**Framework Schedule 1 (Specification)**

This Schedule sets out what we and our buyers want.

The supplier must only provide the Deliverables for the Lot that they have been appointed to.

For all Lots and/or Deliverables, the Supplier must help Buyers comply with any specific applicable Standards of the Buyer.

The Deliverables and any Standards set out in Paragraph 1 below may be refined (to the extent permitted and set out in the Order Form) by a Buyer during a Further Competition Procedure to reflect its Deliverables Requirements for entering a particular Call-Off Contract.

**Our social value priorities**

These are our priorities in this procurement:

* Covid-19 Recovery
* Tackling Economic Inequality
  + Create new businesses, new jobs and new skills
  + Increase supply chain resilience and capacity
* Fighting Climate Change
* Equal Opportunity
  + Reduce the disability employment gap
  + Tackle workforce inequality
* Wellbeing
  + Improve health and wellbeing
  + Improve community integration

The buyer can identify specific social value priorities at call-off. Please refer to Annex 4 - Supplier’s Guide to delivering Social Value through eDisclosure and Review Services RM6336

1. **INTRODUCTION**
   1. The purpose of this Framework Schedule 1 is to provide a description of the Services that the Supplier shall deliver to the Buyer under the Lot-based structure of this Framework Contract.
   2. The Services shall include:

* simple low volume work service packages;
* standard end-to-end service packages;
* provision of document reviewers; and
* high security end-to-end service packages.
  1. The Framework shall comprise of 4 Lots, as detailed in Section 3 – Lot Descriptions.

1. **PURPOSE**
   1. This Framework Contract shall be available to Buyers to provide Electronic Disclosure Services (“eDisclosure Services”) throughout the UK Public Sector.
   2. Many of the terms used to describe the Service requirements within this Framework Schedule 1 are based upon the Electronic Discovery Reference Model (“EDRM”), details of which can be found at:

<https://edrm.net/resources/frameworks-and-standards/edrm-model/>

The term ‘Document’ is used as defined in Part 31 of the Civil Procedure Rules (“CPR”). For the avoidance of doubt, where any terms are defined in the Framework Contract or Call Off Contract, and there is a different definition to that found in the EDRM then the definition in the agreements shall take precedence.

* 1. The Service requirements under the Lot-based structure of this Framework Contract span a wide and diverse customer base and require a variety of specialist services encompassed by the EDRM, but are here divided into the following eight (8) stages:
     1. Strategic Oversight, Advice and Support;
     2. Document Identification;
     3. Document Preservation and Collection;
     4. Document Processing;
     5. Document Review;
     6. Document Production;
     7. Disclosure from Other Opponent Parties; and
     8. Presentation at Trial.
  2. The Framework Contract shall be structured to offer Buyers flexibility and choice. It shall be a matter of judgement for the Buyer to decide which particular Lot(s) are most appropriate to meet with their specific requirements and best deliver their business needs, and to ensure the most appropriate fit for the Buyer’s requirements including value for money.

1. **LOT DESCRIPTIONS**
   1. A Buyer shall not be restricted to the specific Services within each Lot of this Framework Agreement (as long as their requirements are relevant to the broad category of the Lot). Buyers may choose to purchase specific services within the scope of a lot, without for example using a full end-to-end service. The Framework shall be comprised of the following Lots:

| **Lot 1 - Simple Low Volume Work Service Package for documents and data with a security classification up to ‘Official’ (and including ‘Official Sensitive’)**  The scope of this Lot is the provision of e-Disclosure Services in respect of an overall initial dataset (pre-processing) of no more than 5GBs Electronically Stored Information (“ESI”) plus no more than 1,750 pages of hardcopy documents (as defined in Pricing – Attachment 3). The exercise will comprise the processing of one tranche of data (applying one set of date ranges and search terms, plus de-duplication and email threading), provision of a review platform, one production and potentially the loading and review of the other side’s data only.  The Supplier shall be able to provide the following Services, including all Mandatory Requirements that specifically relate to **Lot 1,** as detailed in Section 4 of this Framework Schedule 1:  Mandatory requirements for **Lot 1** aredetailed at 4.6, 4.7, 4.8, 4.9, and 4.11 of this document:   * Document Processing, as detailed in paragraph 4.6; * Document Review, as detailed in paragraph 4.7; * Document Production, as detailed in paragraph 4.8; * Disclosure from Other Opponent Parties, as detailed in paragraph 4.9; and * Security Requirements, as detailed in paragraph 4.11 |
| --- |
| **Lot 2 - End to End Service package for documents and data with a security classification up to ‘Official’ (and including ‘Official Sensitive’)**  The Supplier shall be able to provide the following Services, including all Mandatory Requirements that specifically relate to **Lot 2,** as detailed in Section 4 of this Framework Schedule 1:  **ALL** of the Mandatory requirements relate to **Lot 2.**   * Strategic Oversight, Advice and Support, as detailed in paragraph 4.3; * Document Identification, as detailed in paragraph 4.4; * Data Preservation and Collection, as detailed in paragraph 4.5; * Document Processing, as detailed in paragraph 4.6; * Document Review, as detailed in paragraph 4.7; * Document Reviewers, as detailed in paragraph 4.7A; * Document Production, as detailed in paragraph 4.8; * Disclosure from Other Opponent Parties, as detailed in paragraph 4.9; * Presentation at Trial, as detailed at paragraph 4.10; and * Security Requirements, as detailed in paragraph 4.11 |
| **Lot 3 - Document Reviewers for documents and data with a security classification up to ‘Official’ (and including ‘Official Sensitive’)**  The Supplier shall be able to provide the following Service, including all Mandatory Requirements that specifically relate to **Lot 3,** as detailed in Section 4 of this Framework Schedule 1:  Mandatory requirements for **Lot 3** are detailed at 4.7A and 4.11 of this document:   * Document Reviewers, as detailed at paragraph 4.7A;   and   * Security Requirements, as detailed in paragraph 4.11 |
| **Lot 4 - End to End Service for documents and data with a security classification up to and including ‘Secret’ and ‘Top Secret’**  The Supplier shall be able to provide the following Services, including all Mandatory Requirements that specifically relate to **Lot 4,** as detailed in Section 4 of this Framework Schedule 1:  **ALL** of the Mandatory requirements relate to **Lot 4**:   * Strategic oversight, Advice and Support, as detailed at paragraph 4.3; * Document Identification, as detailed at paragraph 4.4; * Data Preservation and Collection, as detailed at paragraph 4.5; * Document Processing, as detailed at paragraph 4.6; * Document Review, as detailed at paragraph 4.7; * Document Reviewers, as detailed in paragraph 4.7A; * Document Production, as detailed at paragraph 4.8; * Disclosure from Other Opponent Parties, as detailed at paragraph 4.9; * Presentation at Trial, as detailed at paragraph 4.10; and * Security Requirements, as detailed in paragraph 4.11 |

1. **MANDATORY REQUIREMENTS FOR SERVICE PROVISION**

The Supplier shall meet the following requirements in their entirety in order to provide the Services under each Lot as defined in paragraph 3 above, during the Framework Contract Period and until any Call-Off Contracts established under this Framework Contract expire. Where the Buyer is referenced this shall also be interpreted to include the Buyer’s client.

