE:** 9th September 2024

**ORDER EXPIRY DATE:** 9th September 2026

**ORDER INITIAL PERIOD:** 2 Years (24 Months)

**ORDER OPTIONAL EXTENSION:** 1 Year (12 Months)

**DELIVERABLES:**


© Crown Copyright 2020

**Project_26513 – Contract for Cyber Security Assurance Contractor**

This contract is for the provision of one augmented resource – a Cyber Security Assurance Contractor – according to the following resource profile:

| DDAT Role | Quantity | SFIA Level | Clearance | Estimated Working Days (per annum) |
|---|---|---|---|---|
| Cyber Security Assurance Contractor | 1 | 6 | Security Check | 253 |

The Contractor will deliver the outcomes and possess the skills outlined in the Statement of Requirements, which include but are not limited to:

**MAXIMUM LIABILITY:**
The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **£264,000.00** (inclusive of VAT).

**ORDER CHARGES:**
The Supplier's rate card will be used for the purpose of pricing each Statement of Work as per the pricing schedule embedded below:

**[REDACTED]**

**REIMBURSABLE EXPENSES:**
Please find embedded in Annex C to this order form the DWP Policy on Expenses for Business Travel & Accommodation for Contractors, Interim Managers and Consultants:

DWP%20Policy%20o
n%20Expenses%20foı

**PAYMENT METHOD:**
The payment method for this Order Contract is BACS (Capped Time and Materials) made monthly in arrears.

**BUYER'S INVOICE ADDRESS:**
Invoices will be sent to:
**[REDACTED]**
Email: **[REDACTED]**
A copy should also be emailed to **[REDACTED]**


© Crown Copyright 2020

**BUYER'S AUTHORISED REPRESENTATIVE:**
**[REDACTED]**

**BUYER'S ENVIRONMENTAL POLICY:**
The Contracting Authority is committed to a 100% reduction of greenhouse gas emissions and requires the successful Supplier under this procurement to demonstrate an organisational commitment to the 'Net Zero' target.
Further information can be found here:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1054373/Guidance-on-adopting-and-applying-PPN-06_21-_-Selection-Criteria-Jan22__1_.pdf

**BUYER'S SECURITY POLICY:**
The Buyer's security policy is available online and further information can be found here: Security policy framework: protecting government assets - GOV.UK (www.gov.uk)

The Supplier must be ISO27001 compliant and possess Cyber Essentials certification.

**SUPPLIER'S AUTHORISED REPRESENTATIVE:**
**[REDACTED]**

**SUPPLIER'S CONTRACT MANAGER:**
**[REDACTED]**

**PROGRESS REPORT FREQUENCY:**
Progress reporting for each task will be managed via Jira.

**PROGRESS MEETING FREQUENCY:**
Quarterly on the first Working Day of each quarter.

**KEY STAFF:**
**[REDACTED]**

**KEY SUBCONTRACTOR(S):**
SPA Enterprise Service Limited (registered company no. 6933688)

**COMMERCIALLY SENSITIVE INFORMATION:**
[To be determined]


© Crown Copyright 2020

**SERVICE CREDITS:**
Not applicable

**ADDITIONAL INSURANCES:**
Not applicable

**GUARANTEE:**
Not applicable

**SOCIAL VALUE COMMITMENT:**
Please see Order Schedule 4 (Order Tender).

| **For and on behalf of the Supplier:** | | **For and on behalf of the Buyer:** | |
|---|---|---|---|
| Signature: | [REDACTED] | Signature: | [REDACTED] |
| Name: | [REDACTED] | Name: | [REDACTED] |
| Role: | [REDACTED] | Role: | [REDACTED] |
| Date: | 21/08/2024 | Date: | 21/08/2024 |

# Appendix 1

The first Statement(s) of Works shall be inserted into this Appendix 1 as part of the executed Order Form. Thereafter, the Buyer and Supplier shall complete and execute Statement of Works (in the form of the template Statement of Work in Annex 2 to the Order Form in Framework Schedule 6 (Order Form Template and Order Schedules)].

Each executed Statement of Work shall be inserted into this Appendix 1 in chronology.

# Statement of Work 1


© Crown Copyright 2020

| **1. STATEMENT OF WORK ("SOW") DETAILS** | |
|---|---|
| Upon execution, this SOW forms part of the Order Contract (reference below).<br><br>The Parties will execute a SOW for each set of Buyer Deliverables required. Any ad-hoc Deliverables requirements are to be treated as individual requirements in their own right and the Parties should execute a separate SOW in respect of each, or alternatively agree a Variation to an existing SOW.<br><br>All SOWs must fall within the Specification and provisions of the Order Contact.<br><br>The details set out within this SOW apply only in relation to the Deliverables detailed herein and will not apply to any other SOWs executed or to be executed under this Order Contract, unless otherwise agreed by the Parties in writing. | |
| **Date of SOW:** | 9th September 2024 |
| **SOW Title:** | Cyber Security Assurance Contractor |
| **SOW Reference:** | SOW1 |
| **Order Contract Reference:** | Project_26513 |
| **Buyer:** | The Department for Work and Pensions |
| **Supplier:** | Cyber Security Specialists Ltd |
| **SOW Start Date:** | 5th August 2024 |
| **SOW End Date:** | 5th August 2025 |
| **Duration of SOW:** | 12 months (253 working days) |
| **Key Personnel (Buyer)** | **[REDACTED]** |
| **Key Personnel (Supplier)** | **[REDACTED]** |
| **Subcontractors** | SPA Enterprise Service Limited (registered company no. 6933688) |


© Crown Copyright 2020

| **2. ORDER CONTRACT SPECIFICATION - PROGRAMME CONTEXT** | |
|---|---|
| **SOW Deliverables Background** | The Contracting Authority is seeking resources who must have the following technical knowledge and experience:<br>• A working understanding of Identity Access Management (IAM), associated security controls, and implementation at scale in a government organisation, including related technical standards, e.g. SAML, OAuth, OIDC, etc.<br>• A working knowledge of delivering consultancy and advice in a large Government department or public sector organisation.<br>• A working knowledge of OWASP configurations, microservices, API Gateways, event driven architecture, & application security standards<br>• A working knowledge of secure communication and encryption/ cryptographic technologies, tools, and best practice (e.g. IPSec, Kerberos, TLS, and SSL).<br>• Public cloud technologies, cloud hosting, container, and networking design patterns, tools and best practices (especially AWS)<br>• Possession of relevant security qualifications including CISSP, CEH, and CCSK.<br>• The supplier must demonstrate compliance with industry standards and certifications, including AWS Architect, CREST, and ISO 27001. |
| **Delivery phase(s)** | N/A |
| **Overview of Requirement** | The Contracting Authority is seeking to put in place a 24-month Contract that provides for the provision of an Augmented Resource to deliver Cyber Security assurance across multiple teams.<br><br>At a high-level the resource is required to augment teams to support ongoing activity in Identity and Trust Services (ID&T) to deliver specific digital outcomes, which will require specific digital capabilities and capacity. |
| **Accountability Models** | Rainbow Team Accountability Model |

| **3. BUYER REQUIREMENTS – SOW DELIVERABLES** |
|---|


© Crown Copyright 2020

| | | | |
|---|---|---|---|
| **Outcome Description** | The Contracting Authority requires resources with the skills and experience to deliver a suite of high-level service outcomes, accompanied with generic cyber security services as follows:<br>• Consultancy and Advice:<br>o Provide security architecture advice to the product delivery squads in ID&T, blending security, technical (public cloud development and architecture) and behavioural (leadership and communication) skills.<br>o Work with and advise the Lead Security Architect, and solution architects within ID&T and across the wider department to ensure that solutions are secure, consistent, strategically aligned, and interoperable. Actively participate in the ID&T Technical Forum, applying security architecture input to inform decisions and outcomes that apply across the ID&T development teams.<br>o Identify and advise on the appropriate mitigations for cyber security risks within ID&T products and work with the department's Digital Security Risk Management (DSRM) teams to ensure solutions meet security and risk governance controls. Identify security issues in system architectures and provide advice and guidance on the risk impact of vulnerabilities in our existing and future designs and systems.<br>o Demonstrate accountability for the security aspects of product architectures, contributing to product roadmaps and represent product designs at governance forums, providing clear communication of security architecture design and decision making, to gain approval to proceed with designs.<br>o Identify new technologies and work with DWP Digital Design Authority (DDA) and broader security community to look at opportunities to exploit them in business areas. Ensure that solutions meet the Departmental Security Architecture standards, re-using patterns where possible, and support presentation of solutions to the Digital Design Authority (DDA) at various stages of the product development.<br>• Penetration Testing and IT Health Check. | | |
| **Milestone Ref** | **Milestone Description** | **Acceptance Criteria** | **Due date** |
| MS01 | N/A | | |
| MS02 | N/A | | |
| MS03 | N/A | | |
| **Delivery Plan** | N/A | | |
| **Dependencies** | N/A | | |
| **Supplier Resource Plan** | N/A | | |
| **Security Applicable to SOW:** | DWP Minimum Security Schedule (see Schedule 9) | | |


© Crown Copyright 2020

| | |
|---|---|
| **Cyber Security Standards** | Refer to Specification |
| **SOW Standards** | ISO 27001 |
| **Performance Management** | Monthly progress meeting and task reports via Jira. |
| **Additional Requirements** | N/A |
| **Key Supplier Staff** | N/A |
| **Worker Engagement Status** | Resources on company payroll. |
| **SOW Reporting Requirements:** | Monthly progress meeting and task reports via Jira. |

## 4. CHARGES

**Order Contract Charges**

| Role | SFIA Level (Link) | Day Rate (excl. VAT) |
|---|---|---|
| Cyber Security Assurance Contractor | 6 | [REDACTED] |

| | |
|---|---|
| **Rate Cards Applicable** | See above |
| **Financial Model** | N/A |
| **Reimbursable Expenses** | Please refer to Annex C to the Order Form. |

## 5. SIGNATURES AND APPROVALS

**Agreement of this SOW**

BY SIGNING this Statement of Work, the Parties agree that it shall be incorporated into Appendix 1 of the Order Form and incorporated into the Order Contract and be legally binding on the Parties:

**For and on behalf of the Supplier**

| | |
|---|---|
| Name and title | [REDACTED] |
| Date | 21/08/2024 |


© Crown Copyright 2020

| | | |
|---|---|---|
| | Signature | [REDACTED] |
| **For and on behalf of the Buyer** | Name and title | [REDACTED] |
| | Date | 21/08/2024 |
| | Signature | [REDACTED] |

# Statement of Work 1 Data Processing

Prior to the execution of this Statement of Work, the Parties shall review Annex 1 of Joint Schedule 11 (Processing Data) and if the contents of Annex 1 does not adequately cover the Processor / Controller arrangements covered by this Statement of Work, Annex 1 shall be amended as set out below and the following table shall apply to the Processing activities undertaken under this Statement of Work only:

| Description | Details |
|---|---|
| Identity of Controller for each Category of Personal Data | **The Relevant Authority is Controller and the Supplier is Processor**<br>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:<br>• Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Staff) for which the Buyer is the Controller<br><br>**The Supplier is Controller and the Relevant Authority is Processor**<br><br>*The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:*<br><br>• **N/A** |


© Crown Copyright 2020

| | |
|---|---|
| | **The Parties are Joint Controllers**<br><br>*The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:*<br><br>• **N/A**<br><br>**The Parties are Independent Controllers of Personal Data**<br><br>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:<br>• Business contact details of Supplier Personnel for which the Supplier is the Controller,<br>Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller, |
| Duration of the Processing | No Personal data is processed |
| Nature and purposes of the Processing | N/A |
| Type of Personal Data | N/A |
| Categories of Data Subject | N/A |


© Crown Copyright 2020

| | |
|---|---|
| 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 | N/A |

**Annex A**

**1. Off-Payroll Working Rule**

1.1 In this paragraph, the following expressions mean:

| | |
|---|---|
| **Contractor** | means any individual delivering, or forming part of, the SOW Deliverables (or any part of them) |
| **Intermediary** | means any "intermediary" (as defined in section 61M ITEPA) in respect of which any of Conditions A – C within section 61N ITEPA are met |
| **ITEPA** | Income Tax (Earnings and Pensions) Act 2003 |
| **Off-Payroll Working Rules** | means the provisions of Chapter 10 of Part 2 ITEPA relating to the engagement of workers through intermediaries and the provisions of Social Security Contributions (Intermediaries) Regulations 2000/727 (or, in each case, any other provisions under any law having like effect) |
| **Status Determination** | means a status determination pursuant to, and for the purposes of, the Off-Payroll Working Rules |
| **SOW Deliverables** | means any Deliverables to be provided under the relevant Statement of Work |
| **Tax** | means income tax, employee national insurance contributions and employer national insurance contributions (in each case whether or not required to be accounted for under the PAYE rules of the United Kingdom) and any equivalent tax, contribution or similar |


© Crown Copyright 2020

| | |
|---|---|
| | obligations elsewhere, together, in each case, with all related penalties and interest |

1.2 Subject to paragraph 1.3 below, the Supplier warrants and undertakes to the Buyer that (i) each Contractor will be directly engaged exclusively as an employee of the Supplier for the purposes of and when delivering any SOW Deliverables (with all required Tax being withheld, deducted and/or accounted for in respect of any payments or other benefits provided to that Contractor) and (ii) that it is not, nor will at any time be, an Intermediary of any Contractor.

1.3 The Supplier warrants and undertakes to the Buyer that no Contractor will deliver their services through an Intermediary of that Contractor without the Supplier having first obtained the written consent of the Buyer to such Contractor doing so (such consent being at the absolute discretion of the Buyer).

1.4 Promptly upon request from the Buyer, the Supplier shall provide (or procure provision) to the Buyer of all such evidence, information and assistance as the Buyer reasonably requires in order to confirm that the warranties and undertakings given by the Supplier in paragraphs 1.2 and 1.3 are, and remain, true, accurate and correct in all respects.

1.5 The Buyer shall be entitled to make any deductions in respect of Tax, from any payments to the Supplier, which it reasonably considers are required to be made as a result of, or connection with, the application of the Off-Payroll Working Rules.

1.6 In respect of each Contractor or the SOW Deliverables (or any part of them), promptly upon request from the Buyer, the Supplier shall provide (or procure provision) to the Buyer of all such information and assistance as the Buyer reasonably requires in connection with the Off-Payroll Working Rules (including, but not limited to, such information or assistance as the Buyer reasonably requires in order to assess whether or not the Off-Payroll Working Rules apply to the SOW Deliverables (or any part of them) and/or to any arrangements involving the performance of any services by any Contractor, to carry out any Status Determination or to comply with any other requirement or obligation it may have a result of or in connection with the application of the Off-Payroll Working Rules).

1.7 In circumstances where the Supplier, any Contractor or any other person involved (directly or indirectly) in the supply of the SOW Deliverables (or any part of them) wishes to make any representations (or any further representations) to the Buyer that any Status Determination carried out by the Buyer is incorrect, the Supplier shall procure that any such representations are sent to the Buyer.

1.8 The Supplier warrants and undertakes to the Buyer that it shall:

1.8.1 immediately inform the Buyer if, at any time, it becomes aware of any new or additional fact, matter or circumstance, or any change in any fact, matter or circumstance, in each case, from which it appears that (a) the Off-Payroll Working Rules could apply or (b) any change may need to be made to any Status Determination previously carried out, in each case, in relation to the supply of the SOW Deliverables (or any part of them) and / or to any arrangements involving the performance of any services by any Contractor, and the Supplier shall also procure that each Contractor will do the same; and

1.8.2 in circumstances where the Buyer has, in relation to any Contractor, determined that the condition in section 61M(1)(d) ITEPA is not met, manage the delivery of the SOW Deliverables (and any part of them), mange any arrangements involving the performance of any services by that Contractor, and do or not do (as the case


© Crown Copyright 2020

may be) all such things as are necessary, in each case, to ensure that the condition in section 61M(1)(d) ITEPA is not met and remains not met, in relation that Contractor.

1.9 The Supplier warrants and undertakes to the Buyer that it shall, at all times, comply with any and all requirements or obligations it may have as a result of or in connection with the application of the Off-Payroll Working Rules to the provision of the SOW Deliverables (or any part of them) and / or to any arrangements involving the performance of any services by any Contractor, including, but not limited, to any obligation to make any deductions for Tax, and shall procure the compliance of all other parties involved (directly or indirectly) in the supply of the SOW Deliverables (or any part of them).

1.10 The Supplier shall indemnify the Buyer, on demand and on an after-Tax basis, against:

1.10.1 any and all proceedings, claims or demands by any third party (including, but without limitation, HM Revenue & Customs and any successor, equivalent or related body);

1.10.2 any and all Tax and any other liabilities, losses, deductions, contributions or assessments; and

1.10.3 any and all reasonable costs or expenses and any penalties, fines or interest incurred or payable,

in each case, which arise as a result of, in consequence of, or otherwise in connection with, (i) the Supplier, at any time, being in breach of any of the warranties or undertakings given in paragraphs 1.2, 1.3, 1.8 and/or 1.9 and/or (ii) the application of the Off-Payroll Working Rules to the provision of the SOW Deliverables (or any part of them) and / or to any arrangements involving the performance of any services by any Contractor.

