

## DIPS Order Form

### **ORDER FORM**

This Order Form is for the provision of the Call-Off Deliverables. It is issued under the DIPS Framework Contract with a unique reference number starting with RM6249 to be issued by **DD PS Commercial Team**.

The DIPS Framework and this Call-Off Contract are to be for the delivery of service-based outcomes only. This Framework is not for the request and delivery of resource. If specific resources are needed alternative sourcing methods must be used, such as Public Sector Resourcing.

During the Call-Off Contract Period, the Requirement Holder and the Supplier may agree and execute a Statement of Work (in the form of the template set out in Schedule 3 to this **Order Form / Statement of Requirements Template<sup>1</sup>**). Upon execution of any Statement of Work the provisions detailed therein shall be incorporated into the Call-Off Contract to which this Order Form relates.

The Parties agree that when the Requirement Holder seeks further Deliverables within the initial scope of the original Call-off contract from the Supplier that are not provided for in this Call-Off Contract, the Requirement Holder and Supplier will agree and execute a Call-Off Variation Form.

All capitalised terms in this **Order Form / Statement of Requirements Template** shall have the meanings set out in DIPS Framework Joint Schedule 1 (Definitions) unless otherwise stated.

---

<sup>1</sup> This represents DIPS Framework Schedule 6

## DIPS Order Form

### 1. DIPS Requirement Identification

Call-Off Lot	Lot 2 - Dev, Apps, UX, Dev Ops, Sys Design & Support				
Call-Off Reference	RM6249/DIPS(2)037	Version Number	v1.7	Date	15 November 2024
Call-Off Contract title:	PS394 Digital Skills for Defence (DS4D) Client-Side Support				
Call-Off Contract description:	Client-side Professional Service Support (PSS) to ensure that the Authority can administer effective performance management, retain 'intelligent customer' status, and hold the strategic partner to account. This will also enable the programme to access limited term subject matter expertise, including: data analysis, user experience, business analysis, technical, costing and approvals.				
<b>Commercial Strategy</b>					
Further Competition	<input checked="" type="checkbox"/>	Competitive award criteria to be used for undertaking evaluation of proposal(s)	As set out in attachment 2 of the bid pack (How to Bid)		
Direct Award*	<input type="checkbox"/>				
<b>Contract Charges</b>					
Initial Term: £639,990 (ex VAT)					
<b>Timescales</b>					
Call-Off Start Date	DATE CONTRACT FULLY EXECUTED				
Call-Off Initial Period	12 Months				
Call-Off Expiry Date	31 October 2025				
Call-Off Optional Extension Period	<ul style="list-style-type: none"> <li>Extension Option 1: 01 November 2025 to 31 March 2027 (subject to performance and financial approval)</li> <li>Extension Option 2: 01 April 2027 to 31 March 2028 (subject to performance and financial approval)</li> </ul>				

### 1b. Contact details

**DIPS Order Form**

Government Directorate / Organisation Title		Name of Supplier	Capgemini UK PLC
Name of Requirement Holder's Authorised Representative		Name of Supplier's Authorised Representative	
Post title		Post title	
Requirement Holder's Address	Defence Digital Spur C3 Building 405 MOD Corsham	Supplier Address	40 Holborn Viaduct London EC1N 2PB
Postcode	Wiltshire SN13 9NR	Postcode	
Telephone		Telephone	
Email		Email	
Name of Requirement Holder's Project Lead			
Requirement Holder's Secondary Contact Name		Supplier Secondary Contact Name	
Requirement Holder's Secondary Contact Role		Supplier Secondary Contact Role	
Requirement Holder's Secondary Contact Email		Supplier Secondary Contact Email	

**3. Statement of Requirements (SOR)**

As per Schedule 1 of this Order Form

**4. Call-Off Incorporated Terms**

## DIPS Order Form

The following documents are incorporated into this Call-Off Contract. Where numbers are missing those DIPS Framework schedules are not being used in this Call-Off Contract. If the documents conflict, the following order of precedence applies:

1. This Order Form including the General Conditions in section 2(b) and the Call-Off Special Terms in section 2(c).
2. Joint Schedule 1 (Definitions)
3. Any Statement(s) of Work (in the form of the template set out in **Schedule 3** to this **Order Form / Statement of Requirements Template** (Framework Schedule 6)) executed by the Requirement Holder and the Supplier with a corresponding Call-Off Contract reference
4. [Framework Special Terms]
5. The following Schedules in equal order of precedence:
  - Joint Schedules
    - Joint Schedule 2 (Variation Form) ○ Joint Schedule 3 (Insurance Requirements) ○ Joint Schedule 4 (Commercially Sensitive Information)
    - Joint Schedule 5 (Corporate Social Responsibility) ○ Joint Schedule 7 (Financial Difficulties) [Not Used] ○ Joint Schedule 10 (Rectification Plan)
    - Joint Schedule 11 (Processing Data)
  - Call-Off Schedules
    - Call-Off Schedule 2 (Staff Transfer) [Not Used] ○ Call-Off Schedule 3 (Continuous Improvement) ○ Call-Off Schedule 5 (Pricing Details and Expenses Policy) ○ Call-Off Schedule 6 (Intellectual Property Rights and Additional Terms on Digital Deliverables) ○ Call-Off Schedule 8 (Business Continuity and Disaster Recovery) [Not Used] ○ Call-Off Schedule 9 (Security) – Part A ○ Call-Off Schedule 10 (Exit Management) ○ Call-Off Schedule 13 (Implementation Plan and Testing)
    - Call-Off Schedule 14 (Service Levels) [Not Used] ○ Call-Off Schedule 17 (MOD Terms) ○ Call-Off Schedule 25 (Ethical Walls Agreement) ○ Call-Off Schedule 26 (Cyber)
- 1 Core Terms (DIPS version)
- 2 Call-Off Schedule 4 (Call-Off Tender) as long as any parts of the Call-Off Tender that offer a better commercial position for the Requirement Holder (as decided by the Requirement Holder and Commercial) take precedence over the documents above.

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery. Due to the expected nature of the Services, the requirements of Call-Off Schedule 13 will be provided under Buyer guidance as part of the Services and formal implementation and testing plans will not be required.

### 5a. General Conditions

Additional Conditions:



## DIPS Order Form

**Primary Quality Assurance Requirements:**

No specific Quality Management System requirements are defined. This does not relieve the Supplier of providing services to the Buyer's standards under this contract. CoC shall be provided in accordance with DEFCON 627

**Quality Plans**

No Deliverable Quality Plan is required DEFCON 602B.

**Concessions**

Concessions shall be managed in accordance with Def Stan. 05-061, Part 1, Issue 7 – Quality Assurance Procedural Requirements – Concessions

**Contractor Working Parties**

The Authority does not expect contractor working parties to be provided in this contract. In the event they are provided, the below condition must be complied with.

Any contractor working parties shall be provided in accordance with Def Stan, 05-061 Part 4, Issue 4 – Quality Assurance Procedural Requirements – Contractor Working Parties.

**IR35 Assessment**

[REDACTED]

**Cyber Risk Profile**

The Cyber Risk Profile for this requirement has been assessed as low (Risk Assessment Ref: RAR240626A13).

**Security Clearance**

All supplier personnel must hold current and valid SC clearance as a minimum.