* 1. **Mandatory to all lots**
     1. The Supplier shall consider the quality, cost-effectiveness and efficiency of any proposed solution, and shall work to review and improve its systems with regard to these elements on an ongoing basis throughout the duration of the Framework.
     2. The Supplier shall work to meet deadlines agreed with the Buyer at Call-Off and is expected to manage its staff and internal processes to achieve this.
     3. The Supplier shall communicate with the Buyer to ensure timely delivery and appropriate prioritisation of workload where necessary.
     4. Direct management of the Supplier’s own staff and processes focused on day to day management, achieving deliverables and meeting timelines are core elements of the service which are not specific to any given lot and will not attract any additional charge.
     5. The Supplier shall provide budgetary management throughout the duration of the Contract (such to also include regular analysis and reporting to the Buyer on costs to date, the possibility of changes to previously agreed cost estimates (before they occur), and the expected costs of stopping the exercise immediately should the case settle).
     6. The elements referred to in 4.1.4 and 4.1.5 are separate to Strategic Oversight, Advice and Support, which is detailed in 4.3 and concerns the provision of analysis and advice for the eDisclosure exercise as a whole.
     7. Suppliers shall deliver all elements of the services relevant to their given Lot as part of this Framework, whether these are marked as “All Exercises” or “Less Commonly Required”. These distinctions are set out purely to aid the Buyer at Call-Off.
     8. Staff costs and overheads associated with supplying the services set out shall be included in the price for those services and will not attract any additional charge as per the instructions in Attachment 3 (Pricing).
  2. **Mandatory Requirements for Lots 1, 2 and 4**
     1. The Supplier shall respond to project support queries and requests (for example in relation to urgent disclosure issues, as notified by the Buyer) on Call-Off Contracts within four (4) hours.
     2. The Supplier shall implement changes to the platform such as the creation of new tags and batches within four (4) hours.
     3. Under each Call-Off Contract the Supplier shall provide at least three (3) points of contact who shall be responsible and may be contacted by the Buyer for effecting changes to the platform.
  3. **Strategic Oversight, Advice and Support** 
     1. The Supplier shall provide strategic advice and support to the Buyer in relation to best practice, and the most efficient and cost effective methods of conducting the disclosure exercise as a whole.
     2. The Service under this section 4.3 is to include advice in respect of the most appropriate approach to document collection, as well as conducting an initial analysis following receipt of the data and advising at the outset on the potential conduct of the review exercise before it begins including, but not limited to:
        1. possible strategies for managing the overall exercise (as well as costs thereof), including but not limited to ‘rolling disclosure’, data sampling, near deduplication, bulk redaction, batching, and tagging structures;
        2. possible complications/problems typically associated with collected data and recommended strategies for overcoming anticipated difficulties e.g. password protected files, and near duplicates; and
        3. how best to deal with and interrogate the other parties’ disclosure;
     3. Services under this section 4.3 shall also include advice and support in respect of use technology (e.g. technology-assisted review) to best effect including but not limited to :
     4. analytics;
     5. predictive coding;
     6. continuous active learning;
     7. visualisation of data including mapping the way other parties in the dispute worked; concept clustering; and identifying an absence of information;
     8. prioritising keyword responsive documents; and
     9. identifying behaviours (e.g. fraudulent, negligent, incompetent conduct).
     10. The Service referred to in this section 4.3 is to continue for the duration of the Call-Off Contract including regular advice with reviewing of the process, the prompt handling of queries raised from a strategic perspective and advice throughout on the most efficient ways of conducting the exercise.
     11. The Supplier will, if requested by the Buyer, attend and advise the Buyer at case management conferences, meetings or similar; for instance to assist with the completion of the Electronic Documents Questionnaire or agreeing a disclosure protocol with opponents.
     12. The Supplier shall also assist with providing written statements or inputting into draft statements and reports for the consideration of the court (or other relevant tribunals) as required.
     13. If required, the Supplier shall attend court (or other relevant tribunals) in person to give oral evidence.
  4. **Document Identification**

*All exercises*

* + 1. In consultation with the Buyer, the Supplier shall conduct a proportionate exercise investigating and establishing an accurate picture of all the Buyer’s data sources (data mapping) including sources of hardcopy documents not otherwise held electronically.
    2. As advised by the Buyer, the Supplier shall identify potentially relevant ESI sources in relation to the information for proper and defensible completion (by the Buyer) of the Electronic Documents Questionnaire found at the schedule to Practice Direction 31B of the CPR or any other law, rule or regulation that may, from time to time, be relevant, including investigation and consideration of:
       1. internal policies and practices in relation to creation and maintenance of ESI, storage (on-site or off-site), and ultimately destruction thereof;
       2. key witnesses, relevant data custodians, and key time frames;
       3. potentially relevant document and data types;
       4. relevant document management systems used by the Buyer;
       5. types of electronic mail servers used by the Buyer, including hardware, operating systems, software, location of servers, responsible administrators and also relevant data retention polices;
       6. back-up media, retired hardware and disaster recovery systems;
       7. legacy systems, including how data has been migrated from past technologies;
       8. cloud computing or third party-systems; and
       9. additional data sources beyond the servers of the Buyer, including digital voicemail stores, portable devices and mobile telephones, information stored on the Buyer’s intranet, instant messaging, and any other collaborative systems.
    3. As advised by the Buyer, the Supplier shall identify potentially relevant hardcopy document sources held by the Buyer, including investigation and consideration of:
       1. the Buyer’s internal policies and practices in relation to creation and maintenance of paper files or records, storage (on-site or off-site), and ultimately destruction thereof;
       2. key witnesses, relevant data custodians, and key time frames;
       3. off-site storage;
       4. on-site managed filing;
       5. the Buyer’s departmental filing;
       6. personal filing; and
       7. personal possession.
    4. The Supplier shall provide advice and assistance, in the context of the Call-Off Contract, to ensure compliance with current rules, practices and procedures in respect of eDisclosure.

*Less Commonly Required*

* + 1. On request, the Supplier shall document the steps taken for the document identification phase, by way of a comprehensive report to the Buyer detailing compliance with the requirements of Part 31 of the CPR or any other law, rule or regulation that may, from time to time, be relevant, which:
       1. satisfies them that the searches are evidenced by a clear audit trail, are reasonable and proportionate, and comply with the Buyer’s disclosure obligations; and
       2. recommends an early defensible and strategic approach to the collection, preservation, processing, review and production of the Buyer’s information, and includes initial indicative cost estimates and work timetables.
  1. **Data Preservation and Collection**

*For all Exercises*

* + 1. The Supplier shall assist the Buyer to preserve all original potentially relevant data (hardcopy and electronic), for possible use in the litigation process.
    2. The Supplier shall assist the Buyer to securely and forensically acquire all potentially relevant ESI (including metadata) from the sources identified in the document identification phase or otherwise as instructed by the Buyer (whilst maintaining the ESI’s integrity) by way of either:
       1. copying the data to portable media and removing it into the custody of the Supplier, the Buyer or their client department (as advised by the Buyer); or
       2. if required, consolidating the data, including the option of doing so within a database store located on the Buyer’s premises.
    3. Where appropriate and if so instructed by the Buyer, the Supplier shall also visit any site where the Buyer’s data is held and conduct necessary inspections prior to the above activity.
    4. The Supplier shall assist the Buyer to securely acquire all potentially relevant hardcopy documents from the sources identified in the document identification phase or otherwise as instructed by the Authority, and take that material into the Supplier’s possession.

*Less Commonly Required*

* + 1. On request the Supplier shall document the steps taken as above, by way of a comprehensive report to the Buyer detailing compliance with the requirements of Part 31 of the CPR, which will satisfy them that preservation and collection exercises are evidenced by a clear audit trail, and that the steps taken are reasonable and proportionate and comply with the Buyer’s legal obligations.
  1. **Document Processing**

*For all Exercises*

* + 1. The Supplier shall assess the data collected (whether by the Supplier as above or delivered by the Buyer or their client) and report to the Buyer regarding:
       1. precisely what data has been collected, including data type and volume;
       2. possible complications / problems typically associated with such data and recommend appropriate strategies for overcoming anticipated difficulties;
       3. precisely what data has been excluded and why, such as including data type and size; and
       4. where possible, from the Buyer’s data already analysed, provide a basic indicative assessment of the anticipated nature, size and extent of the relevant data held by other litigants, with a view to aiding agreement with other litigants as regards to a proportionate approach to the disclosure exercise.
    2. The Supplier shall prepare the data for processing, including:
       1. restoring back-ups;
       2. converting legacy formats, whilst maintaining the integrity of the originals and recording any conversion anomalies;
       3. extracting files from container files;
       4. cataloguing and itemising all extracted files, emails, attachments and loose documents;
       5. in respect of hardcopy documents, where considered or otherwise required (as agreed in consultation with the Buyer), to bulk scan the aforementioned hardcopy documents into electronic form, including recording key information against each such document (at least author, recipient, subject and date), such to then be stored in electronic form in the same manner and place as ESI collected in the Preservation and Collection phase. This includes placing the documents in a form such that they can be processed in order to electronically extract the text and any other content; and
       6. identifying and eliminating duplicates and/or near duplicates (deduplication).
    3. The Supplier shall identify data that should be moved forward to the Document Review stage, by using a variety of suitable methods agreed with the Buyer, such to include at least the option of:
       1. pre-selected search terms and word strings (as advised by the Buyer), to be applied across all prepared data;
       2. grouping documents at least as follows:
    4. sharing of common concepts; or were created at a particular time or by a particular individual or group of individuals;
    5. email threading, by linking email chains to result in a continuous email exchange from first to last email, across multiple users;
    6. linking any other data threads generally (and recording any relevant audit information that may be available); and
    7. data sampling
    8. where they are receptive to common keyword hits
    9. by date range
    10. by custodian
    11. The Buyer shall transform the data selected for review into a common format necessary for the review platform to be used, whilst also retaining the data in its Native Form. This should include the following options (as elected by the Buyer) of:
        1. cross-referencing documents from different parties with a view to performing searches across responses;
        2. relevance ranking; and
        3. identification (in accordance with parameters set by the Buyer) of near-duplicates (near-duplication).
    12. The Supplier shall implement an appropriate quality assurance procedure to check that the proposed disclosure meets expectations and that any significant variances from expectations are accounted for and explained.