1.11 The provisions of clauses 26.2 – 26.6 of the Core Terms shall not apply to any claim under paragraph 1.10.


© Crown Copyright 2020

## Annex B

## SCHEDULE 9 – MINIMUM SECURITY REQUIREMENTS

### GENERAL

The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Contract which include the requirements set out in this Schedule 9 to the Contract (the "**Authority's Security Requirements**"). The Authority's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority's Systems Environment and the Contractor's Systems Environment.

Terms used in this Schedule 9 which are not defined below shall have the meanings given to them in clause A1 (Definitions and Interpretations) of the Contract.

### 1. DEFINITIONS

1.1 In this Schedule 9, the following definitions shall apply:

| | |
|---|---|
| **"Authority Personnel"** | shall mean all persons employed by the Authority including directors, officers, employees together with the Authority's servants, agents, consultants, contractors and suppliers but excluding the Contractor and any Sub-contractor (as applicable). |
| **"Availability Test"** | shall mean the activities performed by the Contractor to confirm the availability of any or all |


© Crown Copyright 2020

| | |
|---|---|
| | components of any relevant ICT system as specified by the Authority. |
| "**CHECK**" | shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC. |
| "**Cloud**" | shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data. |
| "**Cyber Essentials**" | shall mean the Government-backed, industry-supported scheme managed by the NCSC to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC. |
| "**Cyber Security Information Sharing Partnership**" or "**CiSP**" | shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC. |
| "**Good Security Practice**" | shall mean:<br>a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology);<br>b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally |


© Crown Copyright 2020

recognised authorities and organisations; and

c) the Government's security policies, frameworks, standards and guidelines relating to Information Security.

"**Information Security**" shall mean:

a) the protection and preservation of:

i) the confidentiality, integrity and availability of any Authority Assets, the Authority's Systems Environment (or any part thereof) and the Contractor's Systems Environment (or any part thereof);

ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and

b) compliance with all Law applicable to the processing, transmission, storage and disposal of Authority Assets.

"**Information Security Manager**" shall mean the person appointed by the Contractor with the appropriate experience, authority and expertise to ensure that the Contractor complies with the Authority's Security Requirements.

"**Information Security Management System ("ISMS")**" shall mean the set of policies, processes and systems designed, implemented and maintained by the Contractor to manage Information Security Risk as specified by ISO/IEC 27001.

"**Information Security Questionnaire**" shall mean the Authority's set of questions used to audit and on an ongoing basis assure the Contractor's compliance with the Authority's Security Requirements.

"**Information Security Risk**" shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.


© Crown Copyright 2020

| | |
|---|---|
| "**ISO/IEC 27001, ISO/IEC 27002 and ISO 22301** | shall mean<br>a) ISO/IEC 27001;<br>b) ISO/IEC 27002/IEC; and<br>c) ISO 22301<br><br>in each case as most recently published by the International Organization for Standardization or its successor entity (the "**ISO**") or the relevant successor or replacement information security standard which is formally recommended by the ISO. |
| "**NCSC**" | shall mean the National Cyber Security Centre or its successor entity (where applicable). |
| "**Penetration Test**" | shall mean a simulated attack on any Authority Assets, the Authority's Systems Environment (or any part thereof) or the Contractor's Systems Environment (or any part thereof). |
| "**PCI DSS**" | shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC or its successor entity (the "**PCI**"). |
| "**Risk Profile**" | shall mean a description of any set of risk. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable. |
| "**Security Test"** | shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit. |
| "**Tigerscheme**" | shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd. |
| "**Vulnerability Scan**" | shall mean an ongoing activity to identify any potential vulnerability in any Authority Assets, the Authority's Systems Environment (or any part thereof) or the Contractor's Systems Environment (or any part thereof). |


© Crown Copyright 2020

1.2 Reference to any notice to be provided by the Contractor to the Authority shall be construed as a notice to be provided by the Contractor to the Authority's Representative.

## 2. PRINCIPLES OF SECURITY

2.1 The Contractor shall at all times comply with the Authority's Security Requirements and provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

## 3. ISO/IEC 27001 COMPLIANCE AND AUDIT

3.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with ISO/IEC 27001 in relation to the Services during the Contract Period.

3.2 The Contractor shall appoint an Information Security Manager and shall notify the Authority of the identity of the Information Security Manager on the Commencement Date and, where applicable, within 5 Working Days following any change in the identity of the Information Security Manager.

3.3 The Contractor shall ensure that it operates and maintains the Information Security Management System during the Contract Period and that the Information Security Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:

a) a scope statement (which covers all of the Services provided under this Contract);
b) a risk assessment (which shall include any risks specific to the Services);
c) a statement of applicability;
d) a risk treatment plan; and
e) an incident management plan

in each case as specified by ISO/IEC 27001.

The Contractor shall provide the Information Security Management System to the Authority upon request within 10 Working Days from such request.

3.4 The Contractor shall carry out regular Security Tests in compliance with ISO/IEC 27001 and shall within 10 Working Days after completion of the relevant audit provide any associated security audit reports to the Authority.

3.5 Notwithstanding the provisions of paragraph 3.1 to paragraph 3.4, the Authority may, in its absolute discretion, notify the Contractor that it is not in compliance with the Authority's Security Requirements and provide details of such non-compliance. The Contractor shall, at its own expense, undertake those actions required in order to comply with the Authority's Security Requirements within


© Crown Copyright 2020

one calendar month following such notification or on a date as agreed by the Parties. For the avoidance of doubt, any failure to comply with the Authority's Security Requirements within the required timeframe (regardless of whether such failure is capable of remedy) shall constitute a Default entitling the Authority to exercise its rights under clause 10.4 of the Core Terms.

## 4. CYBER ESSENTIALS SCHEME

4.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to Cyber Essentials (the "Cyber Essentials Certificate") in relation to the Services during Contract Period. The Cyber Essentials Certificate shall be provided by the Contractor to the Authority annually on the dates as agreed by the Parties.

4.2 The Contractor shall notify the Authority of any failure to obtain, or the revocation of, a Cyber Essentials Certificate within 2 Working Days of confirmation of such failure or revocation. The Contractor shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Certificate during the Contract Period after the first date on which the Contractor was required to provide a Cyber Essentials Certificate in accordance with paragraph 4.1 (regardless of whether such failure is capable of remedy) shall constitute a Default entitling the Authority to exercise its rights under clause 10.4 of the Core Terms.

## 5. RISK MANAGEMENT

5.1 The Contractor shall operate and maintain policies and processes for risk management (the **Risk Management Policy**) during the Contract Period which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Authority's Security Requirements are met (the **Risk Assessment**). The Contractor shall provide the Risk Management Policy to the Authority upon request within 10 Working Days of such request. The Authority may, at its absolute discretion, require changes to the Risk Management Policy to comply with the Authority's Security Requirements. The Contractor shall, at its own expense, undertake those actions required in order to implement the changes required by the Authority within one calendar month of such request or on a date as agreed by the Parties.

5.2 The Contractor shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Contractor's Systems Environment or in the threat landscape or (iii) at the request of the Authority. The Contractor shall provide the report of the Risk Assessment to the Authority, in the case of at least annual Risk Assessments, within 5 Working Days of completion of the Risk Assessment or, in the case of all other Risk Assessments, within one


© Crown Copyright 2020

calendar month after completion of the Risk Assessment or on a date as agreed by the Parties. The Contractor shall notify the Authority within 5 Working Days if the Risk Profile in relation to the Services has changed materially, for example, but not limited to, from one risk rating to another risk rating.

5.3 If the Authority decides, at its absolute discretion, that any Risk Assessment does not meet the Authority's Security Requirements, the Contractor shall repeat the Risk Assessment within one calendar month of such request or as agreed by the Parties.

5.4 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Authority in relation to the Authority's own risk management processes regarding the Services.

5.5 For the avoidance of doubt, the Contractor shall pay all costs in relation to undertaking any action required to meet the requirements stipulated in this paragraph 5. Any failure by the Contractor to comply with any requirement of this paragraph 5 (regardless of whether such failure is capable of remedy), shall constitute a Default entitling the Authority to exercise its rights under clause 10.4 of the Core Terms.

## 6. SECURITY AUDIT AND ASSURANCE

6.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, complete the information security questionnaire in the format stipulated by the Authority (the "**Information Security Questionnaire**") at least annually or at the request by the Authority. The Contractor shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.

6.2 The Contractor shall conduct Security Tests to assess the Information Security of the Contractor's Systems Environment and, if requested, the Authority's Systems Environment. In relation to such Security Tests, the Contractor shall appoint a third party which i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Test shall be carried out (i) at least annually, (ii) in the event of a material change in the Contractor's Systems Environment or in the Authority's System Environment or (iii) at the request of the Authority which request may include, but is not limited to, a repeat of a previous Security Test. The content, and format of any report of such Security Tests shall be approved in advance of the Security Test by the Authority. The Contractor shall provide any report of such Security Tests within one calendar month following the completion of such Security Test or on a date agreed by the Parties. The Contractor shall, at its own expense, undertake those actions required to rectify any risks identified by any Security Test in the manner and within the timeframe required by the Authority in its absolute discretion.


© Crown Copyright 2020

6.3 The Authority shall be entitled to send the Authority's Representative to witness the conduct of any Security Test. The Contractor shall provide to the Authority notice of any Security Test at least one month prior to the relevant Security Test.

6.6 The Authority, or an agent appointed by it, may undertake Security Tests in respect of the Contractor's Systems Environment after providing advance notice to the Contractor. If any Security Test identifies any non-compliance with the Authority's Security Requirements, the Contractor shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Authority at its absolute discretion. The Contractor shall provide all such co-operation and assistance in relation to any Security Test conducted by the Authority as the Authority may reasonably require.

6.7 The Authority shall schedule regular security governance review meetings which the Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

## 7. SECURITY POLICIES AND STANDARDS

8.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Security Policies and Standards set out Annex A and B.

8.2 Notwithstanding the foregoing, the Authority's Security Requirements applicable to the Services may be subject to change following certain events including, but not limited to, any relevant change in the delivery of the Services. Where any such change constitutes a Contract Change, any change in the Authority's Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change Procedure. Where any such change constitutes an Operational Change, any change in the Authority's Security Requirements resulting from such Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.

8.3 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with the Security Policies and Standards.

## 8. CYBER SECURITY INFORMATION SHARING PARTNERSHIP

9.1 The Supplier may require a nominated representative of the Supplier to join the Cyber Security Information Sharing Partnership on behalf of the Supplier during the Term, in which case the Supplier's nominated representative shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.


© Crown Copyright 2020

9.2 If the Supplier elects a nominated representative to join the Cyber Security Information Sharing Partnership in accordance with Paragraph 9.1 above, it shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Supplier's Risk Management Policy.

## ANNEX A – AUTHORITY SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

a) Acceptable Use Policy

b) Information Security Policy

c) Personnel Security Policy

d) Physical Security Policy

e) Information Management Policy

f) Email Policy

g) Technical Vulnerability Management Policy

h) Remote Working Policy

i) Social Media Policy

j) Forensic Readiness Policy

k) Microsoft Teams recording and transcription policy

l) SMS Text Policy

m) Privileged Users Security Policy

n) Protective Monitoring Security Policy


© Crown Copyright 2020

o) User Access Control Policy

p) Security Classification Policy

q) Cryptographic Key Management Policy

r) HMG Personnel Security Controls – May 2018 (published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)

s) NCSC Secure Sanitisation of Storage Media (published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

## ANNEX B – SECURITY STANDARDS

The Security Standards are published on: https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

a) SS-001 - Part 1 - Access & Authentication Controls
b) SS-001 - Part 2 - Privileged User Access Controls
c) Security Standard Physical and Electronic Security (Part 1)
d) SS-002 - PKI & Key Management
e) SS-003 - Software Development
f) SS-005 - Database Management System
g) SS-006 - Security Boundaries
h) SS-007 - Use of Cryptography
i) SS-008 - Server Operating System
j) SS-009 - Hypervisor
k) SS-010 - Desktop Operating System
l) SS-011 - Containerisation
m) SS-012 - Protective Monitoring Standard for External Use
n) SS-013 - Firewall Security
o) SS-014 - Security Incident Management
p) SS-015 - Malware Protection
q) SS-016 - Remote Access
r) SS-017 - Mobile Devices
s) SS-018 - Network Security Design
t) SS-019 - Wireless Network
u) SS-022 - Voice & Video Communications
v) SS-023 - Cloud Computing
w) SS-025 - Virtualisation
x) SS-027 - Application Security Testing
y) SS-028 - Microservices Architecture


© Crown Copyright 2020

z) SS-029 - Securely Serving Web Content
aa) SS-030 - Oracle Database
bb) SS-031 - Domain Management
cc) SS-033 – Security Patching
dd) SS-035 – Backup and Recovery
ee) SS-036 – Secure Sanitisation and Destruction

**Annex C**

**DWP Policy on Expenses for Business Travel & Accommodation for Contractors, Interim Managers and Consultants (December 2023)**

# 1. Circumstances where DWP will not reimburse expenses incurred

DWP will not reimburse costs incurred for travel to, or accommodation at, the main base location.

Additionally, in order to comply with Propriety and Regularity, Audit and Tax rules DWP will not pay, or be responsible for the payment of any fines or penalty charges in respect of private vehicles etc. during the undertaking of duties for DWP.

# 2. Circumstances where DWP will reimburse expenses incurred

DWP will re-imburse necessary and reasonable business travel and accommodation costs incurred during the undertaking of duties for DWP. This is subject to:

- All such expenses being agreed with DWP in advance;


© Crown Copyright 2020

- The rules for claiming expenses must be in accordance with the DWP Policy on Expenses for Business Travel & Accommodation for Contractors, Interim Managers and Consultants in force at the time the expense is incurred;
- All such expenses must have been incurred in performing DWP services away from their main base location of DWP work, and be minus the cost of travel to the usual place of work;
- Appropriate documentary evidence, such as receipts and tickets, of such expenses being incurred is provided to the appropriate DWP contact.
- The expenses must be submitted at the same time as the relevant weekly timesheet

# 3. Offshore Personnel

In respect of Contractors/Interim Managers/Consultants who are located outside the UK:

- Business Travel and Accommodation expenses incurred in off-shore locations will not be reimbursed;
- Where the Contractor decides to bring off-shore Contractors/Interim Managers/Consultants into the UK in order to perform DWP services i.e. they become “landed”, then the DWP Policy on Expenses for Business Travel & Accommodation for Contractors, Interim Managers and Consultants may apply to costs incurred within the UK;
- DWP will not be liable for any expenses incurred in order for the Contractors/Interim Managers/Consultants to be “landed” i.e. for travel from the off-shore location to the on-shore location

# 4. General statements on Business Travel and Accommodation

4.1 Before committing to any travel arrangements Contractors/Interim Managers/Consultants must discuss travelling needs with their DWP manager and assess:

- Whether the following could be used:
- video conferencing
- telephone conferencing
- web conferencing
- audio conferencing
- The business need to travel
- The most economical and suitable means of travel, taking into account value for money and sustainability factors

4.2 Business journeys must only be made when face-to-face meetings are essential. Authorisation to travel must be received from DWP manager before committing to make travel arrangements.


© Crown Copyright 2020

4.3 The most cost effective/value for money option should be obtained and Contractors/Interim Managers/Consultants can use their own organisations' booking agent(s) or low cost alternatives. Advantage should be taken of any offers for reduced travel (including Restricted and Advanced Purchase Tickets/Advanced Booking for Rooms) or room rates. Alternatively DWP employees can book travel on behalf of contractors. Please refer to **DWP Guide to Managing Contractors** for guidance. Any claims for the cost of travel and accommodation must be evidenced with supporting documentation and receipts.

4.4 No organisational or personal benefit must be obtained arising from the promotions, offers, or reward schemes that ensue from official travel or accommodation paid for by DWP, whether in advance or by refund. Where such promotions or offers are available, the Contractors/Interim Managers/Consultants should agree with DWP, whenever possible, how to use any such benefits to offset against other expenses payable by DWP.

4.5 DWP reserves the right to reject claims for unreasonable expenses, or expenses which could have been avoided if a journey had been better planned.

# 5. Rates and Expenses type

The types of expenses and the rates payable are given at Annex 1 below and are applicable from 1st March 2015. The rates payable are subject to change.

5.1 Claims for Mobile Phone calls and Internet Use

Costs for mobile telephone calls and Internet use cannot be claimed.

5.2 Public Transport including Rail Travel

On public transport standard class travel must be used. First class travel is strictly prohibited irrespective of the duties undertaken.

The use of Rail, Oyster and other discount cards or schemes is encouraged if evidence is shown that these will save DWP more than their cost.

