**Framework Schedule 6 (Order Form Template and Call-Off Schedules)**

**Order Form**

CALL-OFF REFERENCE: **Project\_5056**

# THE BUYER: The Secretary of State for the Department for Education

BUYER ADDRESS **Sanctuary Buildings, Great Smith Street, London, SW1P 3BT**

THE SUPPLIER: Bytes Software Services Ltd

SUPPLIER ADDRESS: Bytes House, Randalls Way, Leatherhead, KT22 7TW

REGISTRATION NUMBER: 12935776

DUNS NUMBER: 225273754

SID4GOV ID: N/A

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 24th January 2021.

It’s issued under the Framework Contract with the reference number RM6068 for the provision of Technology Products and Associated Services.

CALL-OFF LOT(S):

Lot 3 Software & Associated Services

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off 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 Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6068
3. The following Schedules in equal order of precedence:
   * Joint Schedules for RM6068
     + Joint Schedule 2 (Variation Form)
     + Joint Schedule 3 (Insurance Requirements)
     + Joint Schedule 4 (Commercially Sensitive Information)
     + Joint Schedule 10 (Rectification Plan)
     + Joint Schedule 11 (Processing Data)
   * Call-Off Schedules for Project\_5062
     + Call-Off Schedule 1 (Transparency Reports)
     + Call-Off Schedule 5 (Pricing Details)
     + Call-Off Schedule 9 (Security) Part A
     + Call-Off Schedule 10 (Exit Management) Part B
     + Call-Off Schedule 20 (Call-Off Specification)
4. CCS Core Terms (version 3.0.6)
5. Joint Schedule 5 (Corporate Social Responsibility) RM6068
6. 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 Buyer (as decided by the Buyer) take precedence over the documents above.
7. Annexes A to E Call-Off Schedule 6 (ICT Services)

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.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract: None

CALL-OFF START DATE: 24/01/2021

CALL-OFF EXPIRY DATE: 23/01/2023

CALL-OFF INITIAL PERIOD: 2 years

CALL-OFF OPTIONAL EXTENSION None. PERIOD

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification).

LOCATION FOR DELIVERY

Electronic delivery.

DATES FOR DELIVERY OF THE DELIVERABLES

Licenses must in in place and operating in time for the 24th of January 2021.

TESTING OF DELIVERABLES

None.

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be 90 days.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off 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

# £140,792.80.

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details).

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of a Specific Change in Law or Benchmarking using Call-Off Schedule 16 (Benchmarking) where this is used.

REIMBURSABLE EXPENSES

None.

PAYMENT METHOD

Electronic Payment (BACS).

Monthly invoices shall be submitted against the Buyer’s actual consumption of Google Maps Platform licenses.

BUYER’S INVOICE ADDRESS:

REDACTED

BUYER’S AUTHORISED REPRESENTATIVE

REDACTED

BUYER’S ENVIRONMENTAL POLICY

None.

BUYER’S SECURITY POLICY

Annex 1 – Departmental Security Standards Special Clauses SUPPLIER’S AUTHORISED REPRESENTATIVE

REDACTED

SUPPLIER’S CONTRACT MANAGER

REDACTED

PROGRESS REPORT FREQUENCY

On the first Working Day of each calendar month.

PROGRESS MEETING FREQUENCY

Monthly.

KEY STAFF

REDACTED

KEY SUBCONTRACTOR(S)

N/A

COMMERCIALLY SENSITIVE INFORMATION

None.

SERVICE CREDITS

Not applicable.

ADDITIONAL INSURANCES

Not applicable.

GUARANTEE

Not applicable.

SOCIAL VALUE COMMITMENT

he 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).

**Call-Off 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-](https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles) [update-to-transparency-principles](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 Framework 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.

**Annex A: List of Transparency Reports**

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **Content** | **Format** | **Frequency** |
| Monthly usage and charges  figures | * Licenses usage * Monthly   charges | As preferred by Supplier. | Monthly. |

**Call-Off Schedule 5 (Pricing Details)**

Google Maps Platform is a consumption-based model. Under the terms of the contract, Buyer will pay for the exact quantity used each month. The figures represented in the table below are a forecast of the overall cost over a 24 months consumption.