### 5b. Call-Off Special Terms

The following Special Terms are incorporated into this Call-Off Contract:

None

### 5c. Maximum Liability

The limitation of the Supplier's liability for this Call-Off Contract is stated in Clause 11.4 of the Core Terms. Clause 11.2 is hereby amended such that the Supplier's total liability under this Contract in respect of losses referred to in clauses 8.3(a), 11.2(d), 11.2(e), 12.2 and 14.8(e) of the Core Terms, subject to Clause 11.1, shall be limited in aggregate to £2,000,000.

### 5d. Requirement Holder's Security Policy

Please see Call-Off Schedule 9 and the Security Aspects Letter provided at Appendix 6.

### 5e. Cyber Essentials Scheme

## DIPS Order Form

In accordance with DIPS Framework Call-Off Schedule 26 (Cyber): -	
<b>Cyber Essentials Plus:</b> The Requirement Holder requires the Supplier to have / maintain a <b>Cyber Essentials Plus</b> level Certificate for the work undertaken under this Call-Off Contract.	<input type="checkbox"/>
<b>Cyber Essentials:</b> The Requirement Holder requires the Supplier to have / maintain a <b>Cyber Essentials</b> level Certificate for the work undertaken under this Call-Off Contract.	<input checked="" type="checkbox"/>
The Requirement Holder requires <b>no level of Cyber Essentials</b>	<input type="checkbox"/>

### 5f. Requirement Holder's Environmental Policy

Available online at: [Management of environmental protection in defence \(JSP 418\) - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/publications/management-of-environmental-protection-in-defence-jsp-418)

This version is dated 18<sup>th</sup> August 2023.

### 5g. Social Value Commitment

The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Call-Off Schedule 4 (Call-Off Tender)

### 5h. Quality Assurance Conditions

According to the product or scope of the work to be carried out, the Supplier shall meet the following requirements:

Allied Quality Assurance Publications (AQAP) 2110 – North Atlantic Treaty Organization (NATO) Quality Assurance Requirements for Design, Development and Production.

Certificate of Conformity shall be provided in accordance with DEFCON 627 (*Edn12/10*).

☐

#### Deliverable Quality Plan requirements:

DEFCON 602A (*Edn 12/17*) - Quality Assurance with Quality Plan

☐

DEFCON 602B (*Edn 12/06*) - Quality Assurance without Quality Plan

☒

AQAP 2105:2 – NATO Requirements for Deliverable Quality Plans

☐

#### Software Quality Assurance requirements

Allied Quality Assurance Publications (AQAP) 2210 – North Atlantic Treaty Organization (NATO) Supplementary Software Quality Assurance Requirements to AQAP-2110 shall apply

☐

#### Air Environment Quality Assurance requirements

Defence Standard (DEF STAN) 05-100 – Ministry of Defence Requirements for Certification for Aircraft Flight and Ground Running (Mandatory where flying and/or ground running of issued aircraft is a requirement of the Task)

☐

Relevant MAA Regulatory Publications (See attachment for details)

☐

**DIPS Order Form****5h. Quality Assurance Conditions**

Additional Quality Requirements

Not applicable

☐**Planned maintenance schedule requirement**

The planned maintenance schedule shall meet the following requirements:

Not applicable

☐**5i. Implementation Plan**

Not applicable

☐**3. Additional Insurances**

Details of Additional Insurances required in accordance with Joint Schedule 3 (Insurance Requirements)