5.3 Taxis

Taxi fares may be reimbursed for Business Travel where their use is reasonable in the circumstances. Actual fares only can be claimed in the following circumstances:

- Where there is no other suitable method of public transport
- In exceptional and infrequent circumstances where the saving of official time is important


© Crown Copyright 2020

- When heavy luggage has to be handled
- When shared by colleagues and the fare overall is cheaper than public transport

5.4 Air Travel

Claims for domestic air travel are not permitted unless the flight is over 300 miles. This limit is for one-way flights within the British mainland. In particular, for travel between the destinations shown below air travel is not permitted, journeys must be taken by rail:

- Newcastle and London
- Birmingham and Newcastle
- Manchester and London

Economy Class air travel must always be booked when travelling on domestic flights within the UK. No Business Class or First Class tickets must be booked on domestic flights regardless of the length/duration of journey.

5.5 Private Motor Vehicles

Private Vehicle Use

DWP aims to reduce mileage travelled in private motor vehicles undertaken by Contractors/Interim Managers/Consultants. When considering the use of a vehicle on official business, Contractors/Interim Managers/Consultants must only use their own vehicle for business journeys when there is no other practicable mode of transport including public transport. Permission must be gained from DWP for each business journey carried out in a private vehicle.

Before undertaking such journeys DWP manager must check that the contractor/interim manager/consultant holds a full current driving licence. The private vehicle must be roadworthy and, where required, have a valid MOT Test Certificate. All contractor personnel must ensure their motor vehicle insurance policy includes an Employer Indemnity clause in addition to the Business Use clause. It is the policyholder’s responsibility to check with their insurance company that they have both types of cover and for DWP to validate this.

There are mileage restrictions of a maximum of 1000 miles per financial year and 100 miles per day once authorisation has been obtained. Contractors/Interim Managers/Consultants who genuinely need to travel more than 1000 miles per year or 100 miles per day in their own vehicle must have written permission from DWP in the form of Business Case authorised at least UG7 Grade.

Note: For daily journeys over 100 miles, an exemption is required only if it is likely to be a regular occurrence. One-off situations can be approved locally with no form required.


© Crown Copyright 2020

Reasons for granting permission must be clearly documented in a Business Case (**Annex 2**) and retained for audit purposes.

Mileage rates can be claimed as detailed in Annex 1.

Car parking fees can be claimed on production of the appropriate documentary evidence. Receipts and tickets should be provided to the appropriate DWP contact. However, DWP will not provide remuneration for travel on Toll Roads.

5.6 Overnight Accommodation

5.6.1 Hotel

Where it is necessary for Contractors/Interim Managers/Consultants to stay away from their main base location(s) for the performance of the contract then:

a) Expenses will only be reimbursed where it is not possible for the Contractor Personnel to stay at their home;

b) The following two principles must apply to any accommodation booking:

i) It must be as close to the traveller's end location as possible and within a 5 mile radius; and

ii) It must be the most economical option, having taken into account the whole trip cost, such as public transport costs, taxi fares and travelling time.

Regional maximum limits for claims for overnight hotel accommodation are included at **Annex 1**.

5.6.2 Overnight stay with relatives or friends

Where a contractor/interim manager/consultant elects to stay with friends or relatives rather than in a hotel or other commercial establishment, then the Overnight Accommodation rates do not apply. Alternatively the Friends and relatives allowance is payable at a flat rate to cover accommodation.

# Annex 1

**Expenses rates**

| **Expense Type** | **Conditions/Category** | **Rate as at 1 March 2015** |
|---|---|---|
| **Lodging** | Friends and relatives - Nightly | £25.00 |


© Crown Copyright 2020

| | | |
|---|---|---|
| **Mileage rates (amount per mile)** | Higher standard rate (up to 1,000) | £0.45 |
| | Lower standard rate (over 1,000)* | £0.25 |
| | Motor cycle | £0.24 |

*Restrictions apply and Business Case is required - see Para 5.5

**Regional Limits on Claims for Overnight Hotel Accommodation**

| **Hotel allowance – Upper Limits** | **(£ per night)** |
|---|---|
| **London** | £150 |
| **Rest of the country (except London)** | £100 |

# Annex 2

Business Case for Approval to Exceed the DWP Mileage Restrictions of 100 miles per day or 1000 miles per year

| | | |
|---|---|---|
| **Business Unit:**<br><br>**Name of proposer:**<br><br>**Grade of proposer:** | | |
| **Home Office:**<br><br>**Name of staff the exemption covers** | | |


© Crown Copyright 2020

| | | |
|---|---|---|
| **Short description of journeys undertaken including daily mileage** | | |
| **Are there any reasons, through health or disability, that an exemption should be granted. If yes do not fill in any further.** | | |
| **Reasons why Tele-Conference or Video Conference are unsuitable** | | |
| **Reasons why Public Transport is unsuitable** | | |
| **Authorising Person**<br><br>**Grade of Authorising Person** | | **Date:** |

1. When exemption is granted, please retain a copy of this form for audit purpose


© Crown Copyright 2020

# Joint Schedule 1 (Definitions)

1.1 In each Contract, unless the context otherwise requires, capitalised expressions shall have the meanings set out in this Joint Schedule 1 (Definitions) or the relevant Schedule in which that capitalised expression appears.

1.2 If a capitalised expression does not have an interpretation in this Schedule or any other Schedule, it shall, in the first instance, be interpreted in accordance with the common interpretation within the relevant market sector/industry where appropriate. Otherwise, it shall be interpreted in accordance with the dictionary meaning.

1.3 In each Contract, unless the context otherwise requires:

1.3.1 the singular includes the plural and vice versa;

1.3.2 reference to a gender includes the other gender and the neuter;

1.3.3 references to a person include an individual, company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or Crown Body;

1.3.4 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

1.3.5 the words "**including**", "**other**", "**in particular**", "**for example**" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "**without limitation**";

1.3.6 references to "**writing**" include typing, printing, lithography, photography, display on a screen, electronic and facsimile transmission and other modes of representing or reproducing words in a visible form, and expressions referring to writing shall be construed accordingly;


© Crown Copyright 2020

1.3.7 references to "**representations**" shall be construed as references to present facts, to "**warranties**" as references to present and future facts and to "**undertakings"** as references to obligations under the Contract;

1.3.8 references to **"Clauses"** and **"Schedules"** are, unless otherwise provided, references to the clauses and schedules of the Core Terms and references in any Schedule to parts, paragraphs, annexes and tables are, unless otherwise provided, references to the parts, paragraphs, annexes and tables of the Schedule in which these references appear;

1.3.9 references to **"Paragraphs"** are, unless otherwise provided, references to the paragraph of the appropriate Schedules unless otherwise provided;

1.3.10 references to a series of Clauses or Paragraphs shall be inclusive of the clause numbers specified;

1.3.11 the headings in each Contract are for ease of reference only and shall not affect the interpretation or construction of a Contract; and

1.3.12 where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole.

1.4 In each Contract, unless the context otherwise requires, the following words shall have the following meanings:

| | |
|---|---|
| **"Accreditations and Standards"** | the Accreditations and Standards Filter Category detailed in DPS Schedule 1. |
| **"Additional Insurances"** | insurance requirements relating to an Order Contract specified in the Order Form additional to those outlined in Joint Schedule 3 (Insurance Requirements); |
| **"Admin Fee"** | means the costs incurred by CCS in dealing with MI Failures calculated in accordance with the tariff of administration charges published by the CCS on: http://CCS.cabinetoffice.gov.uk/i-am-supplier/management-information/admin-fees; |
| **"Affected Party"** | the party seeking to claim relief in respect of a Force Majeure Event; |
| **"Affiliates"** | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control of that body corporate from time to time; |
| **"Annex"** | extra information which supports a Schedule; |
| **"Approval"** | the prior written consent of the Buyer and "**Approve**" and "**Approved**" shall be construed accordingly; |
| **"Audit"** | the Relevant Authority's right to: |


© Crown Copyright 2020

| | |
|---|---|
| | a) verify the accuracy of the Charges and any other amounts payable by a Buyer under an Order Contract (including proposed or actual variations to them in accordance with the Contract);<br>b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Services;<br>c) verify the Open Book Data;<br>d) verify the Supplier's and each Subcontractor's compliance with the applicable Law;<br>e) identify or investigate actual or suspected breach of Clauses 27 to 33 and/or Joint Schedule 5 (Corporate Social Responsibility), impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Relevant Authority shall have no obligation to inform the Supplier of the purpose or objective of its investigations;<br>f) identify or investigate any circumstances which may impact upon the financial stability of the Supplier, any Guarantor, and/or any Subcontractors or their ability to provide the Deliverables;<br>g) obtain such information as is necessary to fulfil the Relevant Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General;<br>h) review any books of account and the internal contract management accounts kept by the Supplier in connection with each Contract;<br>i) carry out the Relevant Authority's internal and statutory audits and to prepare, examine and/or certify the Relevant Authority's annual and interim reports and accounts;<br>j) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Relevant Authority has used its resources;<br>k) verify the accuracy and completeness of any Management Information delivered or required by the DPS Contract; |
| **"Auditor"** | a) the Relevant Authority's internal and external auditors;<br>b) the Relevant Authority's statutory or regulatory auditors;<br>c) the Comptroller and Auditor General, their staff and/or any appointed representatives of the National Audit Office;<br>d) HM Treasury or the Cabinet Office; |


© Crown Copyright 2020

| | |
|---|---|
| | e) any party formally appointed by the Relevant Authority to carry out audit or similar review functions; and<br>f) successors or assigns of any of the above; |
| **"Authority"** | CCS and each Buyer; |
| **"Authority Cause"** | any breach of the obligations of the Relevant Authority or any other default, act, omission, negligence or statement of the Relevant Authority, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Relevant Authority is liable to the Supplier; |
| **"BACS"** | the Bankers' Automated Clearing Services, which is a scheme for the electronic processing of financial transactions within the United Kingdom; |
| **"Beneficiary"** | a Party having (or claiming to have) the benefit of an indemnity under this Contract; |
| **"Buyer"** | the relevant public sector purchaser identified as such in the Order Form; |
| **"Buyer Assets"** | the Buyer's infrastructure, data, software, materials, assets, equipment or other property owned by and/or licensed or leased to the Buyer and which is or may be used in connection with the provision of the Deliverables which remain the property of the Buyer throughout the term of the Contract; |
| **"Buyer Authorised Representative"** | the representative appointed by the Buyer from time to time in relation to the Order Contract initially identified in the Order Form; |
| **"Buyer Premises"** | premises owned, controlled or occupied by the Buyer which are made available for use by the Supplier or its Subcontractors for the provision of the Deliverables (or any of them); |
| **"Buyer Property"** | the property, other than real property and IPR, including the Buyer System, any equipment issued or made available to the Supplier by the Buyer in connection with this Order Contract; |
| **"CCS"** | the Minister for the Cabinet Office as represented by Crown Commercial Service, which is an executive agency and operates as a trading fund of the Cabinet Office, whose offices are located at 9th Floor, The Capital, Old Hall Street, Liverpool L3 9PP; |
| **"CCS Authorised Representative"** | the representative appointed by CCS from time to time in relation to the DPS Contract initially identified in the DPS Appointment Form and subsequently on the Platform; |


© Crown Copyright 2020

| | |
|---|---|
| **"Central Government Body"** | a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:<br>a) Government Department;<br>b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);<br>c) Non-Ministerial Department; or<br>d) Executive Agency; |
| **"Change in Law"** | any change in Law which impacts on the supply of the Deliverables and performance of the Contract which comes into force after the Start Date; |
| **"Change of Control"** | a change of control within the meaning of Section 450 of the Corporation Tax Act 2010; |
| **"Charges"** | the prices (exclusive of any applicable VAT), payable to the Supplier by the Buyer under the Order Contract, as set out in the Order Form, for the full and proper performance by the Supplier of its obligations under the Order Contract less any Deductions; |
| **"Claim"** | any claim which it appears that a Beneficiary is, or may become, entitled to indemnification under this Contract; |
| **"Commercially Sensitive Information"** | the Confidential Information listed in the DPS Appointment Form or Order Form (if any) comprising of commercially sensitive information relating to the Supplier, its IPR or its business or which the Supplier has indicated to the Authority that, if disclosed by the Authority, would cause the Supplier significant commercial disadvantage or material financial loss; |
| **"Comparable Supply"** | the supply of Deliverables to another Buyer of the Supplier that are the same or similar to the Deliverables; |
| **"Compliance Officer"** | the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations; |
| **"Confidential Information"** | means any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, Know-How, personnel and suppliers of CCS, the Buyer or the Supplier, including IPRs, together with information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as **"confidential"**) or which ought reasonably to be considered to be confidential; |


© Crown Copyright 2020

| | |
|---|---|
| **"Conflict of Interest"** | a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to CCS or any Buyer under a Contract, in the reasonable opinion of the Buyer or CCS; |
| **"Contract"** | either the DPS Contract or the Order Contract, as the context requires; |
| **"Contracts Finder"** | the Government's publishing portal for public sector procurement opportunities; |
| **"Contract Period"** | the term of either a DPS Contract or Order Contract from the earlier of the:<br>a) applicable Start Date; or<br>b) the Effective Date<br>until the applicable End Date; |
| **"Contract Value"** | the higher of the actual or expected total Charges paid or payable under a Contract where all obligations are met by the Supplier; |
| **"Contract Year"** | a consecutive period of twelve (12) Months commencing on the Start Date or each anniversary thereof; |
| **"Control"** | control in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and "**Controlled**" shall be construed accordingly; |
| **"Controller"** | has the meaning given to it in the GDPR; |
| **"Core Terms"** | CCS' standard terms and conditions for common goods and services which govern how Supplier must interact with CCS and Buyers under DPS Contracts and Order Contracts; |
| **"Costs"** | the following costs (without double recovery) to the extent that they are reasonably and properly incurred by the Supplier in providing the Deliverables:<br>a) the cost to the Supplier or the Key Subcontractor (as the context requires), calculated per Man Day, of engaging the Supplier Staff, including:<br>i) base salary paid to the Supplier Staff;<br>ii) employer's National Insurance contributions;<br>iii) pension contributions;<br>iv) car allowances;<br>v) any other contractual employment benefits;<br>vi) staff training;<br>vii) work place accommodation; |


© Crown Copyright 2020

| | |
|---|---|
| | viii) work place IT equipment and tools reasonably necessary to provide the Deliverables (but not including items included within limb (b) below); and<br>ix) reasonable recruitment costs, as agreed with the Buyer;<br>b) costs incurred in respect of Supplier Assets which would be treated as capital costs according to generally accepted accounting principles within the UK, which shall include the cost to be charged in respect of Supplier Assets by the Supplier to the Buyer or (to the extent that risk and title in any Supplier Asset is not held by the Supplier) any cost actually incurred by the Supplier in respect of those Supplier Assets;<br>c) operational costs which are not included within (a) or (b) above, to the extent that such costs are necessary and properly incurred by the Supplier in the provision of the Deliverables;<br>d) Reimbursable Expenses to the extent these have been specified as allowable in the Order Form and are incurred in delivering any Deliverables;<br>but excluding:<br>a) Overhead;<br>b) financing or similar costs;<br>c) maintenance and support costs to the extent that these relate to maintenance and/or support Deliverables provided beyond the Order Contract Period whether in relation to Supplier Assets or otherwise;<br>d) taxation;<br>e) fines and penalties;<br>f) non-cash items (including depreciation, amortisation, impairments and movements in provisions); |
| **"Crown Body"** | the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf; |
| **"CRTPA"** | the Contract Rights of Third Parties Act 1999; |
| **"Cyber Security Services"** | those Service available under this DPS Contract as documented at DPS Schedule 1 |
| **"Data Loss Event"** | any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or |


© Crown Copyright 2020

| | |
|---|---|
| | actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach; |
| **"Data Protection Legislation"** | (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy; |
| **"Data Protection Impact Assessment"** | an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data; |
| **"Data Protection Officer"** | has the meaning given to it in the GDPR; |
| **"Data Subject"** | has the meaning given to it in the GDPR; |
| **"Data Subject Access Request"** | a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data; |
| **"Deductions"** | all Service Credits, Delay Payments (if applicable), or any other deduction which the Buyer is paid or is payable to the Buyer under an Order Contract; |
| **"Default"** | any breach of the obligations of the Supplier (including abandonment of a Contract in breach of its terms) or any other default (including material default), act, omission, negligence or statement of the Supplier, of its Subcontractors or any Supplier Staff howsoever arising in connection with or in relation to the subject-matter of a Contract and in respect of which the Supplier is liable to the Relevant Authority; |
| **"Default Management Levy"** | has the meaning given to it in Paragraph 8.1.1 of DPS Schedule 5 (Management Levy and Information); |
| **"Delay Payments"** | the amounts (if any) payable by the Supplier to the Buyer in respect of a delay in respect of a Milestone as specified in the Implementation Plan; |
| **"Deliverables"** | Goods and/or Services that may be ordered under the Contract including the Documentation; |
| **"Delivery"** | delivery of the relevant Deliverable or Milestone in accordance with the terms of an Order Contract as confirmed and accepted by the Buyer by confirmation in writing to the Supplier. "**Deliver**" and "**Delivered**" shall be construed accordingly; |
| **"Disaster"** | the occurrence of one or more events which, either separately or cumulatively, mean that the Deliverables, or a material part thereof will be unavailable (or could reasonably be anticipated to be |