It is understood that the below figures are a forecast and that charges may vary monthly based on actual consumption.

REDACTED

**Call-Off Schedule 9 (Security)**

**Part A: Short Form Security Requirements**

# Definitions

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

# Complying with security requirements and updates to them

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

The Supplier shall comply with the requirements in this Schedule in respect of the Security Management Plan. Where specified by a Buyer that has undertaken a Further Competition it shall also comply with the Security Policy and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

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

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.

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.

# Security Standards

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.

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

is in accordance with the Law and this Contract;

as a minimum demonstrates Good Industry Practice;

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

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

The references to standards, guidance and policies contained or set out in Paragraph [3.2](#_bookmark0) 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.

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.

# Security Management Plan

**Introduction**

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.

# Content of the Security Management Plan

The Security Management Plan shall:

 comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

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

 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;

 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;

 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;

 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

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

# Development of the Security Management Plan

Within twenty (20) Working Days after the Start Date and in accordance with Paragraph [4.4](#_bookmark2), 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.

If the Security Management Plan submitted to the Buyer in accordance with Paragraph [4.3.1](#_bookmark1), or any subsequent revision to it in accordance with Paragraph [4.4](#_bookmark2), 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.

The Buyer shall not unreasonably withhold or delay its decision to Approve or not the Security Management Plan pursuant to Paragraph

[4.3.2](#_bookmark1). 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](#_bookmark0) shall be deemed to be reasonable.

Approval by the Buyer of the Security Management Plan pursuant to Paragraph [4.3.2](#_bookmark1) or of any change to the Security Management Plan in accordance with Paragraph [4.4](#_bookmark2) shall not relieve the Supplier of its obligations under this Schedule.

# Amendment of the Security Management Plan

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

 emerging changes in Good Industry Practice;

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

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

 any new perceived or changed security threats; and

 any reasonable change in requirements requested by the Buyer.

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:

 suggested improvements to the effectiveness of the Security Management Plan;

 updates to the risk assessments; and

 suggested improvements in measuring the effectiveness of controls.

Subject to Paragraph [4.4.4](#_bookmark3), 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](#_bookmark2), a request by the Buyer or otherwise) shall be subject to the Variation Procedure.

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.

# Security breach

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.

Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph [5.1](#_bookmark3), the Supplier shall:

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

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

 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;

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

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

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.

**Call-Off Schedule 10 (Exit Management)**

**Part B: Short Form Exit Management Requirements**

1. Within 20 (twenty) working days of the Start Date the Supplier must provide the Buyer with an exit plan which ensures continuity of service and which the Supplier will follow.

1. The Supplier must ensure that the exit plan clearly sets out the Supplier’s methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its Replacement Supplier at the expiry or if the contract ends before the scheduled expiry.
2. The exit plan should set out full details of timescales, activities and roles and responsibilities of the Parties for:

* the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
* the strategy for export and migration of Buyer data from the Supplier system to the Buyer or a Replacement Supplier, including conversion to open standards or other standards required by the Buyer
* the transfer of project- specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
* the testing and assurance strategy for exported Buyer data
* if relevant, TUPE-related activity to comply with the TUPE regulations
* any other activities and information which are reasonably required to ensure continuity of Service during the exit period and an orderly transition

1. When requested, the Supplier will help the Buyer to migrate the Services to a Replacement Supplier in line with the exit plan. This will be at the Supplier’s own expense if the Call-Off Contract ended before the Expiry Date due to Supplier cause. Otherwise any additional costs incurred by the Supplier in providing such assistance shall be subject to the Variation Procedure.

**Call-Off Schedule 20 (Call-Off Specification)**

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract.

The DfE is seeking Google Maps Platform licenses with the following requirements:

* + Google Maps Platform Static Map API (estimate based on 21,923,667 queries per month),
  + Google Maps Platform Dynamic Map API (estimate based on 3,500,000 queries per month),
  + Google Maps Platform Directions API (estimate based on 130,000 queries per month),
  + Google Maps Platform Places API (estimate based on 2,500 queries per month)

Additional information:

* Cost model to be 'pay as you go', based on monthly payments, in line with Google Maps Platform Terms of Service
* Access to the Google Cloud Platform Console’s API Dashboard must be granted to Buyer so that usage can be monitored internally.