**4. Guarantee**

Not applicable

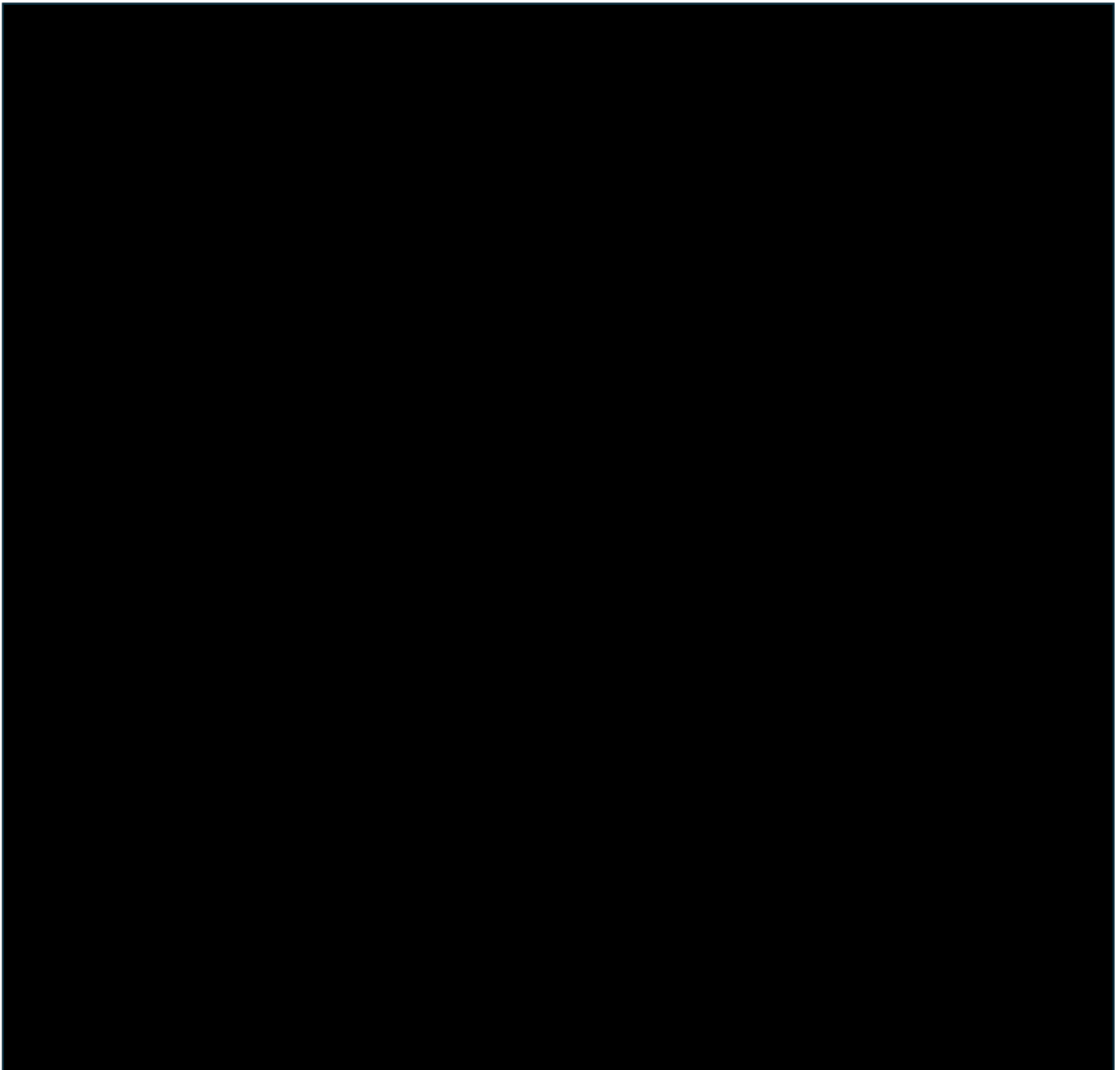
**5i. Proposed Subcontractor(s)**

None

**5j. Commercially Sensitive Information**

## DIPS Order Form

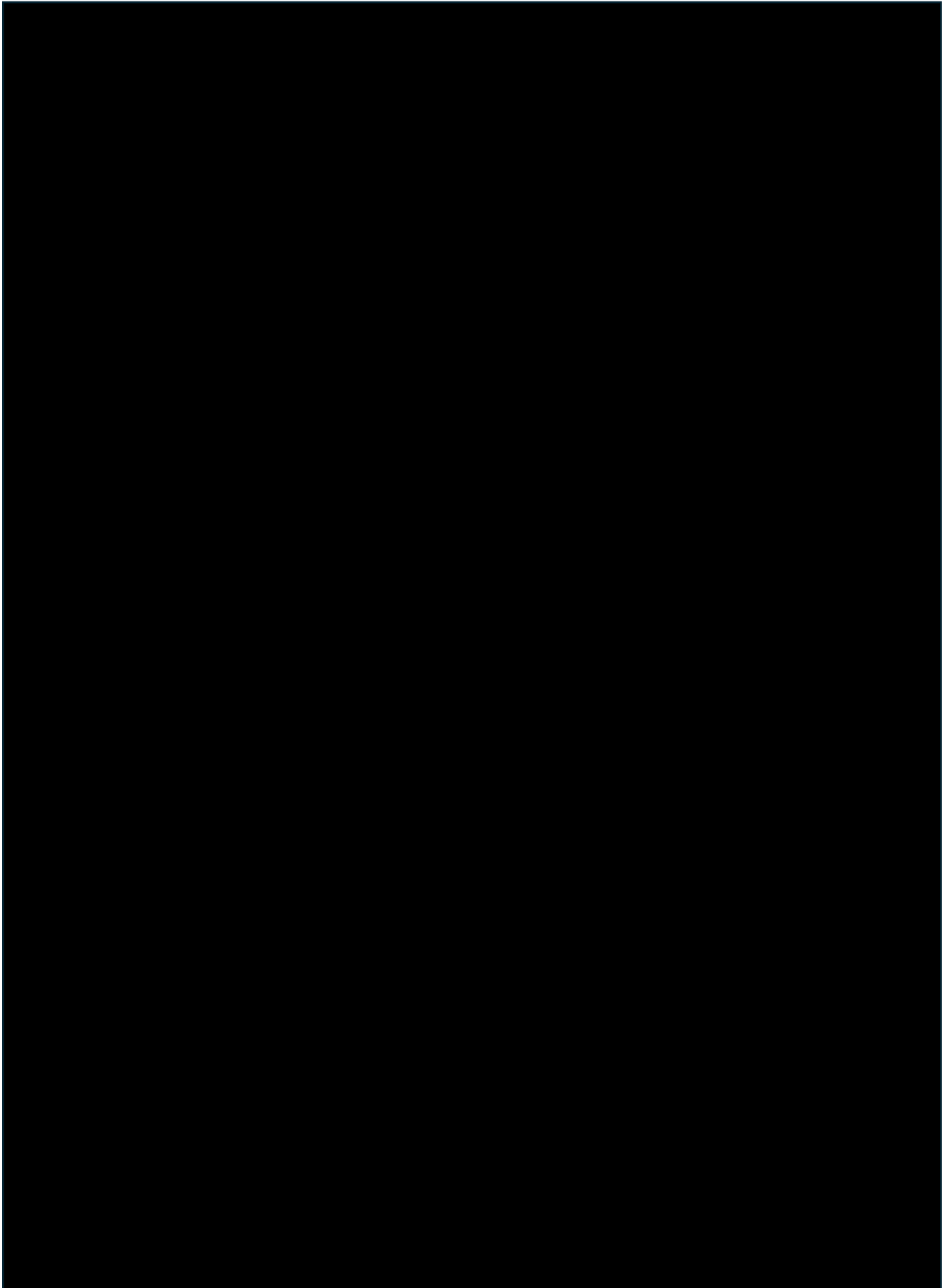
1. Details of the Contractor's methodologies, policies and processes.
2. All information relating to limits of liability, daily fee rates, pricing and charging mechanisms contained in the Agreement.
3. The terms of the Contractor's insurance are strictly confidential and if such information was disclosed it could be commercially damaging to the Contractor.
4. All details relating to personnel including but not limited to the numbers of resources with specific skills, numbers of security cleared staff, staff terms and conditions of employment and staff selection methods are used for the purpose of managing the Contractor's resources to secure trade and generate profit and provides the Contractor with a competitive advantage.
5. Any information relating to other customers of the Contractor that has been obtained as a result of the Services or as a result of procuring the Services (including pre-contract references).





## **DIPS Order Form Template**

### **Schedule 1 – Statement of Requirements (SOR)**



## DIPS Order Form Template

### Appendix 1

Table of Activities Required to be Undertaken. 1.0 Contract Performance  
Management

## DIPS Order Form Template

OFFICIAL SENSITIVE (when complete)

### 2.0 P3M Advisory Services

Reference	Requirement	Outcome	Deliverable	Reporting Period	Deliverable Type	Acceptance criteria	Initial Term Firm Price	Extension Option 1	Extension Option 2
2.0	Support the Authority in a number of key P3M advisory Services.	2.1 Support Programme Governance and development of briefings, Board packs, facilitation of key programme governance meetings, with traceability of senior actions & decisions.	Prepare DS4D Progress Reports & Programme Board Packs  Develop and Maintain Programme Governance Plan, including Record and Decisions log.	Monthly	Firm Price	Robust administration support of Authority governance meetings, including DS4D Programme Board.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)
		2.2 Supporting the iterative development of programme governance/processes, to aid wider programme team coherence and optimise delivery.	Develop Programme Delivery Model with Programme Lifecycle Roadmap.	Monthly	Firm Price	Administration of programme governance which includes scope management across the lifecycle of the programme.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)
		2.3 Stakeholder engagement, including identifying and engaging with stakeholders at all levels to address needs and expectations. Additionally, supporting the Programme Stakeholder Lead to identify and establish effective communication channels to engage with stakeholders throughout programme lifecycle.	Evergreened Communications and Engagement Plan	Monthly	Firm Price	DS4D Communications Plan with Stakeholder Map and Register that effectively supports and tracks Snr stakeholder engagement.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)

## DIPS Order Form Template

		2.4 Support to programme Risk, Assumptions, Issue, Dependency and Opportunity (RAIDO) management, including driving automation of dependency management within the Programme.	Evergreened RAIDO log.  High-Level Programme Risks captured and monitored in ARM.	Monthly	Firm Price	RAIDO log updated on a monthly basis with input from initiative leads as appropriate and tracks PESTLE changes that will affect programme strategic planning.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)
		2.5 Support to Project Controls, including cost and schedule to ensure the programme continues to deliver within the performance, cost, and time envelope agreed within the Full Business Case.	Development and Maintenance of Programme Cost Model.	Monthly	Firm Price	Validated Cost Model, in line with Cost Assurance and Analysis Service (CAAS) Modelling Centre of Excellence (MOE) standards.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)
		2.5.1 Development and maintenance of a revised detailed programme schedule, with key milestones hosted in corporate tooling (Project Online, POL).	Development and Maintenance of Programme Schedule with key milestones.	Monthly	Firm Price	Project schedule developed, with key milestones escalated to POL which is supported by an Agile prioritised backlog.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)
		2.5.2 Maintenance of Programme budgeting and forecasting cost model to track spend and report available funding position.	Development and maintenance of a budgeting and forecasting cost model.	Monthly	Firm Price	Excel based budgeting and forecasting sheet that tracks spend and enables efficient financial planning scalability and is maintained monthly.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)