© Crown Copyright 2020

| | |
|---|---|
| | unavailable) for the period specified in the Order Form (for the purposes of this definition the **"Disaster Period**"); |
| **"Disclosing Party"** | the Party directly or indirectly providing Confidential Information to the other Party in accordance with Clause 15 (What you must keep confidential); |
| **"Dispute"** | any claim, dispute or difference arises out of or in connection with the Contract or in connection with the negotiation, existence, legal validity, enforceability or termination of the Contract, whether the alleged liability shall arise under English law or under the law of some other country and regardless of whether a particular cause of action may successfully be brought in the English courts; |
| **"Dispute Resolution Procedure"** | the dispute resolution procedure set out in Clause 34 (Resolving disputes); |
| **"Documentation"** | descriptions of the Services and Service Levels, technical specifications, user manuals, training manuals, operating manuals, process definitions and procedures, system environment descriptions and all such other documentation (whether in hardcopy or electronic form) is required to be supplied by the Supplier to the Buyer under a Contract as:<br>a) would reasonably be required by a competent third party capable of Good Industry Practice contracted by the Buyer to develop, configure, build, deploy, run, maintain, upgrade and test the individual systems that provide the Deliverables;<br>b) is required by the Supplier in order to provide the Deliverables; and/or<br>c) has been or shall be generated for the purpose of providing the Deliverables; |
| **"DOTAS"** | the Disclosure of Tax Avoidance Schemes rules which require a promoter of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions; |
| **"DPA 2018"** | the Data Protection Act 2018; |
| **"DPS"** | the dynamic purchasing system operated by CCS in accordance with Regulation 34 that this DPS Contract governs access to; |
| **"DPS Application"** | the application submitted by the Supplier to CCS and annexed to or referred to in DPS Schedule 2 (DPS Application); |


© Crown Copyright 2020

| | |
|---|---|
| **"DPS Appointment Form"** | the document outlining the DPS Incorporated Terms and crucial information required for the DPS Contract, to be executed by the Supplier and CCS and subsequently held on the Platform; |
| **"DPS Contract"** | the dynamic purchasing system access agreement established between CCS and the Supplier in accordance with Regulation 34 by the DPS Appointment Form for the provision of the Deliverables to Buyers by the Supplier pursuant to the OJEU Notice; |
| **"DPS Contract Period"** | the period from the DPS Start Date until the End Date or earlier termination of the DPS Contract; |
| **"DPS Expiry Date"** | the date of the end of the DPS Contract as stated in the DPS Appointment Form; |
| **"DPS Incorporated Terms"** | the contractual terms applicable to the DPS Contract specified in the DPS Appointment Form; |
| **"DPS Initial Period"** | the initial term of the DPS Contract as specified in the DPS Appointment Form; |
| **"DPS Optional Extension Period"** | such period or periods beyond which the DPS Initial Period may be extended up to a maximum of the number of years in total specified in the DPS Appointment Form; |
| **"DPS Pricing"** | the maximum price(s) applicable to the provision of the Deliverables set out in DPS Schedule 3 (DPS Pricing); |
| **"DPS Registration"** | the registration process a Supplier undertakes when submitting its details onto the Platform; |
| **"DPS SQ Submission"** | the Supplier's selection questionnaire response; |
| **"DPS Special Terms"** | any additional terms and conditions specified in the DPS Appointment Form incorporated into the DPS Contract; |
| **"DPS Start Date"** | the date of start of the DPS Contract as stated in the DPS Appointment Form; |
| **"Due Diligence Information"** | any information supplied to the Supplier by or on behalf of the Authority prior to the Start Date; |
| **"Effective Date"** | the date on which the final Party has signed the Contract; |
| **"EIR"** | the Environmental Information Regulations 2004; |
| **"Employment Regulations"** | the Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) as amended or replaced or any other Regulations implementing the European Council Directive 77/187/EEC; |
| **"End Date"** | the earlier of: |


© Crown Copyright 2020

| | |
|---|---|
| | a) the Expiry Date (as extended by any Extension Period exercised by the Authority under Clause 10.2); or<br>b) if a Contract is terminated before the date specified in (a) above, the date of termination of the Contract; |
| **"Environmental Policy"** | to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Buyer; |
| **"Estimated Year 1 Contract Charges"** | the anticipated total charges payable by the Supplier in the first Contract Year specified in the Order Form; |
| **"Estimated Yearly Charges"** | means for the purposes of calculating each Party's annual liability under clause 11.2 :<br>i) in the first Contract Year, the Estimated Year 1 Contract Charges; or<br>ii) in any subsequent Contract Years, the Charges paid or payable in the previous Contract Year; or<br>iii) after the end of the Contract, the Charges paid or payable in the last Contract Year during the Contract Period; |
| **"Equality and Human Rights Commission"** | the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time; |
| **"Existing IPR"** | any and all IPR that are owned by or licensed to either Party and which are or have been developed independently of the Contract (whether prior to the Start Date or otherwise); |
| **"Expiry Date"** | the DPS Expiry Date or the Order Expiry Date (as the context dictates); |
| **"Extension Period"** | the DPS Optional Extension Period or the Order Optional Extension Period as the context dictates; |
| **"Filter Categories"** | the number of categories specified in DPS Schedule 1 (Specification), if applicable; |
| **"FOIA"** | the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation; |
| **"Force Majeure Event"** | any event, occurrence, circumstance, matter or cause affecting the performance by either the Relevant Authority or the Supplier of its obligations arising from: |


© Crown Copyright 2020

| | |
|---|---|
| | a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Affected Party which prevent or materially delay the Affected Party from performing its obligations under a Contract;<br>b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare;<br>c) acts of a Crown Body, local government or regulatory bodies;<br>d) fire, flood or any disaster; or<br>e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available but excluding:<br>i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain;<br>ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and<br>iii) any failure of delay caused by a lack of funds; |
| **"Force Majeure Notice"** | a written notice served by the Affected Party on the other Party stating that the Affected Party believes that there is a Force Majeure Event; |
| **"GDPR"** | the General Data Protection Regulation (Regulation (EU) 2016/679); |
| **"General Anti-Abuse Rule"** | a) the legislation in Part 5 of the Finance Act 2013; and<br>b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid National Insurance contributions; |
| **"General Change in Law"** | a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply; |
| **"Goods"** | goods made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form; |
| **"Good Industry Practice"** | standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector; |
| **"Government"** | the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including government ministers and government departments and other |


© Crown Copyright 2020

| | |
|---|---|
| | bodies, persons, commissions or agencies from time to time carrying out functions on its behalf; |
| **"Government Data"** | a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Authority's Confidential Information, and which:<br>i) are supplied to the Supplier by or on behalf of the Authority; or<br>ii) the Supplier is required to generate, process, store or transmit pursuant to a Contract; or<br>b) any Personal Data for which the Authority is the Data Controller; |
| **"Government Procurement Card"** | the Government's preferred method of purchasing and payment for low value goods or services;<br>https://www.gov.uk/government/publications/government-procurement-card--2; |
| **"Guarantor"** | the person (if any) who has entered into a guarantee in the form set out in Joint Schedule 8 (Guarantee) in relation to this Contract; |
| **"Halifax Abuse Principle"** | the principle explained in the CJEU Case C-255/02 Halifax and others; |
| **"HMRC"** | Her Majesty's Revenue and Customs; |
| **"ICT Policy"** | the Buyer's policy in respect of information and communications technology, referred to in the Order Form, which is in force as at the Order Start Date (a copy of which has been supplied to the Supplier), as updated from time to time in accordance with the Variation Procedure; |
| **"Impact Assessment"** | an assessment of the impact of a Variation request by the Relevant Authority completed in good faith, including:<br>a) details of the impact of the proposed Variation on the Deliverables and the Supplier's ability to meet its other obligations under the Contract;<br>b) details of the cost of implementing the proposed Variation;<br>c) details of the ongoing costs required by the proposed Variation when implemented, including any increase or decrease in the DPS Pricing/Charges (as applicable), any alteration in the resources and/or expenditure required by either Party and any alteration to the working practices of either Party;<br>d) a timetable for the implementation, together with any proposals for the testing of the Variation; and<br>e) such other information as the Relevant Authority may reasonably request in (or in response to) the Variation request; |


© Crown Copyright 2020

| | |
|---|---|
| **"Implementation Plan"** | the plan for provision of the Deliverables set out in Order Schedule 13 (Implementation Plan and Testing) where that Schedule is used or otherwise as agreed between the Supplier and the Buyer; |
| **"Indemnifier"** | a Party from whom an indemnity is sought under this Contract; |
| **"Independent Control"** | where a Controller has provided Personal Data to another Party which is not a Processor or a Joint Controller because the recipient itself determines the purposes and means of processing but does so separately from the Controller providing it with Personal Data and "**Independent Controller**" shall be construed accordingly; |
| **"Information"** | has the meaning given under section 84 of the Freedom of Information Act 2000; |
| **"Information Commissioner"** | the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies; |
| **"Initial Period"** | the initial term of a Contract specified on the Platform or the Order Form, as the context requires; |
| **"Insolvency Event"** | a) in respect of a person:<br>b) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors; or<br>c) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation); or<br>d) a petition is presented for its winding up (which is not dismissed within fourteen (14) Working Days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986; or<br>e) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets; or<br>f) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given; or<br>g) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or<br>h) being a "small company" within the meaning of section 382(3) of the Companies Act 2006, a moratorium comes into force pursuant to Schedule A1 of the Insolvency Act 1986; or |


© Crown Copyright 2020

| | |
|---|---|
| | i) where the person is an individual or partnership, any event analogous to those listed in limbs (a) to (g) (inclusive) occurs in relation to that individual or partnership; or<br>j) any event analogous to those listed in limbs (a) to (h) (inclusive) occurs under the law of any other jurisdiction; |
| **"Intellectual Property Rights" or "IPR"** | a) copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade or business names, goodwill, designs, Know-How, trade secrets and other rights in Confidential Information;<br>b) applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction; and<br>c) all other rights having equivalent or similar effect in any country or jurisdiction; |
| **"Invoicing Address"** | the address to which the Supplier shall Invoice the Buyer as specified in the Order Form; |
| **"IPR Claim"** | any claim of infringement or alleged infringement (including the defence of such infringement or alleged infringement) of any IPR, used to provide the Deliverables or otherwise provided and/or licensed by the Supplier (or to which the Supplier has provided access) to the Relevant Authority in the fulfilment of its obligations under a Contract; |
| **"IR35"** | the off-payroll rules requiring individuals who work through their company pay the same tax and National Insurance contributions as an employee which can be found online at: https://www.gov.uk/guidance/ir35-find-out-if-it-applies; |
| **"Joint Controllers"** | where two or more Controllers jointly determine the purposes and means of processing; |
| **"Key Personnel"** | the individuals (if any) identified as such in the Order Form; |
| **"Key Sub-Contract"** | each Sub-Contract with a Key Subcontractor; |
| **"Key Subcontractor"** | any Subcontractor:<br>a) which is relied upon to deliver any work package within the Deliverables in their entirety; and/or<br>b) which, in the opinion of CCS or the Buyer performs (or would perform if appointed) a critical role in the provision of all or any part of the Deliverables; and/or<br>c) with a Sub-Contract with a contract value which at the time of appointment exceeds (or would exceed if appointed) 10% of the |


© Crown Copyright 2020

| | |
|---|---|
| | aggregate Charges forecast to be payable under the Order Contract,<br>and the Supplier shall list all such Key Subcontractors on the Platform and in the Key Subcontractor Section in the Order Form; |
| **"Know-How"** | all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the Deliverables but excluding know-how already in the other Party's possession before the applicable Start Date; |
| **"Law"** | any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply; |
| **"LED"** | Law Enforcement Directive (Directive (EU) 2016/680); |
| **"Losses"** | all losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and "**Loss**" shall be interpreted accordingly; |
| **"Malicious Software"** | any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence; |
| **"Man Hours"** | the hours spent by the Supplier Staff properly working on the provision of the Deliverables including time spent travelling (other than to and from the Supplier's offices, or to and from the Sites) but excluding lunch breaks; |
| **"Management Information"** | the management information specified in DPS Schedule 5 (Management Levy and Information); |
| **"Management Levy"** | the sum specified on the Platform payable by the Supplier to CCS in accordance with DPS Schedule 5 (Management Levy and Information); |
| **"Marketing Contact"** | shall be the person identified in the DPS Appointment Form; |
| **"MI Default"** | means when two (2) MI Reports are not provided in any rolling six (6) month period; |
| **"MI Failure"** | means when an MI report: |


© Crown Copyright 2020

| | |
|---|---|
| | a) contains any material errors or material omissions or a missing mandatory field; or<br>b) is submitted using an incorrect MI reporting Template; or<br>c) is not submitted by the reporting date (including where a declaration of no business should have been filed); |
| **"MI Report"** | means a report containing Management Information submitted to the Authority in accordance with DPS Schedule 5 (Management Levy and Information); |
| **"MI Reporting Template"** | means the form of report set out in the Annex to DPS Schedule 5 (Management Levy and Information) setting out the information the Supplier is required to supply to the Authority; |
| **"Milestone"** | an event or task described as such in the Implementation Plan; |
| **"Milestone Date"** | the target date set out against the relevant Milestone in the Implementation Plan by which the Milestone must be achieved; |
| **"Month"** | a calendar month and "**Monthly**" shall be interpreted accordingly; |
| **"National Insurance"** | contributions required by the National Insurance Contributions Regulations 2012 (SI 2012/1868) made under section 132A of the Social Security Administration Act 1992; |
| **"New IPR"** | a) IPR in items created by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of a Contract and updates and amendments of these items including (but not limited to) database schema; and/or<br>b) IPR in or arising as a result of the performance of the Supplier's obligations under a Contract and all updates and amendments to the same;<br>but shall not include the Supplier's Existing IPR; |
| **"Occasion of Tax Non – Compliance"** | where:<br>a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of:<br>i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation in any jurisdiction that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;<br>ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime in any jurisdiction; and/or |


© Crown Copyright 2020

| | |
|---|---|
| | b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Start Date or to a civil penalty for fraud or evasion; |
| **"Open Book Data"** | complete and accurate financial and non-financial information which is sufficient to enable the Buyer to verify the Charges already paid or payable and Charges forecast to be paid during the remainder of the Order Contract, including details and all assumptions relating to:<br>a) the Supplier's Costs broken down against each Good and/or Service and/or Deliverable, including actual capital expenditure (including capital replacement costs) and the unit cost and total actual costs of all Deliverables;<br>b) operating expenditure relating to the provision of the Deliverables including an analysis showing:<br>i) the unit costs and quantity of Goods and any other consumables and bought-in Deliverables;<br>ii) manpower resources broken down into the number and grade/role of all Supplier Staff (free of any contingency) together with a list of agreed rates against each manpower grade;<br>iii) a list of Costs underpinning those rates for each manpower grade, being the agreed rate less the Supplier Profit Margin; and<br>iv) Reimbursable Expenses, if allowed under the Order Form;<br>c) Overheads;<br>d) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Deliverables;<br>e) the Supplier Profit achieved over the DPS Contract Period and on an annual basis;<br>f) confirmation that all methods of Cost apportionment and Overhead allocation are consistent with and not more onerous than such methods applied generally by the Supplier;<br>g) an explanation of the type and value of risk and contingencies associated with the provision of the Deliverables, including the amount of money attributed to each risk and/or contingency; and<br>h) the actual Costs profile for each Service Period; |
| **"Open Government Licence"** | means the licensing terms for use of government intellectual property at:<br>http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ |


© Crown Copyright 2020

| | |
|---|---|
| **"Order"** | means an order for the provision of the Deliverables placed by a Buyer with the Supplier under a Contract; |
| **"Order Contract"** | the contract between the Buyer and the Supplier (entered into pursuant to the provisions of the DPS Contract), which consists of the terms set out and referred to in the Order Form; |
| **"Order Contract Period"** | the Contract Period in respect of the Order Contract; |
| **"Order Expiry Date"** | the date of the end of an Order Contract as stated in the Order Form; |
| **"Order Form"** | a completed Order Form Template (or equivalent information issued by the Buyer) used to create an Order Contract; |
| **"Order Form Template"** | the template in DPS Schedule 6 (Order Form Template and Order Schedules); |
| **"Order Incorporated Terms"** | the contractual terms applicable to the Order Contract specified under the relevant heading in the Order Form; |
| **"Order Initial Period"** | the Initial Period of an Order Contract specified in the Order Form; |
| **"Order Optional Extension Period"** | such period or periods beyond which the Order Initial Period may be extended up to a maximum of the number of years in total specified in the Order Form; |
| **"Order Procedure"** | the process for awarding an Order Contract pursuant to Clause 2 (How the contract works) and DPS Schedule 7 (Order Procedure); |
| **"Order Special Terms"** | any additional terms and conditions specified in the Order Form incorporated into the applicable Order Contract; |
| **"Order Start Date"** | the date of start of an Order Contract as stated in the Order Form; |
| **"Order Tender"** | the tender submitted by the Supplier in response to the Buyer's Statement of Requirements following an Order Procedure and set out at Order Schedule 4 (Order Tender); |
| **"Other Contracting Authority"** | any actual or potential Buyer under the DPS Contract; |