*Less Commonly Required*

* + 1. On request the Supplier shall document the steps taken for the Document Processing phase by way of a comprehensive report to the Buyer, detailing compliance with the requirements of Part 31 of the CPR, which will provide evidence (as evidenced by a clear audit trail with clear proof of chains of custody) that the steps taken are defensible, reasonable, and proportionate and comply with the Buyer’s legal obligations.
  1. **Document Review**

*For all Exercises*

* + 1. The Supplier shall support the Buyer in their review of the data produced from the data processing stage, and the identification of disclosable information by:
       1. providing access to and support for suitable software solutions to aid the review process at the Buyer premises, their client’s premises, or premises provided by the Supplier, with software to allow for:
    2. lawyer review and selection of disclosable documents;
    3. categorisation of each document identified as disclosable according to a pre-selected set of categories (for example relevance to certain issues in the litigation);
    4. if required, providing and supporting necessary hardware (for example document review workstations) for use in the review process either at the Buyer premises, their client’s premises, or premises provided by the Supplier, together with the aforementioned software;
    5. providing access to and supporting suitable software solutions which provide for the electronic redaction of ESI as part of the review process, such to be capable of:

1. recording, against each redaction, the basis on which it is made (for example legal professional privilege or irrelevance);
2. also maintaining the original document in its un-redacted form and maintaining a link between the two versions; and
3. ensuring consistent redaction across all documents (i.e. consistency in redaction or non-redaction of identical text across all documents) by way of pre-established redaction rules or some other reliable means of ensuring consistency.
4. applying multiple redactions to single documents and batches of documents including the ability to mark the redaction with the reason (e.g. “LPP”, “GDPR”, “Confidential”);
5. where it is necessary to have different versions of a document with different redactions (for example in the context of multi layered confidentiality rings or closed material procedures) be able to maintain the link between different versions of the same document and also production to specified individuals is strictly managed.
   * + 1. providing secure off-site hosting of data subject to the review process, and managing access thereto (whether remotely or otherwise);
     1. On request the Supplier shall document the steps taken for the Document Review phase by way of a comprehensive report to the Buyer, detailing compliance with the requirements of Part 31 of the CPR, which will satisfy them (as evidenced by a clear audit trail with clear proof of chains of custody), that the steps taken are reasonable and proportionate and comply with the Buyer’s legal obligations.

**4.7A Document Reviewers**

*For all Exercises*

**4.7A.1** The Supplier shall design and implement an appropriate solution to conduct a document review exercise that meets the objectives of the Authority including by, at a minimum, supplying the services in paragraphs 4.7A.2-4.7A.4.

**4.7A.2** The Supplier shall supply Reviewers (that as a minimum have an LLB or equivalent degree in Law (Commonwealth common law foreign qualified acceptable) and/or are otherwise admitted to the roll of solicitors or have been called to the Bar) to review, tag and, where necessary, redact documents for:

a) relevance to specific claims or issues within a claim;

b) legal professional privilege;

c) personal data;

d) public interest immunity;

d) business or commercial confidentiality; and

e) any other matters that are required by the Buyer.

**4.7A.3** The Supplier shall be able to supply necessary premises (which may include suitable remote working arrangements) and necessary equipment for Reviewers and the Review Manager to conduct the exercise including, at a minimum, a desk, computer (with the capability to run a eDisclosure platform), monitor, mouse, keyboard and speakers .

**4.7A.4** The Supplier shall ensure that documents (as defined in the Pricing Schedule) are reviewed by the Reviewer and the Review Manager (where appropriate) at a minimum rate of 250 documents per day, unless otherwise agreed with the Buyer.

*Less Commonly Required*

**4.7A.5** The Supplier shall supply a Review Manager (that as a minimum has an LLB or equivalent degree in Law and/or are otherwise admitted to the roll of solicitors or have been called to the Bar) and at least 4 years post-admission experience or otherwise with at least 4 years experience as a Review Manager) to be responsible for providing a managed review service. This service is a managed end to end service to ensure the agreed deliverables are met and to include, at least, the following:

a) conduct quality assurance on a percentage sample, the percentage and sample size to be agreed with the Buyer, of the documents that have been reviewed, tagged and redacted by the Reviewers;

b) manage the review exercise to ensure a consistent and quality approach is taken by reviewers across the review exercise;

c) ensure reviewers meet document review rates agreed between the Supplier and the Buyer;

d) ensure deadlines for the review of tranches of documents and for the review as a whole are met;

e) report on the progress of the review to the Buyer at regular intervals and at least once per fortnight; and

f) raise any issues with the progress or budget of the review within 24 hours of the Review Manager becoming aware of those issues

g) on request, provide advice to the Buyer on managing the review exercise in an efficient and effective way.

* 1. **Document Production**

*For all Exercises*

* + 1. The Supplier shall advise and assist the Buyer with producing disclosure lists, including by reference to any agreement reached as to document production with the opponents, as well as production of disclosable ESI and hardcopy documents, such in compliance with Part 31 of the CPR and Practice Directions (“PD”) 31A and 31B - or any other law, rule or regulation that may, from time to time, be relevant - including:
       1. automated indexing of lists of documents according to a variety of criteria (e.g. document title, sender, recipient, or date);
       2. automated insertion of placeholders for irrelevant documents including within a document family;
       3. automated grouping of documents by:
    2. common concepts; or
    3. time of creation or particular individual or group of individuals creating or party to the documents;
       1. automated linking of email chains to create a continuous common email exchange from first to last email, across multiple users; and
       2. a functionality for cross-referencing of documents from different parties.
    4. The Supplier shall provide in respect of production of data:
       1. production of disclosable ESI in a variety of possible formats including Native, near-native, image or paper form (whilst still retaining the integrity of the original data), and including (as required):
    5. Multiple productions of the same data set with different redactions applied across the productions (e.g. by reference to the different levels of a confidentiality ring)
    6. automated index preparation and pagination of ‘bundles’ of disclosable information and to burn the information onto suitable removable media, and/or in hardcopy form, including an ability to prepare indexed and paginated hardcopy document bundles therefrom;

1. ‘burning’ final redactions identified in the preceding Document Review phase, onto the ESI produced, in a manner that ensures permanency of such redaction whilst meeting the requirements for redactions identified above;
2. production of disclosable hard copy documents in hardcopy form, including an ability to prepare indexed and paginated hardcopy document bundles; and
3. if required, and in respect of the production of ESI, provision of secure information exchange mechanisms (data exchange protocols), that maintain full auditability and chain of custody associated with the information.