## DIPS Order Form Template

		2.6 Support to programme Review Note, anticipated in Q3/Q4 FY24/25, to accelerate delivery of DS4D at pace and scale across Defence. This will include generation of evidence, support to cost modelling and Ministerial Submissions. RAIDO support will be ongoing throughout the lifecycle of the programme.	Inputs from maintained Cost Model, RAIDO log and Activity Backlog.	Q3/Q4 FY24/25	Firm Price	Review Note and MinSub, generated in line with MOD policy and guidance. Cost model in line with JSP655 and JSP507.	Applicable	Not Applicable	Not Applicable
		2.7 Benefits management support using the corporate Benefit Management tools. This includes but not exhaustive: Benefit identification, evaluation and measures to ensure they align and track strategic and programme outcomes and objectives. Ongoing support throughout the lifecycle of the programme.	Develop Benefit Realisation Strategy.	January 2025	Firm Price	Benefit Realisation Strategy & plans in line with JSP655 & JSP507.	Applicable	Not Applicable	Not Applicable
		2.7.1 Implementation of Benefits Management Plan.	Development, Implementation and reporting of Benefits Management Plan.	January 2025, quarterly thereafter.	Firm price	Benefits Management plan, written and reported in line with MOD policies and programme governance.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)
		2.8 Implement a new programme SharePoint infrastructure and Knowledge Information Management (KIM) best practice to effectively manage the Programme's information, facilitating knowledge transfer and continuous improvement through best practices across the lifecycle.	Restructure, implement and maintain an effective Programme document repository and KIM policies.	Monthly	Firm price	Implementation and communication of new SharePoint architecture and KIM best practice in line with JSP441.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)

## DIPS Order Form Template

Acceptance Criteria	<p>2.1 Robust support to key governance meetings including DS4D Programme Board with actions &amp; decisions traceability.</p> <p>2.2 Administration of programme governance which includes scope management across the lifecycle of the programme.</p> <p>2.3 DS4D Communications Plan with Stakeholder Map and Register that effectively supports and tracks Snr stakeholder engagement..</p> <p>2.4 RAIDO log updated on a monthly basis with input from initiative leads as appropriate and tracks PESTLE changes that will affect programme strategic planning.</p> <p>2.5 Validated Cost Model, in line with Cost Assurance and Analysis Service (CAAS) Modelling Centre of Excellence (MOE) standards.</p> <p>2.5.1 Project schedule developed, with key milestones escalated to POL which is supported by an Agile prioritised backlog.</p> <p>2.5.2 Excel based budgeting and forecasting sheet that tracks spend and enables efficient financial planning scalability and is maintained monthly.</p> <p>2.6 Review Note and MinSub, generated in line with MOD policy and guidance. Cost model in line with JSP655 and JSP507.</p> <p>2.7 Benefit Realisation Strategy &amp; plans in line with JSP655 &amp; JSP507.</p> <p>2.7.1 Benefits Management plan, written and reported in line with MOD policies and programme governance. 2.8 Implementation and communication of new SharePoint architecture and KIM best practice in line with JSP441.</p>
---------------------	---

### 3.0 Leading and Managing Projects, Products and Services

Reference	Requirement	Outcome	Deliverable	Reporting Period	Deliverable Type	Acceptance criteria	Initial Term Firm Price	Extension Option 1	Extension Option 2
3.0	3.1 Lead and manage the delivery of targeted interventions in the form of projects, products and services.	<p>3.1.1 Optimising access to Digital Learning across Defence.</p> <p>Optimise the usage of the Digital Learning Experience Platform (DLXP) Minimum Viable Product (MVP) through to March 2025, delivering a compelling User Experience to up to 60,000 Defence staff on MODNet. This continued expansion will focus on delivery to required cohorts of identified users across Defence.</p>	Optimised rollout of DLXP MVP to required cohorts.	By October 2025	Firm Price	Service Management of DLXP MVP with User Feedback incorporation loop, managed in line with Operational Service Management (OSM), End User Services (EUS) and Technical Design Authority (TDA) endorsement.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)

## DIPS Order Form Template

		3.1.2 Work alongside the Original Equipment Manufacturer (Microsoft) and Skillsoft with existing COTS products (Viva Learning and Percipio respectively) to continue to optimise the access to Digital learning content for all Users within the scope of the programme.	DLXP Continuous Improvement Loop with activity backlog.	Monthly	Firm Price	Agile User Experience Continuous Improvement cycle for DLXP built in collaboration with OEM vendors and Defence stakeholders.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)
		3.1.3 Implement and refine the Access Target Operating Model for the preferred solution, to ensure effective embedding as Business as Usual, with a continued and evergreened capability.	Access Target Operating Model with BAU Implementation Plan.	May 2026	Firm Price	Access Target Operating Model to accommodate minimum 100k active monthly users, developed in accordance with OSM, EUS and TDA policies and processes and communicated to Senior stakeholders.	Not Applicable	To be agreed	Not Applicable
3.0	3.2 Lead and manage the delivery of targeted	3.2.1 Future State Digital Learning Experience Platform (DLXP) design and implementation.	Updated DLXP User Requirement.	February 2026	Firm Price	An updated User Requirement, with evidence to support why requirements have evolved	Not Applicable	To be agreed	Not Applicable

	interventions in the form of projects, products and services.	Refine and develop the existing DLXP User Requirement from the Technical Feasibility Study, ensuring that they are suitably robust and underpinned by evidence to support.				where applicable and how they meet User Satisfaction and Engagement measures.			
--	---	--	--	--	--	---	--	--	--

## DIPS Order Form Template

		3.2.2 Work with key stakeholders including the Digital Skills for Defence programme board to determine the preferred technology solution. This may involve transition planning to a new platform if required.	Future DLXP Technology Solution Options Analysis.	March 2026	Firm Price	DX4D Stakeholder endorsed Options Analysis for preferred DLXP delivery technology solution.	Not Applicable	To be agreed	Not Applicable
		3.2.3 Support delivery of the preferred approach. (Note: this is a variable element given the preferred approach is yet to be confirmed).	Future DLXP Transition Plan for DLXP migration.	April 2026	Variable, based on agreed rate card.	Development and implementation of DLXP Transition Plan of chosen technology solution minimising capability.	Not Applicable	To be agreed	Not Applicable
3.0	3.3 Lead and manage the delivery of targeted interventions in the form of projects, products and services.	3.3.1 Mapping the Digital Learning Ecosystem.  Maintaining and managing a register of all digital learning products, services and providers the across Digital learning ecosystem	Digital Learning Ecosystem Mapping Register.	Monthly	Firm Price	Persistent stakeholder engagement to identify new and existing digital learning initiatives across the Defence ecosystem, utilisation of third-party visualisation tools to track relationships and dependencies of initiatives.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)
		3.3.2 Communicating Defence's Digital Learning Ecosystem findings to improve stakeholder understanding and decisionmaking.	Digital Learning Ecosystem Report.	Monthly	Firm Price	Reporting and presenting ecosystem mapping findings, highlighting risks and opportunities of duplication/de-duplication to inform Senior stakeholder decisionmaking and improve Value for Money for Defence.	Applicable	To be agreed (up to a maximum scaling factor of x5)	To be agreed (up to a maximum scaling factor of x5)
Acceptance Criteria	3.1.1 Service Management of DLXP MVP with User Feedback incorporation loop, managed in line with Operational Service Management (OSM), End User Services (EUS) and Technical Design Authority (TDA) endorsement. 3.1.2 Agile User Experience Continuous Improvement cycle for DLXP MVP built in collaboration with OEM vendors.								