**ANNEX 1 – DEPARTMENTAL SECURITY STANDARDS SPECIAL CLAUSES**

**Departmental Security Standards for Business Services and ICT Contracts**

|  |  |
| --- | --- |
| “BPSS”  “Baseline Personnel Security Standard” | means the Government’s HMG Baseline Personal Security Standard . Further information can be found at: [https://www.gov.uk/government/publications/go](https://www.gov.uk/government/publications/government-baseline-personnel-security-standard) [vernment-baseline-personnel-security-standard](https://www.gov.uk/government/publications/government-baseline-personnel-security-standard) |
| “CCSC”  “Certified Cyber Security Consultancy” | is the National Cyber Security Centre’s (NCSC) approach to assessing the services provided by consultancies and  confirming that they meet NCSC's standards. See website:  [https://www.ncsc.gov.uk/scheme/certified-](https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy) [cyber-consultancy](https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy) |
| “CCP”  “Certified Professional” | is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession. See website:  [https://www.ncsc.gov.uk/information/about-](https://www.ncsc.gov.uk/information/about-certified-professional-scheme) [certified-professional-scheme](https://www.ncsc.gov.uk/information/about-certified-professional-scheme) |
| “CPA”  “Commercial Product Assurance”  [formerly called “CESG Product Assurance”] | is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards.. See website: [https://www.ncsc.gov.uk/scheme/commercial-](https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa) [product-assurance-cpa](https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa) |
| “Cyber Essentials” “Cyber Essentials Plus” | Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme. |

|  |  |
| --- | --- |
|  | There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to these providers:  [https://www.cyberessentials.ncsc.gov.uk/getting](https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body)  [-certified/#what-is-an-accreditation-body](https://www.cyberessentials.ncsc.gov.uk/getting-certified/#what-is-an-accreditation-body) |
| “Data”  “Data Controller”  “Data Protection Officer” “Data Processor” “Personal Data”  “Personal Data requiring Sensitive Processing”  “Data Subject”, “Process” and “Processing” | shall have the meanings given to those terms by the Data Protection Act 2018 |
| "Department’s Data" “Department’s Information” | is any data or information owned or retained in order to meet departmental business objectives and tasks, including:   1. any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:    1. supplied to the Contractor by or on behalf of the Department; or    2. which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or 2. any Personal Data for which the Department is the Data Controller; |
| “DfE”  “Department” | means the Department for Education |
| “Departmental Security Standards” | means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver. |

|  |  |
| --- | --- |
| “Digital Marketplace / G-Cloud” | means the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. |
| End User Devices | means the personal computer or consumer devices that store or process information. |
| “Good Industry Practice” “Industry Good Practice” | means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “Good Industry Standard” “Industry Good Standard” | means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector. |
| “GSC”  “GSCP” | means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: [https://www.gov.uk/government/publications/go](https://www.gov.uk/government/publications/government-security-classifications) [vernment-security-classifications](https://www.gov.uk/government/publications/government-security-classifications) |
| “HMG” | means Her Majesty’s Government |
| “ICT” | means Information and Communications Technology (ICT) and is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution |
| “ISO/IEC 27001” “ISO 27001” | is the International Standard for Information Security Management Systems Requirements |
| “ISO/IEC 27002” “ISO 27002” | is the International Standard describing the Code of Practice for Information Security Controls. |
| “ISO 22301” | is the International Standard describing for Business Continuity |
| “IT Security Health Check (ITSHC)” “IT Health Check (ITHC)” | means an assessment to identify risks and  vulnerabilities in systems, applications and networks which may compromise the |

|  |  |
| --- | --- |
| “Penetration Testing” | confidentiality, integrity or availability of information held on that IT system. |
| “Need-to-Know” | means the Need-to-Know principle employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties. |
| “NCSC” | The National Cyber Security Centre (NCSC) is the UK government’s National Technical Authority for Information Assurance. The NCSC website is [https://www.ncsc.gov.uk](https://www.ncsc.gov.uk/) |
| “OFFICIAL”  “OFFICIAL-SENSITIVE” | the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP).  the term ‘OFFICIAL–SENSITIVE is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the GSCP. |
| “RBAC”  “Role Based Access Control” | means Role Based Access Control. A method of restricting a person’s or process’ access to information depending on the role or functions assigned to them. |
| “Storage Area Network” “SAN” | means an information storage system typically presenting block based storage (i.e. disks or virtual disks) over a network interface rather than using physically connected storage. |
| “Secure Sanitisation” | means the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level.  NCSC Guidance can be found at: [https://www.ncsc.gov.uk/guidance/secure-](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media) [sanitisation-storage-media](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media) |