© Crown Copyright 2020

| | |
|---|---|
| **"Overhead"** | those amounts which are intended to recover a proportion of the Supplier's or the Key Subcontractor's (as the context requires) indirect corporate costs (including financing, marketing, advertising, research and development and insurance costs and any fines or penalties) but excluding allowable indirect costs apportioned to facilities and administration in the provision of Supplier Staff and accordingly included within limb (a) of the definition of "Costs"; |
| **"Parliament"** | takes its natural meaning as interpreted by Law; |
| **"Party"** | in the context of the DPS Contract, CCS or the Supplier, and in the in the context of an Order Contract the Buyer or the Supplier. "**Parties**" shall mean both of them where the context permits; |
| **"Performance Indicators" or "PIs"** | the performance measurements and targets in respect of the Supplier's performance of the DPS Contract set out in DPS Schedule 4 (DPS Management); |
| **"Personal Data"** | has the meaning given to it in the GDPR; |
| **"Personal Data Breach"** | has the meaning given to it in the GDPR; |
| **"Personnel"** | all directors, officers, employees, agents, consultants and suppliers of a Party and/or of any Subcontractor and/or Subprocessor engaged in the performance of its obligations under a Contract; |
| **"Platform"** | the online application operated on behalf of CCS to facilitate the technical operation of the DPS; |
| **"Prescribed Person"** | a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies; |
| **"Processing"** | has the meaning given to it in the GDPR; |
| **"Processor"** | has the meaning given to it in the GDPR; |
| **"Processor Personnel"** | all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract; |
| **"Progress Meeting"** | a meeting between the Buyer Authorised Representative and the Supplier Authorised Representative; |
| **"Progress Meeting Frequency"** | the frequency at which the Supplier shall conduct a Progress Meeting in accordance with Clause 6.1 as specified in the Order Form; |
| **"Progress Report"** | a report provided by the Supplier indicating the steps taken to achieve Milestones or delivery dates; |


© Crown Copyright 2020

| | |
|---|---|
| **"Progress Report Frequency"** | the frequency at which the Supplier shall deliver Progress Reports in accordance with Clause 6.1 as specified in the Order Form; |
| **"Prohibited Acts"** | a) to directly or indirectly offer, promise or give any person working for or engaged by a Buyer or any other public body a financial or other advantage to:<br>i) induce that person to perform improperly a relevant function or activity; or<br>ii) reward that person for improper performance of a relevant function or activity;<br>b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with each Contract; or<br>c) committing any offence:<br>i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act); or<br>ii) under legislation or common law concerning fraudulent acts; or<br>iii) defrauding, attempting to defraud or conspiring to defraud a Buyer or other public body; or<br>d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct had been carried out in the UK; |
| **"Protective Measures"** | appropriate technical and organisational measures which may include pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it including those outlined in DPS Schedule 9 (Cyber Essentials), if applicable, in the case of the DPS Contract or Order Schedule 9 (Security), if applicable, in the case of an Order Contract; |
| **"Recall"** | a request by the Supplier to return Goods to the Supplier or the manufacturer after the discovery of safety issues or defects (including defects in the right IPR rights) that might endanger health or hinder performance; |
| **"Recipient Party"** | the Party which receives or obtains directly or indirectly Confidential Information; |
| **"Rectification Plan"** | the Supplier's plan (or revised plan) to rectify its breach using the template in Joint Schedule 10 (Rectification Plan Template)which shall include: |


© Crown Copyright 2020

| | |
|---|---|
| | a) full details of the Default that has occurred, including a root cause analysis;<br>b) the actual or anticipated effect of the Default; and<br>c) the steps which the Supplier proposes to take to rectify the Default (if applicable) and to prevent such Default from recurring, including timescales for such steps and for the rectification of the Default (where applicable); |
| **"Rectification Plan Process"** | the process set out in Clause 10.4.3 to 10.4.5 (Rectification Plan Process); |
| **"Regulations"** | the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context requires); |
| **"Reimbursable Expenses"** | the reasonable out of pocket travel and subsistence (for example, hotel and food) expenses, properly and necessarily incurred in the performance of the Services, calculated at the rates and in accordance with the Buyer's expenses policy current from time to time, but not including:<br>a) travel expenses incurred as a result of Supplier Staff travelling to and from their usual place of work, or to and from the premises at which the Services are principally to be performed, unless the Buyer otherwise agrees in advance in writing; and<br>b) subsistence expenses incurred by Supplier Staff whilst performing the Services at their usual place of work, or to and from the premises at which the Services are principally to be performed; |
| **"Relevant Authority"** | the Authority which is party to the Contract to which a right or obligation is owed, as the context requires; |
| **"Relevant Authority's Confidential Information"** | a) all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, property rights, trade secrets, Know-How and IPR of the Relevant Authority (including all Relevant Authority Existing IPR and New IPR);<br>b) any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered confidential which comes (or has come) to the Relevant Authority's attention or into the Relevant Authority's possession in connection with a Contract; and<br>information derived from any of the above; |
| **"Relevant Requirements"** | all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State pursuant to section 9 of the Bribery Act 2010; |


© Crown Copyright 2020

| | |
|---|---|
| **"Relevant Tax Authority"** | HMRC, or, if applicable, the tax authority in the jurisdiction in which the Supplier is established; |
| **"Reminder Notice"** | a notice sent in accordance with Clause 10.6 given by the Supplier to the Buyer providing notification that payment has not been received on time; |
| **"Replacement Deliverables"** | any deliverables which are substantially similar to any of the Deliverables and which the Buyer receives in substitution for any of the Deliverables following the Order Expiry Date, whether those goods are provided by the Buyer internally and/or by any third party; |
| **"Replacement Subcontractor"** | a Subcontractor of the Replacement Supplier to whom Transferring Supplier Employees will transfer on a Service Transfer Date (or any Subcontractor of any such Subcontractor); |
| **"Replacement Supplier"** | any third party provider of Replacement Deliverables appointed by or at the direction of the Buyer from time to time or where the Buyer is providing Replacement Deliverables for its own account, shall also include the Buyer; |
| **"Request For Information"** | a request for information or an apparent request relating to a Contract for the provision of the Deliverables or an apparent request for such information under the FOIA or the EIRs; |
| **"Required Insurances"** | the insurances required by Joint Schedule 3 (Insurance Requirements) or any additional insurances specified in the Order Form; |
| **"Schedules"** | any attachment to a DPS or Order Contract which contains important information specific to each aspect of buying and selling; |
| **"Sectors and Domains"** | the Sectors and Domains Filter Category defined in DPS Schedule 1; |
| **"Security Management Plan"** | the Supplier's security management plan prepared pursuant to Order Schedule 9 (Security) (if applicable); |
| **"Security Policy"** | the Buyer's security policy, referred to in the Order Form, in force as at the Order Start Date (a copy of which has been supplied to the Supplier), as updated from time to time and notified to the Supplier; |
| **"Self Audit Certificate"** | means the certificate in the form as set out in DPS Schedule 8 (Self Audit Certificate); |
| **"Serious Fraud Office"** | the UK Government body named as such as may be renamed or replaced by an equivalent body from time to time; |
| **"Service Levels"** | any service levels applicable to the provision of the Deliverables under the Order Contract (which, where Order Schedule 14 (Service Credits) is used in this Contract, are specified in the Annex to Part A of such Schedule); |


© Crown Copyright 2020

| | |
|---|---|
| **"Service Period"** | has the meaning given to it in the Order Form; |
| **"Services"** | services made available by the Supplier as specified in DPS Schedule 1 (Specification) and in relation to an Order Contract as specified in the Order Form; |
| **"Service Transfer"** | any transfer of the Deliverables (or any part of the Deliverables), for whatever reason, from the Supplier or any Subcontractor to a Replacement Supplier or a Replacement Subcontractor; |
| **"Service Transfer Date"** | the date of a Service Transfer; |
| **"Service Type"** | means the Service Types Filter Category detailed in DPS Schedule 1 |
| **"Sites"** | any premises (including the Buyer Premises, the Supplier's premises or third party premises) from, to or at which:<br>a) the Deliverables are (or are to be) provided; or<br>b) the Supplier manages, organises or otherwise directs the provision or the use of the Deliverables; |
| **"SME"** | an enterprise falling within the category of micro, small and medium sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium enterprises; |
| **"Special Terms"** | any additional Clauses set out in the DPS Appointment Form or Order Form which shall form part of the respective Contract; |
| **"Specific Change in Law"** | a Change in Law that relates specifically to the business of the Buyer and which would not affect a Comparable Supply where the effect of that Specific Change in Law on the Deliverables is not reasonably foreseeable at the Start Date; |
| **"Specification"** | the specification set out in DPS Schedule 1 (Specification), as may, in relation to an Order Contract, be supplemented by the Order Form; |
| **"Standards"** | any:<br>a) standards published by BSI British Standards, the National Standards Body of the United Kingdom, the International Organisation for Standardisation or other reputable or equivalent bodies (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with;<br>b) standards detailed in the specification in DPS Schedule 1 (Specification); |


© Crown Copyright 2020

| | |
|---|---|
| | c) standards detailed by the Buyer in the Order Form or agreed between the Parties from time to time;<br>d) relevant Government codes of practice and guidance applicable from time to time; |
| **"Start Date"** | in the case of the DPS Contract, the date specified on the DPS Appointment Form, and in the case of an Order Contract, the date specified in the Order Form; |
| **"Statement of Requirements"** | a statement issued by the Buyer detailing its requirements in respect of Deliverables issued in accordance with the Order Procedure; |
| **"Storage Media"** | the part of any device that is capable of storing and retrieving data; |
| **"Sub-Contract"** | any contract or agreement (or proposed contract or agreement), other than an Order Contract or the DPS Contract, pursuant to which a third party:<br>a) provides the Deliverables (or any part of them);<br>b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or<br>c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them); |
| **"Subcontractor"** | any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person; |
| **"Subprocessor"** | any third party appointed to process Personal Data on behalf of that Processor related to a Contract; |
| **"Supplier"** | the person, firm or company identified in the DPS Appointment Form; |
| **"Supplier Assets"** | all assets and rights used by the Supplier to provide the Deliverables in accordance with the Order Contract but excluding the Buyer Assets; |
| **"Supplier Authorised Representative"** | the representative appointed by the Supplier named in the DPS Appointment Form, or later defined in an Order Contract; |
| **"Supplier's Confidential Information"** | a) any information, however it is conveyed, that relates to the business, affairs, developments, IPR of the Supplier (including the Supplier Existing IPR) trade secrets, Know-How, and/or personnel of the Supplier;<br>b) any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential and which comes (or has come) to the Supplier's attention or into the Supplier's possession in connection with a Contract;<br>c) Information derived from any of (a) and (b) above; |


© Crown Copyright 2020

| | |
|---|---|
| **"Supplier's Contract Manager"** | the person identified in the Order Form appointed by the Supplier to oversee the operation of the Order Contract and any alternative person whom the Supplier intends to appoint to the role, provided that the Supplier informs the Buyer prior to the appointment; |
| **"Supplier Equipment"** | the Supplier's hardware, computer and telecoms devices, equipment, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from the Buyer) in the performance of its obligations under this Order Contract; |
| **"Supplier Non-Performance"** | where the Supplier has failed to:<br>a) Achieve a Milestone by its Milestone Date;<br>b) provide the Goods and/or Services in accordance with the Service Levels ; and/or<br>c) comply with an obligation under a Contract; |
| **"Supplier Profit"** | in relation to a period, the difference between the total Charges (in nominal cash flow terms but excluding any Deductions and total Costs (in nominal cash flow terms) in respect of an Order Contract for the relevant period; |
| **"Supplier Profit Margin"** | in relation to a period or a Milestone (as the context requires), the Supplier Profit for the relevant period or in relation to the relevant Milestone divided by the total Charges over the same period or in relation to the relevant Milestone and expressed as a percentage; |
| **"Supplier Staff"** | all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor engaged in the performance of the Supplier's obligations under a Contract; |
| **"Supply Chain Information Report Template"** | the document at Annex 1 of Joint Schedule 12 (Supply Chain Visibility); |
| **"Supporting Documentation"** | sufficient information in writing to enable the Buyer to reasonably assess whether the Charges, Reimbursable Expenses and other sums due from the Buyer under the Order Contract detailed in the information are properly payable; |
| **"Termination Notice"** | a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate a Contract on a specified date and setting out the grounds for termination; |
| **"Test"** | any test required to be carried out pursuant to the Order Contract i) as set out in the Test Plan agreed pursuant to Part B of Order Schedule 13, ii) or as specified elsewhere in this Order Contract, and "Testing" and "Tested" shall be construed accordingly; |


© Crown Copyright 2020

| | |
|---|---|
| **"Third Party IPR"** | Intellectual Property Rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables; |
| **"Transferring Supplier Employees"** | those employees of the Supplier and/or the Supplier's Subcontractors to whom the Employment Regulations will apply on the Service Transfer Date; |
| **"Transparency Information"** | the Transparency Reports and the content of a Contract, including any changes to this Contract agreed from time to time, except for –<br>(i) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Relevant Authority; and<br>(ii) Commercially Sensitive Information; |
| **"Transparency Reports"** | the information relating to the Deliverables and performance of the Contracts which the Supplier is required to provide to the Buyer in accordance with the reporting requirements in Order Schedule 1 (Transparency Reports); |
| **"US-EU Privacy Shield Register"** | a list of companies maintained by the United States of America Department for Commence that have self-certified their commitment to adhere to the European legislation relating to the processing of personal data to non-EU countries which is available online at: https://www.privacyshield.gov/list; |
| **"Variation"** | has the meaning given to it in Clause 24 (Changing the contract); |
| **"Variation Form"** | the form set out in Joint Schedule 2 (Variation Form); |
| **"Variation Procedure"** | the procedure set out in Clause 24 (Changing the contract); |
| **"VAT"** | value added tax in accordance with the provisions of the Value Added Tax Act 1994; |
| **"VCSE"** | a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives; |
| **"Worker"** | any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; and |
| **"Working Day"** | any day other than a Saturday or Sunday or public holiday in England and Wales unless specified otherwise by the Parties in the Order Form. |


© Crown Copyright 2020

# Joint Schedule 2 (Variation Form)

This form is to be used in order to change a contract in accordance with Clause 24 (Changing the Contract)

| **Contract Details** | |
|---|---|
| This variation is between: | **[delete** as applicable: CCS / Buyer**]** (**"CCS" "the Buyer"**)<br>And<br>**[insert** name of Supplier**]** (**"the Supplier"**) |
| Contract name: | **[insert** name of contract to be changed] **("the Contract")** |
| Contract reference number: | **[insert** contract reference number] |
| **Details of Proposed Variation** | |
| Variation initiated by: | **[delete** as applicable: CCS/Buyer/Supplier] |
| Variation number: | **[insert** variation number] |
| Date variation is raised: | **[insert** date] |
| Proposed variation | |


© Crown Copyright 2020

| | | |
|---|---|---|
| Reason for the variation: | **[insert** reason] | |
| An Impact Assessment shall be provided within: | **[insert** number] days | |
| **Impact of Variation** | | |
| Likely impact of the proposed variation: | **[Supplier to insert** assessment of impact] | |
| **Outcome of Variation** | | |
| Contract variation: | This Contract detailed above is varied as follows:<br>• **[CCS/Buyer to insert** original Clauses or Paragraphs to be varied and the changed clause] | |
| Financial variation: | Original Contract Value: | £ **[insert** amount] |
| | Additional cost due to variation: | £ **[insert** amount] |
| | New Contract value: | £ **[insert** amount] |

1. This Variation must be agreed and signed by both Parties to the Contract and shall only be effective from the date it is signed by **[delete** as applicable: CCS / Buyer**]**

2. Words and expressions in this Variation shall have the meanings given to them in the Contract.

3. The Contract, including any previous Variations, shall remain effective and unaltered except as amended by this Variation.


© Crown Copyright 2020

Signed by an authorised signatory for and on behalf of the **[delete** as applicable: CCS / Buyer**]**

Signature .....

Date .....

Name (in Capitals) .....

Address .....

.....

Signed by an authorised signatory to sign for and on behalf of the Supplier

Signature .....

Date .....

Name (in Capitals) .....

Address .....