## DIPS Order Form Template

	<p>3.1.3 Access Target Operating Model to accommodate minimum 100k active monthly users, developed in accordance with OSM, EUS and TDA policies and processes and communicated to Senior stakeholder.</p> <p>3.2.1 An updated User Requirement, with evidence to support why requirements have evolved where applicable, and how they meet User Satisfaction and Engagement measures.</p> <p>3.2.2 DX4D Stakeholder endorsed Options Analysis for preferred DLXP delivery technology solution.</p> <p>3.2.3 Development and implementation of DLXP Transition Plan of chosen technology solution minimising capability Impact.</p> <p>3.3.1 Persistent stakeholder engagement to identify new and existing digital learning initiatives across the Defence ecosystem, utilisation of third-party visualisation tools to track relationships and dependencies of initiatives.</p> <p>3.3.2 Reporting and presenting ecosystem mapping findings, highlighting risks and opportunities of duplication/de-duplication to inform Senior stakeholder decision-making and improve Value for Money for Defence.</p>
--	---

## **DIPS Order Form Template Schedule 2 – Pricing Response**

### **Call Off Contract Charges**

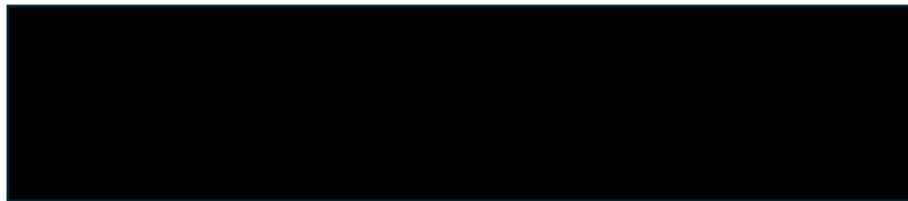
This schedule sets out the Charges that shall be payable.

Table 1 sets out the total Charges for the Initial Term. The monthly payments of the Charges are set out in the Milestone Payment Plan section of this Schedule.

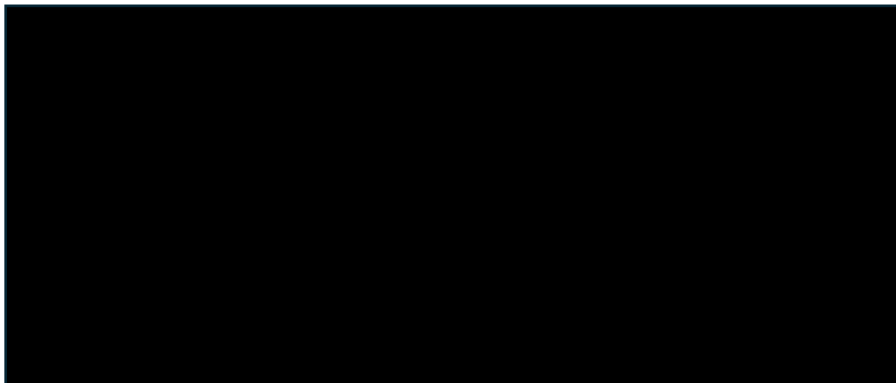
Table 2 sets out the maximum Charges for Extension Option 1 and Extension Option 2. The actual Charges and Milestone Payment Plan for these optional extensions shall be agreed and documented should the Buyer elect to use these options.

The Charges are based on no staff transfer occurring on the transfer of services. Should any staff transfer be identified, the Supplier shall be allowed to claim any additional related costs.

**Table 1: Initial Term Charges**

A large black rectangular box redacting the content of Table 1.

**Table 2: Extension Option Charges**

A large black rectangular box redacting the content of Table 2.

DIPS Order Form Template Milestone

Payment Plan

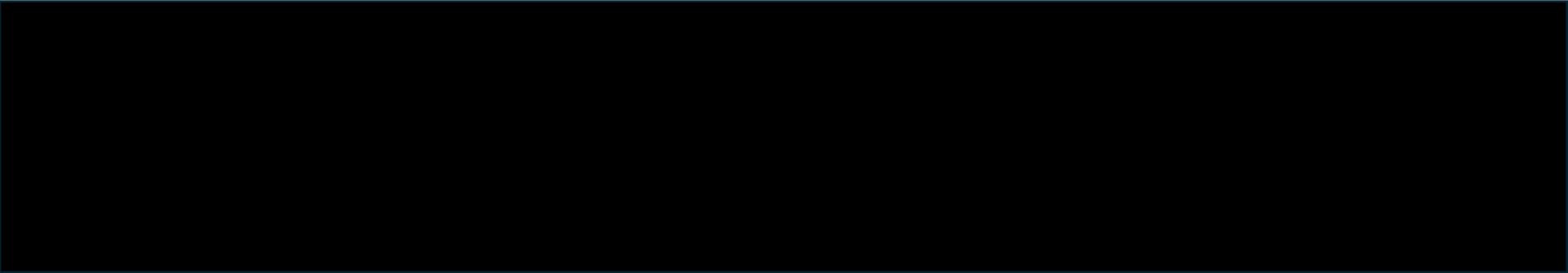
A large black rectangular box redacting the content of the table.

Table 3: Initial Term Milestone Payment Plan

In consideration of the delivery of the Services, the amount in the Total row of this Table 3: Initial Term Milestone Payment Plan shall become payable at the end of each calendar month in the Initial Term (Milestone Payments) columns.

## DIPS Order Form Template

#	Deliverable Description	Extension Option 1 (01-Nov25 to 31-Mar-27)	Extension Option 2 (01-Apr-27 to 31-Mar-28)
1.1	Strategic Partner Deliverables Feedback report	✓	✓
1.2	Strategic Partner Contract Performance Feedback report	✓	✓
1.3	Strategic Partner Deliverables Tracking dashboard	✓	✓
2.1	DS4D Progress Reports & Programme Board Packs	✓	✓
2.2	Programme Delivery Model & Lifecycle Roadmap	✓	✓
2.3	Programme Communications and Engagement Plan	✓	✓
2.4	Programme RAIDO Log	✓	✓
2.5	Programme Cost Model	✓	✓
2.5.1	Programme Schedule with key milestones	✓	✓
2.5.2	Programme budgeting and forecasting cost model	✓	✓
2.7.1	Programme Benefit Management Plan	✓	✓
2.8	Programme Document Repository and KIM Policies	✓	✓
3.1.1	Optimised rollout of DLXP MVP to required cohorts	✓	✓
3.1.2	DLXP MVP Continuous Improvement Loop	✓	✓
3.1.3	Access Target Operating Model with BAU Implementation Plan	✓	n/a
3.2.1	Updated DLXP User Requirement	✓	n/a
3.2.2	DLXP Technology Solution Options Analysis	✓	n/a
3.2.3	DLXP Transition Plan	✓	n/a
3.3.1	Digital Learning Ecosystem Mapping Register	✓	✓
3.3.2	Digital Learning Ecosystem Report	✓	✓

**Table 3: Indicative deliverables anticipated in Extension Options**

The Authority anticipates a scaling-up of the DS4D client-side support activity from the start of Extension Option 1 onwards. The anticipated scaling factor of relevant and applicable outputs is set out in Appendix 1 of the SoR (Table of Activities Required to be Undertaken) and has been used to calculate the Not to Exceed price for the extension periods.