*Less Commonly Required*

* + 1. On request the Supplier shall document the steps taken for the Production phase by way of a comprehensive report to the Buyer that will satisfy them (as evidenced by a clear audit trail with clear proof of chains of custody), that the steps taken are reasonable and proportionate and comply with the Buyer’s legal obligations. Such report shall also constitute the final project report, and certify that the entire exercise has been carried out in a manner that fulfils the Buyer’s obligations pursuant to Part 31 of the CPR, PD 31A and 31B thereto - or any other law, rule or regulation that may, from time to time, be relevant - and any agreements with other litigants, relevant court orders and directions.
  1. **Disclosure from Other Opponent Parties**

*For all Exercises*

* + 1. The Supplier shall also be required to provide the following Services in respect of receipt of disclosure documents from other parties (by the Buyer), including possibly as part of a rolling or staged disclosure exercise (and therefore simultaneously with the above-mentioned Services).
    2. The Supplier shall provide document receipt and processing:
       1. to engage with the other parties’ eDisclosure provider in order to agree the most suitable means and form (including load file) for receiving their data;
    3. The Supplier shall provide output if required, transforming the data into a common format necessary for the review platform being used, whilst also retaining the data in the form provided.
    4. The Supplier shall regularly analyse and validate data and results achieved, throughout all of the above stages, in order to ensure that overall results are as intended and handling decisions are correct and defensible.
    5. At the output stage, the Supplier shall implement an appropriate quality assurance procedure which ensures that the proposed output meets initial expectations, and that any significant variances from expectations are accounted for and explained.
    6. The Supplier shall provide document review support to the Buyer in their review of the data produced (from the Document Processing stage above) by:
       1. providing access to and support for suitable software solutions to aid the review process at Buyer’s premises, their client’s premises, or premises provided by the Supplier, such software to allow for:
    7. lawyer review of the other parties’ disclosure, and selection of individual documents for further consideration; and
    8. categorisation of each document selected for further consideration according to a pre-selected set of categories (for example relevance to certain issues in the litigation);
       1. provide secure off-site hosting of data subject to review, and managing access thereto (whether remotely or otherwise).

*Less Commonly Required*

* + 1. The supplier shall assess the data received and report to the Buyer regarding precisely what data has been received (including data size and type), possible complications or problems and recommend strategies for overcoming them;
    2. The Supplier shall advise and recommend strategies for review, and then implement such strategies in a manner agreed with the Buyer, such strategies to include:
    3. preparation of the data for review, including at least the following options:

1. identifying and eliminating duplicates (deduplication), if any;
2. applying pre-selected search terms and word strings (as advised by the Buyer) across all prepared data;
3. grouping documents which either share common concepts or were created at a particular time or by a particular individual or group of individuals;
4. linking email chains to result in a continuous email exchange from first to last email, across multiple users;
5. linking any other data threads generally (and recording any relevant audit information that may be available);
6. cross-referencing documents from different parties with a view to performing searches across responses;
7. relevance ranking; and
8. identification of near-duplicates in accordance with parameters set by the Buyer (near- duplication).
9. A suitable tagging structure
   * 1. The Supplier shall document the steps taken by way of a comprehensive report to the Buyer, detailing compliance with the requirements of Part 31 of the CPR or any other law, rule or regulation that may, from time to time, be relevant, that will evidence (as evidenced by a clear audit trail with clear proof of chains of custody), the steps taken are reasonable and proportionate and enable the Buyer to properly and effectively review the other litigants’ disclosure.
     2. The Supplier shall provide document review support to the Buyer in their review of the data produced (from the Document Processing stage above) by:
        1. if required, providing and supporting necessary hardware (for example document review workstations) for use in the review process at the Buyer’s premises, their client’s premises, or premises provided by the Supplier, together with the aforementioned software;
     3. The Supplier shall document the steps taken by way of a comprehensive report to the Buyer that will satisfy them (as evidenced by a clear audit trail with clear proof of chains of custody), that the steps taken are reasonable and proportionate and meet the stated requirements of the legal team.
   1. **Presentation at Trial**

*For all Exercises*

* + 1. The Supplier shall assist with the presentation of ESI or hardcopy documents at court (or other relevant tribunals) as directed by the Buyer. Such assistance shall include an ability to offer the following methods of visual presentation:
       1. on-screen projection (for example PowerPoint presentation);
       2. computer monitor display using presentation software; and
       3. production of oversized print versions of documents in hardcopy form.
    2. The Supplier shall be able to offer the following further Services:
       1. creating bundles of Documents;
       2. ordering, re‐ordering, and customising bundles;
       3. creating and exporting bundle indices (typically Excel spreadsheet);
       4. tabbing of Documents, sections and alike;
       5. bundle pagination;
       6. communication of page, folder and volume counts for bundles;
       7. insertion of Documents to existing or newly created bundles, without affecting existing tabbing, sectioning, numbering, indexing and pagination;
       8. exporting bundles;
       9. printing bundles;
       10. delivery of bundles either in hardcopy format or electronically, in the required document format, as advised by the Authority;
       11. delivery of Documents in the required document format and/or Native Format together with indices and load files containing family relationship information for use by the Buyer’s opponents, electronic trial presentation providers and alike;
       12. maintaining accurate records of bundles of Documents and indices including details such as:
    3. creation dates;
    4. amendment dates; and
    5. version control of Documents and indices.
       1. advising and assisting the legal team in developing an appropriate presentation strategy;
       2. preparing and testing exhibits chosen by the legal team and certifying their suitability for use as required;
       3. assisting with presenting such exhibits in court; and
       4. thereafter, storing and maintaining the exhibits for future use if necessary and required by the Buyer.
  1. **Security Requirements**
     1. The Supplier shall comply with the security requirements contained within Annexes 1 and/or 2 and/or 3, as appropriate. For the avoidance of doubt, where material being handled under Lot 4 includes both documents and / or data protectively marked at Secret and Top Secret and (b) documents and / or data with a lower protective marking, then the requirements of Annex 3 will apply in respect of the Secret / Top Secret material but the requirements of Annex 1 will apply in respect of the rest.

**ANNEX 1**

**INFORMATION SECURITY REQUIREMENTS FOR e-DISCLOSURE EXERCISES AT ‘OFFICIAL’ CLASSIFICATION (Lots 1 – 2)**

1. **INTRODUCTION**
   1. These security requirements apply in respect of all e-Disclosure exercises called- off and conducted under this Framework Contract, such always being exercises where the Buyer’s mitigating measures are influenced by the current and previous HMG protective marking schemes. This Annex 1 is in respect of information protectively marked at OFFICIAL and OFFICIAL-Sensitive and/or, in respect of the predecessor scheme, UNCLASSIFIED, PROTECT, RESTRICTED, CONFIDENTIAL, and related security controls recommended for protecting information marked under either scheme.
   2. These controls are spread across the technology, processes and people involved in delivering any specific system, service or solution. It is with this understanding that this information security requirement has been developed.
   3. The Supplier shall be required, for the duration of the Framework Contract and any Call-Off Contracts, to provide Services that comply with the following:
      1. legislation:
         1. Data Protection Act 2018 and General Data Protection Regulation
         2. Computer Misuse Act 1990 as amended
         3. Part 2 of the Serious Crime Act 2015
         4. Communications Act 2003
         5. Regulatory and Investigatory Powers Act 2000
      2. HMG security requirements (as per the relevant hyperlinks below):

[10 Steps to Cyber Security](https://www.ncsc.gov.uk/collection/10-steps)

[Security considerations for protecting OFFICIAL information on a corporate network](https://www.gov.uk/guidance/security-considerations-for-common-enterprise-it-decisions)

[Cloud Security Principles](https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles)

[End User Device security](https://www.ncsc.gov.uk/guidance/end-user-device-security); and

Browser Security – supplier to ensure eDisclosure solution is compatible with Chrome, Explorer and the Edge Browser

* 1. Whilst it shall always be for the Supplier to ensure compliance with the above-mentioned legislation and HMG security requirements when providing Services under the Framework Contract, the broad sets of controls that follow in the remainder of this document are considered the minimum that the Supplier shall have in place. Where information is deemed by the Buyer and/or their client to be particularly sensitive, the Supplier may be required to enter into further consultation with the Buyer and/or their client’s security personnel to agree additional minimum controls.