|  |  |
| --- | --- |
|  | The disposal of physical documents and hardcopy materials advice can be found at: <https://www.cpni.gov.uk/secure-destruction> |
| “Security and Information Risk Advisor” “CCP SIRA”  “SIRA” | means the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also:  [https://www.ncsc.gov.uk/articles/about-certified-](https://www.ncsc.gov.uk/articles/about-certified-professional-scheme) [professional-scheme](https://www.ncsc.gov.uk/articles/about-certified-professional-scheme) |
| “Senior Information Risk Owner” “SIRO” | means the Senior Information Risk Owner (SIRO) responsible on behalf of the DfE Accounting Officer for overseeing the management of information risk across the organisation. This includes its executive agencies, arms length bodies (ALBs), non- departmental public bodies (NDPBs) and devolved information held by third parties. |
| “SPF”  “HMG Security Policy Framework” | means the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. [https://www.gov.uk/government/publications/se](https://www.gov.uk/government/publications/security-policy-framework) [curity-policy-framework](https://www.gov.uk/government/publications/security-policy-framework) |

* 1. The Contractor shall be aware of and comply the relevant [HMG security policy](https://www.gov.uk/government/publications/security-policy-framework) [framework](https://www.gov.uk/government/publications/security-policy-framework), [NCSC guidelines](https://www.ncsc.gov.uk/section/advice-guidance/all-topics) and where applicable DfE Departmental Security Standards for Contractors which include but are not constrained to the following clauses.
  2. Where the Contractor will provide products or services or otherwise handle information at OFFICIAL for the Department, the requirements of [Cabinet](https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification) [Office Procurement Policy Note – Use of Cyber Essentials Scheme](https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification) [certification](https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification) - [Action Note 09/14](https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification) dated 25 May 2016, or any subsequent updated document, are mandated; that “contractors supplying products or services to HMG shall have achieved, and will be expected to retain certification at the appropriate level for the duration of the contract. The

certification scope shall be relevant to the services supplied to, or on behalf of, the Department.

* 1. Where clause 12.2 above has not been met, the Contractor shall have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Management Systems Requirements).

The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department. The scope of certification and the statement of applicability must be acceptable, following review, to the Department, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).

* 1. The Contractor shall follow the UK Government Security Classification Policy (GSCP) in respect of any Departmental Data being handled in the course of providing this service and will handle all data in accordance with its security classification. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).
  2. Departmental Data being handled in the course of providing an ICT solution or service must be separated from all other data on the Contractor’s or sub-contractor’s own IT equipment to protect the Departmental Data and enable the data to be identified and securely deleted when required in line with clause 12.14.
  3. The Contractor shall have in place and maintain physical security to premises and sensitive areas in line with ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access), CCTV, alarm systems, etc.
  4. The Contractor shall have in place and maintain an appropriate user access control policy for all ICT systems to ensure only authorised personnel have access to Departmental Data. This policy should include appropriate segregation of duties and if applicable role based access controls (RBAC).
  5. The Contractor shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Departmental Data, including but not limited to:
     + physical security controls;
     + good industry standard policies and processes;
     + malware protection;
     + boundary access controls including firewalls;
     + maintenance and use of fully supported software packages in accordance with vendor recommendations;
     + software updates and patching regimes including malware signatures, for operating systems, network devices, applications and services;
     + user access controls, and;
     + the creation and retention of audit logs of system, application and security events.
  6. The contractor shall ensure that any departmental data (including email) transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device shall be encrypted when transmitted.
  7. The contractor shall ensure that any departmental data which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the department except where the department has given its prior written consent to an alternative arrangement.
  8. The contractor shall ensure that any device which is used to process departmental data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security>and [https://www.ncsc.gov.uk/collection/end-user-device-security/eud-](https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles) [overview/eud-security-principles](https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles).
  9. Whilst in the Contractor’s care all removable media and hardcopy paper documents containing Departmental Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.