The precise scaling, scope and milestone payments will be agreed by way of a Statement of Work and exercised through the DIPS Contract Variation process and will be subject to performance and financial approval.

The DIPS Rate Card has been used as a basis of determining the contract charges under this Order Form, noting that the price is a Firm Price based on the successful Supplier's **Pricing Response** schedule detailing the Role Rates for the DIPS Lot specified and the associated Labour Resource allowances provided within their commercial submission and included at this Schedule 2. Pricing is based upon a 7.5 hour working day, in line with the Supplier's standard employment contract.

	-	-	
	-	-	
	-	-	
	-	-	
	-	-	
	-	-	
Mobilise	-	-	
Mobilise	-	-	-
Influence Enable		-	

**Table 5: Role Rates and Associated Labour Resource Allowance (Initial Term)**

### Reimbursable Expenses:

None

### Schedule 3 – Statement of Work [Template]

The Requirement Holder and Supplier may propose and execute additional Statement of Work (in the form of the **Statement of Work Template** to be obtained from PS Commercial Officer).

## **DIPS Order Form Template**

### **Schedule 4- Security Aspects Letter**

**DIPS Order Form Template**

OFFICIAL-SENSITIVE COMMERCIAL

Digital Skills for Defence (DS4D)  
 Spur C3, Bldg 405,  
 MOD Corsham  
 Westwells Road, CORSHAM, SN13 9NR



For the personal attention of:

Capgemini UK PLC  
 1 Forge End  
 Woking  
 GU21 6DB  
 United Kingdom

15 November 2024

**ITT/CONTRACT NUMBER & TITLE: PS394 - Digital Skills for Defence (DS4D) Client-side Support**

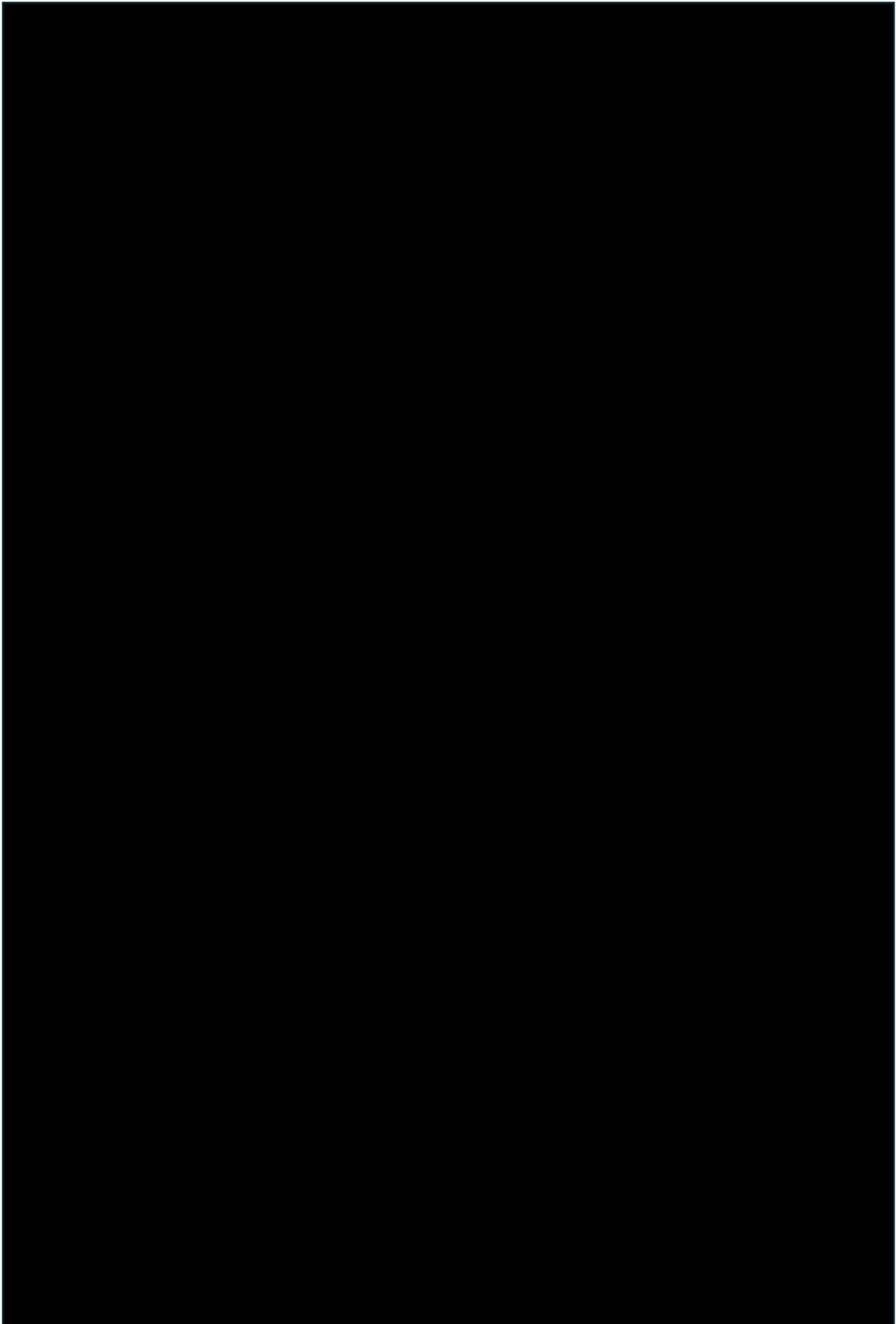
- On behalf of the Secretary of State for Defence, I hereby give you notice of the information or assets connected with, or arising from, the referenced Contract that constitute classified material.
- Aspects that constitute OFFICIAL-SENSITIVE for the purpose of DEFCON 660 are specified below. These aspects must be fully safeguarded. The enclosed Security Condition ['Annex C'] outlines the minimum measures required to safeguard OFFICIAL-SENSITIVE assets and information.

ASPECTS	CLASSIFICATION
Material released in support of the execution of this contract will include project and programme documentation that has sensitive aspects. This may include electronic, physical documentation and discussions at meetings.	Official - Sensitive
For example and not limited to: <ul style="list-style-type: none"> <li>Documentation related to the extended Minimum Viable Product (MVP) of the Learner Experience Platform (LXP)</li> <li>Documentation related to Optimising access and mapping of the Digital Ecosystem of Digital Learning across Defence.</li> <li>Documentation related to the Future State LXP design and implementation.</li> <li>Digital skills data (anonamised data)</li> <li>Programme artefacts and reports</li> </ul>	

OFFICIAL-SENSITIVE COMMERCIAL

OFFICIAL SENSITIVE

## DIPS Order Form Template





## DIPS Order Form Template

OFFICIAL-SENSITIVE COMMERCIAL

### **ANNEX C: UK OFFICIAL AND UK OFFICIAL-SENSITIVE CONTRACTUAL SECURITY CONDITIONS**

#### **Purpose**

1. This document provides guidance for Contractors where classified material provided to or generated by the Contractor is graded UK OFFICIAL or UK OFFICIAL-SENSITIVE. Where the measures requested below cannot be achieved or are not fully understood, further advice should be sought from the UK Designated Security Authority (Email: SPODSR-IIPCSy@mod.gov.uk).