1. **GOVERNANCE REQUIREMENTS**
   1. The Supplier shall be accredited to (and remain so accredited throughout the duration of this Framework Contract and all Call-Off Contracts) Information Security Management System ISO 27001:2013, confirming that their IT systems/service including the segment that delivers e-Disclosure Services to the Buyer and/or their client, is compliant with information security best practice. This would mean that there is a recognisable operational mechanism and governance structure (information security management system – ISMS) in place.
   2. The Supplier shall, for the duration of the Framework and any Call-Off Contracts, also present a current and valid Cyber Essentials Plus certificate which has been awarded by one of the government approved Cyber Essentials accreditation bodies within the most recent 12 months.
   3. Additionally, the Supplier shall, for the duration of the Framework Contract and any Call-Off Contract, must maintain an ISO 27001:2013 certified Information Security Management System across their IT operations delivering the e-Disclosure services.
2. **REQUIRED OPERATIONAL ENVIRONMENT FOR OFFICIAL INFORMATION**
   1. There are at least three key design and implementation scenarios that the Supplier shall consider when bidding for an e-Disclosure exercise: a cloud service configuration used by the Supplier for delivery, a supplier-hosted service, and a Supplier service hosted at the Buyer’s or their client’s site. Any solution or service proposed by the Supplier must, by default, comply with these minimum requirements for information marked at OFFICIAL. Where additional requirements are necessary for information marked as more sensitive, the Buyer shall advise the Supplier of such requirements in advance. Any solution or Service will be individually accredited by the Buyer and/or its client, with reference to those particular requirements. The following are the minimum Information Assurance (IA) requirements which the Supplier shall meet:
      1. Where the Supplier proposes shared cloud services, it shall conduct a security assessment of those services against the NCSC’s [Cloud Security principles](https://www.ncsc.gov.uk/collection/cloud), to demonstrate end-to-end protection. Where the use of a cloud service imposes a specific security requirement (e.g. Two-Factor Authentication or Multi-Factor Authentication), the Supplier shall ensure that such requirement is complied with as below.
      2. The Supplier shall ensure that the security of End User Devices (EUDs) - including but not limited to laptops, iPads, and Android tablets, connecting to their services, meets the relevant information security standards set out below, and in so doing should have specific reference to National Cyber Security Centre (NCSC) published guidance [End User device security](https://www.ncsc.gov.uk/guidance/end-user-device-security) and best practice information [BYOD Guidance: Device Security Considerations](https://www.gov.uk/government/publications/byod-guidance-device-security-considerations/byod-guidance-device-security-considerations).
3. **REQUIRED SECURITY OPERATIONAL PROCEDURES FOR E-DISCLOSURE EXERCISES**
   1. The Supplier shall, as a minimum requirement, have the following appropriate policies, processes and procedures in place to ensure the operational security of their infrastructure:
4. Vulnerability management (patch management):
5. The Supplier shall have a defined policy and supporting process to identify vulnerabilities, and prioritise and mitigate those vulnerabilities. The Supplier’s policy shall specify specific patch application periods and a process for auditing compliance. As a minimum critical vulnerabilities shall be patched within 14 days, important vulnerabilities within 30 days and other vulnerabilities within 60 days. Where the Supplier knows that vulnerability is being actively exploited then mitigating action (e.g. patch applied) shall be taken immediately.
6. Where a Supplier is unable to deploy a patch within the above minimum timescales then the Supplier shall take alternative mitigating action within the same timescales including for example, but not limited to, disabling or reducing access to the vulnerable service.

1. Secure configuration:
2. The Supplier shall ensure that all IT systems, software and services are appropriately configured to reduce the level of inherent vulnerability. In particular the Supplier shall ensure that applications, services, processes and ports not required are disabled by default.
3. The Supplier shall ensure that default passwords are changed immediately, especially for any administrative functions.
4. The Supplier shall keep configuration control of applications installed and technology that it uses. All changes and new versions of applications shall be recorded and managed (including a formal approval and documentation process) by the Supplier.
5. The Supplier shall ensure that devices, systems and services have the capability to detect, isolate and respond to malicious software.
6. Physical security:
7. The Supplier shall ensure that appropriately secure accommodation and appropriate policies and practices governing its use are in place to protect personnel, hardware, programs, networks and data from loss, damage or compromise. For services processing OFFICIAL information, the Supplier’s accommodation from where the e-Disclosure service will be hosted must be compliant with the ISO27001:2013 security standard controls, specifically physical and environmental security (A.11).
8. The Supplier must ensure that their cloud service processing and storing HMG data must be limited to the UK, the Netherlands and Ireland, with the UK preferred.
9. Protective monitoring and intrusion detection:
10. The Supplier shall collect and retain event data and undertake activities that will help it detect actual or potential security incidents. The Supplier shall have a protective monitoring policy that describes the conditions they aim to detect, which can be used to define event data collection. That policy shall include both detection of technical attacks as well as important abuses of business processes. These terms do not describe any specific event to collect or incident to detect. Rather, the requirement is that the Supplier has thought about and documented its collection and analysis requirements and that this has led to the Supplier’s approach to protective monitoring and intrusion detection. The Supplier’s policy in this regard shall be made available to the Authority on demand.
11. In respect of the Supplier’s cloud services, the Supplier shall ensure that Cloud Security Principle 5.3 Protective Monitoring is fully addressed and met in its overall monitoring strategy. A cloud service will only provide monitoring with respect to the service provisioned. If the Supplier consumes Infrastructure as a Service (“IaaS”) or Platform as a Service (“PaaS”), it shall be responsible for monitoring of capability deployed onto the infrastructure. If the Supplier is consuming Software as a Service (“SaaS”), it shall clearly articulate and address how it will be able to monitor for any potential abuse of business process or privilege.
12. In respect of End User Devices, the Supplier shall ensure that the capability associated with EUD Security Principle 11: Event Collection for Enterprise Analysis forms part of its overall monitoring strategy.
13. Security incident response:
14. The Supplier shall have an incidents management and response policy and process in place, so that when incidents do occur they can act quickly to contain the incident, limit harm, ensure appropriate escalation and learn lessons for the future. The Supplier shall report all incidents relating to any Call-Off Contract conducted under this Framework Contract to the Buyer as soon as possible.
15. The Supplier shall have a security incident management plan, which it tests periodically. This shall include named responsible owners and pre-defined processes to respond to common forms of attack. Such a plan shall be presented to the Buyer on demand.
16. In the event of an incident the Supplier shall provide the Buyer with audit logs holding user activities, exceptions and information security events to assist in investigations.
17. End User Devices must form part of the incident response plan. The Supplier’s response plans shall include how to manage mobile devices should they get lost or be stolen, in compliance with EUD Security Principle 12: Incident Response.
18. **AUTHENTICATION AND ACCESS CONTROL**
    1. The Supplier shall ensure that accounts are provisioned with privileges appropriate for the user's needs. Administrator (or other high privilege) accounts shall only be provisioned to users who need those privileges. Administrators shall not conduct ‘normal’ day-to-day business from their high privilege account. Privileges shall be periodically reviewed and removed where no longer required.
    2. The Supplier shall ensure that users identify and authenticate to devices and Services. For passwords, the Supplier shall, with reference to CESG’s published best practice ‘[Three random words password guidance](https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words)’:
19. ensure that all passwords are changed from defaults;
20. not allow password/account sharing;
21. ensure that high-privilege users (i.e. administrators) use different passwords for their high-privilege and low-privilege accounts;
22. combine passwords with some other form of strengthening authentication, such as lockouts, throttling or two-factor authentication;
23. ensure that passwords are never stored as plain text, but are (as a minimum) hashed using a cryptographic function capable of multiple iterations and/or a variable work factor. It is advisable to add a ‘salt’ before hashing passwords.
    1. In respect of End User Devices, the Supplier shall ensure that users identify and authenticate to devices and Services. Additionally the Supplier shall ensure that only appropriately authorised devices are provided with access to Services, in compliance with EUD Security Principle 3: Authentication.
    2. In respect of the Supplier’s cloud services, the Supplier shall ensure that users, administrators and service providers identify and authenticate to all Services, in compliance with EUD Security Principle: External Interface Protection, and EUD Security Principle: Device Update Policy. The set of EUD Principles are found [here](https://www.ncsc.gov.uk/guidance/end-user-devices-security-principles)
24. **BOUNDARY PROTECTION AND INTERFACES**
    1. The Supplier shall ensure that its network used for delivery of the Services has appropriately configured boundary protection between their network/Services and the internet or any other network traffic, Services and content are limited to that required to support the Services (for example, by setting effective firewall rule sets). Services presented outside of the protected enterprise (online services for staff, mobile working etc.), shall be delivered from an appropriate architecture, with access to any core information or services constrained. The architecture shall include Services to identify malware at the gateway. Where encryption prevents this, the Supplier shall implement an equivalent level of protection at the end point.
    2. In respect of unmanaged devices/personal laptops, the Supplier shall not have access to the Buyer or its client’s information being processed as part of the Services. Where an unmanaged device is proposed for use, the Supplier shall have the data owner’s (Buyer or their client) permission before allowing unmanaged devices to access the data. Additionally, the Supplier shall ensure that any unmanaged device:
    3. is not able to use the service in an unmediated fashion;
    4. accesses the eDisclosure service through an appropriately secured connection, for example, at the network layer via a Virtual Private Network (“VPN”), or at the application layer via a protocol that implements Transport Layer Security (“TLS”); and
    5. is authenticated prior to the eDisclosure information being accessed with a mechanism that does not solely rely on a username and password.
25. **PROTECTING DATA AT REST AND IN TRANSIT**
    1. The Supplier shall ensure that data is protected by default whilst at rest and in transit. This shall be within the Supplier’s secure data storage systems, but may include physical protection (e.g. when data is removed from the storage systems and placed on removable media for physical transport) and encryption (e.g. when data is vulnerable at rest or in transit).
    2. Where data is released via vulnerable channels (e.g. unprotected email, or removable media), the Supplier shall ensure that the user must make an active decision and pays due regard to any applicable handling instructions for that information.
26. **USER AND ADMINISTRATOR SEPARATION OF E-DISCLOSURE DATA** 
    1. The Supplier shall ensure that appropriate separation exists between multiple users of the Supplier’s IT services. The Supplier shall ensure that there is capability to mediate user access to data to the minimal amount necessary to support the Services. There shall be separation (however it is achieved) between users who have access to the data which is subject of the Services and users with no access to that information.
    2. In respect of the Supplier’s cloud (or shared) service, the Supplier shall ensure that separation exists between the consumers of the Services to prevent a malicious or compromised user from affecting another, in compliance with Principle 3: Separation between consumers. The Supplier shall ensure that users are separately authenticated to more privileged access services (i.e. management interfaces), in compliance with Cloud Security Principle 9 Secure Consumer Management. [www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles](http://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles)
27. **THE SUPPLIER’S PERSONNEL**
    1. The Supplier shall ensure that its staff or contractors have undergone pre-employment checks which are aligned with at least the Baseline Personnel Security Standard (BPSS).
    2. The Supplier shall ensure that their staff are trained to understand their obligations with regards to system security, data handling, and acceptable use.
28. **SEPARATION OF SERVICES**
    1. The Supplier shall ensure that the Buyer’s data is separate from other Buyers’ data hosted on the same infrastructure.