© Crown Copyright 2020

# Joint Schedule 3 (Insurance Requirements)

## 2. The insurance you need to have

2.1 The Supplier shall take out and maintain, or procure the taking out and maintenance of the insurances as set out in the Annex to this Schedule, any additional insurances required under an Order Contract (specified in the applicable Order Form) ("**Additional Insurances**") and any other insurances as may be required by applicable Law (together the "**Insurances**"). The Supplier shall ensure that each of the Insurances is effective no later than:

2.1.1 the DPS Start Date in respect of those Insurances set out in the Annex to this Schedule and those required by applicable Law; and

2.1.2 the Order Contract Effective Date in respect of the Additional Insurances.

2.2 The Insurances shall be:

2.2.1 maintained in accordance with Good Industry Practice;

2.2.2 (so far as is reasonably practicable) on terms no less favourable than those generally available to a prudent contractor in respect of risks insured in the international insurance market from time to time;

2.2.3 taken out and maintained with insurers of good financial standing and good repute in the international insurance market; and

2.2.4 maintained for at least six (6) years after the End Date.

2.3 The Supplier shall ensure that the public and products liability policy contain an indemnity to principals clause under which the Relevant Authority shall be indemnified in respect of claims made against the Relevant Authority in respect of death or bodily injury or third party property damage arising out of or in connection with the Deliverables and for which the Supplier is legally liable.

## 3. How to manage the insurance

3.1 Without limiting the other provisions of this Contract, the Supplier shall:

3.1.1 take or procure the taking of all reasonable risk management and risk control measures in relation to Deliverables as it would be reasonable to expect of a prudent contractor acting in accordance with Good Industry Practice, including the investigation and reports of relevant claims to insurers;

3.1.2 promptly notify the insurers in writing of any relevant material fact under any Insurances of which the Supplier is or becomes aware; and

3.1.3 hold all policies in respect of the Insurances and cause any insurance broker effecting the Insurances to hold any insurance slips and other


© Crown Copyright 2020

evidence of placing cover representing any of the Insurances to which it is a party.

## 4. What happens if you aren't insured

4.1 The Supplier shall not take any action or fail to take any action or (insofar as is reasonably within its power) permit anything to occur in relation to it which would entitle any insurer to refuse to pay any claim under any of the Insurances.

4.2 Where the Supplier has failed to purchase or maintain any of the Insurances in full force and effect, the Relevant Authority may elect (but shall not be obliged) following written notice to the Supplier to purchase the relevant Insurances and recover the reasonable premium and other reasonable costs incurred in connection therewith as a debt due from the Supplier.

## 5. Evidence of insurance you must provide

5.1 The Supplier shall upon the Start Date and within 15 Working Days after the renewal of each of the Insurances, provide evidence, in a form satisfactory to the Relevant Authority, that the Insurances are in force and effect and meet in full the requirements of this Schedule.

## 6. Making sure you are insured to the required amount

6.1 The Supplier shall ensure that any Insurances which are stated to have a minimum limit "in the aggregate" are maintained at all times for the minimum limit of indemnity specified in this Contract and if any claims are made which do not relate to this Contract then the Supplier shall notify the Relevant Authority and provide details of its proposed solution for maintaining the minimum limit of indemnity.

## 7. Cancelled Insurance

7.1 The Supplier shall notify the Relevant Authority in writing at least five (5) Working Days prior to the cancellation, suspension, termination or non-renewal of any of the Insurances.

7.2 The Supplier shall ensure that nothing is done which would entitle the relevant insurer to cancel, rescind or suspend any insurance or cover, or to treat any insurance, cover or claim as voided in whole or part. The Supplier shall use all reasonable endeavours to notify the Relevant Authority (subject to third party confidentiality obligations) as soon as practicable when it becomes aware of any relevant fact, circumstance or matter which has caused, or is reasonably likely to provide grounds to, the relevant insurer to give notice to cancel, rescind, suspend or void any insurance, or any cover or claim under any insurance in whole or in part.

## 8. Insurance claims

8.1 The Supplier shall promptly notify to insurers any matter arising from, or in relation to, the Deliverables, or each Contract for which it may be entitled to


© Crown Copyright 2020

claim under any of the Insurances. In the event that the Relevant Authority receives a claim relating to or arising out of a Contract or the Deliverables, the Supplier shall co-operate with the Relevant Authority and assist it in dealing with such claims including without limitation providing information and documentation in a timely manner.

8.2 Except where the Relevant Authority is the claimant party, the Supplier shall give the Relevant Authority notice within twenty (20) Working Days after any insurance claim in excess of 10% of the sum required to be insured pursuant to Paragraph 5.1 relating to or arising out of the provision of the Deliverables or this Contract on any of the Insurances or which, but for the application of the applicable policy excess, would be made on any of the Insurances and (if required by the Relevant Authority) full details of the incident giving rise to the claim.

8.3 Where any Insurance requires payment of a premium, the Supplier shall be liable for and shall promptly pay such premium.

8.4 Where any Insurance is subject to an excess or deductible below which the indemnity from insurers is excluded, the Supplier shall be liable for such excess or deductible. The Supplier shall not be entitled to recover from the Relevant Authority any sum paid by way of excess or deductible under the Insurances whether under the terms of this Contract or otherwise.


© Crown Copyright 2020

## ANNEX: REQUIRED INSURANCES

1. The Supplier shall hold the following [standard] insurance cover from the DPS Start Date in accordance with this Schedule:

   1.1 professional indemnity insurance with cover (for a single event or a series of related events and in the aggregate) of not less than one million pounds (£1,000,000);

   1.2 public liability insurance [with cover (for a single event or a series of related events and in the aggregate)] of not less than five million pounds (£5,000,000); and

   1.3 employer's liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000).


© Crown Copyright 2020

# Joint Schedule 4 (Commercially Sensitive Information)

## 2. What is the Commercially Sensitive Information?

2.1 In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

2.2 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 applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

2.3 Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

| No. | Date | Item(s) | Duration of Confidentiality |
|---|---|---|---|
| | [insert date] | [insert details] | [insert duration] |


© Crown Copyright 2020

# Joint Schedule 5 (Corporate Social Responsibility)

## 1. What we expect from our Suppliers

1.1 In September 2017, HM Government published a Supplier Code of Conduct setting out the standards and behaviours expected of suppliers who work with government. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/646497/2017-09-13_Official_Sensitive_Supplier_Code_of_Conduct_September_2017.pdf)

1.2 CCS expects its suppliers and subcontractors to meet the standards set out in that Code. In addition, CCS expects its suppliers and subcontractors to comply with the standards set out in this Schedule.

1.3 The Supplier acknowledges that the Buyer may have additional requirements in relation to corporate social responsibility. The Buyer expects that the Supplier and its Subcontractors will comply with such corporate social responsibility requirements as the Buyer may notify to the Supplier from time to time.

## 2. Equality and Accessibility

2.1 In addition to legal obligations, the Supplier shall support CCS and the Buyer in fulfilling its Public Sector Equality duty under S149 of the Equality Act 2010 by ensuring that it fulfils its obligations under each Contract in a way that seeks to:

2.1.1 eliminate discrimination, harassment or victimisation of any kind; and

2.1.2 advance equality of opportunity and good relations between those with a protected characteristic (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership) and those who do not share it.

## 3. Modern Slavery, Child Labour and Inhumane Treatment

**"Modern Slavery Helpline"** means the mechanism for reporting suspicion, seeking help or advice and information on the subject of modern slavery available online at https://www.modernslaveryhelpline.org/report or by telephone on 08000 121 700.

3.1 The Supplier:

3.1.1 shall not use, nor allow its Subcontractors to use forced, bonded or involuntary prison labour;

3.1.2 shall not require any Supplier Staff or Subcontractor Staff to lodge deposits or identify papers with the Employer and shall be free to leave their employer after reasonable notice;


© Crown Copyright 2020

3.1.3 warrants and represents that it has not been convicted of any slavery or human trafficking offences anywhere around the world.

3.1.4 warrants that to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere around the world.

3.1.5 shall make reasonable enquires to ensure that its officers, employees and Subcontractors have not been convicted of slavery or human trafficking offences anywhere around the world.

3.1.6 shall have and maintain throughout the term of each Contract its own policies and procedures to ensure its compliance with the Modern Slavery Act and include in its contracts with its Subcontractors anti-slavery and human trafficking provisions;

3.1.7 shall implement due diligence procedures to ensure that there is no slavery or human trafficking in any part of its supply chain performing obligations under a Contract;

3.1.8 shall prepare and deliver to CCS, an annual slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business with its annual certification of compliance with Paragraph 3;

3.1.9 shall not use, nor allow its employees or Subcontractors to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its employees or Subcontractors;

3.1.10 shall not use or allow child or slave labour to be used by its Subcontractors;

3.1.11 shall report the discovery or suspicion of any slavery or trafficking by it or its Subcontractors to CCS, the Buyer and Modern Slavery Helpline.

## 4. Income Security

4.1 The Supplier shall:

4.1.1 ensure that all wages and benefits paid for a standard working week meet, at a minimum, national legal standards in the country of employment;

4.1.2 ensure that all Supplier Staff are provided with written and understandable Information about their employment conditions in respect of wages before they enter;

4.1.3 ensure that all workers are provided with written and understandable Information about their employment conditions in respect of wages


© Crown Copyright 2020

before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid;

4.1.4 not make deductions from wages:

(a) as a disciplinary measure

(b) except where permitted by law; or

(c) without expressed permission of the worker concerned;

4.1.5 record all disciplinary measures taken against Supplier Staff; and

4.1.6 ensure that Supplier Staff are engaged under a recognised employment relationship established through national law and practice.

## 5. Working Hours

5.1 The Supplier shall:

5.1.1 ensure that the working hours of Supplier Staff comply with national laws, and any collective agreements;

5.1.2 ensure that the working hours of Supplier Staff, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week unless the individual has agreed in writing;

5.1.3 ensure that use of overtime is used responsibly, taking into account:

(a) the extent;

(b) frequency; and

(c) hours worked;

by individuals and by the Supplier Staff as a whole;

5.2 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by Paragraph 5.3 below.

5.3 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

5.3.1 this is allowed by national law;

5.3.2 this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;

5.3.3 appropriate safeguards are taken to protect the workers' health and safety; and

5.3.4 the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

5.4 All Supplier Staff shall be provided with at least one (1) day off in every seven (7) day period or, where allowed by national law, two (2) days off in every fourteen (14) day period.


© Crown Copyright 2020

## 6. Sustainability

6.1 The supplier shall meet the applicable Government Buying Standards applicable to Deliverables which can be found online at:

https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs


© Crown Copyright 2020

# Joint Schedule 6 (Key Subcontractors)

## 3. Restrictions on certain subcontractors

3.1 The Supplier is entitled to sub-contract its obligations under the DPS Contract to the Key Subcontractors identified on the Platform.

3.2 The Supplier is entitled to sub-contract its obligations under an Order Contract to Key Subcontractors listed on the Platform who are specifically nominated in the Order Form.

3.3 Where during the Contract Period the Supplier wishes to enter into a new Key Sub-contract or replace a Key Subcontractor, it must obtain the prior written consent of CCS and the Buyer and the Supplier shall, at the time of requesting such consent, provide CCS and the Buyer with the information detailed in Paragraph 1.4. The decision of CCS and the Buyer to consent or not will not be unreasonably withheld or delayed. Where CCS consents to the appointment of a New Key Subcontractor then they will be added to the Platform. Where the Buyer consents to the appointment of a New Key Subcontractor then they will be added to the Key Subcontractor section of the Order Form. CCS and the Buyer may reasonably withhold their consent to the appointment of a Key Subcontractor if it considers that:

3.3.1 the appointment of a proposed Key Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;

3.3.2 the proposed Key Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or

3.3.3 the proposed Key Subcontractor employs unfit persons.

3.4 The Supplier shall provide CCS and the Buyer with the following information in respect of the proposed Key Subcontractor:

3.4.1 the proposed Key Subcontractor’s name, registered office and company registration number;

3.4.2 the scope/description of any Deliverables to be provided by the proposed Key Subcontractor;

3.4.3 where the proposed Key Subcontractor is an Affiliate of the Supplier, evidence that demonstrates to the reasonable satisfaction of the CCS and the Buyer that the proposed Key Sub-Contract has been agreed on "arm’s-length" terms;

3.4.4 for CCS, the Key Sub-Contract price expressed as a percentage of the total projected DPS Price over the DPS Contract Period;

3.4.5 for the Buyer, the Key Sub-Contract price expressed as a percentage of the total projected Charges over the Order Contract Period; and


© Crown Copyright 2020

3.5 If requested by CCS and/or the Buyer, within ten (10) Working Days of receipt of the information provided by the Supplier pursuant to Paragraph 1.4, the Supplier shall also provide:

3.5.1 a copy of the proposed Key Sub-Contract; and

3.5.2 any further information reasonably requested by CCS and/or the Buyer.

3.6 The Supplier shall ensure that each new or replacement Key Sub-Contract shall include:

3.6.1 provisions which will enable the Supplier to discharge its obligations under the Contracts;

3.6.2 a right under CRTPA for CCS and the Buyer to enforce any provisions under the Key Sub-Contract which confer a benefit upon CCS and the Buyer respectively;

3.6.3 a provision enabling CCS and the Buyer to enforce the Key Sub-Contract as if it were the Supplier;

3.6.4 a provision enabling the Supplier to assign, novate or otherwise transfer any of its rights and/or obligations under the Key Sub-Contract to CCS and/or the Buyer;

3.6.5 obligations no less onerous on the Key Subcontractor than those imposed on the Supplier under the DPS Contract in respect of:

(a) the data protection requirements set out in Clause 14 (Data protection);

(b) the FOIA and other access request requirements set out in Clause 16 (When you can share information);

(c) the obligation not to embarrass CCS or the Buyer or otherwise bring CCS or the Buyer into disrepute;

(d) the keeping of records in respect of the goods and/or services being provided under the Key Sub-Contract, including the maintenance of Open Book Data; and

(e) the conduct of audits set out in Clause 6 (Record keeping and reporting);

3.6.6 provisions enabling the Supplier to terminate the Key Sub-Contract on notice on terms no more onerous on the Supplier than those imposed on CCS and the Buyer under Clauses 10.4 (When CCS or the Buyer can end this contract) and 10.5 (What happens if the contract ends) of this Contract; and

3.6.7 a provision restricting the ability of the Key Subcontractor to sub-contract all or any part of the provision of the Deliverables provided to the Supplier under the Key Sub-Contract without first seeking the written consent of CCS and the Buyer.


© Crown Copyright 2020

# Joint Schedule 10 (Rectification Plan)

| **Request for [Revised] Rectification Plan** | | | |
|---|---|---|---|
| Details of the Default: | [**Guidance:** Explain the Default, with clear schedule and clause references as appropriate] | | |
| Deadline for receiving the [Revised] Rectification Plan: | [**add** date (minimum 10 days from request)] | | |
| Signed by [CCS/Buyer] : | | Date: | |
| **Supplier [Revised] Rectification Plan** | | | |
| Cause of the Default | [**add** cause] | | |
| Anticipated impact assessment: | [**add** impact] | | |
| Actual effect of Default: | [**add** effect] | | |
| Steps to be taken to rectification: | **Steps** | **Timescale** | |
| | 1. | [date] | |
| | 2. | [date] | |
| | 3. | [date] | |
| | 4. | [date] | |
| | […] | [date] | |
| Timescale for complete Rectification of Default | [X] Working Days | | |
| Steps taken to prevent recurrence of Default | **Steps** | **Timescale** | |
| | 1. | [date] | |
| | 2. | [date] | |
| | 3. | [date] | |
| | 4. | [date] | |
| | […] | [date] | |
| Signed by the Supplier: | | Date: | |
| **Review of Rectification Plan [CCS/Buyer]** | | | |


© Crown Copyright 2020

| | | | |
|---|---|---|---|
| Outcome of review | [Plan Accepted] [Plan Rejected] [Revised Plan Requested] | | |
| Reasons for Rejection (if applicable) | [**add** reasons] | | |
| Signed by [CCS/Buyer] | | Date: | |


© Crown Copyright 2020

# Joint Schedule 11 (Processing Data)

**Status of the Controller**

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA. A Party may act as:

(a) "Controller" in respect of the other Party who is "Processor";

(b) "Processor" in respect of the other Party who is "Controller";

(c) "Joint Controller" with the other Party;

(d) "Independent Controller" of the Personal Data where there other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(Processing Personal Data)* which scenario they think shall apply in each situation.

**Where one Party is Controller and the other Party its Processor**

2. Where a Party is a Processor, the only processing that it is authorised to do is listed in Annex 1 *(Processing Personal Data*) by the Controller.

3. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

4. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:


© Crown Copyright 2020

(a) Process that Personal Data only in accordance with Annex 1 *(Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that :

(i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 *(Processing Personal Data*));

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);

(B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

(i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;

(ii) the Data Subject has enforceable rights and effective legal remedies;


© Crown Copyright 2020

(iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and

(iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and

(e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.