#### **Definitions**

2. The term "*Authority*" for the purposes of this Annex means the HMG Contracting Authority.
3. The term "*Classified Material*" for the purposes of this Annex means classified information and assets.

#### **Security Grading**

4. The SENSITIVE caveat is used to denote UK OFFICIAL material that is of a particular sensitivity and where there is a need to reinforce the 'need to know'. The Security Aspects Letter, issued by the Authority shall define the UK OFFICIAL-SENSITIVE material that is provided to the Contractor, or which is to be developed by it, under this Contract. The Contractor shall mark all UK OFFICIAL and UK OFFICIAL-SENSITIVE documents which it originates or copies during the Contract with the applicable security grading.

#### **Security Conditions**

5. The Contractor shall take all reasonable steps to adhere to the provisions specified in the Contract or listed in this Annex. The Contractor shall make sure that all individuals employed on any work in connection with the Contract have notice that these provisions apply to them and shall continue so to apply after the completion or earlier termination of the Contract. The Authority must state the data retention periods to allow the Contractor to produce a data management policy. If you are a Contractor located in the UK your attention is also drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular.

#### **Protection of UK OFFICIAL and UK OFFICIAL-SENSITIVE Classified Material**

6. The Contractor shall protect UK OFFICIAL and UK OFFICIAL-SENSITIVE material provided to or generated by it in accordance with the requirements detailed in this Security Condition and any other conditions that may be specified by the Authority. The Contractor shall take all reasonable steps to prevent the loss or compromise of classified material whether accidentally or from deliberate or opportunist attack.

OFFICIAL-SENSITIVE COMMERCIAL

OFFICIAL SENSITIVE



## DIPS Order Form Template

OFFICIAL-SENSITIVE COMMERCIAL

7. Once the Contract has been awarded, where Contractors are required to store or process UK MOD classified information electronically, they are required to register the IT system onto the Defence Assurance Risk Tool (DART). Details on the registration process can be found in the 'Industry Security Notices (ISN)' on Gov.UK website. ISNs 2017/01, 04 and 06, Defence Condition 658 and Defence Standard 05-138 details the DART registration, IT security accreditation processes, risk assessment/management and Cyber security requirements which can be found in the following links:

<https://www.gov.uk/government/publications/industry-security-notices-isns>.  
<http://dstan.gateway.isg-r.r.mil.uk/standards/defstans/05/138/000002000.pdf>  
<https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down>

8. All UK classified material including documents, media and other assets must be physically secured to prevent unauthorised access. When not in use UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be handled with care to prevent loss or inappropriate access. As a minimum UK OFFICIAL-SENSITIVE material shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be subject to a level of control.

9. Disclosure of UK OFFICIAL and UK OFFICIAL-SENSITIVE material must be strictly controlled in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than to a person directly employed by the Contractor or sub-Contractor.

10. Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any information issued or provided by or on behalf of the Authority otherwise than for the purpose of the Contract, and, same as provided for in paragraph 8 above, the Contractor shall not make use of any article or part thereof similar to the articles for any other purpose.

11. Subject to any intellectual property rights of third parties, nothing in this Security Condition shall restrict the Contractor from using any specifications, plans, drawings and other documents generated outside of this Contract.

12. Any samples, patterns, specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and must be returned on completion of the Contract or, if directed by the Authority, destroyed in accordance with paragraph 34.

### Access

13. Access to UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be confined to those individuals who have a "need-to-know", have been made aware of the requirement to protect the information and whose access is essential for the purpose of their duties.

14. The Contractor shall ensure that all individuals requiring access to UK OFFICIAL-SENSITIVE information have undergone basic recruitment checks. This should include establishing proof of identity; confirming that they satisfy all legal requirements for employment by the Contractor; and verification of their employment record. Criminal record checks should also be undertaken where

OFFICIAL-SENSITIVE COMMERCIAL



## DIPS Order Form Template

OFFICIAL-SENSITIVE COMMERCIAL

permissible under national/local laws and regulations. This is in keeping with the core principles set out in the UK Government (HMG) Baseline Personnel Security Standard (BPSS) which can be found at:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/714002/HMG\\_Baseline\\_Personnel\\_Security\\_Standard\\_-\\_May\\_2018.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf)

### Hard Copy Distribution

15. UK OFFICIAL and UK OFFICIAL-SENSITIVE documents may be distributed, both within and outside Contractor premises in such a way as to make sure that no unauthorised person has access. It may be sent by ordinary post in a single envelope. The words UK OFFICIAL or UK OFFICIAL-SENSITIVE must not appear on the envelope. The envelope must bear a stamp or marking that clearly indicates the full address of the office from which it was sent. Commercial Couriers may be used.

16. Advice on the distribution of UK OFFICIAL-SENSITIVE documents abroad or any other general advice including the distribution of UK OFFICIAL-SENSITIVE shall be sought from the Authority.

### Electronic Communication and Telephony and Facsimile Services

17. UK OFFICIAL information may be emailed unencrypted over the internet. UK OFFICIAL-SENSITIVE information shall normally only be transmitted over the internet encrypted using either a National Cyber Security Centre (NCSC) Commercial Product Assurance (CPA) cryptographic product or a UK MOD approved cryptographic technique such as Transmission Layer Security (TLS). In the case of TLS both the sender and recipient organisations must have TLS enabled. Details of the required TLS implementation are available at:

<https://www.ncsc.gov.uk/guidance/tls-external-facing-services>

Details of the CPA scheme are available at:

<https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa>

18. Exceptionally, in urgent cases UK OFFICIAL-SENSITIVE information may be emailed unencrypted over the internet where there is a strong business need to do so, but only with the prior approval of the Authority. However, it shall only be sent when it is known that the recipient has been made aware of and can comply with the requirements of these Security Conditions and subject to any explicit limitations that the Authority require. Such limitations including any regarding publication, further circulation or other handling instructions shall be clearly identified in the email sent with the material.

19. UK OFFICIAL information may be discussed on fixed and mobile telephones with persons located both within the country of the Contractor and overseas. UK OFFICIAL-SENSITIVE information may be discussed on fixed and mobile telephones only where there is a strong business need to do so and only with the prior approval of the Authority.

OFFICIAL-SENSITIVE COMMERCIAL



## DIPS Order Form Template

OFFICIAL-SENSITIVE COMMERCIAL

20. UK OFFICIAL information may be faxed to recipients located both within the country of the Contractor and overseas, however UK OFFICIAL-SENSITIVE information may be transmitted only where there is a strong business case to do so and only with the prior approval of the Authority.

### Use of Information Systems

21. The detailed functions that must be provided by an IT system to satisfy the minimum requirements cannot all be described here in specific detail; it is for the implementers to identify possible means of attack and ensure proportionate security mitigations are applied to prevent a successful attack.

22. The Contractor should ensure **10 Steps to Cyber Security** (Link below) is applied in a proportionate manner for each IT and communications system storing, processing or generating UK OFFICIAL or UK OFFICIAL-SENSITIVE information. The Contractor should ensure competent personnel apply 10 Steps to Cyber Security.

<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>.

23. As a general rule, any communication path between an unauthorised user and the data can be used to carry out an attack on the system or be used to compromise or ex-filtrate data.