**ANNEX 2**

**INFORMATION SECURITY REQUIREMENTS FOR PROVISION OF REVIEWERS INCLUDING A MANAGED REVIEW SERVICES (Lot 3)**

1. It is anticipated that the reviewers under Lot 3 will connect to the Supplier’s/third party’s/in-house e-Disclosure system either using their own devices or such as may be provided by the Supplier. The following requirements shall apply:
   1. The Supplier shall ensure that reviewers use Two-Factor Authentication or Multi-Factor Authentication in order to access the e-Disclosure system from their device(s).
   2. The Supplier shall ensure that the device(s) used are checked for compliance with connecting and/or access conditions for the e-Disclosure system.
      1. This will include the latest patch levels and latest anti-virus and anti-malware. If the device(s) are not up to date then access to the e-Disclosure system shall be suspended.
   3. If the reviewer(s) are not able to use their own device and/or if said device does not meet the standards in paragraphs 1.1 and 1.2, then the Supplier shall provide appropriately secured devices for the reviewer(s) to connect to the e-Disclosure system.
   4. Additionally, where reviewers are sharing a common network to which access has been provided by the Supplier, the security requirements specified in Annex 1 shall apply.
2. The Supplier shall ensure that its staff or contractors have undergone pre-employment checks which are aligned with at least the Baseline Personnel Security Standard (BPSS), or if the information is SECRET then a Security Check (SC) clearance must be in place.
3. The Supplier shall ensure that their staff are trained to understand their obligations with regards to system security, data handling, and acceptable use.
4. For SC and Developed Vetting (DV) clearances, the Supplier shall ensure that aftercare documents for the respective security clearances shall be presented by the reviewers.

**ANNEX 3**

**INFORMATION SECURITY REQUIREMENTS FOR e-DISCLOSURE EXERCISES UP TO ‘SECRET’ AND ‘TOP SECRET’ CLASSIFICATION (Lot 4 only)**

1. **INTRODUCTION**
   1. These security requirements apply in respect of all e-Disclosure exercises called-off and conducted under Lot 4 of this Framework Contract, such always being exercises where the Buyer’s mitigating measures are influenced by the current and previous HMG protective marking schemes. This Annex 3 refers to information protectively marked at SECRET or TOP SECRET and the related security controls recommended for protecting information marked under either scheme.
   2. These controls are spread across the technology, processes and people involved in delivering any specific highly sensitive IT system, service or solution. It is with this understanding that this information security requirement has been developed.
   3. The Supplier shall be required, for the duration of the Framework Contract and any Call-Off Contracts, to provide Services that comply with the following:
      1. legislation:
         1. Data Protection Act 2018 and General Data Protection Regulation
         2. Computer Misuse Act 1990 as amended
         3. Part 2 of the Serious Crime Act 2015
         4. Communications Act 2003
         5. Regulatory and Investigatory Powers Act 2000
      2. HMG security requirements (as per the relevant hyperlinks below) for the Lot 4 computing environment where laptops are hardened and are either standalone or if networked, there is no access to the Internet (air-gapped):

[10 Steps to Cyber Security](https://www.ncsc.gov.uk/collection/10-steps) – adopted for Lot 4

[End User device security](https://www.ncsc.gov.uk/guidance/end-user-device-security) – adopted for Lot 4

Browser Security – adopted for Lot 4 – ensure version of browser is fully patched and compatible with eDisclosure solution

[Security requirements for List X Contractors](https://www.gov.uk/government/publications/security-requirements-for-list-x-contractors)

* 1. Whilst it shall always be for the Supplier to ensure compliance with the abovementioned legislation and HMG security requirements when providing Services under the Framework Contract, the broad sets of controls that follow in the remainder of this document are considered the minimum that the Supplier shall have in place. Where information is deemed by the Buyer and / or their client to be particularly sensitive, the Supplier may be required to enter into further consultation with the Buyer and/or their client’s security personnel to agree additional controls that are needed for any given call-off contract.