6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:

(a) receives a Data Subject Request (or purported Data Subject Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event.

7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller in phases, as details become available.

8. Taking into account the nature of the Processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;


© Crown Copyright 2020

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Data Loss Event; and/or

(e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

(a) the Controller determines that the Processing is not occasional;

(b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or

(c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

12. Before allowing any Sub-processor to Process any Personal Data related to the Contract, the Processor must:

(a) notify the Controller in writing of the intended Subprocessor and Processing;

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and

(d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

13. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

14. The Relevant Authority may, at any time on not less than 30 Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).


© Crown Copyright 2020

15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

**Where the Parties are Joint Controllers of Personal Data**

16. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

**Independent Controllers of Personal Data**

17. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

18. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.

21. The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under the Contract;

(b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and

(c) where it has recorded it in Annex 1 *(Processing Personal Data).*

22. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational


© Crown Copyright 2020

measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.

23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 GDPR and shall make the record available to the other Party upon reasonable request.

24. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract **("Request Recipient")**:

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

(i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

(ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:

(a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and


© Crown Copyright 2020

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

26. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 *(Processing Personal Data).*

27. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 *(Processing Personal Data)*.

28. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs16 to 27 of this Joint Schedule 11.


© Crown Copyright 2020

Annex 1 - Processing Personal Data A) Template

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.
The contact details of the Relevant Authority's Data Protection Officer are:
**[REDACTED]**

The contact details of the Supplier's Data Protection Officer are: **[REDACTED]**

1.1 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
1.2 Any such further instructions shall be incorporated into this Annex.

| Description | Details |
|---|---|
| Identity of Controller for each Category of Personal Data | **The Relevant Authority is Controller and the Supplier is Processor**<br>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:<br>• Business contact details of any directors, officers, employees, agents, consultants and contractors of Buyer (excluding the Supplier Staff) for which the Buyer is the Controller<br><br>**The Supplier is Controller and the Relevant Authority is Processor**<br><br>*The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Relevant Authority is the Processor in accordance with paragraph 2 to paragraph 15 of the following Personal Data:*<br><br>• **N/A**<br><br>**The Parties are Joint Controllers**<br><br>*The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:* |


© Crown Copyright 2020

| | |
|---|---|
| | • **N/A**<br><br>**The Parties are Independent Controllers of Personal Data**<br><br>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:<br>• Business contact details of Supplier Personnel for which the Supplier is the Controller,<br>• Business contact details of any directors, officers, employees, agents, consultants and contractors of Relevant Authority (excluding the Supplier Personnel) engaged in the performance of the Relevant Authority's duties under the Contract) for which the Relevant Authority is the Controller, |
| Duration of the Processing | No Personal data is processed |
| Nature and purposes of the Processing | N/A |
| Type of Personal Data | N/A |
| Categories of Data Subject | N/A |
| Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to | N/A |


© Crown Copyright 2020

| | |
|---|---|
| preserve that type of data | |


© Crown Copyright 2020

## B) DPS Contract Personal Data Processing

| Description | Details |
|---|---|
| Identity of Controller for each Category of Personal Data | **CCS is Controller and the Supplier is Processor**<br>The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 and for the purposes of the Data Protection Legislation, CCS is the Controller and the Supplier is the Processor of the Personal Data recorded below |
| Duration of the Processing | Up to 7 years after the expiry or termination of the DPS Contract |
| Nature and purposes of the Processing | To facilitate the fulfilment of the Supplier's obligations arising under this DPS Contract including<br>i. Ensuring effective communication between the Supplier and CSS<br>ii. Maintaining full and accurate records of every Order Contract arising under the Framework Agreement in accordance with Core Terms Clause 15 ( Record Keeping and Reporting) |
| Type of Personal Data | Includes:<br>i. Contact details of, and communications with, CSS staff concerned with management of the DPS Contract<br>ii. Contact details of, and communications with, Buyer staff concerned with award and management of Order Contracts awarded under the DPS Contract,<br>iii. Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this DPS Contract<br>Contact details, and communications with Supplier staff concerned with management of the DPS Contract |
| Categories of Data Subject | Includes:<br>i. CSS staff concerned with management of the DPS Contract<br>ii. Buyer staff concerned with award and management of Call-Off Contracts awarded under the DPS Contract |


© Crown Copyright 2020

| | |
|---|---|
| | iii. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from this DPS Contract<br><br>Supplier staff concerned with fulfilment of the Supplier's obligations arising under this DPS Contract |
| 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 | All relevant data to be deleted 7 years after the expiry or termination of this DPS Contract unless longer retention is required by Law or the terms of any Order Contract arising hereunder |

**Annex 2 - Joint Controller Agreement – Not Applicable**


© Crown Copyright 2020

# Order Schedule 1 (Transparency Reports)

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

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

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

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


© Crown Copyright 2020

# Annex A: List of Transparency Reports

| Title | Content | Format | Frequency |
|---|---|---|---|
| Performance against KPI's (as included in the Statement of Requirements) | Format to be agreed post Contract Award. | Excel | Quarterly |
| Social Value | A report showing progress against each of the Social Value commitments set out in the Call-Off Tender | Word | Annually |


© Crown Copyright 2020

# Order Schedule 4 (Order Tender)

**Guidance for Buyers:** If the Supplier's bid has additional detail that you would like included in the contract, insert the Supplier's bid here.

[**REDACTED**]


© Crown Copyright 2020

# Order Schedule 7 (Key Supplier Staff)

3.7 1. The Annex 1 to this Schedule lists the key roles ("**Key Roles**") and names of the persons who the Supplier shall appoint to fill those Key Roles at the Start Date.

3.8

3.9 2. The Supplier shall ensure that the Key Staff fulfil the Key Roles at all times during the Contract Period.

3.10

3.11 3. The Buyer may identify any further roles as being Key Roles and, following agreement to the same by the Supplier, the relevant person selected to fill those Key Roles shall be included on the list of Key Staff.

3.12

3.13 4. The Supplier shall not and shall procure that any Subcontractor shall not remove or replace any Key Staff unless:

3.14

4.1 requested to do so by the Buyer or the Buyer Approves such removal or replacement (not to be unreasonably withheld or delayed);

4.2 the person concerned resigns, retires or dies or is on maternity or long-term sick leave; or

4.3 the person's employment or contractual arrangement with the Supplier or Subcontractor is terminated for material breach of contract by the employee.

3.15 5. The Supplier shall:

5.1 notify the Buyer promptly of the absence of any Key Staff (other than for short-term sickness or holidays of two (2) weeks or less, in which case the Supplier shall ensure appropriate temporary cover for that Key Role);

5.2 ensure that any Key Role is not vacant for any longer than ten (10) Working Days;

5.3 give as much notice as is reasonably practicable of its intention to remove or replace any member of Key Staff and, except in the cases of death, unexpected ill health or a material breach of the Key Staff's employment contract, this will mean at least 1 Months' notice;

5.4 ensure that all arrangements for planned changes in Key Staff provide adequate periods during which incoming and outgoing staff work together to transfer responsibilities and ensure that such change does not have an adverse impact on the provision of the Deliverables; and


© Crown Copyright 2020

5.5 ensure that any replacement for a Key Role has a level of qualifications and experience appropriate to the relevant Key Role and is fully competent to carry out the tasks assigned to the Key Staff whom he or she has replaced.

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


© Crown Copyright 2020

# Annex 1- Key Roles

| Key Role | Key Staff | Contact Details |
|---|---|---|
| Cyber Security Assurance Contractor | TBD | TBD |
| | | |
| | | |
| | | |
| | | |
| | | |


© Crown Copyright 2020

# Order Schedule 8 (Business Continuity and Disaster Recovery)

1. **BCDR PLAN**

1.1 At the Supplier's request, the Customer shall provide the Supplier with a copy of its Business Continuity & Disaster Recovery ("BCDR") Plan.

1.2 The Supplier shall develop a BCDR Plan and ensure that it is linked and integrated with the Buyer's BCDR Plan and the Supplier shall review and amend its BCDR Plan on a regular basis and as soon as is reasonably practicable on receipt of an amended Buyer BCDR Plan from the Buyer.

1.3 The Supplier shall ensure that its Sub-Contractor's BCDR Plans are integrated with the Supplier's BCDR Plan.

1.4 If there is a Disaster, the Parties shall, where applicable, implement their respective BCDR Plans and use all reasonable endeavours to re-establish their capacity to fully perform their obligations under this Order Contract. A Disaster will only relieve a Party of its obligations to the extent it constitutes a Force Majeure Event in accordance with Clause 20 (Circumstances Beyond Your Control).


© Crown Copyright 2020

# Order Schedule 9 (Security)

# Part A: Short Form Security Requirements

## 4. Definitions

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

| | |
|---|---|
| **"Breach of Security"** | the occurrence of:<br>a) any unauthorised access to or use of the Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or<br>b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,<br>in either case as more particularly set out in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 2.2; |
| **"Security Management Plan"** | the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and as updated from time to time; |

## 5. Complying with security requirements and updates to them

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

5.2 The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer as part of its


© Crown Copyright 2020

Order Procedure it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

5.3 Where the Security Policy applies the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

5.4 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Deliverables it may propose a Variation to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall be subject to the Variation Procedure.

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

## 6. Security Standards

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

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

6.2.1 is in accordance with the Law and this Contract;

6.2.2 as a minimum demonstrates Good Industry Practice;

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

6.2.4 where specified by the Buyer in accordance with paragraph 2.2 complies with the Security Policy and the ICT Policy.

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

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


© Crown Copyright 2020

## 7. Security Management Plan

### 7.1 Introduction

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

### 7.2 Content of the Security Management Plan

7.2.1 The Security Management Plan shall:

(a) comply with the principles of security set out in Paragraph 4.2 and any other provisions of this Contract relevant to security;

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

(c) detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Deliverables, processes associated with the provision of the Deliverables, the Buyer Premises, the Sites and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

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

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

(f) set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with paragraph 2.2 the Security Policy; and

(g) be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Deliverables and shall only


© Crown Copyright 2020

reference documents which are in the possession of the Parties or whose location is otherwise specified in this Schedule.

### 7.3 Development of the Security Management Plan

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

7.3.2 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3.1, or any subsequent revision to it in accordance with Paragraph 4.4, is Approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not Approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for Approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

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

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

### 7.4 Amendment of the Security Management Plan

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

(a) emerging changes in Good Industry Practice;

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

(c) where necessary in accordance with paragraph 2.2, any change to the Security Policy;

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


© Crown Copyright 2020

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

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

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

(b) updates to the risk assessments; and

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

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

7.4.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

## 8. Security breach

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

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

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

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

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

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


© Crown Copyright 2020

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

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with paragraph 2.2) or the requirements of this Schedule, then any required change to the Security Management Plan shall be at no cost to the Buyer.


© Crown Copyright 2020

# Part B: Long Form Security Requirements

## 9. Definitions

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

| | |
|---|---|
| **"Breach of Security"** | means the occurrence of:<br>a) any unauthorised access to or use of the Goods and/or Deliverables, the Sites and/or any Information and Communication Technology ("ICT"), information or data (including the Confidential Information and the Government Data) used by the Buyer and/or the Supplier in connection with this Contract; and/or<br>b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Government Data), including any copies of such information or data, used by the Buyer and/or the Supplier in connection with this Contract,<br>in either case as more particularly set out in the security requirements in the Security Policy where the Buyer has required compliance therewith in accordance with paragraph 3.4.3 d; |
| **"ISMS"** | the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Schedule; and |
| **"Security Tests"** | tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security. |

## 10. Security Requirements

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

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


© Crown Copyright 2020

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

**11. [REDACTED]**

11.1 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

11.2 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

11.3 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Government Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Government Data remains under the effective control of the Supplier at all times.

11.4 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

11.5 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

**12. Information Security Management System (ISMS)**

12.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Start Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.6.

12.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Deliverables, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

12.3 The Buyer acknowledges that;

12.3.1 If the Buyer has not stipulated during an Order Procedure that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

12.3.2 Where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's Approval.


© Crown Copyright 2020

12.4 The ISMS shall:

12.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Deliverables and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

12.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 7;

12.4.3 at all times provide a level of security which:

(a) is in accordance with the Law and this Contract;

(b) complies with the Baseline Security Requirements;

(c) as a minimum demonstrates Good Industry Practice;

(d) where specified by a Buyer that has undertaken a Further Competition - complies with the Security Policy and the ICT Policy;

(e) complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4)(https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework)

(f) takes account of guidance issued by the Centre for Protection of National Infrastructure https://www.cpni.gov.uk/

(g) complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm);

(h) meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

(i) addresses issues of incompatibility with the Supplier's own organisational security policies; and

(j) complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 7;

12.4.4 document the security incident management processes and incident response plans;

12.4.5 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the


© Crown Copyright 2020

potential impact on the Deliverables of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

12.4.6 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

12.5 Subject to Paragraph 2 the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

12.6 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

12.7 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the ISMS is not Approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not Approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.6 shall be deemed to be reasonable.

12.8 Approval by the Buyer of the ISMS pursuant to Paragraph 3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

## 13. Security Management Plan

13.1 Within twenty (20) Working Days after the Start Date, the Supplier shall prepare and submit to the Buyer for Approval in accordance with Paragraph


© Crown Copyright 2020

4.3 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

13.2 The Security Management Plan shall:

13.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

13.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with paragraph 3.4.3 d, the Security Policy;

13.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

13.2.4 detail the process for managing any security risks from Subcontractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) and any system that could directly or indirectly have an impact on that information, data and/or the Deliverables;

13.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Deliverables and all processes associated with the delivery of the Deliverables, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any ICT, Information and data (including the Buyer's Confidential Information and the Government Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Deliverables;

13.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Deliverables and all processes associated with the delivery of the Deliverables and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Deliverables comply with the provisions of this Schedule (including the requirements set out in Paragraph 3.4);

13.2.7 demonstrate that the Supplier's approach to delivery of the Deliverables has minimised the Buyer and Supplier effort required to comply with this Schedule through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);


© Crown Copyright 2020

13.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Start Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

13.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

13.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

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

13.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is Approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for Approval. The Parties shall use all reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

13.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Schedule.

## 14. Amendment of the ISMS and Security Management Plan

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

14.1.1 emerging changes in Good Industry Practice;

14.1.2 any change or proposed change to the Supplier System, the Deliverables and/or associated processes;

14.1.3 any new perceived or changed security threats;

14.1.4 where required in accordance with paragraph 3.4.3 d, any changes to the Security Policy;


© Crown Copyright 2020

14.1.5 any new perceived or changed security threats; and

14.1.6 any reasonable change in requirement requested by the Buyer.

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

14.2.1 suggested improvements to the effectiveness of the ISMS;

14.2.2 updates to the risk assessments;

14.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

14.2.4 suggested improvements in measuring the effectiveness of controls.

14.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to Annex nnex **1** (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Buyer.

14.4 The Buyer may, acting reasonably, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the purposes of formalising and documenting the relevant change or amendment.

## 15. Security Testing

15.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Deliverables and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

15.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.


© Crown Copyright 2020

15.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Deliverables so as to meet the KPIs, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

15.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Baseline Security Requirements) to this Schedule) or the requirements of this Schedule, the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

15.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

## 16. Complying with the ISMS

16.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with paragraph 3.4.3 d.

16.2 If, on the basis of evidence provided by such security audits, it is the Buyer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy are not being achieved by the Supplier, then the Buyer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to implement and remedy. If the Supplier does not become compliant within the required time then the Buyer shall have the right to obtain an independent audit against these standards in whole or in part.


© Crown Copyright 2020

16.3 If, as a result of any such independent audit as described in Paragraph the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

## 17. Security Breach

17.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

17.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

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

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

(b) remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Property and/or Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

(c) apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Deliverables so as to meet the relevant Service Level Performance Indicators, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

(d) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

(e) supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and


© Crown Copyright 2020

(f) as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

17.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Schedule, then any required change to the ISMS shall be at no cost to the Buyer.

## 18. Vulnerabilities and fixing them

18.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the ICT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

18.2 The severity of threat vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

18.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

18.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

18.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

18.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

18.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or


© Crown Copyright 2020

18.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

18.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

18.4.1 where upgrading such COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

18.4.2 is agreed with the Buyer in writing.

18.5 The Supplier shall:

18.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

18.5.2 ensure that the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

18.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the ICT Environment by actively monitoring the threat landscape during the Contract Period;

18.5.4 pro-actively scan the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.4.5;

18.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each Month detailing both patched and outstanding vulnerabilities in the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

18.5.6 propose interim mitigation measures to vulnerabilities in the ICT Environment known to be exploitable where a security patch is not immediately available;


© Crown Copyright 2020

18.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the ICT Environment); and

18.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the ICT Environment and provide initial indications of possible mitigations.

18.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

18.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.