24. Within the framework of the 10 Steps to Cyber Security, the following describes the minimum security requirements for processing and accessing UK OFFICIAL-SENSITIVE information on IT systems.

a. Access. Physical access to all hardware elements of the IT system is to be strictly controlled. The principle of “*least privilege*” will be applied to System Administrators. Users of the IT System (Administrators) should not conduct ‘standard’ User functions using their privileged accounts.

b. Identification and Authentication (ID&A). All systems are to have the following functionality:

- (1). Up-to-date lists of authorised users.
- (2). Positive identification of all users at the start of each processing session.

c. Passwords. Passwords are part of most ID&A security measures. Passwords are to be “*strong*” using an appropriate method to achieve this, e.g. including numeric and “*special*” characters (if permitted by the system) as well as alphabetic characters.

d. Internal Access Control. All systems are to have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

e. Data Transmission. Unless the Authority authorises otherwise, UK OFFICIAL-SENSITIVE information may only be transmitted or accessed electronically (e.g. point to point computer

OFFICIAL-SENSITIVE COMMERCIAL



## DIPS Order Form Template

OFFICIAL-SENSITIVE COMMERCIAL

links) via a public network like the Internet, using a CPA product or equivalent as described in paragraph 16 above.

f. Security Accounting and Audit. Security relevant events fall into two categories, namely legitimate events and violations.

(1). The following events shall always be recorded:

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

(2). For each of the events listed above, the following information is to be recorded:

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

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

g. Integrity & Availability. The following supporting measures are to be implemented:

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

h. Logon Banners. Wherever possible, a “*Logon Banner*” will be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. A suggested format for the text (depending on national legal requirements) could be:

*“Unauthorised access to this computer system may constitute a criminal offence”*

OFFICIAL-SENSITIVE COMMERCIAL



## DIPS Order Form Template

OFFICIAL-SENSITIVE COMMERCIAL

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

j. Internet Connections. Computer systems must not be connected direct to the Internet or “*un-trusted*” systems unless protected by a firewall (a software based personal firewall is the minimum but risk assessment and management must be used to identify whether this is sufficient).

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

### Laptops

25. Laptops holding any UK OFFICIAL-SENSITIVE information shall be encrypted using a CPA product or equivalent as described in paragraph 16 above.

26. Unencrypted laptops and drives containing personal data are not to be taken outside of secure sites<sup>1</sup>. For the avoidance of doubt the term “*drives*” includes all removable, recordable media e.g. memory sticks, compact flash, recordable optical media (CDs and DVDs), floppy discs and external hard drives.

27. Any token, touch memory device or password(s) associated with the encryption package is to be kept separate from the machine whenever the machine is not in use, left unattended or in transit.

28. Portable CIS devices holding the Authorities’ data are not to be left unattended in any public location. They are not to be left unattended in any motor vehicles either in view or in the boot or luggage compartment at any time. When the vehicle is being driven the CIS is to be secured out of sight in the glove compartment, boot or luggage compartment as appropriate to deter opportunist theft.

### Loss and Incident Reporting

29. The Contractor shall immediately report any loss or otherwise compromise of any OFFICIAL or OFFICIAL-SENSITIVE material to the Authority. In addition any loss or otherwise compromise of any UK MOD owned, processed or UK MOD Contractor generated UK OFFICIAL or UK OFFICIAL-SENSITIVE material is to be immediately reported to the UK MOD Defence Industry Warning, Advice and Reporting Point (WARP), within the Joint Security Co-ordination Centre (JSyCC) below. This will assist the JSyCC in formulating a formal information security reporting process and the management of any associated risks, impact analysis and upward reporting to the UK MOD’s Chief Information Officer (CIO) and, as appropriate, the Contractor concerned.

---

<sup>1</sup> Secure Sites are defined as either Government premises or a secured office on the contractor premises.

OFFICIAL-SENSITIVE COMMERCIAL



## DIPS Order Form Template

OFFICIAL-SENSITIVE COMMERCIAL

The UK MOD WARP will also advise the Contractor what further action is required to be undertaken.

### **JSyCC WARP Contact Details**

**Email:** [DefenceWARP@mod.gov.uk](mailto:DefenceWARP@mod.gov.uk) (OFFICIAL with no NTK restrictions)

**RLI Email:** [defencewarp@modnet.rli.uk](mailto:defencewarp@modnet.rli.uk) (MULTIUSER)

**Telephone (Office hours):** +44 (0) 30 6770 2185

**JSyCC Out of hours Duty Officer:** +44 (0) 7768 558863

**Mail:** JSyCC Defence Industry WARP

X007 Bazalgette Pavilion,

RAF Wyton, HUNTINGDON, Cambridgeshire, PE28 2EA.

30. Reporting instructions for any security incidents involving MOD classified material can be found in Industry Security Notice 2017/03 as may be subsequently updated at:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/651683/ISN\\_2017-03 - Reporting of Security Incidents.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/651683/ISN_2017-03_-_Reporting_of_Security_Incidents.pdf)

### **Sub-Contracts**

31. Where the Contractor wishes to sub-contract any elements of a Contract to sub-Contractors within its own country or to Contractors located in the UK such sub-contracts will be notified to the Contracting Authority. The Contractor shall ensure that these Security Conditions are incorporated within the sub-contract document.

32. The prior approval of the Authority shall be obtained should the Contractor wish to sub-contract any UK OFFICIAL-SENSITIVE elements of the Contract to a sub-Contractor facility located in another (third party) country. The first page of Appendix 5 (MOD Form 1686 (F1686) of the GovS 007 Security Contractual Process chapter is to be used for seeking such approval. The MOD Form 1686 can be found at Appendix 5 at:

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/710891/2018\\_May\\_Contractual\\_process.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/710891/2018_May_Contractual_process.pdf)

33. If the sub-contract is approved, the Contractor will flow down the Security Conditions in line with paragraph 30 above to the sub-Contractor. Contractors located overseas may seek further advice and/or assistance from the Authority with regards the completion of F1686.

### **Publicity Material**

34. Contractors wishing to release any publicity material or display assets that arises from a Contract to which these Security Conditions apply must seek the prior approval of the Authority. Publicity material includes open publication in the Contractor's publicity literature or website or through the media; displays at exhibitions in any country; lectures or symposia; scientific or technical papers, or any other occasion where members of the general public may have access to the information even if organised or sponsored by the UK Government

OFFICIAL-SENSITIVE COMMERCIAL

## DIPS Order Form Template

OFFICIAL-SENSITIVE COMMERCIAL

### Physical Destruction

35. As soon as no longer required, UK OFFICIAL and UK OFFICIAL-SENSITIVE material shall be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Advice shall be sought from the Authority when information/material cannot be destroyed or, unless already authorised by the Authority, when its retention is considered by the Contractor to be necessary or desirable. Unwanted UK OFFICIAL-SENSITIVE information/material which cannot be destroyed in such a way shall be returned to the Authority.

### Interpretation/Guidance

36. Advice regarding the interpretation of the above requirements should be sought from the Authority.

37. Further requirements, advice and guidance for the protection of UK classified information at the level of UK OFFICIAL-SENSITIVE may be found in Industry Security Notices at:

<https://www.gov.uk/government/publications/industry-security-notices-isns>

### Audit

38. Where considered necessary by the Authority the Contractor shall provide evidence of compliance with this Security Condition and/or permit the inspection of the Contractors processes and facilities by representatives of the Contractors' National/Designated Security Authorities or the Authority to ensure compliance with these requirements.

OFFICIAL-SENSITIVE COMMERCIAL