1. **GOVERNANCE REQUIREMENTS**
   1. The Supplier shall be accredited to (and remain so accredited throughout the duration of this Framework Contract and all Call Off Contracts) Information Security Management System ISO 27001:2013, confirming that their IT systems/service including the segment that delivers eDisclosure Services to the Authority and/or their client, is compliant with information security best practice. This would mean that there is a recognisable operational mechanism and governance structure (information security management system – ISMS) in place.
   2. The Supplier shall have, for the duration of the Framework Contract and any Call-Off Contracts, a current and valid Cyber Essentials Plus certificate or equivalent, which has been awarded by one of the government approved Cyber Essentials accreditation bodies within the most recent 12 months.
   3. The supplier will have a valid Accreditation certificate for the List X facilities before entering into any call-off competition(s).
   4. Additionally, the Supplier shall, for the duration of the Framework Contract and any Call-Off Contract, must maintain an ISO 27001:2013 certified Information Security Management System across their IT operations delivering the e-Disclosure services.
2. **REQUIRED OPERATIONAL ENVIRONMENT FOR SECRET AND TOP SECRET INFORMATION**
   1. There are at least two key design and implementation scenarios that the Supplier shall consider when bidding for an e-Disclosure exercise: a Supplier-hosted closed network service with no internet access, and a Supplier closed network service hosted at the Buyer or their client’s site. The following are the minimum Information Assurance (IA) standards which the Supplier shall meet:
   2. Any solution or Service proposed by the Supplier shall, by default, provide greater controls than those in Annex 1, by way of additional mandatory requirements for information marked at SECRET or TOP SECRET. The Buyer shall advise the Supplier of these specific handling caveats or technical controls. Any solution or Service will be independently assured by the Buyer and/or its client, with reference to those particular requirements.
   3. The Supplier shall ensure that the security of End User Devices (EUDs) - including laptops, printers and PCs - connecting to their Services meets the relevant information security standards set out below, and in so doing should have specific reference to NCSC’s published guidance [End User Device Security](https://www.ncsc.gov.uk/guidance/eud-security-guidance-windows-10).
3. **REQUIRED SECURITY OPERATIONAL PROCEDURES FOR E-DISCLOSURE EXERCISES**
   1. The Supplier shall have appropriate policies, processes and procedures in place to ensure the operational security of their infrastructure as follows.
4. Vulnerability management (patch management)
5. The Supplier shall ensure that any exploitable vulnerability is managed. To that end the Supplier shall have a defined policy and supporting process to identify vulnerabilities, and prioritise and mitigate those vulnerabilities. The Supplier’s policy shall specify specific patch application periods and a process for auditing compliance. As a minimum, critical vulnerabilities shall be patched within 14 days, important vulnerabilities within 28 days and other vulnerabilities within 60 days. Where the Supplier knows that a vulnerability is being actively exploited then mitigating action (e.g. patch applied) shall be taken immediately.
6. Where a Supplier is unable to deploy a patch within the above minimum timescales then the Supplier shall take alternative mitigating action within the same timescales including for example, but not limited to, disabling or reducing access to the vulnerable service.
7. Secure configuration
8. The Supplier shall ensure that all IT systems, software and services are appropriately configured to reduce the level of inherent vulnerability. In particular the Supplier shall ensure that applications, services, processes and ports not required are disabled by default.
9. The Supplier shall ensure that default passwords are changed immediately, especially for any administrative functions.
10. The Supplier shall keep configuration control of applications installed and technology that it uses. All changes and new versions of applications shall be recorded and managed (including a formal approval and documentation process) by the Supplier.
11. The Supplier shall ensure that devices, systems and services have the capability to detect, isolate and respond to malicious software.
12. Physical security
13. The Supplier shall ensure that appropriately secure accommodation and appropriate policies and practices governing its use are in place to protect personnel, hardware, programs, networks and data from loss, damage or compromise. For services processing SECRET and TOP SECRET information, the Supplier’s accommodation from where the e-Disclosure service will be hosted must be in accordance with the requirements specified in:

<https://www.gov.uk/government/publications/security-requirements-for-list-x-contractors>

any further handling caveats or technical controls will be given to the Supplier to implement for the facilities by the Buyer/ their clients security personnel.

1. Protective monitoring and intrusion detection
2. The Supplier shall collect and retain event data and undertake activities that will help it detect actual or potential security incidents. The Supplier shall have a protective monitoring policy that describes the conditions they aim to detect, which can be used to define event data collection. The policy shall include both detection of technical attacks as well as important abuses of business processes. These terms do not describe any specific event to collect or incident to detect. Rather, the requirement is that the Supplier has thought about and documented its collection and analysis requirements and that this has led to the Supplier’s approach to protective monitoring and intrusion detection. The Supplier’s policy in this regard shall be made available to the Buyer on demand.
3. In respect of End User Devices, the Supplier shall ensure that the capability associated with EUD Security Principle 11: Event Collection for Enterprise Analysis forms part of its overall monitoring strategy.
4. Security incident response
5. The Supplier shall be prepared for incidents so that when they do occur they can act quickly to contain the incident, limit harm, ensure appropriate escalation and learn lessons for the future. The Supplier shall report all incidents relating to any Call-Off Contract conducted under this Framework Contract to the Buyer as soon as possible.
6. The Supplier shall have a security incident management plan, which it tests periodically. This shall include named responsible owners and pre-defined processes to respond to common forms of attack. Such a plan shall be presented to the Buyer on demand.
7. In the event of an incident the Supplier shall provide the Buyer with audit logs holding user activities, exceptions and information security events to assist in investigations.
8. End User Devices must form part of the incident response plan. The Supplier’s response plans include how to manage mobile devices should they get lost or be stolen, in compliance with EUD Security Principle 12: Incident Response.
9. **AUTHENTICATION AND ACCESS CONTROL**
   1. The Supplier shall ensure that accounts are provisioned with privileges appropriate for the user's needs. Administrator (or other high privilege) accounts shall only be provisioned to users who need those privileges. Administrators shall not conduct ‘normal’ day-to-day business from their high privilege account. Privileges shall be periodically reviewed and removed where no longer required.
   2. The Supplier shall have its own ’crypto custodian’ to handle NCSC UKKPA’s encryption keys and cryptographic equipment, like standalone laptops, removable drives or IT equipment on CLOSED (processing data classified as SECRET or TOP SECRET) networks, in accordance with List X Guidance. Such an individual shall be responsible for the custody, handling, protection and destruction of all cryptographic material.
   3. The Supplier shall ensure that users identify and authenticate to devices and IT Services. The Supplier’s crypto custodian shall manage this process.
   4. For passwords, the Supplier shall, implement with reference to NCSC’s published best practice ‘[Three random words password guidance](https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words)’:
10. ensure that all passwords are changed from defaults;
11. not allow password/account sharing;
12. ensure that high-privilege users (i.e. administrators) use different passwords for their high-privilege and low-privilege accounts;
13. combine passwords with some other form of strengthening authentication, such as lockouts, throttling or two-factor authentication;
14. ensure that passwords are never stored as plain text, but are (as a minimum) hashed using a cryptographic function capable of multiple iterations and/or a variable work factor. It is advisable to add a ‘salt’ before hashing passwords.
    1. In respect of End User Devices, the Supplier shall ensure that users identify and authenticate to devices and Services. Additionally, the Supplier shall ensure that only appropriately authorised devices are provided with access to Services, in compliance with EUD Security Principle 3: Authentication.
15. **BOUNDARY PROTECTION AND INTERFACES**
    1. The Supplier shall ensure that its proposed closed network used for delivery of the Services has appropriately configured boundary protection between their network/Services. More specific controls may be added once a design has been agreed with the Authority’s IT Accreditor**.**
16. **PROTECTING DATA AT REST AND IN TRANSIT**
    1. The Supplier shall ensure that data is protected by default whilst at rest and in transit. This shall be within the Supplier’s storage systems, but may include physical protection (e.g. when data is removed from the storage systems and placed on removable media for physical transport) and encryption (e.g. when data is vulnerable at rest or in transit).
17. **USER AND ADMINISTRATOR SEPARATION OF E-DISCLOSURE DATA** 
    1. The Supplier shall ensure that appropriate separation exists between multiple users of the Supplier’s IT services. The Supplier shall ensure that there is capability to mediate user access to data to the minimal amount necessary to support the Services. There shall be separation (however it is achieved) between users who have access to the data which is subject of the Services and users with no access to that information. This applies if the supplier is hosting the closed networked service at their premises.
18. **THE SUPPLIER’S PERSONNEL**
    1. The Supplier shall ensure that its staff or contractors who have administrative privileges (for example, users who are able to reconfigure the network or system administrators), have undergone pre-employment checks which are aligned with at least the Security Cleared (SC) or Developed Vetting (DV) level, respectively.
    2. The Supplier shall ensure that its staff are trained to understand their obligations with regards to system security, data handling, and acceptable use.
19. **SEPARATION of SERVICES**
    1. The Supplier shall ensure that the Buyer’s IT systems and data are on stand-alone systems not shared with other Buyers’ data hosted on the same infrastructure.

**ANNEX 4**

**SUPPLIER’S GUIDE TO DELIVERING SOCIAL VALUE THROUGH E-DISCLOSURE AND REVIEW SERVICES RM6336**

**1.1 Introduction**

This guide has been created to set out how Social Value will be delivered through CCS Framework Agreement E-Disclosure and Review Services - RM6336 and related Call-Off Agreements.

The guidance provides further information on how the parties to the Framework Agreement, CCS, Suppliers, and Buyers, will seek to address Social Value requirements through the delivery of E-Disclosure and Review Services.