© Crown Copyright 2020

# Part B – Annex 1:

# Baseline security requirements

## 1. Handling Classified information

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

## 2. End user devices

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

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

## 3. Data Processing, Storage, Management and Destruction

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

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


© Crown Copyright 2020

3.3 The Supplier shall:

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

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

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

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

## 4. Ensuring secure communications

4.1 The Buyer requires that any Government Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using a product or system component which has been formally assured through a certification process recognised by CESG, to at least Foundation Grade, for example, under CPA.

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

## 5. Security by design

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

5.2 When designing and configuring the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a CESG Certified Professional certification (https://www.ncsc.gov.uk/articles/cesg-certification-ia-professionals-and-guidance-certification-ia-professionals-documents) for all bespoke or complex components of the ICT Environment (to the extent that the ICT Environment is within the control of the Supplier).

## 6. Security of Supplier Staff

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

6.2 The Supplier shall agree on a case by case basis Supplier Staff roles which require specific government clearances (such as 'SC') including system


© Crown Copyright 2020

administrators with privileged access to IT systems which store or process Government Data.

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

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

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

## 7. Restricting and monitoring access

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

## 8. Audit

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

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

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


© Crown Copyright 2020

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

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


© Crown Copyright 2020

# Part B – Annex 2 - Security Management Plan

[ ]


© Crown Copyright 2020

# Order Schedule 15 (Order Contract Management)

2. DEFINITIONS

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

| | |
|---|---|
| **"Operational Board"** | the board established in accordance with paragraph 5.1 of this Schedule; |
| **"Project Manager"** | the manager appointed in accordance with paragraph 2.1 of this Schedule; |

3. PROJECT MANAGEMENT

3.1 The Supplier and the Buyer shall each appoint a Project Manager for the purposes of this Contract through whom the provision of the Services and the Deliverables shall be managed day-to-day.

3.2 The Parties shall ensure that appropriate resource is made available on a regular basis such that the aims, objectives and specific provisions of this Contract can be fully realised.

3.3 Without prejudice to paragraph 4 below, the Parties agree to operate the boards specified as set out in the Annex to this Schedule.

4. ROLE OF THE SUPPLIER CONTRACT MANAGER

The Supplier's Contract Manager shall be:

4.1.1 the primary point of contact to receive communication from the Buyer and will also be the person primarily responsible for providing information to the Buyer;

4.1.2 able to delegate his position to another person at the Supplier but must inform the Buyer before proceeding with the delegation and it will be the delegated person's responsibility to fulfil the Contract Manager's responsibilities and obligations;

4.1.3 able to cancel any delegation and recommence the position himself; and

4.1.4 replaced only after the Buyer has received notification of the proposed change.


© Crown Copyright 2020

The Buyer may provide revised instructions to the Supplier's Contract Manager in regards to the Contract and it will be the Supplier's Contract Manager's responsibility to ensure the information is provided to the Supplier and the actions implemented.

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

5. CONTRACT RISK MANAGEMENT

Both Parties shall pro-actively manage risks attributed to them under the terms of this Order Contract.

The Supplier shall develop, operate, maintain and amend, as agreed with the Buyer, processes for:

5.1.1 the identification and management of risks;

the identification and management of issues; and

monitoring and controlling project plans.

The Supplier allows the Buyer to inspect at any time within working hours the accounts and records which the Supplier is required to keep.

The Supplier will maintain a risk register of the risks relating to the Order Contract which the Buyer and the Supplier have identified.

**9.**

6. Role of the Operational Board

6.1 The Operational Board shall be established by the Buyer for the purposes of this Contract on which the Supplier and the Buyer shall be represented.

6.2 The Operational Board members, frequency and location of board meetings and planned start date by which the board shall be established are set out in the Order Form.

6.3 In the event that either Party wishes to replace any of its appointed board members, that Party shall notify the other in writing for approval by the other Party (such approval not to be unreasonably withheld or delayed). Each Buyer board member shall have at all times a counterpart Supplier board member of equivalent seniority and expertise.

6.4 Each Party shall ensure that its board members shall make all reasonable efforts to attend board meetings at which that board member’s attendance is required. If any board member is not able to attend a board meeting, that person shall use all reasonable endeavours to ensure that a delegate attends the Operational Board meeting in his/her place (wherever possible) and that


© Crown Copyright 2020

the delegate is properly briefed and prepared and that he/she is debriefed by such delegate after the board meeting.

6.5 The purpose of the Operational Board meetings will be to review the Supplier's performance under this Contract. The agenda for each meeting shall be set by the Buyer and communicated to the Supplier in advance of that meeting.

# Annex: Contract Boards

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

**Quarterly performance review meetings to be held virtually. Agendas to be agreed in advance.**


© Crown Copyright 2020

# Order Schedule 20 (Order Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Order Contract

Microsoft Word Document


© Crown Copyright 2020

# Order Schedule 22 – Secret Matters

**Associated definitions:**

In this Order Schedule 22, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

| | |
|---|---|
| **"Document"** | includes specifications, plans, drawings, photographs and books; |
| **"Secret Matter"** | means any matter connected with or arising out of the performance of this Order Contract which has been, or may hereafter be, by a notice in writing given by the Customer to the Supplier be designated 'top secret', 'secret', or 'confidential'; |
| **"Servant"** | where the Supplier is a body corporate shall include a director of that body and any person occupying in relation to that body the position of director by whatever name called. |

## 1. Disclosure

1.1 The Supplier shall not, either before or after the completion or termination of this Order Contract, do or permit to be done anything which it knows or ought reasonably to know may result in information about a Secret Matter being:

1.1.1 without the prior consent in writing of the Buyer, disclosed to or acquired by a person who is an alien or who is a British subject by virtue only of a certificate of naturalisation in which his name was included;

1.1.2 disclosed to or acquired by a person as respects whom the Buyer has given to the Supplier a notice in writing which has not been cancelled stating that the Buyer requires that Secret Matters shall not be disclosed to that person;

1.1.3 without the prior consent in writing of the Buyer, disclosed to or acquired by any person who is not a Servant of the Supplier; or

1.1.4 disclosed to or acquired by a person who is an employee of the Supplier except in a case where it is necessary for the proper performance of this Order Contract that such person shall have the information.

## 2. Safeguarding

2.1 Without prejudice to the provisions of Paragraph 1, the Supplier shall, both before and after the completion or termination of this Order Contract, take all reasonable steps to ensure:


© Crown Copyright 2020

2.1.1 no such person as is mentioned in Paragraph 1.1, 1.1.1 or 1.1.2, thereof shall have access to any item or Document under the control of the Supplier containing information about a Secret Matter except with the prior consent in writing of the Buyer;

2.1.2 that no visitor to any premises in which there is any item to be supplied under this Order Contract or where Goods are being supplied shall see or discuss with the Supplier or any person employed by him any Secret Matter unless the visitor is authorised in writing by the Buyer so to do;

2.1.3 that no photograph of any item to be supplied under this Order Contract or any portions of the Goods shall be taken except insofar as may be necessary for the proper performance of this Order Contract or with the prior consent in writing of the Buyer, and that no such photograph shall, without such consent, be published or otherwise circulated;

2.1.4 that all information about any Secret Matter and every Document, model or other item which contains or may reveal any such information is at all times strictly safeguarded, and that, except insofar as may be necessary for the proper performance of this Order Contract or with the prior consent in writing of the Buyer, no copies of or extracts from any such Document, model or item shall be made or used and no designation of description which may reveal information about the nature or contents of any such Document, model or item shall be placed thereon; and

2.1.5 that if the Buyer gives notice in writing to the Supplier at any time requiring the delivery to the Customer of any such Document, model or item as is mentioned in Paragraph 2.1.4, that Document, model or item (including all copies of or extracts therefrom) shall forthwith be delivered to the Buyer who shall be deemed to be the owner thereof and accordingly entitled to retain the same.

## 3. Decision of the Buyer

3.1 The decision of the Buyer on the question whether the Supplier has taken or is taking all reasonable steps as required by the foregoing provisions of this Order Schedule 22 shall be final and conclusive.

## 4. Particulars of People

4.1 If and when directed by the Buyer, the Supplier shall furnish full particulars of all people who are at any time concerned with any Secret Matter.

## 5. Official Secrets Act

5.1 If and when directed by the Buyer, the Supplier shall secure that any person employed by it who is specified in the direction, or is one of a class of people who may be so specified, shall sign a statement that he understands that the Official Secrets Act, 1911 to 1989 and, where applicable, the


© Crown Copyright 2020

Atomic Energy Act 1946, apply to the person signing the statement both during the carrying out and after expiry or termination of the Order Contract.

## 6. Information concerning the Contract

6.1 If, at any time either before or after the expiry or termination of this Order Contract, it comes to the notice of the Supplier that any person acting without lawful authority is seeking or has sought to obtain information concerning this Order Contract or anything done or to be done in pursuance thereof, the matter shall be forthwith reported by the Supplier to the Buyer and the report shall, in each case, be accompanied by a statement of the facts, including, if possible, the name, address and occupation of that person, and the Supplier shall be responsible for making all such arrangements as it may consider appropriate to ensure that if any such occurrence comes to the knowledge of any person employed by it, that person shall forthwith report the matter to the Supplier with a statement of the facts as aforesaid.

## 7. Duty to observe obligations

7.1 The Supplier shall place every person employed by it, other than a Sub contractor, who in its opinion has or will have such knowledge of any Secret Matter as to appreciate its significance, under a duty to the Supplier to observe the same obligations in relation to that Secret Matter as are imposed on the Supplier by Paragraphs 1 and 2 and shall, if directed by the Buyer, place every person who is specified in the direction or is one of a class of people so specified, under the like duty in relation to any Secret Matter which may be specified in the direction, and shall at all times use its best endeavours to ensure that every person upon whom obligations are imposed by virtue of this Order Schedule 22 observes the said obligations, and the Supplier shall give such instructions and information to every such person as may be necessary for that purpose, and shall, immediately upon becoming aware of any act or omission which is or would be a breach of the said obligations, report the facts to the Supplier with all necessary particulars.

## 8. Sub-Contract Obligations

8.1 The Supplier shall, if directed by the Buyer, include in the Sub-Contract provisions in such terms as the Buyer may consider appropriate for placing the Sub-Contractor under obligations in relation to secrecy and security corresponding to those placed on the Supplier by this Order Schedule 22, but with such variations (if any) as the Buyer may consider necessary. Further the Supplier shall:

8.1.1 give such notices, directions, requirements and decisions to its Sub Contractors as may be necessary to bring the provisions relating to secrecy and security which are included in Sub-Contracts under this Order Schedule 22 into operation in such cases and to such extent as the Buyer may direct;


© Crown Copyright 2020

8.1.2 if there comes to its notice any breach by the Sub-Contractor of the obligations of secrecy and security included in their Sub-Contracts in pursuance of this Order Schedule 22, notify such breach forthwith to the Customer; and

8.1.3 if and when so required by the Buyer, exercise its power to determine the Sub-Contract under the provision in that Sub-Contract which corresponds to Paragraph 11.

## 9. Information to the Buyer

9.1 The Supplier shall give the Buyer such information and particulars as the Buyer may from time to time require for the purposes of satisfying the Buyer that the obligations imposed by or under the foregoing provisions of this Order Schedule 22 have been and are being observed and as to what the Supplier has done or is doing or proposes to do to secure the observance of those obligations and to prevent any breach thereof, and the Supplier shall secure that a representative of the Buyer duly authorised in writing shall be entitled at reasonable times to enter and inspect any premises in which anything is being done or is to be done under this Order Contract or in which there is or will be any item to be supplied under this Order Contract, and also to inspect any Document or item in any such premises or which is being made or used for the purposes of this Order Contract and that any such representative shall be given all such information as he may require on the occasion of, or arising out of, any such inspection.

## 10. Exclusion

10.1 Nothing in this Order Schedule 22 shall prevent any person from giving any information or doing anything on any occasion when it is, by virtue of any enactment, the duty of that person to give that information or do that thing.

## 11. Grounds for Termination

11.1 If the Buyer shall consider that any of the following events has occurred:

11.1.1 that the Supplier has committed a breach of, or failed to comply with any of, the foregoing provisions of this Order Schedule 22; or

11.1.2 that the Supplier has committed a breach of any obligations in relation to secrecy or security imposed upon it by any other contract with the Buyer, or with any department or person acting on behalf of the Crown; or

11.1.3 that by reason of an act or omission on the part of the Supplier, or of a person employed by the Supplier, which does not constitute such a breach or failure as is mentioned in Paragraph

11.1.4 information about a Secret Matter has been or is likely to be acquired by a person who, in the opinion of the Buyer, ought not to have such information;


© Crown Copyright 2020

11.1.5 and shall also decide that the interests of the state require the termination of this Order Contract, the Buyer may by notice in writing terminate this Order Contract forthwith.

## 12. Buyer Decision to Terminate

12.1 A decision of the Buyer to terminate this Order Contract in accordance with the provisions of Paragraph 11 shall be final and conclusive and it shall not be necessary for any notice of such termination to specify or refer in any way to the event or considerations upon which the Buyer's decision is based.

## 13. Supplier's notice

13.1 The Supplier may within five (5) Working Days of the termination of this Order Contract in accordance with the provisions of Paragraph 11, give the Buyer notice in writing requesting the Buyer to state whether the event upon which the Buyer's decision to terminate was based is an event mentioned in Paragraphs 11.1.1, 11.1.2 or 11.1.3 and to give particulars of that event; and

13.2 the Buyer shall within ten (10) Working Days of the receipt of such a request give notice in writing to the Supplier containing such a statement and particulars as are required by the request.

## 14. Matters pursuant to termination

14.1 The termination of this Order Contract pursuant to Paragraph 11 shall be without prejudice to any rights of either Party which shall have accrued before the date of such termination;

14.2 The Supplier shall be entitled to be paid for any work or thing done under this Order Contract and accepted but not paid for by the Buyer at the date of such termination either at the price which would have been payable under this Order Contract if the Order Contract had not been terminated, or at a reasonable price;

14.3 The Buyer may take over any work or thing done or made under this Order Contract (whether completed or not) and not accepted at the date of such termination which the Buyer may by notice in writing to the Supplier given within thirty (30) Working Days from the time when the provisions of this Order Schedule 22 shall have effect, elect to take over, and the Supplier shall be entitled to be paid for any work or thing so taken over a price which, having regard to the stage which that work or thing has reached and its condition at the time it is taken over, is reasonable. The Supplier shall in accordance with directions given by the Buyer, deliver any work or thing taken over under this Paragraph 14.3, and take all such other steps as may be reasonably necessary to enable the Buyer to have the full benefit of any work or thing taken over under this Paragraph 14.3 ; and

14.4 Save as aforesaid, the Supplier shall not be entitled to any payment from the Buyer after the termination of this Order Contract.


© Crown Copyright 2020

## 15. Rights & Obligations after Termination

15.1 If, after notice of termination of this Order Contract pursuant to the provisions of Paragraph 11:

15.1.1 the Buyer shall not within ten (10) Working Days of the receipt of a request from the Supplier, furnish such a statement and particulars as are detailed in Paragraph 13.1; or

15.1.2 the Buyer shall state in the statement and particulars detailed in Paragraph 13.2 that the event upon which the Buyer's decision to terminate this Order Contract was based is an event mentioned in Paragraph.11.1.3,

15.1.3 the respective rights and obligations of the Supplier and the Buyer shall be terminated in accordance with the following provisions:

15.2 the Buyer shall take over from the Supplier at a fair and reasonable price all unused and undamaged materials, bought-out parts and components and articles in course of manufacture in the possession of the Supplier upon the termination of this Order Contract under the provisions of Paragraph 11 and properly provided by or supplied to the Supplier for the performance of this Order Contract, except such materials, bought-out parts and components and articles in course of manufacture as the Supplier shall, with the concurrence of the Buyer, elect to retain;

15.3 the Supplier shall prepare and deliver to the Buyer within an agreed period or in default of agreement within such period as the Buyer may specify, a list of all such unused and undamaged materials, bought-out parts and components and articles in course of manufacture liable to be taken over by or previously belonging to the Buyer and shall deliver such materials and items in accordance with the directions of the Buyer who shall pay to the Supplier fair and reasonable handling and delivery charges incurred in complying with such directions;

15.4 the Buyer shall indemnify the Supplier against any commitments, liabilities or expenditure which are reasonably and properly chargeable by the Supplier in connection with this Order Contract to the extent to which the said commitments, liabilities or expenditure would otherwise represent an unavoidable loss by the Supplier by reason of the termination of this Order Contract;

15.5 if hardship to the Supplier should arise from the operation of this Paragraph 15 it shall be open to the Supplier to refer the circumstances to the Buyer who, on being satisfied that such hardship exists shall make such allowance, if any, as in its opinion is reasonable and the decision of the Buyer on any matter arising out of this Paragraph 15.5 shall be final and conclusive; and


© Crown Copyright 2020

15.6 subject to the operation of Paragraphs15.2, 15.3, 15.4, and 15.5 termination of this Order Contract shall be without prejudice to any rights of either party that may have accrued before the date of such termination.


© Crown Copyright 2020