The term ‘lock and key’ is defined as: “securing information in a lockable desk drawer, cupboard or filing cabinet which is under the user’s sole control and to which they hold the keys”.

* 1. When necessary to hand carry removable media and/or hardcopy paper documents containing Departmental Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.

The term ‘under cover’ means that the information is carried within an opaque folder or envelope within official premises and buildings and within a closed briefcase or other similar bag or container when outside official premises or buildings.

* 1. In the event of termination of contract due to expiry, liquidation or non- performance, all information assets provided, created or resulting from the service shall not be considered as the supplier’s assets and must be returned to the department and written assurance obtained from an appropriate officer of the supplying organisation that these assets regardless of location and format have been fully sanitised throughout the organisation in line with clause 12.15.
  2. In the event of termination, equipment failure or obsolescence, all Departmental information and data, in either hardcopy or electronic format, that is physically held or logically stored by the Contractor must be accounted for and either physically returned or securely sanitised or destroyed in accordance with the current HMG policy using an NCSC approved product or method.

Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as data stored in a cloud system, Storage Area Network (SAN) or on shared backup tapes, then the Contractor or sub-

contractor shall protect the Department’s information and data until such time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.

Evidence of secure destruction will be required in all cases.

* 1. Access by Contractor or sub-contractor staff to Departmental Data shall be confined to those individuals who have a “need-to-know” in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Contractor or sub-contractor staff must complete this process before access to Departmental Data is permitted.
  2. All Contractor or sub-contractor employees who handle Departmental Data shall have annual awareness training in protecting information.
  3. The Contractor shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Contractor has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
  4. Any suspected or actual breach of the confidentiality, integrity or availability of Departmental Data handled in the course of providing this service shall be recorded as an incident. This includes any non-compliance with these Departmental Security Standards for Contractors, or other Security Standards pertaining to the solution.

Incidents shall be reported to the department immediately, wherever practical, even if unconfirmed or when full details are not known, but always within 24 hours of discovery. If incident reporting has been delayed by more than 24 hours, the contractor should provide an explanation about the delay.

Incidents shall be reported through the department’s nominated system or service owner.

Incidents shall be investigated by the contractor with outcomes being notified to the Department.

* 1. The Contractor shall ensure that any IT systems and hosting environments that are used to handle, store or process Departmental Data shall be subject to independent IT Health Checks (ITHC) using an NCSC CHECK Scheme ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Department and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.
  2. The Contractor or sub-contractors providing the service will provide the Department with full details of any actual or future intent to develop, manage, support, process or store Departmental Data outside of the UK mainland. The Contractor or sub-contractor shall not go ahead with any such proposal without the prior written agreement from the Department.
  3. The Department reserves the right to audit the Contractor or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Contractor’s, and any sub-contractors’, compliance with the clauses contained in this Section.
  4. The Contractor and sub-contractors shall undergo appropriate security assurance activities and shall provide appropriate evidence including the production of the necessary security documentation as determined by the department. This will include obtaining any necessary professional security resources required to support the Contractor’s and sub-contractor’s security assurance activities such as: a Security and Information Risk Advisor (SIRA) certified to NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Cyber Professional (CCP) schemes.
  5. Where the Contractor is delivering an ICT solution to the Department they shall design and deliver solutions and services that are compliant with the HMG Security Policy Framework in conjunction with current NCSC Information Assurance Guidance and Departmental Policy. The Contractor will provide the Department with evidence of compliance for the solutions and services to be delivered. The Department’s expectation is that the Contractor shall provide written evidence of:
* Compliance with HMG Minimum Cyber Security Standard.
* Any existing security assurance for the services to be delivered, such as: ISO/IEC 27001 / 27002 or an equivalent industry level certification.
* Any existing HMG security accreditations or assurance that are still valid including: details of the awarding body; the scope of the accreditation; any caveats or restrictions to the accreditation; the date awarded, plus a copy of the residual risk statement.
* Documented progress in achieving any security assurance or accreditation activities including whether documentation has been produced and submitted. The Contractor shall provide details of who the awarding body or organisation will be and date expected.
  1. The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this