**1.2 The wider context for Social Value**

The Civil Society Strategy for England defines social value as “enriched lives and a fairer society for all”. This strategy acknowledges that partnership and collaboration are essential to achieving this vision. The inclusion of social value when spending public funds is a fundamental part of securing value for money and selecting the most economically advantageous tender. Accordingly, this framework will take into account the social value priorities outlined below and CCS will be actively seeking partners who share the Government's commitment to building a future that works for everyone. More information on the Civil Society Strategy can be found here:

<https://www.gov.uk/government/publications/civil-society-strategy-building-a-future-that-works-for-everyone>

An introductory guide to social value can be found at

<https://www.gov.uk/government/publications/social-value-act-introductory-guide>.

**1.3 Our Social Value priorities**

CCS have set out what CCS (in conjunction with Buyers) sees as the priority social value areas for this Framework Agreement, and set out where elements of the Framework Agreement link directly to these priorities.

CCS expects that Suppliers will primarily deliver Social Value through Buyer Call-Off Contracts awarded under this Framework Agreement.

Buyers using the Framework Agreement can adopt any of the following approaches as part of the Call-Off Procedure:

* They may provide Suppliers with the Social Value priority statement set out in Framework Schedule 1 Specification and ask the Suppliers to outline what they can deliver to help meet these priorities, including a commitment to targets;
* They may set specific targets based on the Social Value priority statement within Framework Schedule 1 Specification and ask Suppliers to deliver these targets through their Call-Off Contract;
* They may include new Social Value measures based on the specific priorities of their organisation which are aligned to the policy areas set out in Framework Schedule 1 Specification, and then adopt approach a) or b) above.

**2.1**    **Delivering a diverse Supply Chain**

The Framework sets out the minimum requirements of suppliers, to help us ensure a diverse base of suppliers and resilient supply chains as follows:

 CCS expect our Suppliers to support and build supply chain diversity through:

* Subcontracting opportunities are open to Small to Medium Sized Enterprises (SMEs) and Social Enterprises (SEs), including the advertisement of all subcontracting opportunities over £10,000 on Contracts Finder (Joint Schedule 12, Supply Chain Visibility);
* Cascading prompt payment throughout Supplier supply chains (Section 4: Pricing and Payments, Core Terms);
* Supply chain processes that enable the participation of Micro, Small to Medium Sized Enterprises (SMEs) and Social Enterprises (SEs).

Other ways in which Suppliers can help CCS and our Buyers deliver this include providing advice and support to SMEs & SEs to develop resilient local supply chains, for example:

* Providing funded training opportunities e.g. health & safety, marketing, digital skills and other professional development opportunities;
* Mentoring and B2B learning and networking opportunities;
* Providing facilities / equipment to enable sectors to expand and grow i.e. meeting/training venues.

**2.2**    **Safe & Secure Supply Chains: Addressing Modern Slavery and exploitation in our Supply Chain**

It is our role to ensure the suppliers with whom CCS and our Buyers do business understand the risks of modern slavery in supply chains, and take appropriate action to identify and address those risks, with particular focus on supporting victims of modern slavery.

CCS require Suppliers to comply with the provisions of the [Supplier Code of Conduct](https://www.gov.uk/government/publications/supplier-code-of-conduct) and the standards set out in Joint Schedule 5 on Corporate Social Responsibility including the reporting (see Framework Schedule 5 Management Charges and Information) and continuous improvement (see Call-Off Schedule 3 Continuous Improvement) requirements.

CCS expect our Suppliers to mitigate the risk of Modern Slavery in their supply chains associated with the service / solutions offered under this Framework Agreement, for example by:

1. Undertaking activities to increase awareness on Modern Day Slavery;
2. Provision of training to employees and supply chain partners;
3. Audits on Modern Day Slavery carried out internally (within the suppliers organisation) and externally across supply chains;

**2.3**   **Fair, inclusive and ethical employment practices & skills development**

CCS consider the delivery of high quality public services to be critically dependent on a workforce that is inclusive, well-motivated, well-led and has appropriate opportunities for training and skills development.

By law, all organisations with 250 or more employees must publish and report specific figures about their gender pay gap, and CCS expect our suppliers to progress towards equalising this.

CCS expect our Suppliers and Supplier Supply Chains to support and encourage employment and skills development opportunities through the performance of this Framework Agreement, with a specific focus on opportunities for priority groups, including (but not limited to):

* people with disabilities;
* Ex-offenders;
* BAME;
* long-term unemployed.

 This support may be through various activities such as, for example:

* Apprenticeship and work experience placements;
* Part-time and full-time employment and flexible working opportunities;
* Providing stable employment and hours of work, and avoiding exploitative employment practices including, for example, no inappropriate use of zero hour contracts or other forms of demand driven contracts;
* Supporting individuals to fulfil their potential with further education, employment or training e.g. coaching, mentoring, CV and interview skills;
* Providing funded training and professional development opportunities for existing employees;
* Providing funded training opportunities (for individuals not employed by Supplier);
* Fair and equal pay policy;
* Offering a range of employee assistance schemes.

Ethical behaviour standards:

Taxpayers expect that government’s suppliers will behave ethically and CCS expect the highest standards of business ethics from suppliers and their agents in the supply of goods and services funded by the public purse.

CCS expect suppliers to be explicit about the standards they demand of executives, employees, partners and subcontractors and to have the governance and audit processes to monitor and enforce these standards.

Buyers may test Suppliers’ proposed methods for delivering skills development within the local community as relevant to their specific requirements as part of the Call-Off Procedure.

**2.4**   **Environmental Sustainability: Promoting sustainable production and consumption and an improvement in environmental quality in support of the 25 Year Environment Plan**

Framework Schedule 1 (Specification) refers suppliers to the 25 Year Environment Plan (<https://www.gov.uk/government/publications/25-year-environment-plan>)

.

**2.5**    **Wellbeing & Community Benefits**

CCS expects our Suppliers to positively impact individual wellbeing and contribute to transforming our local communities in a real and sustainable manner.

Ways in which the Supplier may be able to support wellbeing and community benefits include (but are not limited to):

* Supporting local businesses (not currently part of the existing supply chain) e.g. SMEs & VCSEs;
* Improving the experience of service users with specific diversity profiles or needs e.g. ensuring accessibility, undertaking staff sensitivity training, fostering a culture of respect for Buyers of diverse profiles;
* Creating cohesive communities: initiatives to support vulnerable people and address social issues such as homelessness, loneliness such as (but not limited to) donations to charities, staff volunteering, fundraising activities, befriending schemes etc;
* Staff wellbeing e.g. promoting awareness about mental health, substance misuse, domestic abuse, first aid training, anti-bullying campaigns, gender equality and diversity training etc.

It is expected that Buyers may have different wellbeing and community benefits priorities specific to their local communities, and that they may therefore test Suppliers’ proposed methods for delivering wellbeing and community benefits as relevant to these specific requirements as part of the Call-Off Procedure.

**2.6 COVID 19 recovery**

CCS expects our Suppliers to help local communities to manage and recover from the impact of COVID 19.

Ways in which the Supplier may be able to support include but are not limited to:

* Create employment, re-training and other return to work opportunities for those left unemployed by COVID-19, particularly new opportunities in high growth sectors.
* Support people and communities to manage and recover from the impacts of COVID-19, including those worst affected or who are shielding.
* Support organisations and businesses to manage and recover from the impacts of COVID-19, including where new ways of working are needed to deliver services.
* Support the physical and mental health of people affected by COVID-19, including reducing the demand on health and care services.
* Improve workplace conditions that support the COVID-19 recovery effort including effective social distancing, remote working, and sustainable travel solutions.

**3.  Measurement and reporting**

Suppliers are required to develop and maintain a plan throughout the life of the Framework Agreement detailing how the Supplier will contribute to the overall achievement of our Social Value priorities.  For the avoidance of doubt:

* The Social Value commitments and targets made during the Call-Off Procedure will form part of the contractual agreement between the Buyer and the Supplier, therefore bidders should only commit to activities that are within their capacity and capability to deliver.
* Social value forms part of the quality criteria and will be evaluated independently of price. Suppliers are therefore strongly advised not to include any additional costs related to social value as part of the price submission as this may negatively impact the competitiveness of Supplier overall tender submission.
* The Supplier must provide an implementation plan to the Buyer detailing how the required Social Value commitments will be delivered through the Call-Off Contract.
* Buyers and Suppliers will jointly agree the timeline for delivering the targets and measures that were committed to by the Supplier during the Call Off Procedure.